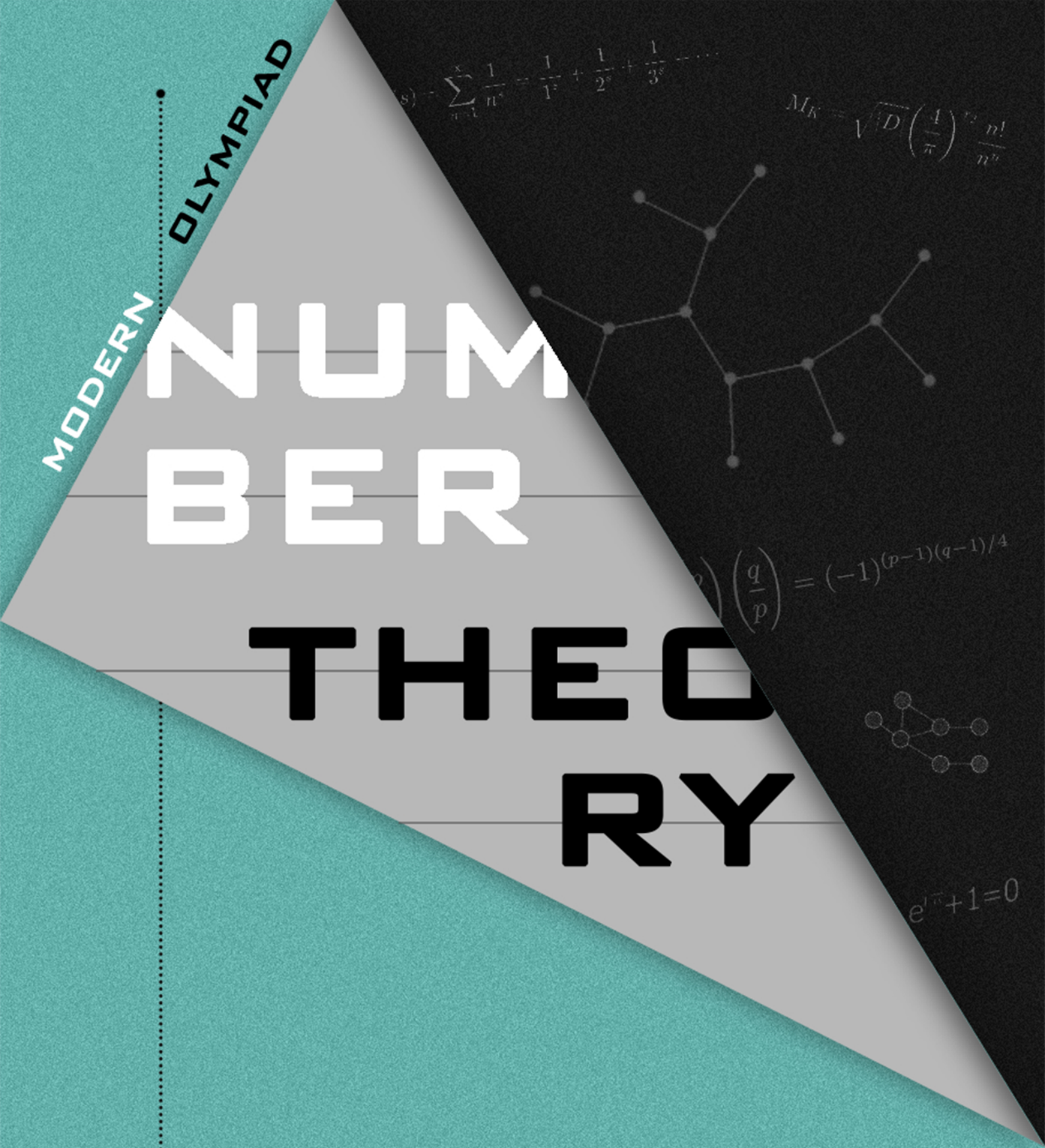
MODERN OLYMPIAD

NUMBER THEORY



ADITYA KHURMI

Modern Olympiad Number Theory

Aditya Khurmi

Contents

Preface

Number Theory has been studied and discussed since the dawn of man; be it counting apples or studying Pythagorean triples. It is the heart of mathematics. With time and years of work, people started to unravel new and beautiful properties of these numbers. Despite having developed all the advanced tools today, the Elementary tools are still very powerful. A good understanding of these is required to do almost anything in maths today.

Olympiads today aren't what they were when they started; the problems are much more diverse and harder. One needs a lot of practice and experience to get their hand on these. The best part, however, is that even the hardest of problems have solutions with the simplest of ideas. However, the tree of possible approaches branches out very fast and it is our intuition that leads us through the dark. This book is intended to give a more **conceptual approach** to the discipline, and each topic is explained in depth and focused more into building a clear map of all the topics: the explanations in this book are done in the way I have understood these topics, and the methods I use to make connections across all areas in Number Theory are presented here. The **solved examples** are precisely handpicked that depict special ideas and teach you how to think on these problems. The most challenging part was to choose these problems; there are the great classics, and there are problems from today's Olympiads. Hence, I have tried to keep a balance between the two throughout the book. I have to admit that I did not cover certain topics in Olympiad Number Theory such as irreducibility criterion and functional equations over $\mathbb{N}$, but have largely covered all the other important topics.

I would like to share the pattern of this book before we start. Each chapter contains theory with solved examples. I personally suggest that you read the solved examples with care and try to pin point the main ideas, because that's how you will learn new ideas much better. At times I leave certain details by writing **why?** in a bracket. You should try to answer this in order to check if you are on the same page with me. Many sections have a subsection called **Problems for Practice**, which would generally include some very important results/lemmas you should remember that we would use in the future. The results I choose shouldn't be very hard to prove, but still enough to test your understanding.Occasionally, these contain some cute and easy yet instructive problems too. The end of each chapter contains a section on some final **example problems**, which include some of the hardest problems you would see in the chapter. The **Problems section** starts off with easy problems and moves on towards some very hard and challenging problems.

The component of book that I am the most excited about is the **hints and solutions system**. While I have added solutions only to some of the hardest or most elegant problems,

I have added hints to almost all of them, which might just help you hit the key step you were missing, or even make a hard problem you otherwise couldn't approach more approachable by giving a step-by-step guide. Some chapters also have a **Special Section** at the end, which contain an interesting topic related to our discussion that might not be so mainstream to have been covered in the theory before, however still very elegant or useful (or just interesting in its own right).

While this is a Number Theory book, staying away from Combinatorial ideas is impossible. One idea that will be very recurrent in this book is the idea of **looking at the larger picture**, which is why you will find many tables in this book. This basically means to look at all possibilities at once together instead of treating them as different. You will understand this much better once you read the book. Another suggestion is to try to **visualize things** as much as possible. The more visual the approach, the better chances of you finding the right path.

As per the **pre-requisites**, I would assume the knowledge of basic pre-calculus topics, mainly basic Set Theory, the Binomial Theorem and AP, GP sequences. The knowledge of complex numbers and logarithms is occasionally useful too. Also, some common proof writing techniques such as the method of contradiction and the principle of mathematical induction.

I hope that you enjoy this book. Have fun!

Aditya Khurmi
India

Acknowledgements

This was a big project, and I would like to thank many people for this. A special thanks to **Evan Chen** for helping me out with LaTeX, especially the hints system. **Rishabh Dhiman** for helping me out with LaTeX. **Ashmita Goradia** and **Evan Chen** for helping me out with legal matters. **Shuborno Das** for sharing some problems whenever I asked him to. **Samuel Goodman** for letting me use his problem. The countless users on **AoPS**[1] who have posted thousands of problems and solutions. **Falak Khurmi**, my sister, for designing the very creative cover page. Also, thanks to my **Mom** and **Dad** for being ever-supportive.

Any problem and/or solution with a source mentioned belongs to them and I claim no rights over these. Further, all the sources are written to the best of my knowledge and any incorrect (or blank) source is nothing more than an unintentional mistake.

This content is for educational purpose only and is not meant for commercial usage by any entity or individual

[1] "The Art of Problem Solving" website

Part I

Fundamentals of Number Theory

Chapter 1

Divisibility

Divisibility is the first chapter we start Number Theory with. The ideas involved in a number being divisible by another leads to all sorts of definitions and results. We explore some of them in this chapter.

1.1 Multiplication Tables

To truly understand divisibility, we must look at its source; multiplication tables. Let's pick an example, the table of 5.

$$\begin{aligned}
&\vdots \\
-2 \times 5 &= -10 \\
-1 \times 5 &- -5 \\
0 \times 5 &= 0 \\
1 \times 5 &= 5 \\
2 \times 5 &= 10 \\
3 \times 5 &= 15 \\
4 \times 5 &= 20 \\
5 \times 5 &= 25 \\
6 \times 5 &= 30 \\
7 \times 5 &= 35 \\
&\vdots
\end{aligned}$$

So, the set of multiples of 5 is:

$$\mathcal{M} = \{\ldots, -10, -5, 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, \ldots\}.$$

We haven't even started yet and we already have our first definition: any number in this list is called a **multiple** of 5, and is said to be **divisible** by 5. In general, we have the following definition:

Definition 1.1.1. *A number n is said to be a **multiple** of m if it appears in the multiplication table of m.*

The concept of divisibility deals with the division operation. We recall that a number m **divides** n if n is in the multiplication table of m. In Number Theory, we have a special symbol for this:

Definition 1.1.2. *A number n is **divisible** by m if n is a multiple of m. Also, we say m **divides** n and write this symbolically as*

$$m \mid n.$$

This is read as "m divides n." For example, we have $7 \mid 14, 8 \mid 0$ and $17 \mid -34$. Please note that the number *after* " $\mid$ " is the multiple, unlike in fractions, where we would write the multiple first as n/m (for instance $14/7 = \frac{14}{7} = 2$, so $7 \mid 14$). Don't get confused!

1.2 Divisibility Properties

1.2.1 Basic Results

Now that we have defined a notation, let's investigate its properties. Firstly, we write down some obvious ones.

Theorem 1.2.1. *Let x, y, z be integers.*

- *We have $x \mid x$.*
- *We always have $1 \mid x$ and $x \mid 0$.*
- *If $x \mid y$ and $y \mid z$, then $x \mid z$.*
- *If $x \mid y$, we can find an integer k so that $y = kx$. Here, k can be negative.*

The last one is particularly useful. It basically says:

$$m \mid n \iff \frac{n}{m} \in \mathbb{Z}.$$

This property will be used a lot when we want to convert divisibility into algebra. For example, using this, we can prove the third property. Suppose $x \mid y$ and $y \mid z$. Then $\frac{y}{x}, \frac{z}{y} \in \mathbb{Z}$. Hence

$$\frac{z}{x} = \frac{y}{x} \cdot \frac{z}{y} \in \mathbb{Z} \Leftrightarrow x \mid z.$$

Let's now talk about some special properties.

1.2.2 Special Property 1

Look again at the multiplication table of 5, only the positive numbers this time. If $x \mid y$, then x must be "smaller" than y. This feels true. But should it always be? Let's try to answer this.

Suppose $x \mid y$. So, y must be an element from the set

$$\{\dots, -3x, -2x, -x, 0, x, 2x, 3x, \dots\}.$$

Which numbers are larger than x here? Right, only about half of these. However, considering the absolute value, we find $|y| \geqslant |x|$ always except if $y = 0$. Hence our intuition was right. Let's write this down:

Theorem 1.2.2. *If $x \mid y$ for two integers, then either $y = 0$ or $|x| \leqslant |y|$.*

The case $y = 0$ is very easy to miss and an extremely important result! If you miss it, you have an incomplete solution. Not just that, it is often the key idea in a solution. Remember that! Also, the absolute value must not be forgotten.

Question 1.2.1. *In which cases can you ignore the absolute value sign?*

1.2.3 Our First Formal Proof

Here we formally prove the lemma above (this is not to say our previous argument was wrong, but this is another one that you would generally find in books):

Proof. Write $y = kx$. Then if $k = 0$, then $y = 0$. Otherwise if $k \neq 0$, then $k \geq 1$ as it's an integer. Then $y = kx \geqslant x$. □

Wait, did we not need the absolute signs then? Here's the trick. In inequalities, if you multiply by a negative number, the sign reverses. For instance $5 > 2$ but $-5 < -2$.

Question 1.2.2. *Find another mistake in the proof.*

In $y = kx$, you do remember k can be negative, right? That's why we need absolute signs. So here's the correct proof.

Proof: Write $y = kx$. If $k = 0$, then $y = 0$. Otherwise $k \neq 0$ implies

$$|y| = |k| \cdot |x| \geqslant |x|.$$

Here, note that we needed $|k| \geqslant 1$. Why is this true? Well, $k \neq 0$ and since $|k|$ is a natural number (hence positive), hence $|k| \geqslant 1$.

1.2.4 Special property 2

There's one more important property about divisibility I would like to point out. Let $\mathcal{M}$ be the set of multiples of 5 again, i.e.

$$\mathcal{M} = \{\dots, -5, 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, \dots\}.$$

Let c be any integer. What happens if we multiply any number in this set by c? The resulting number still stays in $\mathcal{M}$. Do you see why?

So $n \in \mathcal{M} \implies cn \in \mathcal{M}$ for any integer c.

Now consider any two elements of $\mathcal{M}$, and add them. For instance, $10 + 30 = 40$. Is the number still in $\mathcal{M}$? Yes! This is true because $5a + 5b = 5(a + b)$ is always divisible by 5.

So $x, y \in \mathcal{M} \implies x + y \in \mathcal{M}$.

Combining the above two results we can write:

Lemma 1.2.1. *For any two numbers $x, y \in \mathcal{M}$, we have $ax + by \in \mathcal{M}$ for any integers a, b.*

The above is true since $ax, by \in \mathcal{M}$, and hence so is their sum. What does this mean? This means that $5 \mid x, y$ implies $5 \mid ax$ and $5 \mid by$ for any a, b. Further, $5 \mid ax + by$. In particular, when b is negative, we get results like $5 \mid x - y, 2x - 3y$ and so on.

Again, let's generalize this to any number instead of 5. The general version gives us one of the most useful property of divisibility:

Theorem 1.2.3. *Suppose $c \mid x, y$. Then $c \mid ax + by$ for any $a, b \in \mathbb{Z}$.*

We finish this discussion with a list of properties, some of which we discussed above, and the others which I leave as exercises to prove.

Theorem 1.2.4. *Let x, y, z be integers.*

- $x \mid x$.
- $1 \mid x$ *and* $x \mid 0$.
- $x \mid y, y \mid z \implies x \mid z$.
- *If $z \mid x, y$, then $z \mid ax + by$ for any integers a, b (possibly negative).*
- *If $x \mid y$, then either $y = 0$, or $|x| \leq |y|$.*
- *If $x \mid y$ and $y \mid x$, then $x = \pm y$, i.e. $|x| = |y|$.*
- *$x \mid y$ if and only if $xz \mid yz$ for some* ***non-zero*** *integer z.*
- *$x \mid y \implies x \mid yz$ for any z.*

The two special properties we discussed and the last property given above would be the most useful in problem solving. For instance, suppose we had $n \mid 2n + 1$. Then we can subtract $2n$ (why?) from the right side to get $n \mid 1$ which implies $n = \pm 1$. In general, in divisibility relations like these, clever expressions are added/subtracted/multiplied to reduce the right side to something more manageable.

Problems for Practice

Problem 1.2.1. Show that if $n > 1$ is an integer, we can't have $n \mid 2n^2 + 3n + 1$.

Problem 1.2.2. Let $a > b$ be natural numbers. Show that we can't have $a \mid 2a + b$.

Problem 1.2.3. For 2 fixed integers x, y, prove that

$$x - y \mid x^n - y^n$$

for any integer n. (Hint: Long division)

1.3 Euclid's Division Lemma

This is one of the first theorems that people use to start studying Number Theory. Consider again the (positive) multiples of 5 :

$$\mathcal{M} = \{0, 5, 10, 15, 20, 25, 30, 35, 40, \dots\}$$

These contain some of the natural numbers. What about other naturals not in this list? For instance, where would we insert 32 in the list?

Yes, we write 32 between 30 and 35, and write $32 = 30 + 2 = 5 \times 6 + 2$. Similarly,

$$33 = 5 \times 6 + 3$$
$$34 = 5 \times 6 + 4$$
$$35 = 5 \times 6 + 5$$
$$36 = 5 \times 6 + 6.$$

However, the numbers $35, 36$ won't come in between $30, 35$. So better ways to write them is:

$$35 = 5 \times 7 + 0$$
$$36 = 5 \times 7 + 1.$$

As usual, our question is to generalize our tricks.

Lemma 1.3.1. *For any integers b, a, we can find a number $0 \leq r < a$ such b is r more than a multiple of a.*

The important bit here is $0 \leq r < a$. This is the same idea as when we wrote 36 as $5 \times 7 + 1$ instead of $5 \times 6 + 6$.

Question 1.3.1. *Why do we need $0 \leq r$ and not $0 < r$? Also, why $r < a$ and not $r \leq a$?*

What's a more mathematical way to write this?

Theorem 1.3.1 (Euclid's Division Lemma)**.** *For any integers b, a, we can find **unique** integers q, r such that*

$$b = aq + r, \qquad 0 \leq r < a.$$

Here, q is called the **quotient**, and r the **remainder**. Don't be scared by this statement, this is what you have always been doing in long division.

1.4 Primes

So now is the time to study primes. A number is called a **prime** if it has only two divisors, 1 and the number itself. The list of primes is:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots$$

It is important here to note that 2 is the only even prime. So at times, parity arguments work well with problems related to primes.

Question 1.4.1. *Is* 1 *a prime?*

Primes lie at the heart of Number Theory. As we will soon see, they form the atoms of all numbers, and understanding them is equivalent to understanding all numbers. However, life isn't so simple. There is no known pattern in primes (we will soon prove that no polynomial pattern is possible) and just the fact that factorizing into large primes is hard forms the base of cryptography. There have been many estimates related to primes, one of the most notable being the Prime Number Theorem, which states

$$\pi(n) \sim \frac{n}{\log n}.$$

What this means is the number of primes less than a number n is approximately equal to $n/\log n$, and this estimate gets better as n gets larger. Crazy right?

I can talk about primes all day. However, let's not get too ahead of ourselves for now. A simple question we can ask right now is the following: how many primes are there? This was answered by Euclid over 2000 years back! He proved that there are infinitely many primes. We will look at the proof later.

Problems for Practice

Problem 1.4.1. Find all positive integers n for which $3n-4, 4n-5$, and $5n-3$ are all prime numbers.

Problem 1.4.2. If $p < q$ are two consecutive odd prime numbers, show that $p+q$ has at least 3 prime factors (not necessarily distinct). **Sol:** pg. 277

1.4.1 Fundamental Theorem of Arithmetic

Clearly, you can reduce any composite number into a product of primes. The best part is the following:

Theorem 1.4.1 (Fundamental Theorem of Arithmetic)**.** *Any natural number greater than* 1 *has a* ***unique*** *prime factorization upto order.*

Unique means two things: there is at least one way and also at most one way. So you would be able to write any number as a product of primes, and there would be no other way

to do so (except for changing the order, like writing 2×5 as 5×2. These are considered the same.) So, for instance, you can write $45 = 3^2 \times 5$ but not in any other way.

Thus, any number n can be written as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1, \ldots, p_k$ are primes and $\alpha_1, \ldots, \alpha_k$ are non-negative integer. Note that an exponent can be zero too. For instance $24 = 2^3 \times 3^1 \times 5^0$.

Note here that 1 is the only natural number that does not have a prime factorization.

One of the most useful tips I can give you for this chapter is this: Imagine a number by its prime factors! I will use this idea a lot and expect you to keep this in mind as it would be used in problems more than you can imagine. The next section is based on this idea:

1.5 Looking at Numbers as Multisets

Considering how every number can be broken down into its prime factors, and these prime factors are the identity of the number, it's often useful to think of numbers as sets of prime factors.

So here's how it goes. The number 1 is the empty set. The number 6 would be the set $\{2, 3\}$ as $6 = 2 \times 3$. The number 70 would similarly be $\{2, 5, 7\}$. But what about the number $4 = 2^2$? We know that a set can't have repeated elements. So how do we write this? The solution is to consider multisets, which are the same as sets but allow repeated elements. So $4 \equiv \{2, 2\}$. In general,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \equiv \{\underbrace{p_1, \ldots, p_1}_{\alpha_1 \text{ times}}, \underbrace{p_2, \ldots, p_2}_{\alpha_2 \text{ times}}, \ldots, \underbrace{p_k, \ldots, p_k}_{\alpha_k \text{ times}}\}.$$

Note that we use the symbol $\equiv$, which means they are "equivalent". In this chapter, we would use small letters to denote numbers, and capital letters to denote their sets (unless otherwise stated). So if $n = 20$, then $N = \{2, 2, 5\}$. If the number is negative, we can just add -1 to the set. For instance -20 would be $\{-1, 2, 2, 5\}$

We clearly have the following theorem:

Theorem 1.5.1 (Divisibility in Sets)**.** *Let a, b be two integers. Then*

$$a \mid b \iff A \subset B.$$

What is the advantage of thinking in terms of sets? Well, sets have Venn Diagrams. Thinking geometrically/pictorially is always better (that's how the human brain functions). A lot of properties of GCD, LCM are, for instance, trivialized when you think about them as sets and use Theorem 1.5.1.

1.6 GCD and LCM

We can now define the GCD.

Definition 1.6.1. *The GCD, or the* ***Greatest Common Divisor*** *of two numbers is the number obtained by the set of common prime factors. For two numbers m, n, it is denoted by $\gcd(m, n)$, or often just (m, n).*

This is often called the HCF, i.e. the Highest Common Factor. Suppose you have $m = 2^2 \times 5^3 \times 7^1$ and $n = 2^3 \times 3^2 \times 7^2$, then $\gcd(m, n) = 2^2 \times 7$. In general,

$$\gcd(m, n) = M \cap N.$$

Clearly $\gcd(a, b)$ divides both a, b. However the "greatest" in GCD has a special purpose:

Lemma 1.6.1. *Let a, b be integers. The GCD of a, b is the* ***largest*** *number which divides* ***both*** *a, b. In particular, $\gcd(a, b) \leq a, b$.*

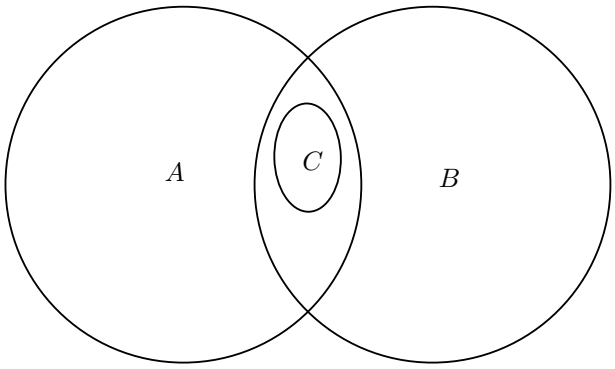
Why are these definitions the same? To explain this, think in terms of the prime factors! Suppose the GCD is not the largest. Then some other number is the largest one, call x. But any common prime factors of a, b are already contained in $\gcd(a, b)$. So x cannot have anything more.

Now we have the following useful property which you should find easy to prove:

Lemma 1.6.2. *Let a, b, c be three integers. Then*

$$c \mid a, c \mid b \implies c \mid \gcd(a, b).$$

I will give a geometric interpretation of this lemma, which also makes it very easy to prove.



We have the two sets A, B. The common region is $\gcd(a, b)$ by definition. The shape in the common region is C. Since c divides both a, b, hence $C \subset A$ and $C \subset B$. Thus, C lies in the $A \cap B$ region, which is the same as saying $c \mid \gcd(a, b)$ by Theorem 1.5.1. Hence proved!

I will now let you reason out why the following is true:

Lemma 1.6.3 (The Prime Factorization of GCD)**.** *Let a, b be two integers with prime factorization:*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

where α_i, β_i are non-negative integers (possibly 0). Then

$$\gcd(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \dots p_k^{\min\{\alpha_k, \beta_k\}}.$$

We can similarly define the LCM, the **Least Common Multiple** in two equivalent ways:

Definition 1.6.2. *Let a, b be two integers.*

1. *We have*
$$\operatorname{lcm}(a, b) = A \cup B.$$
2. *The LCM of a, b is the **least** number divisible by **both** a, b. In particular, $a, b \leq \operatorname{lcm}(a, b)$.*
3. *If the prime factorizations of a, b are*
$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$
where α_i, β_i are non-negative integers (possibly 0), then
$$\operatorname{lcm}(a, b) = p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \dots p_k^{\max\{\alpha_k, \beta_k\}}.$$

Just like Lemma 1.6.2, we have the following (which is useful)

Lemma 1.6.4. *Let a, b, c be integers. Then*

$$a \mid c, b \mid c \implies \operatorname{lcm}(a, b) \mid c.$$

I will let the proof as an exercise (just look at the venn diagram again).

Now we have the following property that connect the GCD and LCM, that you might have seen:

Lemma 1.6.5 (Product of GCD and LCM)**.** *Let a, b be two integers. Then*

$$\gcd(a, b) \operatorname{lcm}(a, b) = ab.$$

There are two ways to prove this. The first one is

$$\begin{aligned}\gcd(a,b)\,\mathrm{lcm}(a,b) &= \left(p_1^{\min(\alpha_1,\beta_1)+\max(\alpha_1,\beta_1)}\right)\ldots\left(p_k^{\min(\alpha_k,\beta_k)+\max(\alpha_k,\beta_k)}\right)\\ &= p_1^{\alpha_1+\beta_1}\ldots p_k^{\alpha_k+\beta_k} = ab.\end{aligned}$$

The second proof is by looking at the venn diagram. Note that the sum of $A\cup B$ and $A\cap B$ gives the sum of A, B (why?) This proves the lemma!

Comment 1.6.1: Recall that the sum of two sets A, B, which we denote by $A+B$, is kind of like the union in which we include all the elements of A, B, and the multiplicity of each element is added in $A+B$. For example if $A=\{2,2,3\}$ and $B=\{2,3,3,5\}$, then $A\cup B=\{2,2,3,3,5\}$, $A\cap B=\{2,3\}$ while $A+B=\{2,2,2,3,3,3,5\}$, which is different from both $A\cup B$ and $A\cap B$. Check that $(A\cup B)+(A\cap B)=A+B$ (by the Venn Diagram). This fact corresponds to the Principle of Inclusion-Exclusion for two sets:

$$|A\cup B|+|A\cap B| = |A|+|B|.$$

Before we end, here's an important definition:

Definition 1.6.3. *Two numbers a, b are called **coprime** or relatively prime if* $\gcd(a,b)=1$.

In other words, they have no common prime factors. These types of numbers come a lot, and we will come across them a lot.

A simple question that stood for long was: how many primes are there? This was answered by Euclid as back as in 300 BC. Now that we have a fair understanding of divisibility and primes, let us discuss his proof.

Theorem 1.6.1 (Euclid)**.** *Prove that there are infinitely many primes.*

This is an amazing proof. It goes by the powerful method of contradiction, by assuming there are only finitely many primes $\{p_1,p_2,\ldots,p_k\}$. The key trick now is to define the number

$$N = p_1p_2\ldots p_k+1.$$

Now, clearly N is pairwise coprime[1] to all $p_1,p_2,\ldots,p_k$. However, clearly $N>1$ and so by the Fundamental Theorem of Arithmetic, it must have a prime divisor p. However, p would be different from all $p_1,p_2,\ldots,p_k$, contradicting the fact that $\{p_1,\ldots,p_k\}$ are all the primes. This is the desired contradiction!

[1]If a number x is "pairwise coprime" to some numbers a,b,c, then that means it is coprime to each number, i.e. $\gcd(x,a)=\gcd(x,b)=\gcd(x,c)=1$. We define "pairwise coprime" for more than 3 numbers similarly.

Problems for Practice

Problem 1.6.1. Prove that $\gcd(a, b) = a$ if and only if $a \mid b$.

Problem 1.6.2. If p is a prime, prove that $\gcd(a, p) \in \{1, p\}$.

Problem 1.6.3. Let a, b be relatively prime. Show that if $a \mid c, b \mid c$, then $ab \mid c$.

1.7 Euclid's Division Algorithm

Key tip: Think of the gcd in terms of common prime factors!

Suppose $m = p^2q$ and $n = pq^2r$. Clearly $\gcd(m, n) = pq$. Now, $m + n = p^2q + pq^2r = pq(p + qr) = \gcd(m, n)(p + qr)$. In general, the thing we can take common outside in $m + n$ is $\gcd(m, n)$. And the 2 things inside would have no common factor (why?). Now answer the following:

Question 1.7.1. *Why is* $\gcd(a + b, b) = \gcd(a, b)$?

Question 1.7.2. *Why is* $\gcd(a + 3b, b) = \gcd(a, b)$?

Generalizing the above problems, we have

Lemma 1.7.1. *Let a, b be integers. We can write $a = bq+r$ for integers q, r where $0 \leq r < b$. Then the lemma states that*

$$\gcd(a, b) = \gcd(r, b).$$

It is often helpful to remember things pictorially:

$$\overset{\gcd(a,b)}{\overbrace{}}\; a = b \times q + r \;\underset{\gcd(b,r)}{\underbrace{}}$$

The more useful fact to remember is that $\gcd(a, b) = \gcd(a \pm kb, b)$. Just like in " $\mid$ " divisibility, you subtract things carefully to simplify expressions. This lemma is a consequence of this idea since:

$$\gcd(a, b) = \gcd(bq + r, b) = \gcd(bq + r - b(q), b) = \gcd(r, b).$$

One consequence of the above is the so called **Division Algorithm**. Suppose want to find $\gcd(370, 100)$. Write

$$370 = 3 \times 100 + 70.$$

By the lemma, we find $\gcd(370, 100) = \gcd(70, 100)$. Then write

$$100 = 70 \times 1 + 30.$$

So $\gcd(70, 100) = \gcd(70, 30)$. Then we can similarly proceed and get the chain:

$$\gcd(370, 100) = \gcd(70, 100) = \gcd(70, 30) = \gcd(10, 30) = 10.$$

The last part is because 10 divides 30.

The general algorithm is defined in a similar way, just keep on reducing $\gcd(a, b)$ to $\gcd(b, r)$ and eventually one number will divide the other.

Question 1.7.3. *Why must the algorithm terminate? That is, why does it stop eventually and not go on forever?*

I will give another example: let's find $\gcd(124, 440)$.

$$\begin{aligned} 440 &= 124 \times 3 + 68 \\ 124 &= 68 \times 1 + 56 \\ 68 &= 56 \times 1 + 12 \\ 56 &= 12 \times 4 + 8 \\ 12 &= 8 \times 1 + 4 \\ 8 &= 2 \times 4 + 0. \end{aligned}$$

We stop when get 0 as a remainder. Thus, we get the chain

$$\gcd(440, 124) = \gcd(124, 68) = \gcd(68, 56) = \gcd(56, 12) = \gcd(12, 8)\gcd(8, 4) = 4.$$

Problems for Practice

Problem 1.7.1. Find $\gcd(120, 500)$ using the algorithm.

Problem 1.7.2. Show that $\gcd(4n + 3, 2n) \in \{1, 3\}$.

Problem 1.7.3. Let a, b be integers. We can write $a = bq + r$ for integers q, r where $0 \leq r < b$. Then our lemma states that

$$\gcd(a, b) = \gcd(r, b).$$

However, is $\text{lcm}(a, b) = \text{lcm}(r, b)$?

1.8 Bézout's Theorem

Try the following problem:

Problem 1.8.1. Let a, b, x, y, n be integers such that

$$ax + by = n.$$

Prove that $\gcd(a, b)$ divides n.

After all the work we have done, can you see a one line proof? We now talk more about this equation. A natural question that arises is, given a, b, what values can $ax + by$ take as $x, y \in \mathbb{Z}$? Call a number n *special* if

$$ax + by = n$$

has a solution in (x, y). Let $a = 2, b = 4$. Which ones are *special*? We look at the larger picture now (you read the preface, didn't you?), and consider all elements of the form $2x+4y$. This forms the following table: (the top row is the value of x, the column that of y, and the element in column X, row Y is $2X + 4Y$)

	-2	-1	0	1	2	$\dots$	x
-2	-12	-10	2	4	6	$\dots$	$\vdots$
-1	-8	-6	4	6	8	$\dots$	$\vdots$
0	-4	-2	0	2	4	$\dots$	$\vdots$
1	0	2	4	6	8	$\dots$	$\vdots$
2	4	6	8	10	12	$\dots$	$\vdots$
3	8	10	12	14	16	$\dots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
y	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$2x + 4y$

Every *special* number is obviously divisible by 2 (why?). It seems that every multiple of 2 is in the table. In particular so is $\gcd(2, 4) = 2$.

Let's not get too ahead of ourselves and directly ask about all the numbers in the table. First we ask ourselves does $\gcd(a, b)$ always appear in the table of (a, b), i.e. is $\gcd(a, b)$ always *special*?

Example 1.8.1

Let $(a, b) = (3, 6)$. Then $\gcd(3, 6) = 3$ and

$$3(1) + 6(0) = 3$$

If $(a, b) = (35, 42)$, then $\gcd(a, b) = 7$ and

$$35(5) + 42(-4) = 7.$$

So our conjecture is true for the pairs $(3, 6), (35, 42)$.

Problem 1.8.2. Let $(a, b) = (8, 12)$. Find $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b).$$

Problem 1.8.3. Let $(a, b) = (7, 12)$. Find $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b).$$

So our conjecture is $\gcd(a, b)$ is always *special.*

In fact, if $ax + by = \gcd(a, b)$ has a solution $(x, y) = (x_0, y_0)$, then

$$a(mx_0) + b(my_0) = m(ax_0 + by_y) = m \gcd(a, b)$$

for any m. So every multiple of $\gcd(a, b)$ is expressible as $ax + by$. In other words, every multiple of $\gcd(a, b)$ is *special*!

This is the famous Bézout's lemma:

Theorem 1.8.1 (Bézout's theorem)**.** *Let a, b be integers. Then the equation*

$$ax + by = n$$

has a solution if and only if $\gcd(a, b)$ *divides* n.

Note the *if and only if.* It means two things (as usual): If $ax + by = n$, then $\gcd(a, b) \mid n$ (we did this earlier). Also, if $\gcd(a, b) \mid n$, then we can find x_0, y_0 integers such that $ax_0 + by_0 = n$.

We will not prove this now, rather prove it in the example problems.

Example 1.8.2 (Euclid's Lemma)

If $c \mid ab$ and $\gcd(c, a) = 1$, then $c \mid b$.

One way to do this is to look at the prime factors. Since $c \mid ab$, hence $C \subset A + B$. However, $\gcd(c, a) = 1$ implies $C \cap A = \phi$ and so C must entirely be inside B, which means $c \mid b$. (in other words, a has no contribution in the divisibility so ignore it.)

However the proof using Bézout's lemma has its own elegance. The idea is this: as $\gcd(c, a) = 1$, hence there exist integers x, y such that $cx + ay = 1$. Then

$$cbx + aby = b.$$

Now clearly c divides cbx. Also, c divides ab, and so c divides aby. Hence it divides $cbx + aby$, i.e. the left side. So $c \mid b$. Hence done!

Example 1.8.3 (PUTNAM 2000)

Prove the expression

$$\frac{\gcd(m,n)}{n}\binom{n}{m}$$

is an integer for all pairs of integers $n \geq m \geq 1$.

This is one of my favorite applications. This one is not very easy to approach directly. However, if we write $\gcd(m,n) = mx+ny$ by using Bézout's Lemma, with $x, y \in \mathbb{Z}$ (the fact that $x, y \in \mathbb{Z}$ is the important one), then

$$\frac{\gcd(m,n)}{n}\binom{n}{m} = \frac{mx+ny}{n}\binom{n}{m} = x \cdot \frac{m}{n}\binom{n}{m} + y\binom{n}{m}.$$

The second term is clearly an integer. For the first term, it's not so direct why it should be an integer. It may seem like this depends on x, which would only make the problem harder. However, it turns out it is independent of x as the binomial coefficient "absorbs" the m/n fraction:

$$x \cdot \frac{m}{n}\binom{n}{m} = x \cdot \frac{m}{n} \cdot \frac{n!}{m!(n-m)!} = x \cdot \frac{(n-1)!}{(m-1)!(n-m)!} = x\binom{n-1}{m-1} \in \mathbb{Z}$$

and so we are done.

1.9 Base Systems

How do we write numbers? The answer is pretty simple and the question is dumb. However, if we truly investigate this question, we can do some interesting stuff.

Any number is written using the digits $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. Further, we write, say 514567 as

$$514567 = 5 \times 10^5 + 1 \times 10^4 + 4 \times 10^3 + 5 \times 10^2 + 6 \times 10^1 + 7 \times 10^0.$$

All these digits are at most 10. Hence this system is called the **base 10** representation.

Suppose you had only the digits $0, 1$. Then $2 = 1 \times 2^1 + 0 \times 2^0$, and so we would write 2 as "10", if we were to do something similar to base 10. Since we are talking of base 2 (which is also called **binary**), we write 2 as $10_{(2)}$. As $3 = 1 \times 2^1 + 1 \times 2^0$, so $3 = 11_{(2)}$. Now, 4 would become $1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$, so we write 4 as $100_{(2)}$. We similarly write other numbers:

$$\begin{aligned} 5 &= 101_{(2)} \\ 6 &= 110_{(2)} \\ 7 &= 111_{(2)} \\ 8 &= 1000_{(2)} \\ 9 &= 1001_{(2)} \\ 10 &= 1010_{(2)} \\ &\vdots \end{aligned}$$

I guess you would be able to see a pattern by now. How do we add numbers in base 2? This is exactly similar to normal addition, except a carry over of 1 is taken for $1 + 1 = 10_{(2)}$.

Question 1.9.1. *Why don't we have the digit* 2 *in base* 2*? Answer this in terms of the base* 2 *expansion, i.e.* $a_0 + 2a_1 + 4a_2 + \dots$.

Now, we can very similarly define other base systems. For instance, 9 in base 4 would be $21_{(4)}$. How do we write a number in some other base? Suppose you have 52, and we want to write this in base 3. So we would have

$$52 = a_0 \times 3^0 + a_1 \times 3^1 + a_2 \times 3^2 + \cdots + a_k \times 3^k.$$

Over here, we assume $a_k \neq 0$ (why?), and hence $a_k \geq 1$. Now divide 52 by 3. Since $a_1 \times 3^1 + a_2 \times 3^2 + \dots$ is divisible by 3, hence the remainder on dividing 52 by 3 has to be a_0, which comes out to 1. So we write $52 = 1 + 51$. Next we have

$$51 = a_1 \times 3^1 + a_2 \times 3^2 + \cdots + a_k \times 3^k \implies 17 = a_1 \times 3^0 + a_2 \times 3^1 + \cdots + a_k \times 3^{k-1}.$$

Again, a_1 is the only term on the right that isn't divisible by 3 now. So, a_1 is the remainder when 17 is divided by 3, which is 2.

We can similarly keep going and find $52 = 1221_{(3)}$. The above way was nice and algorithmic (and so always works), but for smaller numbers guessing is a better job. How do we guess it? Well, the key observation is that

$$a_0 \times 3^0 + a_1 \times 3^1 + a_2 \times 3^2 + \cdots + a_k \times 3^k \geq 3^k$$

and

$$a_0 \times 3^0 + a_1 \times 3^1 + a_2 \times 3^2 + \cdots + a_k \times 3^k \leq 2(3^0 + 3^1 + \cdots + 3^k) = 2 \times \frac{3^{k+1} - 1}{3 - 1} = 3^{k+1} - 1.$$

Hence, $3^k \leq 52 < 3^{k+1}$ (why?). So we basically want to know between which powers of 3 does 52 lie. This is easy; we can see that $k = 3$. Further, $1 \cdot 3^3 \leq 52 < 2 \cdot 3^3$, hence $a_k = 1$ (why?) and $k = 3$. So now consider $52 - 3^3 = 25$. Now 25 lies between 9 and 27, and further we $2 \cdot 3^2 \leq 25 < 3 \cdot 3^2$ and so $a_{k-1} = 2$. We can similarly find the rest of the digits.

The second method is easier to do for small numbers. To find the leading digit, we find between which powers does n lie (this is what we have always been doing in base 10, right?).

Problem 1.9.1. Find 37 in base 5. Find 69 in base 2.

Problem 1.9.2. Show that any power of 2 is of the form $100\dots0$ in base 2.

Problem 1.9.3. Prove in general that if $n = a_0 \times \ell^0 + \cdots + a_k \times \ell^k$, then k is such that $\ell^k \leq n < \ell^{k+1}$ and a_k is such that $a_k \ell^k \leq n < (a_k + 1)\ell^k$.

Problem 1.9.4. Let k be the integer just less than (or equal to) $\log_\ell(n)$. Show that n has exactly $k + 1$ digits in base ℓ.

An important question we haven't answer yet is the following: is a base representation unique? That is, is it possible that a number n has two different representations in base ℓ? The answer is no, and this is an incredibly useful fact about base system:

Theorem 1.9.1. *Any number n has a unique representation in base ℓ.*

1.10 Extra Results as Problems

In this section, we prove some more basic results related to divisibility. The first one is a classic:

Example 1.10.1

Prove that $\sqrt{p}$ is irrational for any prime p.

Assume on the contrary, and write $\sqrt{p} = m/n$, for some positive integers m, n. The key assumption we make at this point is that m, n are coprime. Clearly we can assume this, since otherwise just cancel out any common factors.

The most natural thing we can do now is square both the sides (since that is how the square root is even defined), so we get $m^2 = pn^2$. Hence, $p \mid m^2$. Since p is a prime, hence $p \mid m$. Write $m = pm^*$.

Putting this back, we find $p^2(m^*)^2 = pn^2$, so that $n^2 = p(m^*)^2$. Hence, $p \mid n^2$. Again, p is a prime so $p \mid n$. Hence, we have $p \mid m$ and $p \mid n$, contradicting our assumption that m, n were coprime. □

Question 1.10.1. *Where did we use the fact that p is a prime?*

The next result is useful too:

Example 1.10.2

Prove that if p is a prime and $0 < k < p$, then $\binom{p}{k}$ is divisible by p.

For this, write

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = p \cdot \frac{(p-1)(p-2)\dots(p-k+1)}{k(k-1)\dots 1} = pS.$$

Now p divides this if S is an integer. Here's the trick: we know pS is an integer. Since p is coprime to all $k, k-1, \dots, 1$ (why?), hence p has no contribution in making pS an integer (basically Example 1.8.2). Hence, S must be an integer, and we are done.

Example 1.10.3 (Euclid's Division Lemma)

Let a, b be integers. Prove that there exists unique integers q, r such that $b = aq + r$ with $0 \leq r < a$.

We have seen why this is true, however never gave a formal proof. Even though the proof is almost identical to what we did, it is important since it is an application of the extremal principle[2].

[2]The extreme principle (or extremal principle) is a problem-solving technique that involves looking at objects with extreme properties, such as the largest or smallest element. This is possible for sets which have a smallest or largest object defined (for instance, the set $\mathbb{N}$ has no largest element but has a smallest element).

Proof. Just like what we did before, pick two multiples of a such that b lies between them. This is the same as saying pick a q such that $aq \leq b < a(q+1)$. It is easy to see that such a q is unique. Now, define $r = b - aq$, which is uniquely defined by a, b. We claim that this pair of (q, r) works.

Indeed, $0 \leq r$ is clear since $b \geq aq$ by assumption. Now, since $aq + q > b$, hence $q > b - aq = r$. Hence, the q, r exist and are unique, and r satisfies $0 \leq r < a$. So we are done. □

A very similar idea is seen in Example 1.11.8. The next example is a very useful result.

Example 1.10.4

Let a, m, n be positive integers. Prove that

$$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1.$$

First let's get a feel of why this is true. If we get the gcd is something of the form $a^d - 1$, then $a^d - 1 \mid a^m - 1$ and $a^n - 1$ both. So $d \mid m, n$ and the largest d (which we need for the **greatest** common divisor) would be $\gcd(m, n)$. Let's now try to prove the result more formally:

We present the more natural way to approach this question. Suppose $m \geq n$. Then

$$g = \gcd(a^m - 1, a^n - 1) = \gcd((a^m - 1) - (a^n - 1), a^n - 1) = \gcd(a^{m-n} - 1, a^n - 1).$$

Now again, if $m - n \geq n$, we can get $g = \gcd(a^{m-2n} - 1, a^n - 1)$. In fact, if $m = nk + r$ with $r < n$, we can get $g = \gcd(a^r - 1, a^n - 1)$. Now, $n > r$, so we can reduce n to $n - r$ and so on. The key observation is that the exponents are following Euclid's division algorithm (think why). Hence, we would at the end have $g = a^{\gcd(m,n)-1}$. This is hard to think of, so I suggest you take some examples (such as $(m, n) = (15, 4)$) and see convince yourself.

We will see a simpler solution to this problem in the next chapter. For now, let's prove Bézout's theorem.

Example 1.10.5 (Bézout's Theorem)

Let a, b be integers with $\gcd(a, b) = d$. Then there exist integers x, y such that $ax + by = d$.

There are two proofs to this that we will discuss. The first one will give us an algorithm on how to find x, y explicitly. The second one will be an existence type proof, where we just show x, y exist, without knowing anything about them (we will such similar themes in the Constructions chapter.)

Suppose we want to express 5 as a linear combination of 45 and 65. We write

$$65 = 45 \times 1 + 20$$
$$45 = 20 \times 2 + 5$$
$$20 = 5 \times 4 + 0$$

So, we reverse the above to get 5 in terms of $45, 65$.

$$\begin{aligned} 5 &= 45 - 20 \times 2 \\ &= 45 - (65 - 45(1)) \times 2 \\ &= 45(3) - 65(2). \end{aligned}$$

Let's do another example. Suppose we want to express 1 as a linear combination of $7, 12$. Firstly,

$$\begin{aligned} 12 &= 7 \times 1 + 5 \\ 7 &= 5 \times 1 + 2 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 1 \times 2. \end{aligned}$$

Reversing,

$$\begin{aligned} 1 &= 5 - 2(2) \\ &= (12 - 7(1)) - (7 - 5(1))(2) \\ &= 12 - 7(1) - 7(2) + (12 - 7(1))(2) \\ &= 12 - 7(3) + 12(2) - 7(2) \\ &= 12(3) - 7(5) \end{aligned}$$

The basic idea is to keep replacing the remainders. This works in general too.

Of course the above proof was not rigorous. So to write a formal proof, we say "consider Euclid's division algorithm, and start working in the reverse order. In each step, replace the remainders." This is a valid argument, although doesn't give a complete feel about the proof. So I explained it using examples.

The second proof is more combinatorial in nature (and again, matches with our theme of looking at the larger picture)

Proof. The larger picture in this case is ALL the elements of the form $ax+by$, i.e. we consider the set $\mathcal{S} = \{ax + by \mid x, y \in \mathbb{Z}\}$. Clearly, each element is an integer. Now, as we saw in the table, the elements are all multiples of $\gcd(a, b)$, so that the smallest positive element is $\gcd(a, b)$. So this is the idea: Take the smallest **positive** element of $\mathcal{S}$, say d, achieved for (x_0, y_0). We need to show $d = \gcd(a, b)$.

Now, $ax_0 + by_0 = d$. We need to show $d = \gcd(a, b)$. Now showing equality is hard in number theory, so we show $d \mid \gcd(a, b)$ and $\gcd(a, b) \mid d$. The latter is clearly true (why?), so let's focus on the former. For this, we must try to show that d divides both a, b (why?).

Suppose not. Write $a = dk + r$ with $0 < r < d$ (why $0 < r$ not $0 \leq r$?). Then $r = a - dk = a - (ax_0 + by_0)k = a(1 - x_0k) + b(y_0k)$. Hence, $r \in \mathcal{S}$ with $0 < r < d$. However this contradicts our assumption. Hence, $d \mid a$. Similarly, $d \mid b$ and we are done. □

Example 1.10.6 (Four Number Lemma)

Let a, b, c, and d be positive integers such that $ab = cd$. Show that there exists positive integers p, q, r, s such that

$$a = pq, \quad b = rs, \quad c = ps, \quad d = qr.$$

Proof. This is not very hard to show: since

$$\frac{a}{c} = \frac{d}{b},$$

hence the two fraction both equal a common reduced fraction, say $\frac{q}{s}$ with $\gcd(q, s) = 1$. Then, $(a, c) = (pq, ps)$ for some p and $(b, d) = (rs, rq)$ for some r. So we are done. □

The result is useful in problems. For instance, show the following:

Problem 1.10.1. Prove that if $ab = cd$, then $a + b + c + d$ is not a prime number.

1.11 Example Problems

Let's begin with an easy problem.

Example 1.11.1 (All Russia Mathematics Olympiad 1995)

Let m, n be positive integers such that

$$\gcd(m,n) + \operatorname{lcm}(m,n) = m + n.$$

Show that one of the two numbers is divisible by the other.

Let $\gcd(m,n) = g$. The simplest thing we can do is to convert the LCM into GCD. So

$$g + \frac{mn}{g} = m + n \implies mn + g^2 = g(m+n) \implies (m-g)(n-g) = 0$$

which gives either $g = m$ or $g = n$. Why is this enough?

Example 1.11.2

If p is an odd prime, and a, b are coprime, show that

$$\gcd\left(\frac{a^p + b^p}{a+b}, a+b\right) \in \{1, p\}.$$

Write

$$\frac{a^p + b^p}{a+b} = a^{p-1} - a^{p-2}b + \cdots + b^{p-1}.$$

We divide the above by $(a+b)$. Do this using long division to find the remainder when the above is divided by $a+b$. This gives us

$$\begin{aligned} &a^{p-1} - a^{p-2}b + \cdots + b^{p-1} \\ &= (a+b)(a^{p-2} - 2a^{p-2}b + 3a^{p-3}b^2 - \cdots - pb^{p-2}) + pb^{p-1}. \end{aligned}$$

So,

$$\gcd\left(\frac{a^p + b^p}{a+b}, a+b\right) = \gcd(a+b, pb^{p-1}).$$

Now $a+b$ and b^{p-1} are coprime as a and b are coprime. So, the above *gcd* equals $\gcd(a+b, p)$, which is either 1 or p. □

Example 1.11.3 (Iran 2005)

Let $n, p > 1$ be positive integers and p be prime. Given that $n \mid p-1$ and $p \mid n^3 - 1$, prove that $4p - 3$ is a perfect square.

This is an amazing problem. In these types of problems, we try to extract as much information as we can, by bounding and simplifying the multiple. So $n \mid p-1$ implies $p \geq n+1$, and also $p = nk+1$.

Also $p \mid (n-1)(n^2+n+1)$ implies $p \mid n-1$ or $p \mid n^2+n+1$ (why?). However, $p \mid n-1$ is impossible (why?). So $p \mid n^2+n+1$. This gives $p \leq n^2+n+1$. Further,

$$nk+1 \mid n^2+n+1 \mid kn^2+kn+k \implies nk+1 \mid kn^2+kn+k-n(nk+1) = nk+k-n.$$

So, $nk+1 \leq nk+k-n \implies n+1 \leq k$. In terms of p, this means $n(n+1)+1 \leq nk+1 = p$. Does this ring a bell? Earlier we had $p \leq n^2+n+1$. So $p = n^2+n+1$ holds! This then directly gives $4p-3 = (2n+1)^2$.

Question 1.11.1. *Since $nk+1 \mid nk+k-n \implies nk+1 \leq |nk+k-n|$. Why we did we not consider the absolute value?*

Example 1.11.4 (APMO)

Are there distinct prime numbers a, b, c which satisfy

$$a|bc+b+c, b|ca+c+a, c|ab+a+b?$$

Think of $bc+b+c$ as $(b+1)(c+1)-1$. So $a \mid (b+1)(c+1)-1$. To make the right side more symmetric, we can multiply the relation by $(a+1)$ to get $a \mid (a+1)(b+1)(c+1)-a-1$. We can of course, add a to the right term to get $a \mid (a+1)(b+1)(c+1)-1$. This is completely symmetric, and so we get

$$a, b, c \mid (a+1)(b+1)(c+1)-1.$$

Normally, this would imply $\text{lcm}(a,b,c) \mid (a+1)(b+1)(c+1)-1$ (why?). However, in this case $\text{lcm}(a,b,c) = 1$ (why?). So we get

$$abc \mid (a+1)(b+1)(c+1)-1. \implies abc \mid (a+1)(b+1)(c+1)-1-abc = ab+bc+ca+a+b+c.$$

Now, we turn to size arguments, since the right side doesn't seem to be something of the form $abc, 2abc, 3abc, \ldots$ (it seems to be much less). So, we get

$$1 \leq \frac{1}{ab}+\frac{1}{bc}+\frac{1}{ca}+\frac{1}{a}+\frac{1}{b}+\frac{1}{c}.$$

At this point, we see that the right side gets very small very soon. To formalize this idea, we assume $a < b < c$, and so we get

$$1 \leq \frac{1}{ab}+\frac{1}{bc}+\frac{1}{ca}+\frac{1}{a}+\frac{1}{b}+\frac{1}{c} \leq \frac{3}{a^2}+\frac{3}{a}.$$

This fails if $a \geq 4$. So, $a \leq 3$. Since a is a prime, hence $a \in \{2,3\}$. Now, this becomes a classic casework type problem.

1. Suppose $a = 2$. Then

$$1 \leq \frac{1}{2b} + \frac{1}{2c} + \frac{1}{bc} + \frac{1}{b} + \frac{1}{c} + \frac{1}{2} \implies \frac{1}{2} \leq \frac{3(b+c)+2}{2bc}.$$

So, $bc \leq 3(b+c)+2$. Considering the left side is a product and the right a sum, it is expected that this cannot hold for large values of b, c. So a small test would be sufficient. However, we can do it faster by writing it as $(b-3)(c-3) \leq 11$. Then keeping in mind that b, c are primes, we can do a casework again to find possible values of b, c. Keep in mind that $2 = a < b < c$.

Once we bound the values of b, c, we plug them in back in $abc \mid (a+1)(b+1)(c+1)-1$ and check which works.

2. Suppose $a = 3$. This case is also similarly dealt with (we can use $3 = a < b < c$ to reduce some work of ours).

Spoiler alert: the answer is that no such primes exist.

Next, we try a really nice problem, which shows how clever rearranging, an "algebra thing", can be useful.

Example 1.11.5 (AMM)

Show that for all prime numbers p,

$$\mathbb{Q}(p) = \prod_{k=1}^{p-1} k^{2k-p-1}$$

is an integer.

The product is

$$\mathbb{Q}(p) = \frac{(1^1 \cdot 2^2 \dots (p-1)^{p-1})^2}{(1 \cdot 2 \dots (p-1))^{p+1}}.$$

Looking at the numerator, it is quite natural to regroup terms as

$$\big(1 \cdot 2 \cdot 3 \dots (p-1)\big)\big(2 \cdot 3 \dots (p-1)\big)\big(3 \dots (p-1)\big) \dots \big((p-1)\big).$$

This product is clearly

$$(p-1)! \cdot \frac{(p-1)!}{1!} \cdot \frac{(p-1)!}{2!} \cdots \frac{(p-1)!}{(p-2)!}.$$

Hence, we can write

$$\mathbb{Q}(p) = \left(\frac{((p-1)!)^{p-1}}{1! \cdot 2! \dots (p-2)!}\right)^2 \cdot \frac{1}{((p-1)!)^{p+1}} = \frac{((p-1)!)^{p-1}}{(1! \cdot 2! \dots (p-1)!)^2}.$$

We again rearrange cleverly to get

$$\mathbb{Q}(p) = \frac{1}{p^{p-1}} \frac{(p!)^{p-1}}{(1! \cdot 2! \dots (p-1)!)^2} = \left(\frac{1}{p} \cdot \frac{p!}{1!(p-1)!}\right)\left(\frac{1}{p} \cdot \frac{p!}{2!(p-2)!}\right) \dots \left(\frac{1}{p} \cdot \frac{p!}{(p-1)!1!}\right)$$

Hence we obtain the amazing result that

$$\mathbb{Q}(p) = \prod_{k=1}^{p-1} \frac{\binom{p}{k}}{p}.$$

Now each fraction is an integer (why?), hence so is the product. We are thus done.

Example 1.11.6 (HMMT 2017)

Find all pairs (a, b) of positive integers such that $a^{2017} + b$ is a multiple of ab.

Usually, products are much easier to deal with than summations in divisibility. Here we have the term ab. Now we are not able to simplify this equation if use ab, but we can use a and b individually. We get $a \mid a^{2017} + b$ and $b \mid a^{2017} + b$. So we get $a \mid b$ and $b \mid a^{2017}$. The first one is simpler than the second, so we use that. Let $b = ak$. So put this back and the problem becomes

$$ak \mid a^{2016} + k.$$

Did you see what just happened? This is excatly identical to the problem, except that we reduced 2017 to 2016. The interesting part is that we can do this again and again. At the end, we will end up with $a\ell \mid 1 + \ell$ for some ℓ (why?). So $\ell = 1$ and hence $a \in \{1, 2\}$.

If $a = 1$, it is easy to get $b = 1$. If $a = 2$, then $2b \mid 2^{2017} + b$ and so $b \mid 2^{2017}$. Hence, b is a power of 2, write $b = 2^\omega$ with $\omega \leq 2017$. Then

$$2^{\omega+1} \mid 2^{2017} + 2^\omega = 2^\omega \left(2^{2017-\omega} + 1\right).$$

So, $2 \mid 2^{2017-\omega} + 1$, which is possible only if $2017 = \omega$. Hence, we get the solution pairs $(a, b) = (1, 1), (2, 2^{2017})$.

The next problem is a nice application of the four number lemma.

Example 1.11.7 (India Practice TST 2017 D2 P2)

Let a, b, c, d be pairwise distinct positive integers such that

$$\frac{a}{a+b} + \frac{b}{b+c} + \frac{c}{c+d} + \frac{d}{d+a}$$

is an integer. Prove that $a + b + c + d$ is not a prime number

Proof. Let X be the sum. We also define

$$Y = \frac{b}{a+b} + \frac{c}{b+c} + \frac{d}{c+d} + \frac{a}{d+a}.$$

Now observe that $X + Y = 4$. In particular, Y is also an integer. Further,

$$\begin{aligned} X &= \frac{a}{a+b} + \frac{b}{b+c} + \frac{c}{c+d} + \frac{d}{d+a} \\ &> \frac{a}{a+b+c+d} + \frac{b}{a+b+c+d} + \frac{c}{a+b+c+d} + \frac{d}{a+b+c+d} = 1. \end{aligned}$$

Similarly, $Y > 1$. Now since X, Y are integers that add to 4, hence $X = Y = 2$. But then

$$\begin{aligned} 0 = X - Y &= \frac{a-b}{a+b} + \frac{b-c}{b+c} + \frac{c-d}{c+d} + \frac{d-a}{d+a} \\ &= \frac{ac + ad - bc - bd + ac - ad + bc - bd}{(a+b)(c+d)} + \frac{ab - ac + bd - cd + bd - ab + cd - ac}{(b+c)(a+d)} \\ &= 2(ac - bd)\left(\frac{(b+c)(a+d) - (a+b)(c+d)}{(a+b)(b+c)(c+d)(d+a)}\right) \\ &= 2(ac - bd) \cdot \frac{(a-c)(b-d)}{(a+b)(c+d)(a+d)(b+c)}. \end{aligned}$$

So $ac = bd$. Hence, by the Four Number Lemma, we find integers $p, q, r, s \geq 1$ such that $a = pq, b = pr, c = rs, d = qs$. So $a + b + c + d = (p + q)(r + s)$ is not a prime. □

We finish by a nice combinatorial problem, which showcases the ideas and intuition we developed in this chapter.

Example 1.11.8 (STEMS 2019 Maths A Subjective P2)

Find all subsets $\mathcal{S} \subset \mathbb{Z}$ that satisfy $a, b \in \mathcal{S} \implies 2a - b \in \mathcal{S}$.

Observe that the arithmetic mean of $b, 2a - b$ is b. So practically the condition tells us that if we are given two numbers, then the next number in the AP formed by them is also in the list. Further, so is the previous number in the AP (why?).

Now if $\mathcal{S} = \{\ldots, x - d, x, x + d, \ldots\}$ is an AP, then it works: if $a = x + kd, b = x + \ell d$, we have $2a - b = x + (2k - \ell)d \in \mathcal{S}$. Hence all AP sequences works. Now the question is, does there exist a non-AP set $\mathcal{S}$? This is where we use our intuition from multiplication tables (which are AP sequences themselves).

The idea is to pick one AP and show no element cannot be outside that AP. Which AP do we pick? We know that any two elements generate an AP. We would want to choose the AP which is the "longest" and "densest", in the sense that it covers the other APs. This is the same as the common difference being the lowest. So this is the key trick: Pick r such that r is the smallest difference between two elements, i.e. $r = \min_{a,b \in \mathcal{S}} |a - b|$.

Now if $a - b = r$, then we have the AP

$$\{\dots, b - r, b, b + r, \dots\} \subset \mathcal{S}.$$

Suppose we have an element outside this AP, say c. Then it must lie between two elements. However, then it would be a distance less than r from some element of the AP! That is, pick k such that $b+kr \leq c < b+(k+1)r$. Then $c-(bk+r) < (b+(k+1)r)-(bk+r) = r$, contradicting the minimality of r (do you observe the resemblance of this with euclid's division lemma?). Hence, we are done. $\square$

1.12 Practice Problems

Problem 1.12.1. Show that any composite number n has a prime factor $\leq \sqrt{n}$.

Problem 1.12.2 (IMO 1959/1). Prove that for any natural number n, the fraction

$$\frac{21n+4}{14n+3}$$

is irreducible. **Hints:** 306

Problem 1.12.3. Let x, y, a, b, c be integers.

1. Prove that $2x+3y$ is divisible by 17 if and only if $9x+5y$ is divisible by 17.
2. If $4a+5b-3c$ is divisible by 19, prove that $6a-2b+5c$ is also divisible by 19.

Hints: 137 91 276

Problem 1.12.4. Define the nth Fermat number F_n by $F_n = 2^{2^n}+1$. Show that F_m, F_n are coprime for any m, n. [3]

Problem 1.12.5. Prove that for each positive integer n, there is a positive integer m such that each term of the infinite sequence $m+1, m^m+1, m^{m^m}+1, \ldots$ is divisible by n. **Hints:** 403 421

Problem 1.12.6 (Romania Mathematical Olympiad). Let a, b be positive integers such that there exists a prime p with the property $\text{lcm}(a, a+p) = \text{lcm}(b, b+p)$. Prove that $a = b$. **Hints:** 59 281 261

Problem 1.12.7 (St. Petersburg 1996). Find all positive integers n such that

$$3^{n-1}+5^{n-1} \mid 3^n+5^n.$$

Hints: 329 378

Problem 1.12.8 (Russia 2001 grade 11 Day 2/2). Let a, b be naturals such that $ab(a+b)$ is divisible by a^2+ab+b^2. Show that $|a-b| > \sqrt[3]{ab}$. **Hints:** 177 223 **Sol:** pg. 277

Problem 1.12.9 (Germany). Let m and n be two positive integers relatively prime to each other. Prove that for every positive integer k, the following statements are equivalent:

1. $n+m$ is a divisor of n^2+km^2;
2. $n+m$ is a divisor of $k+1$.

[3] Here $2^{2^n} = 2^{(2^n)}$, i.e. we calculate 2^n first. For instance, $2^{2^3} = 2^8 = 256$. In general, for such towers, we start from the top. So $2^{2^{2^2}} = 2^{2^4} = 2^{16} = 65536$.

Hints: 392

Problem 1.12.10 (Japan 2020 Junior Finals P3). Find all tuples of positive integers (a, b, c) such that

$$\operatorname{lcm}(a, b, c) = \frac{ab + bc + ca}{4}.$$

Hints: 343 226 401

Problem 1.12.11 (Iran MO 2017 Round 2/1). Prove the following:

1. There doesn't exist a sequence $a_1, a_2, a_3, \ldots$ of positive integers such that for all $i < j$, we have $\gcd(a_i + j, a_j + i) = 1$.
2. Let p be an odd prime number. Prove that there exists a sequence $a_1, a_2, a_3, \ldots$ of positive integers such that for all $i < j$, $p \nmid \gcd(a_i + j, a_j + i)$.

Hints: 390 458 301

Problem 1.12.12 (All Russian Olympiad 2017 Day1 Grade 10 P5). Suppose n is a composite positive integer. Let $1 = a_1 < a_2 < \cdots < a_k = n$ be all the divisors of n. It is known, that $a_1 + 1, \ldots, a_k + 1$ are all divisors for some m (except $1, m$). Find all such n. **Hints:** 237 73 477

Problem 1.12.13 (IMO 2002/1). Let $n \geq 2$ be a positive integer, with divisors $1 = d_1 < d_2 < \ldots < d_k = n$. Prove that $d_1d_2 + d_2d_3 + \ldots + d_{k-1}d_k$ is always less than n^2, and determine when it is a divisor of n^2. **Hints:** 305 5 235 34

Problem 1.12.14 (Russia 2001 Grade 10 Day 2/4). Find all odd positive integers $n > 1$ such that if a and b are relatively prime divisors of n, then $a + b - 1$ divides n. **Hints:** 389 312 103 377 209

Problem 1.12.15 (INMO 2019/3[4]). Let m, n be distinct positive integers. Prove that

$$\gcd(m, n) + \gcd(m + 1, n + 1) + \gcd(m + 2, n + 2) \leq 2|m - n| + 1.$$

Further, determine when equality holds. **Hints:** 304 83 277 **Sol:** pg. 278

Problem 1.12.16 (USAMO 2007/1). Let n be a positive integer. Define a sequence by setting $a_1 = n$ and for each $k > 1$, letting a_k to be the unique integer in the range $0 \leq a_k \leq k - 1$ for which $a_1 + a_2 + \cdots + a_k$ is divisible by k. For instance, when $n = 9$, the obtained sequence is $9, 1, 2, 0, 3, 3, 3, \ldots$. Prove that for any n, the sequence $a_1, a_2, \ldots$ eventually becomes constant. **Hints:** 136 264 **Sol:** pg. 278

Problem 1.12.17 (USAMO 2007/5). Prove that for every nonnegative integer n, the number $7^{7^n} + 1$ is the product of at least $2n + 3$ (not necessarily distinct) primes. **Hints:** 49 310 **Sol:** pg. 278

[4]Indian National Mathematical Oolympiad (the USAMO of India)

Problem 1.12.18 (ELMO 2017/1). Let $a_1, a_2, \ldots, a_n$ be positive integers with product P, where n is an odd positive integer. Prove that

$$\gcd(a_1^n + P, a_2^n + P, \ldots, a_n^n + P) \leq 2 \cdot \gcd(a_1, a_2, \ldots, a_n)^n.$$

Hints: 418 85 196 424 **Sol:** pg. 279

Problem 1.12.19 (IMO 2001/6). Let $a > b > c > d$ be positive integers and suppose that

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Prove that $ab + cd$ is not prime. **Hints:** 468 90 78 168 **Sol:** pg. 279

✠ A special Factorization Trick

This section is not a direct part of the chapter's theory, however presents a useful trick in some factorization problems.

Lemma 1.12.1 (Factorizing Polynomials)**.** *Let*

$$f(x) = \sum_{0 \le i \le p-1} x^{a_i},$$

where a_i are non-negative integers and p is a prime. If they form a reduced residue system modulo p, then $f(x)$ is divisible by

$$g(x) = \sum_{0 \le i \le p-1} x^i.$$

Here, a "reduced residue class mod p" basically means that the remainders on division by p cover all the numbers $0, 1, \ldots, p-1$ (see the next chapter). This is based on the fact that any polynomial which has ζ_p as a root is divisible by $1 + x + \cdots + x^{p-1}$, where ζ_p is the pth root of unity (an analogue of the Factor Theorem. This is discussed more in the special section of Integer Polynomials)

A classic problem is to factorize $x^5 + x + 1$. A clever but unmotivated route is to write it as

$$x^5 - x^2 + x^2 + x + 1 = x^2(x^3 - 1) + (x^2 + x + 1) = (x^2 + x + 1)(x^3 - x + 1).$$

However, once we observe that $\omega^5 + \omega + 1 = \omega^2 + \omega + 1 = 0$ (or say $\{5, 1, 0\}$ is a complete class modulo 3), we can directly say that $x^2 + x + 1$ would be a factor and then use long division! Here's a similar problem:

Problem 1.12.20 (AwesomeMath 2019 Admission Test A). Show that $2019^{2018}+2020$ has at least 3 primes factors.

As a hint, write the given as $2019^{2018}+2019+1$. This is something of the form $x^{2018}+x+1$. By the lemma, $x^2 + x + 1$ is a factor, and that's the key part of the problem.

Try the following problem now:

Problem 1.12.21. Prove that 1280000401 is composite.

As an exercise, try extending the lemma to any number n instead of just a prime. You might wanna read about reduced residue class modulo n from the next chapter before.

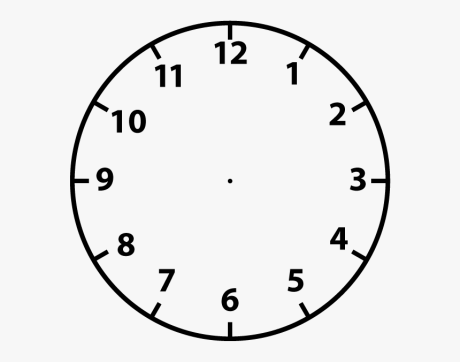
Chapter 2

Modular Arithmetic Basics

2.1 Motivation

In divisibility, we saw that dealing with remainders was at times more useful, for instance if $r = 0$ we have divisibility. The main reason for this is that remainders are smaller than the original numbers. This was the idea on which Euclid's Algorithm was based. Modular arithmetic dwells on this idea in much more depth. We start off by a different motivation, and we would later see the remainder idea is the same.

Consider the following clock face



The clock has only the numbers from 1 to 12. Where to place the other numbers? If we think about it, we would place 13 over 1. So then $13 \equiv 1$ on a clock. (we don't write $13 = 1$ since that's not true, but $\equiv$ means "equivalent to", which fits here).

Also, $26 \equiv 2$ and $100 \equiv 4$. We would in general write $a \equiv b$ if a, b are the same points on the clock.

Question 2.1.1. *Give a mathematical characterization/formula of when two points are the same on the clock.*

If you said $12 \mid a - b$, then congrats, you got it right. So $a \equiv b$ on the clock when $12 \mid a - b$. But there are more things than a clock in this world. How would the general " $\equiv$ " be defined?

In general, for any integer n we would write

$$a \equiv b \pmod{n}$$

if $n \mid a - b$.

Question 2.1.2. *Is* $131 \equiv 32 \pmod{11}$?

Question 2.1.3. *Why is* $131 \equiv -1 \pmod{11}$?

So, negative numbers are also allowed.

Problems for Practice

Problem 2.1.1. Show that $a + n \equiv a \pmod{n}$.

Problem 2.1.2. Let a, n be fixed integers. Show that the set of integers b such that $b \equiv a \pmod{n}$ form an arithmetic progression. What is the common difference?

Problem 2.1.3. Show that the set of integers a such that $a \equiv 0 \pmod{n}$ is the set of multiples of a.

2.2 Remainder Idea

The set of integers a such that $a \equiv 2 \pmod{5}$ is infinite, which is $\mathcal{S}_2 = \{\dots, -8, -3, 2, 7, 12, 17, \dots\}$.
The set of integers a such that $a \equiv 9 \pmod{5}$ is infinite, which is $\mathcal{S}_4 = \{\dots, -6, -1, 4, 9, 14, 19, \dots\}$.

Infinite sets can be harder to deal with. So instead, we only consider the smallest non-negative element here.

Question 2.2.1. *In the set of integers a such that $a \equiv b \pmod{n}$ for some fixed n, convince yourself that the smallest non-negative element is the remainder when b is divided by n.*

For example, for $a \equiv 9 \pmod{5}$, the smallest element is 4, which is the remainder when 9 is divided by 5.

In general, when we write $a \equiv r \pmod{n}$, we try and keep the second number as the remainder for simplicity. Thus,

$$\begin{aligned} 12 &\equiv 2 \pmod{10} \\ 120 &\equiv 0 \pmod{15} \\ 11 &\equiv 11 \pmod{21} \end{aligned}$$

So in $a \equiv r \pmod{n}$, if r is the remainder, we would have $0 \leq r < n$ (why?).

2.3 Residue classes

Suppose $n = 3$. There are only 3 possible remainders on division by $3 : 0, 1$ and 2. So we can put every integer in one column of the following table:

$0 \pmod 3$	$1 \pmod 3$	$2 \pmod 3$
$\vdots$	$\vdots$	$\vdots$
-6	-5	-4
-3	-2	-1
0	1	2
3	4	5
6	7	8
$\vdots$	$\vdots$	$\vdots$

In Divisibility, we studied the multiplication table which was the first column. So, modular arithmetic gives us a better grip over ALL integers. So in some sense, the whole chapter that we did on divisibility is only the first column of our table!

The three columns above are called the 3 "residue classes" modulo 3. In general we have the following:

Definition 2.3.1. *Pick a natural number n, and a non-negative number $r < n$. Then the r**th residue class** is the set of integers a that satisfy $a \equiv r \pmod n$. Equivalently, it is the set of all integers that leave r as a remainder when divided by n.*

These integers are:

$$\{\dots, r-2n, r-n, r, r+n, r+2n, r+3n, \dots\}.$$

Problems for Practice

Problem 2.3.1. Guess why the above classes are called "residue" classes.

Problem 2.3.2. Show that the number of the classes modulo n is exactly n.

2.4 Basic Properties

As in divisibility, does modular arithmetic respect addition? That is, is the following true?

$$a \equiv r \pmod n, b \equiv s \pmod n \implies a + b \equiv r + s \pmod n?$$

Question 2.4.1. *We have $10 \equiv 1 \pmod 3$ and $8 \equiv 2 \pmod 3$. What is $10 + 8 \pmod 3$? Is it $1 + 2$?*

The answer is yes! To see why, write $a = nx + r$ and $b = ny + s$. Then

$$a + b = n(x + y) + (r + s).$$

Ok, so do they preserve multiplication? That is,

$$a \equiv r \pmod{n}, b \equiv s \pmod{n} \implies ab \equiv rs \pmod{n}?$$

Question 2.4.2. *We have* $10 \equiv 1 \pmod 3$ *and* $8 \equiv 2 \pmod 3$. *What is* $10 \times 8 \pmod 3$? *Is it* 1×2?

Again, the answer is yes! I will leave it as an exercise to prove.

Thus, we have the following two very important properties:

Theorem 2.4.1 (Properties of Modulus)**.** *Let* a, b, r, s *be integers such that for a given integer* n, *we have* $a \equiv r \pmod n$ *and* $b \equiv s \pmod n$. *Then*

1. $a + b \equiv r + s \pmod n$.
2. $ab \equiv rs \pmod n$.

This is better than Theorem 1.3.1 to find the remainder since we can directly use the second property here without having to completely multiply $a = nx + r$ and $b = ny + s$.

2.4.1 Why congruence is more useful than equality

A small note on why this modular symbol is *really* helpful. As we have seen, showing equality is hard in number theory, and there are more interesting relations between numbers than being equal. The $\equiv$ sign just behave likes the $=$ sign, since we can add, subtract and multiply anything on the two sides just as in equations (later we will see how to divide). We can exponentiate stuff and practically anything we can do with $=$ applies here.

$$a \equiv b \pmod{n} \implies a + c \equiv b + c, \quad ac \equiv bc, \quad a^c \equiv b^c \pmod{n}.$$

Thus, how $=$ helps us in linear equations and all, $\equiv$ helps us in showing divisibility and related stuff.

Problems for Practice

Problem 2.4.1. Show that ab has remainder rs mod n by writing $a = nx + r$ and $b = ny + s$ and evaluating ab.

Problem 2.4.2. Find the remainder when 2^{10} is divided by 10.

Problem 2.4.3. Find $1002 \times 560 \pmod 7$.

Problem 2.4.4. Show that if $a \equiv b \pmod n$, then $ka \equiv kb \pmod n$ for any integer k.

We can now destroy some problems from the last chapter that were challenging back then:

Problem 2.4.5. Show that $a - b \mid a^n - b^n$ for any integer n.

Problem 2.4.6. If p is an odd prime, and a, b are coprime, show that

$$\gcd\left(\frac{a^p + b^p}{a+b}, a+b\right) \in \{1, p\}.$$

Some interesting results can be very easily derived using modular arithmetic:

Problem 2.4.7 (Very Important). Let f be a polynomial with integer coefficients. Show that $a - b \mid f(a) - f(b)$ for any integers a, b. This is the same as saying $f(a+d) \equiv f(a) \pmod{d}$.

Problem 2.4.8 (Important). Show that $ka \equiv kb \pmod{n}$ implies $a \equiv b \pmod{n}$ if and only if $\gcd(k, n) = 1$.

Let's try a nice problem together:

Example 2.4.1 (Russia 2001)

Find all primes p and q such that $p + q = (p - q)^3$.

Firstly, test some values of (p, q) and guess the answer. After that let's try to solve it systematically.

Directly expanding the right side won't be so useful. Let's take the equation modulo something special. The most obvious choices are mod p and mod q. We can try both. Mod p gives $q \equiv -q^3 \pmod{p}$ and so $p \mid q(q^2+1)$. Mod q gives $p \equiv p^3 \pmod{q}$ and so $q \mid p(p^2-1)$. Not very useful.

However, here's the trick. As $p + q = (p - q)^3$, we also have $(p + q) \mid (p - q)^3$. So, $(p - q)^3 \equiv 0 \pmod{p+q}$. But $p - q \equiv -2q \pmod{p+q}$ so $(-2q)^3 \equiv 0 \implies (p+q) \mid 8q^3$.

Now what we note is that if $\gcd(p+q, q) \neq 1$, then $\gcd(p, q) = \gcd(p+q, q) \neq 1$ implies $p = q$. In that case, however, we get $p + p = (p - p)^3 = 0$, which is impossible.

So $\gcd(p+q, q) = 1$. Hence in $p+q \mid 8q^3$, we must have $p+q \mid 8$ because the q^3 contributes nothing. So $p + q \in \{1, 2, 4, 8\}$. We can now manually list positive numbers that add to 8, which are $(1, 7), (2, 6), (3, 5), (4, 4)$. As p, q are primes, the only possible pair is $(p, q) = (3, 5)$ or $(5, 3)$. Is this the answer you guessed?

2.5 Two special Equal Sets

Consider any number a and a prime p so that $\gcd(a, p) = 1$ (this is the same as saying $a \neq 0 \pmod{p}$). Let's see what happens to the non-negative multiples of a :

$$\mathcal{S} = \{0, a, 2a, 3a, \dots\} \pmod{p}.$$

It's better if we work with an example. Suppose $a = 3$ and $p = 7$. Then

$$\mathcal{S} = \{0, a, 2a, \dots\} = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, \dots\}.$$

If we consider the elements of the set modulo 7, then

$$\mathcal{S} \equiv \{0, 3, 6, 2, 5, 1, 4, 0, 3, 6, 2, 5, 1, 4, 0, 3, 6, \dots\} \pmod 7.$$

We observe the sequence is periodic.

Question 2.5.1. *What's the periodicity?*

In general too, we observe that $ia \equiv (i + p)a \pmod p$ and so we can write $\mathcal{S} = \{0, a, 2a, \dots, (p-1)a\}$ because elements don't repeat in sets (we are talking about sets here, not multisets). Can we shorten this set further? That is, are there any more equal numbers in here?

Let's take the help of our example once more. Suppose $a = 3$ and $p = 7$. Then

$$\mathcal{S} = \{0, a, 2a, \dots, 6a\} = \{0, 3, 6, 9, 12, 15, 18\} = \{0, 3, 6, 2, 5, 1, 4\} \pmod 7.$$

Aha! No elements are equal. Can we prove this in general?

Suppose two elements were equal. Then they would be of the form ai, aj for $0 \leq i \neq j \leq (p-1)$. Then

$$ai \equiv aj \pmod p \implies a(i-j) \pmod p \equiv 0 \implies p \mid a(i-j).$$

But we assumed $\gcd(a, p) = 1$ at the start! Hence, we get $p \mid (i-j)$ (why?). Is this possible?

Question 2.5.2. *Try and find two integers $i \neq j$ between $0, p-1$ such that $p \mid i - j$.*

If you tried to, you would realize this is not possible. And the reason is simple, as $0 \leq i \neq j < p$, hence $0 < |i - j| < p$. Thus, this is impossible, and we are done!

Now note that $\{0, a, 2a, \dots, (p-1)a\}$ has p elements, and all these are distinct. However, since there are only p remainders possible, hence this set must be the set of ALL remainders! For instance, in our example we saw that

$$\{0, a, 2a, \dots, 6a\} = \{0, 3, 6, 9, 12, 15, 18\} = \{0, 3, 6, 2, 5, 1, 4\} \pmod 7,$$

and observe that the last set contains all the remainders mod 7. Cool, isn't it!

2.5.1 Interlude (Equal Sets)

What do equal sets mean? These are sets with the same elements. So what's the difference in them?

$$\{1, 4, 6, 2\} = \{4, 6, 1, 2\}.$$

That's right, the only difference between them is the order of elements. In problem solving, whenever we prove two sets are equal, the most common things we do is to equate the sum of

elements, the sum of squares of elements and the product of element, because these operation don't depend on the order. Out of all these, sum of elements is the most useful, and is very strong in its applications. It should be the first thing you do on seeing equal sets!

So, in our context, we basically derived that $\mathcal{S} = \{0, 1, 2 \ldots, (p-1)\}$ modulo p. Note here that the element 0 in $\mathcal{S}$ is $0 \times a$ and in $\{0, 1, \ldots, (p-1)\}$ is the first element. So we can delete 0 from both the sets. Then we obtain:

Theorem 2.5.1 (Two Equal Sets)**.** *Let p be a prime and consider $\mathcal{S} = \{1, 2, \ldots, p-1\}$ to be the set of non-zero remainder modulo p. Let a be any integer coprime to p.. Then*

$$a\mathcal{S} \equiv \mathcal{S} \pmod{p}.$$

Here, $a\mathcal{S}$ means the set obtained on multiplying each element of $\mathcal{S}$ by a. This gives us many interesting results.

2.6 Fermat's Little Theorem

Now let's see where can we use this theorem. Firstly, let's multiply the elements of both the sets and equate them:

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}.$$

This gives

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}.$$

Now, $\gcd((p-1)!, p) = 1$, hence we can divide both the sides by $(p-1)!$ by Problem 2.4.8. Hence $a^{p-1} \equiv 1$

Now comes the interesting part: Since a was any number coprime to p, hence we obtain the famous Fermat's Little Theorem:

Theorem 2.6.1 (Fermat's Little Theorem)**.** *Let a be any number relatively prime to a prime p. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

This is a very powerful result. It helps us compute a^n for large n. Don't forget the "relatively prime" part of the theorem.

In fact, we also have the following:

Theorem 2.6.2 (Fermat's Little Theorem)**.** *Let a be any number. Then*

$$a^p \equiv a \pmod{p}.$$

You can say we just multiplied both sides by a, so what's special. The reason is that you don't need a, p relatively prime here!

Problems for Practice

Problem 2.6.1. Show that $a^p \equiv a \pmod{p}$ holds in the case when $\gcd(a, p) \neq 1$.

Problem 2.6.2. Let a, b be integers and p a prime. Show that p divides $ab^p - a^p b$.

Problem 2.6.3. Find

$$2^{50} \pmod{7}.$$

2.7 Inverses

Now let's look at the definition of "equal sets". It means that for any integer $0 < b < p$, we can find an integer x such that

$$ax \equiv b \pmod{p}.$$

In particular, if $b = 1$, then $ax \equiv 1 \pmod{p}$.

What this means is if $\gcd(a, p) = 1$, then there always exists a multiple of a which is 1 mod p.

Theorem 2.7.1 (Inverses)**.** *Let p be a prime and a be an integer coprime to p. Then there always exists an integer x such that*

$$ax \equiv 1 \pmod{p}.$$

*This integer x is called the **inverse** of a.*

For instance, let's try and find the inverse of 3 modulo 7. Write down the first $(p-1)$ multiples (why first $(p-1)$?) and check:

$$3 \times 1 \equiv 3, \quad 3 \times 2 \equiv 6, \quad 3 \times 3 \equiv 2 \pmod{7}$$
$$3 \times 4 \equiv 5, \quad 3 \times 5 \equiv 1, \quad 3 \times 6 \equiv 4 \pmod{7}$$

So, 5 is the inverse of 3.

We **denote** the inverse of a by a^{-1}. At times we even use $\frac{1}{a}$.

The existence of inverse allows us to divide! For instance, if $b \not\equiv 0 \pmod{p}$, then

$$\frac{a}{b} \equiv a \cdot b^{-1} \pmod{p}.$$

For instance, check the following are true:

$$\frac{2}{3} \equiv 2 \cdot 3^{-1} \equiv 3 \pmod{7}, \quad \frac{3}{8} \equiv 3 \cdot 8^{-1} \equiv 3 \pmod{7}, \quad \frac{20}{46} \equiv \frac{-1}{2} \equiv 3 \pmod{7}. \quad (2.1)$$

Now if we want to solve the equation $ax \equiv b \pmod{p}$ with $a \not\equiv 0 \pmod{p}$, we can easily do so. The solution is $x \equiv \frac{b}{a} = b \cdot a^{-1} \pmod{p}$.

Let me clear a possible confusion at this point. No, inverses do not always exist. For example mod 6, we don't have an inverse of 2 since:

$$\begin{aligned} 2 \times 1 \equiv 2, \quad 2 \times 2 \equiv 4, \quad 2 \times 3 \equiv 0 \pmod 6 \\ 2 \times 4 \equiv 2, \quad 2 \times 5 \equiv 4 \pmod 6 \end{aligned}$$

We observe that 1 never appears, hence 2 does not have an inverse here. So modulo 6, we cannot divide by 2.

Thus, the fact that an inverse always exists modulo a prime is very special (and useful). I hope the above example helps you appreciate Theorem 2.7.1.

2.7.1 Inverses behave like fractions

As if the existence of an inverse wasn't special enough, we also have the fact that inverses add and multiply like fractions. This basically means you can literally use inverses like fractions without worrying! For instance, in normal fractions,

$$\frac{2}{3} + \frac{3}{8} = \frac{16+9}{24} = \frac{25}{24}. \tag{2.2}$$

Modulo 7, the left side is (using equation 2.1)

$$\frac{2}{3} + \frac{3}{8} = 2 \cdot 3^{-1} + 3 \cdot 8^{-1} = 3 + 3 = 6 \pmod 7.$$

The right side of 2.2 is

$$\frac{25}{24} \equiv \frac{4}{3} \equiv 4 \cdot 3^{-1} \equiv 6 \pmod 7.$$

Thus, 2.2 holds modulo 7 too, despite the fact that these are not really fractions modulo 7. In general:

Lemma 2.7.1 (Inverses add like Fractions)**.** *Let $b, d \not\equiv 0 \pmod p$. Then for any a, c, we have*

$$\frac{a}{b} + \frac{c}{d} \equiv a \cdot b^{-1} + c \cdot d^{-1} \equiv (ad + bc) \cdot (bd)^{-1} \equiv \frac{ad+bc}{bd} \pmod p$$

just like normal fractions.

More important than the proof of this is the following:

Question 2.7.1. *Convince yourself that this is not obvious.*

If you truely believe that Lemma 2.7.1 is not obvious, then let me prove it for you.

Proof. Observe that

$$bd(a \cdot b^{-1} + c \cdot d^{-1}) = bd(a \cdot b^{-1}) + bd(c \cdot d^{-1}) \equiv ad + bc \pmod p.$$

Dividing both the sides by bd we get the result. □

Multiplication of inverses is also similar:

Lemma 2.7.2 (Inverses multiply like Fractions)**.** *Let* $b, d \not\equiv 0 \pmod{p}$*. Then for any* a, c*, we have*

$$\frac{a}{b} \cdot \frac{c}{d} \equiv (a \cdot b^{-1}) \cdot (c \cdot d^{-1}) \equiv (ac) \cdot (bd)^{-1} \equiv \frac{ac}{bd} \pmod{p}$$

just like normal fractions.

Here's an example: In normal fractions,

$$\frac{2}{3} \cdot \frac{3}{8} = \frac{1}{4}. \tag{2.3}$$

Viewing these fractions as inverse, the left side modulo 7 is

$$\frac{2}{3} \cdot \frac{3}{8} \equiv (2 \cdot 3^{-1}) \cdot (3 \cdot 8^{-1}) = 3 \cdot 3 \equiv 2 \pmod{7}$$

On the other hand, the right side of of 2.3 is

$$\frac{1}{4} \equiv 4^{-1} \equiv 2 \pmod{7}.$$

Thus, 2.3 holds modulo 7 too.

Proving Lemma 2.7.2 is rather easy and so I leave it as an exercise.

Problems for Practice

Problem 2.7.1. Prove Lemma 2.7.2.

Problem 2.7.2. Find the inverse of all $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ modulo 11.

Problem 2.7.3. Show that 0 does not have an inverse modulo p. What about p?

(If you say this is because $1/0$ is not defined or is ∞, then that argument is true for normal fractions, but not here. This proof fails modulo p because inverses aren't exactly division. Find a different proof.)

Problem 2.7.4. Prove that if $a \not\equiv 0 \pmod{p}$, then

$$a^{p-2} \equiv a^{-1} \pmod{p}.$$

Problem 2.7.5. Prove that the inverse of a^n is the nth power of the inverse of a. That is,

$$(a^{-1})^n \equiv (a^n)^{-1} \pmod{p}.$$

Using this, find the inverse of 256 modulo 47.

2.8 Simple Properties of Inverses and Wilson's Theorem

I will talk about some simple properties of inverses here. Firstly note that an inverse is unique. What I mean is a^{-1} is unique modulo p. For instance you can't have both $2a \equiv 1 \pmod{p}$ AND $7a \equiv 1 \pmod{p}$. The number x such that $ax \equiv 1 \pmod{p}$ would be unique.

The reason is simple. If $ax \equiv 1 \pmod{p}$ and $ay \equiv 1 \pmod{p}$ for $0 \leq x, y \leq p-1$, then $ax \equiv ay \implies p \mid a(x-y)$. As $\gcd(a,p) = 1$, hence $p \mid x-y$. But $0 < x-y < p$ so this is impossible.

Another simple property is that if a is the inverse of b then b is the inverse of a. That is,

$$a \equiv b^{-1} \implies a^{-1} \equiv b \pmod{p}.$$

Don't read ahead till this feels obvious to you too!

So we can basically pair up numbers with their inverses. For example modulo 11, we have the following pairs:

$$\{1,2,3,4,5,6,7,8,9,10\} \implies (1,1),(2,6),(3.4),(5,9),(7,8),(10,10). \tag{2.4}$$

Wait, the pairs $(1,1),(10,10)$ have the same elements. So now we ask when is a the inverse of a. This is the same as saying $a \cdot a \equiv 1 \pmod{p}$, i.e. $p \mid (a-1)(a+1)$. Hence $p \mid (a-1)$ or $p \mid (a+1)$ (why?). This is the same as saying $a \equiv 1$ or $a \equiv -1$. So these are the only cases in which a is the inverse of a.

Thus, if we ignore these *bad* pairs, then in any pair (a,b) we would have $a \neq b$. Further every remainder mod p is in some pair. So, if we multiply ALL of them, we get something very interesting:

$$\begin{aligned} 2 \cdot 3 \cdot 4 \ldots 9 &= (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \\ &= 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 = 1 \pmod{11}. \end{aligned}$$

So if we multiply both the sides by $1 \cdot 10 \equiv -1 \pmod{11}$, we find

$$10! \equiv -1 \pmod{11}.$$

Interesting right? This is a special case of a much more general result, the famous Wilson's theorem:

Theorem 2.8.1 (Wilson's Theorem)**.** *Let p be a prime. Then*

$$(p-1)! \equiv -1 \pmod{p}.$$

This is proved exactly in the same way as we did for 10!, that is pairing up with inverses. This is a very cool theorem and probably the most used one when it comes to factorials modulo something.

Actually, I would be lying to you if I said this was Wilson's theorem. There's a bit more to it. It also says that if n is any natural satisfying $(n-1)! \equiv -1 \pmod{n}$, then n must be a prime. Woah. This is one of the rare criterions/formulas that we have for testing if a number is prime. So if you want to check if n is a prime, then you just calculate $(n-1)!$ and check if it's -1 modulo n.

Sadly, finding $(n-1)!$ is hard and not feasible even for a computer for large values of n. To get an idea of how large factorials get, 100! has 158 digits. Nonetheless, I will write the full theorem here:

Theorem 2.8.2 (Wilson's Theorem)**.** *For any integer n, we have*

$$(n-1)! \equiv -1 \pmod{n}$$

if and only if n is a prime.

Note here the "if and only if" means two things: if $(n-1)! \equiv -1 \pmod{n}$, then n is a prime, and also if n is a prime, then $(n-1)! \equiv -1 \pmod{n}$.

Practice Problems

Problem 2.8.1. Prove that if n is any natural satisfying $(n-1)! \equiv -1 \pmod{n}$, then n must be a prime.

Problem 2.8.2. Let p be a prime. Show that the remainder when $(p-1)!$ is divided by $p(p-1)$ is $p-1$.

Problem 2.8.3. Let n be an integer. Calculate

$$\gcd(n! + 1, (n+1)!).$$

2.9 General Equal Sets

Earlier we got

$$aS \equiv S \pmod{p}$$

for any a with $\gcd(a, p) = 1$ and $S = \{1, 2, \ldots, p-1\}$. Let's try to generalize this to any integer n instead of just a prime p. Note that the only fact we used in the proof was that a and any element in $\mathcal{S}$ is coprime to p. (Confirm this by reading the proof again.)

I will leave it as an exercise to prove this, but here's the full result:

Theorem 2.9.1 (General Equal Sets)**.** *Let n be any integer. Let S be the set of integers less than n and relatively prime to n. Let a be any integer coprime to n. Then*

$$aS \equiv S \pmod{n}.$$

The proof is exactly the same. Note that $\mathcal{S}$ is not $\{1, 2, 3, \ldots, n-1\}$. It is only the set of integers coprime to n. Note that $1 \in \mathcal{S}$ always holds (why?).

For example, if $n = 15$ and $a = 4$, then $\mathcal{S} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. So

$$\begin{aligned} 4S =& \{4, 8, 16, 28, 32, 44, 52, 56\} \\ \equiv& \{4, 8, 1, 13, 2, 14, 7, 11\} \pmod{15}. \end{aligned}$$

Check that the second set is the same as $\mathcal{S}$. Now we will do exactly what we did before to obtain general Fermat's Little Theorem and general Inverses. Before we move on, let me just clarify the following:

Definition 2.9.1. *The set $\mathcal{S}$ is called a **reduced residue system** modulo n.*

2.10 Euler's Theorem

We obtained Fermat's theorem by multiplying the elements of $a\mathcal{S}$ and $\mathcal{S}$ and equating them. Let's do the same here. Let $|\mathcal{S}|$ be the number of elements in $\mathcal{S}$. Then

$$(a \cdot 1) \ldots (a \cdot (n-1)) \equiv 1 \cdots (n-1) \pmod{n}.$$

Hence,

$$a^{|\mathcal{S}|} \prod_{\substack{1 \le i < n \\ \gcd(i,n)=1}} i \equiv \prod_{\substack{1 \le i < n \\ \gcd(i,n)=1}} i \pmod{n}.$$

The product here means the product of all numbers between $1, n$ that are coprime to n.

Again, we can cancel this product from both the sides using Problem 2.4.8 since it is coprime to n (why?). Thus we get

$$a^{|\mathcal{S}|} \equiv 1 \pmod{n} \quad \text{for all } a \text{ coprime to } n \tag{2.5}$$

This is cooler than Fermat's little theorem since we have a general mod here.

Question 2.10.1. *Check that when $n = p$ is a prime, we have $\mathcal{S} = \{1, 2, 3, \ldots, p-1\}$ and hence $|S| = p - 1$ in that case. Thus confirm that this result implies Fermat's Little theorem and hence is more general.*

For instance, when $n = 15$, we have $\mathcal{S} = \{1, 2, 4, 7, 8, 11, 13, 14\}$, and so $|\mathcal{S}| = 8$. So, for any a coprime to 15 we have $a^8 \equiv 1 \pmod{15}$. For instance check that $11^8 \equiv 1 \pmod{15}$.

However, this would be better if we had a formula for $|S|$ in general. Turns out, mathematicians left nothing hanging. Here's what we are looking for:

2.10.1 Euler's Totient Function

Recall that S was the set of integers less than n coprime to n. So we need to find how many numbers less than n are coprime to it. This function was discovered by Euler, and is called **Euler's Totient Function**[1]

[1] Fun Fact: even though Euler was the first one to use this function (officially), it took over 100 years for the current notation and name to be coined!

Definition 2.10.1. *Let n be a positive integer. The function $\varphi(n)$ is called Euler's totient function, and it denotes the number of positive integers less than n that are coprime to it.*

Question 2.10.2. *Find $\varphi(2), \varphi(3), \varphi(4), \varphi(5), \varphi(6), \varphi(7), \varphi(8), \varphi(9)$ and $\varphi(10)$.*

Question 2.10.3. *Show that $\varphi(p) = p - 1$ when p is a prime.*

How do we find $\varphi(100)$?

Ok, I won't trouble you much. I would just give you the formula.

Theorem 2.10.1 (Euler's Totient Function)**.** *Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ be its prime factorization. Then*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right).$$

Another way of writing is (which is easier to use)

$$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_k^{\alpha_k - 1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1).$$

The way I like to remember it is that for each prime p, reduce the power of p by 1 and multiply by $(p - 1)$.

This formula is derived by a lemma, that is incredibly useful in itself so I will mention it here:

Lemma 2.10.1 (φ is multiplicative)**.** *For any two **coprime** integers m, n, we have*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

People often forget the coprime part. Don't make the same mistake!

Comment 2.10.1: A function $f : \mathbb{N} \to \mathbb{C}$ is called **multiplicative** if

$$f(mn) = f(m)f(n) \quad \text{for all coprime } m, n.$$

It is called **completely multiplicative** if

$$f(mn) = f(m)f(n) \quad \text{for all } m, n.$$

We will talk about these more in the chapter on arithmetic functions.

Back to our previous discussion, 2.5 gives us the so called Euler's Theorem:

Theorem 2.10.2 (Euler's Theorem)**.** *Let $n \geq 2$ be an integer and a be any integer coprime to n. then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Problems for Practice

Problem 2.10.1. Find $2^{98} \pmod{33}$

Problem 2.10.2. Find 5^{30} modulo 62.

Problem 2.10.3. What happens if $\gcd(a, n) \neq 1$? Does there exist any integer m such that $a^m \equiv 1 \pmod{n}$?

Problem 2.10.4. Show that $n \mid 2^{n!} - 1$ for all odd n.

2.11 General Inverses

Look again at Theorem 2.9.1. Using that we obtain that there is some integer $x \in S$ for which $ax \equiv 1 \pmod{n}$. We call x the **inverse** of n. Remember the condition that $\gcd(a, n) = 1$. Thus:

Theorem 2.11.1 (General Inverses)**.** *Let $n \geq 2$ be any positive integer. Then every number a with $\gcd(a, n) = 1$ has an inverse, that is a number x such that*

$$ax \equiv 1 \pmod{n}.$$

We write $x = a^{-1}$.

This is an amazing theorem. We can now divide modulo any number, well almost. In fact, we have only proved that if $\gcd(a, n) = 1$, then a has an inverse. What if $\gcd(a, n) \neq 1$? Does an inverse exist in that case?

Turns out the answer is no. Let's take an example. Suppose $n = 9$ and $a = 3$. Then

$$\begin{aligned} &3 \times 1 \equiv 3, \quad 3 \times 2 \equiv 6, \quad 3 \times 3 \equiv 0 \pmod{9} \\ &3 \times 4 \equiv 3, \quad 3 \times 5 \equiv 6, \quad 3 \times 6 \equiv 0 \pmod{9} \\ &3 \times 7 \equiv 3, \quad 3 \times 8 \equiv 6, \quad 3 \times 9 \equiv 0 \pmod{9} \end{aligned}$$

We do not find a 1 in there, so 3 does not have an inverse modulo 9. So we have

Lemma 2.11.1 (Inverses don't always exist)**.** *If n is a natural number, and a is an integer, then a has an inverse modulo n if and only if $\gcd(a, n) = 1$. In particular, if $\gcd(a, n) > 1$, then a does not have an inverse.*

Problems for Practice

Problem 2.11.1. Find the inverse of all $\{1, 3, 5, 7\}$ modulo 8. What do you observe? Can you explain this?

Problem 2.11.2. Does there exist an inverse for 5 modulo 10? What about 4?

Problem 2.11.3. Show that $\gcd(a^{-1}, n)$ is also 1.

Problem 2.11.4. Prove that if $\gcd(a, n) \neq 1$, then a cannot have an inverse.

2.12 Extra Results as Problems

It should not be surprising that there are a lot of interesting results in modular arithmetic. We present a few as problems here.

Example 2.12.1

Let a, m, n be integers. Suppose d sastifies

$$a^m \equiv 1 \pmod{d} \quad \text{and} \quad a^n \equiv 1 \pmod{d}.$$

Then,

$$a^{\gcd(m,n)} \equiv 1 \pmod{d}.$$

This is very useful, and is just a modular analgoue of Example 1.10.4 (see comments below). However, proving this using modular arithmetic is easier. Using Bézout's lemma, we find $x, y \in \mathbb{Z}$ such that $mx + ny = \gcd(m, n)$. So

$$a^{mx+ny} \equiv a^{mx} \cdot a^{ny} \equiv (a^m)^x \cdot (a^n)^y \equiv 1 \pmod{d}$$

and we are done.

Comment 2.12.1: Let's try to prove Example 1.10.4 using this. Suppose $d = \gcd(a^m-1, a^n-1)$. To show $d = a^{\gcd(m,n)}-1$, we show $a^{\gcd(m,n)}-1 \mid d$ and $d \mid a^{\gcd(m,n)}-1$.

The former is easier to prove: just note that $a^{\gcd(m,n)} - 1$ divides both $a^m - 1, a^n - 1$, hence it divides their gcd d. Next, since

$$a^m \equiv 1 \pmod{d} \quad \text{and} \quad a^n \equiv 1 \pmod{d},$$

the above example problem tells us that $d \mid a^{\gcd(m,n)} - 1$. Hence we conclude $d = a^{\gcd(m,n)} - 1$.

Example 2.12.2

Suppose $a, b, d \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $ad \equiv bd \pmod{n}$. Show that

$$a \equiv b \left(\mod \frac{n}{\gcd(n, d)} \right).$$

For example, $6 \equiv 2 \pmod{4} \implies 3 \equiv 1 \pmod{2}$, not $3 \equiv 1 \pmod{4}$. In other words, if we want to cancel out a common factor of a, b, we would also have to reduce the thing inside mod. In particular, note that $ka \equiv kb \pmod{n}$ implies $a \equiv b \pmod{n}$ if and only if $\gcd(k, n) = 1$ (this is Problem 2.4.8).

Proof. We have $n \mid d(a - b)$. Now, the d contributes only to $\gcd(d, n)$ in this divisibility. Hence, $n/\gcd(d, n)$ divides $a - b$, as needed.

A more formal argument would be to write $n = gn^*, d = gd^*$ with $g = \gcd(n, d)$. Then $n^* \mid d^*(a-b)$ but since n^*, d^* are coprime, hence $n^* \mid a - b$ (by Euclid's lemma, Example 1.8.2). □

Example 2.12.3 (Freshman's Dream)

Let $a.b$ be integers and p be a prime. Prove that

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

The is mockingly called the Freshman's dream because $(x+y)^n = x^n + y^n$ is a very common mistake made by Freshmen. However, their mistake is not a mistake anymore modulo p.

The proof of this is to use the binomial theorem:

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \cdots + b^p \pmod{p}.$$

Now, if you try to take examples, you will observe that p divides all the binomial coefficient above. This is in fact true and a very useful result:

$$p \mid \binom{p}{k} \quad \forall 1 \leq k \leq p-1.$$

The proof of this is not very hard, since $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ and the numerator is divisible by p, while the denominator isn't. So, using this we obtain that all the coefficients are 0 modulo p, and so we get $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Problem 2.12.1. Use Freshman's dream and induction to prove Fermat's Little Theorem.

Comment 2.12.2 (Just some facts): The result $(a+b)^p = a^p + b^p$ is not true over integers, but is true over integers modulo p. We often denote the set of integers modulo p by $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{F}_p$ (we will use the second notation in this book). If we think of $\mathbb{F}_p$ as a "structure", i.e. a system of certain numbers, then this identity holds over this system. Turns out there are more interesting and general systems over which this holds true. However, they are beyond the scope of this book.

Also, if we define a function σ over $\mathbb{F}_p$ by saying $\sigma(t) = t^p$, then we just showed $\sigma(a+b) = \sigma(a) + \sigma(b)$. The function σ is called a **Frobenius endomorphism** and is also defined over general systems about which we talked above.

Since I mentioned a very convenient notation in the comments, I would highlight it here too:

Definition 2.12.1. *The set of integers modulo p is denoted by $\mathbb{F}_p$, where p is a prime. It is also denoted by $\mathbb{Z}/p\mathbb{Z}$.*

Here, it is important to note that p is a prime. Writing $\mathbb{F}_{10}$ is an incorrect use of the notation. However, you can use $\mathbb{Z}/10\mathbb{Z}$ to denote the set of integers modulo 10. The notations might seem obscure at this point, however it is explained better using the notion of fields and quotient rings from abstract algebra. So if you fight the notation right now, you would be contradicting yourself a few years later in college. So just use the notation blindly, as it is convenient.

Problem 2.12.2. Use induction to show that

$$(a+b)^{p^i} \equiv a^{p^i} + b^{p^i} \pmod{p}$$

for any prime p and any non-negative integer i.

Example 2.12.4

Let p be a prime. Prove that

$$x^p - x = x(x-1)(x-2)\dots(x-(p-1)) \pmod{p}$$

for any x.

Just see that for any x, one of $x, x-1, \dots, x-(p-1)$ is 0 modulo p. Hence, the right side becomes 0 modulo p. What about the left side? Well, that is zero for any residue too by Fermat's Little Theorem! Hence, if we define the polynomials $f(x) = x^p - x$ and $g(x) = x(x-1)\dots(x-(p-1))$, then $f(x) \equiv g(x) \pmod{p}$ for any x.

If you see carefully, this doesn't say that the polynomials $f(x), g(x)$ are the same (i.e. have the same coefficients modulo p), it merely says it would give the same value. For instance, $x^p \equiv x \pmod{p}$ is true for all x value-wise, but the polynomials x^p and x are obviously different.

So the natural question now is if $f(x), g(x)$ are equal as polynomials too. We answer this question in the special section of the chapter "Modular Arithmetic Advanced".

Example 2.12.5 (Wolstenholme's Theorem)

Let $p > 3$ be a prime. Prove that if

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} = \frac{m}{n},$$

where m, n are coprime integers, then $p^2 \mid m$.

The above theorem can be stated by saying

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\equiv 0 \pmod{p^2} \tag{2.6}$$

since denominators make sense as long as they are coprime to p^2 (why?). For instance, if $p=7$, then this says that $49/20$ is divisible by 49.

We have to prove Equation 2.6. A common theme in problem solving is to solve a simplified problem. In this case, we try to prove Equation 2.6 modulo p instead of p^2. Suppose $p=7$. Then

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}=\frac{49}{20}.$$

If we try to find this sum in a different way, we must look at it as an algebraic sum instead of a number theoretic one. One common trick in such algebra problems is Gaussian pairing, which is pairing of "opposite terms" (the same technique Gauss used to find sum of $1+2+\cdots+100$, the old folklore). This works here if we form the pairs $\frac{1}{i}+\frac{1}{p-i}$ since the numerator is p. For instance, when $p=7$,

$$1+\frac{1}{2}+\cdots+\frac{1}{7}=\left(1+\frac{1}{6}\right)+\left(\frac{1}{2}+\frac{1}{5}\right)+\left(\frac{1}{3}+\frac{1}{4}\right)=\frac{7}{1\times 6}+\frac{7}{2\times 5}+\frac{7}{3\times 4}.$$

Clearly, each term is divisible by 7 and hence so is their sum!

In general, since $p>2$, $p-1$ is even and we can pair off terms smoothly. Writing our observation succinctly using the sigma notation, we find

$$\sum_{i=1}^{p-1}\frac{1}{i}=\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{1}{i}+\frac{1}{p-i}\right)=p\sum_{i=1}^{\frac{p-1}{2}}\frac{1}{i(p-i)}\equiv 0 \pmod{p}.$$

And that's how we get the result modulo p. What about p^2 though? We now only need to show

$$\sum_{i=1}^{\frac{p-1}{2}}\frac{1}{i(p-i)}\equiv 0 \pmod{p}.$$

Well, at this point we must try something new. First of all, since $(p-i)\equiv -i \pmod{p}$, hence each denominator above can be replaced by $-i^2$. Now, pairing did work well for us, however it complicated one thing, the number of terms. Luckily, we can multiply by 2 to restore (why?). So

$$2\sum_{i=1}^{\frac{p-1}{2}}\frac{1}{i(p-i)}\equiv\sum_{i=1}^{p-1}\frac{1}{i^2} \pmod{p}.$$

Since we are dealing with terms of the form $1/i=i^{-1}$, hence there is no way we can miss inverses; they can easily help us get rid of the fractions. However, we don't know what i^{-1} would be. Let's fall back to our example of $p=7$. We can calculate

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\frac{1}{6^2}\equiv 1^2+4^2+5^2+2^2+3^2+6^2 \pmod{7}.$$

We immediately observe that each residue appears in the sum. Luckily, observing this fact is harder than proving it. The proof just follows since $\{1^{-1}, 2^{-1}, \ldots, (p-1)^{-1}\} \equiv \{1, 2, \ldots, p-1\} \pmod{p}$ (why? If $i^{-1} \equiv j^{-1}$, then cross multiplying gives $i \equiv j \pmod{p}$). So

$$\begin{aligned}\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{(p-1)^2} &\equiv -(1^2 + 2^2 + \cdots + (p-1)^2) \\ &= -\frac{(p-1)p(2p-1)}{6} \pmod{p},\end{aligned}$$

where we used the sum of first n squares formula. We must show the above is 0 mod p. But since $p > 3$, hence $\gcd(p, 6) = 1$. Thus p has no contribution in making $\frac{p(p-1)(2p-1)}{6}$ an integer, and hence $\frac{(p-1)(2p-1)}{6}$ is also an integer. So the right side is p times an integer, which is thus $0 \pmod{p}$. So we are done!

Too much discussion happened here. Let's try and neatly summarize our argument into one equation! (note where we used $=$ and where $\equiv$, denoting where we used algebraic facts vs number theoretic facts)

$$\begin{aligned}2\sum_{i=1}^{p-1} \frac{1}{i} &= \sum_{i=1} \left(\frac{1}{i} + \frac{1}{p-i}\right) \\ &= \sum_{i=1}^{p-1} \frac{p}{i(p-i)} \\ &\equiv p\sum_{i=1}^{p-1} \frac{-1}{i^2} \\ &\equiv -p\sum_{i=1}^{p-1} i^2 \\ &= -\frac{p^2(p-1)(2p-1)}{6} \equiv 0 \pmod{p^2}.\end{aligned}$$

Can you link each line above with our discussion?

2.13 Example Problems

I will try to cover a variety of problems in this section. Some may be clever, some may be boring problems with not much insight. However, you should learn to face the truth!

Example 2.13.1 (USAMO 1991/3)

Show that, for any fixed integer $n \geq 1$, the sequence

$$2,\ 2^2,\ 2^{2^2},\ 2^{2^{2^2}}, \ldots \pmod{n}$$

is eventually constant.

(The tower of exponents is defined by $a_1 = 2,\ a_{i+1} = 2^{a_i}$. In other terms, we start working from the top, for instance $2^{2^{2^2}} = 2^{2^4} = 2^{16} = 65536$.)

For convenience, define a_i to be the ith term of the sequence. Firstly, assume n is odd. Since $2^{\varphi(n)} \equiv 1 \pmod{n}$, hence if we can $a_k \equiv a_{k+1} \equiv a_{k+2} \equiv \ldots \pmod{\varphi(n)}$ for some k, we would get

$$\underbrace{2^{a_k}}_{=a_{k+1}} \equiv \underbrace{2^{a_{k+1}}}_{=a_{k+2}} \equiv \underbrace{2^{a_{k+2}}}_{=a_{k+3}} \equiv \ldots \pmod{n},$$

which is what we want. So if we can show if the sequence $\langle a_i \rangle$ eventually becomes constant modulo $\varphi(n)$, we can conclude that it eventually becomes constant modulo n as well. So we have to prove the same problem for $\varphi(n)$ instead.

The key observation now is $\varphi(n) < n$. So we have reduced the problem from case n to a smaller case. Hence, we can use (strong) induction! Here's how it goes:

Proof. Check the base case of $n = 1$, and assume the result till some $n - 1$. If n is odd, we can reduce the problem to smaller case $\varphi(n)$, for which it is true by the induction hypothesis. We just have to manage n even now. In this case, we try to eliminate the "even part" of n and work. So if $n = 2^m n^*$ with n^* odd, then pick k large enough such that $a_k > m$. So

$$2^{a_k} \equiv 2^{a_{k+1}} \pmod{n} \Leftrightarrow 2^{a_k - m} \equiv 2^{a_{k+1} - m} \pmod{n^*}$$

and again use the induction hypothesis as $n^* < n$ (here we used the result from Example 2.12.2). □

Sometimes, simple modular considerations can be useful:

Example 2.13.2

Given

$$34! = 295232799039a041408476186096435b0000000,$$

in decimal representation, find the numbers a and b.

Proof. We know that $9|34!$. Also we know from the rule of divisibility by 9 that for all naturals n, $n \equiv S(n) \pmod 9$, where $S(n)$ is the sum of digits of n. Hence, $9|a+b+136$ and so $a+b \in \{8, 17\}$, as $0 \leq a, b \leq 9$.

We also know that $11|34!$. Also, a number modulo 11 is congruent to the alternating sum of the digits in the number, read from left to right. Therefore, $11|(77+a)-(59+b) = 18+a-b$ and so $a-b \in \{-7, 4\}$ as $0 \leq a, b \leq 9$.

Now, note that $a+b$ and $a-b$ have the same parity. Hence, the only possibilities are $(a+b, a-b) = (8, 4)$ and $(17, -7)$, and the two cases yield $(a, b) = (6, 2)$ or $(a, b) = (5, 12)$, respectively. But since $a, b \leq 9$, hence the second case is impossible. Thus, $(a, b) = (6, 2)$ proving the claim. □

Another example where modular constraints help us bound things:

Example 2.13.3 (St. Petersburg 2008)

Given three distinct natural a, b, c show that

$$\gcd(ab+1, bc+1, ca+1) \leq \frac{a+b+c}{3}$$

Proof. Suppose $d = \gcd(ab+1, bc+1, ca+1)$. Then $ab, bc, ca \equiv -1 \pmod d$, and so $ab-bc = b(a-c) \equiv 0 \pmod d$. Now if b, d have a common factor, say $p > 1$, then $p \mid d \mid ab+1$. Combining with $p \mid b$, we get $p \mid ab+1-b(a) = 1$, a contradiction. Hence b, d are coprime and so $d \mid a-c$.

Similarly, $d \mid a-b, b-c$. Thus, $a \equiv b \equiv c \pmod d$. Now, assume without loss of generality that $a > b > c$ (strict inequalities since they are given to be distinct). Hence $a \geq b+d \geq c+2d$. So

$$a+b+c \geq 3a+3d \geq 3d \implies \frac{a+b+c}{3} \geq d.$$

Hence we are done. □

Not all problems are nice and sweet, some may involve simple ideas with which you work a lot, typically means a lot of case work. For instance the following:

Example 2.13.4 (Azerbaijan Balkan Math Olympiad Third TST 2015)

Find all natural numbers n for which there exist primes p and q such that the following conditions are satisfied:

1. $p+2 = q$, and
2. $2^n + p$ and $2^n + q$ are both primes

Proof. We will show that such primes exist if and only if $n \in \{1, 3\}$. By these conditions, we have that $(p, p+2, p+2^n, p+2^n+2)$ are all primes.

Clearly, $p \neq 2$ because else $q = 4$, which is not a prime. Let us assume for the moment that $p \neq 3$. Thus, $p \geq 5$.

1. If n is even, then $(p, p+2, p+2^n, p+2^n+2) \equiv (p, p+2, p+1, p) \pmod 3$ and so at least one of $p, p+2$, or $p+2^n$ is divisible by 3. This is clearly false since we assumed these numbers are primes and $p \geq 5$.

2. If n is odd, then $(p, p+2, p+2^n, p+2^n+2) \equiv (p, p+2, p+2, p+1) \pmod 3$ and so at least one of $p, p+2$, or $p+2^n+2$ is divisible by 3, and since they are all primes, one of them must be 3. This is again a contradiction because we assumed $p \geq 5$.

Hence, we must have $p = 3$ and $(3+2^n, 5+2^n)$ is a pair of primes. It is easy to see that this condition is satisfied for $n = 1$ and $n = 3$ but not for $n = 2$. We will show that there is no $n > 3$ that satisfies this condition. First, notice that if $n > 3$, then

$$5 + 2^n > 3 + 2^n > 13.$$

If n is even, say $n = 2z$, then $5 + 2^n = 5 + 4^z \equiv 5 + 1 \equiv 0 \pmod 3$, but since $5 + 2^n > 3$, this number cannot be a prime, a contradiction. Thus, n is odd. Set $n = 2k + 1$ for some integer k.

If k is even, then

$$\begin{aligned} 3 + 2^n &= 3 + 2 \cdot 2^{n-1} = 3 + 2 \cdot 4^k \\ &\equiv 3 + 2 \cdot (-1)^k \\ &\equiv 3 + 2 \equiv 0 \pmod 5, \end{aligned}$$

which is a contradiction because $3 + 2^n > 5$. So, k is odd. Set $k = 2r + 1$ for some integer r, and so $n = 4r + 3$.

If $r \equiv 1 \pmod 3$, write $r = 3z + 1$. Then, we have

$$\begin{aligned} 5 + 2^n &= 5 + 2^{4r+3} = 5 + 8 \cdot 16^r \\ &\equiv 5 + 2^r \\ &\equiv 5 + 2^{3z+1} \\ &\equiv 5 + 2 \cdot 8^z \\ &\equiv 5 + 2 \equiv 0 \pmod 7, \end{aligned}$$

and we get a similar contradiction to the ones previous cases.

If $r \equiv 2 \pmod 3$, say $r = 3z + 2$, then

$$\begin{aligned} 3 + 2^n &= 3 + 2^{4r+3} = 3 + 8 \cdot 16^r \\ &\equiv 3 + 2^r \\ &\equiv 3 + 2^{3z+2} \\ &\equiv 3 + 4 \cdot 8^z \\ &\equiv 3 + 4 \equiv 0 \pmod 7, \end{aligned}$$

a contradiction.

This means that $3|r$. Write $r = 3s$ for some integer s so that $n = 12s + 3$. Thus,

$$\begin{aligned} 5 + 2^n &= 5 + 2^{12s+3} \\ &= 5 + 8 \cdot \left(2^{12}\right)^s \\ &\equiv 5 + 8 \equiv 0 \pmod{13}, \end{aligned}$$

a contradiction.

Hence, we have exhausted all the possibilities and so $n = 1$ and $n = 3$ are the only possible solutions. □

Finally, we look at an amazing combinatorial-number theory problem. Euclid gave a construction for showing the infinitude of primes. Somebody made a problem out of that construction.

Example 2.13.5

Let $\mathcal{P}$ be the set of all prime numbers over naturals. Let M be a subset of $\mathcal{P}$ with at least 3 elements. Choose any proper subset A of M. Consider the number

$$n_A := -1 + \prod_{p \in A} p$$

Suppose that any prime divisor of n_A lies in M for all $A \subset M$.

Show that $M \equiv \mathcal{P}$.

We start by trying to manually show each prime is in M, at least for as many primes as we can. Firstly, M has at least 3 elements. So choose an odd prime $p \in M$. Then $n_{\{p\}}$ is even and so $2 \in M$.

Next, if a prime p of the form $3k + 1$ lies in M, then $n_{\{p\}}$ is divisible by 3. Otherwise there exists a prime p of the form $3k + 2$ and so $n_{\{2,p\}} = -1 + 2p$ is divisible by 3. Thus, in either case we get that $3 \in M$.

Then $n_{\{2,3\}} = 5$ implies that $5 \in M$. Also, $n_{\{3,5\}} \implies 7 \in M$. The problem has the same construction as that of Euclid's. So this problem is screaming at us to try to do what he did, show that the "set" is infinite; in case the set of primes, and in our case the set M.

Claim. *M is an infinite set*

Proof. Assume on the contrary, and set $M = \{p_1, p_2, \cdots p_n\}$. We can't directly consider n_M since the subset we choose must be a proper subset.

Hence, choose $S = \{p_1, p_2, \cdots, p_{i-1}, p_{i+1}, \cdots, p_n\}$, i.e. we have removed p_i from M. Let P be the product of the elements of M. Then every factor of n_S must be in M, and so we must have

$$\frac{P}{p_i} - 1 = p_i^a \quad \text{for some } a$$

This is true because $\gcd(n_S, p_j) = 1$ for all $j \neq i$. Now this holds for all primes $p_i \in M$. We act greedily and choose $p_i = 2$. Then

$$\frac{P}{2} - 1 = 2^a$$

Note that $7|P$ since $7 \in M$. Hence considering this equation modulo 7 yields

$$2^a \equiv -1 \pmod 7$$

It is easy to see that this has no solutions and so we are done. □

(We could also have done this mod 15 as $3, 5 \in M$.)

Now we just need to show that given any prime q, there exists some good set of primes A from M such that $q|n_A$. The best we can do is to choose a set of equal primes from M, but this is not possible since we can't use repeated elements. But we can fix this idea.

Note that M is infinite so mod q some residue occurs infinitely many times in M. Suppose that $p_1 \equiv p_2 \equiv \cdots$ modulo q. Then take A to be the first $q - 1$ elements from p_i. Then

$$n_A \equiv p_1^{q-1} - 1 \equiv 0 \pmod q$$

and we are done!

2.14 Practice Problems

Problem 2.14.1. How many prime numbers p are there such that $29^p + 1$ is a multiple of p?

Problem 2.14.2 (Useful Result). Let p be a prime and $0 \leq k \leq p-1$ be an intger. Prove that

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

Hints: 180

Problem 2.14.3 (IMO 1979/1). Let a and b be natural numbers such that

$$\frac{a}{b} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{1318} + \frac{1}{1319}.$$

Prove that a is divisible by 1979. (Note: 1979 is a prime) **Hints:** 350 407

Problem 2.14.4 (RMO 2016 P6[2]). Let $\{a_1, a_2, a_3, \ldots,\}$ be a strictly increasing sequence of positive integers in an arithmetic progression. Prove that there is an infinite subsequence of the given sequence whose terms are in a geometric progression. **Hints:** 288

Problem 2.14.5. Let $f(x)$ be a polynomial with integer coefficients. Show that there does not exist a N such that $f(x)$ is a prime for all $x \geq N$. In other words, $f(x)$ is not eventually always a prime. This problem shows that prime numbers don't follow any polynomial pattern either. **Hints:** 308

Problem 2.14.6 (IMO 2005/4). Determine all positive integers relatively prime to all the terms of the infinite sequence

$$a_n = 2^n + 3^n + 6^n - 1, \ n \geq 1.$$

Hints: 130

Problem 2.14.7 (IMO 1986/1). Let d be any positive integer not equal to 2, 5, or 13. Show that one can find distinct a and b in the set $\{2, 5, 13, d\}$ such that $ab-1$ is not a perfect square. **Hints:** 379 84 9

Problem 2.14.8. Let a and b be two relatively prime positive integers, and consider the arithmetic progression $a, a+b, a+2b, a+3b, \ldots$

1. `(G. Polya)` Prove that there are infinitely many terms in the arithmetic progression that have the same prime divisors. **Hints:** 265 156 349
2. Prove that there are infinitely many pairwise relatively prime terms in the arithmetic progression. **Hints:** 487 37

[2]Regional Mathematical Oolympiad (the AIME of India)

Problem 2.14.9. Prove that

1. every positive integer has at least as many divisors of the for $4k+1$ as divisors of the form $4k+3$;
2. there exist infinitely many positive integers which have as many divisors of the form $4k+1$ as divisors of the form $4k+3$;
3. there exist infinitely many positive integers which have more divisors of the form $4k+1$ than divisors of the form $4k+3$.

Hints: 457 116 435

Problem 2.14.10 (IberoAmerican 2005/3). Let $p > 3$ be a prime. Prove that if

$$\sum_{i=1}^{p-1} \frac{1}{i^p} = \frac{m}{n}$$

with $\gcd(m,n) = 1$, then $p^3 \mid m$. **Hints:** 357 207 284 231

Problem 2.14.11 (Sierpiński). Prove that for any positive integer s, there is a positive integer n whose sum of digits is s and $s \mid n$. **Hints:** 200 397 197 **Sol:** pg. 280

Problem 2.14.12 (IMO Shortlist 2001 N4). Let $p \geq 5$ be a prime number. Prove that there exists an integer a with $1 \leq a \leq p-2$ such that neither $a^{p-1}-1$ nor $(a+1)^{p-1}-1$ is divisible by p^2. **Hints:** 204 218 467 66

Problem 2.14.13 (USAMO 2018/4). Let p be a prime, and let $a_1, \ldots, a_p$ be integers. Show that there exists an integer k such that the numbers

$$a_1 + k, a_2 + 2k, \ldots, a_p + pk$$

produce at least $\frac{1}{2}p$ distinct remainders upon division by p. **Hints:** 194 241 115 **Sol:** pg. 281

Problem 2.14.14 (Balkan 2016/3). Find all monic polynomials f with integer coefficients satisfying the following condition: there exists a positive integer N such that p divides $2(f(p)!)+1$ for every prime $p > N$ for which $f(p)$ is a positive integer. (A monic polynomial has a leading coefficient equal to 1.) **Hints:** 341 321 67 436

Problem 2.14.15 (Iran 3rd round 2017 Numbers theory final exam P1). Let x and y be integers and let p be a prime number. Suppose that there exist relatively prime positive integers m and n such that

$$x^m \equiv y^n \pmod{p}$$

Prove that there exists an unique integer z modulo p such that

$$x \equiv z^n \pmod{p} \quad \text{and} \quad y \equiv z^m \pmod{p}.$$

Hints: 20 365 108 **Sol:** pg. 281

Problem 2.14.16 (IMO Shortlist 2015 N3). Let m and n be positive integers such that $m > n$. Define

$$x_k = \frac{m+k}{n+k}$$

for $k = 1, 2, \ldots, n+1$. Prove that if all the numbers $x_1, x_2, \ldots, x_{n+1}$ are integers, then $x_1 x_2 \ldots x_{n+1} - 1$ is divisible by an odd prime. **Hints:** 104 328 192 471 **Sol:** pg. 281

Problem 2.14.17 (ELMO 2019/5). Let $\mathcal{S}$ be a nonempty set of positive integers such that, for any (not necessarily distinct) integers a and b in $\mathcal{S}$, the number $ab+1$ is also in $\mathcal{S}$. Show that the set of primes that do not divide any element of $\mathcal{S}$ is finite. **Hints:** 233 30 10 480 **Sol:** pg. 282

✠ More on Binomial Coefficients

One property of the binomial coefficient we have seen so far is

$$p \mid \binom{p}{k} \quad \forall 1 \leq k \leq p-1.$$

Another interesting property is Problem 2.14.2. In this special section, we discuss more.

Lucas's Theorem

This theorem is very useful in understanding how binomial coefficients behave modulo primes. But first, we do a problem:

Example 2.14.1

Show that the coefficients of a binomial expansion $(a+b)^n$ where n is a positive integer, are all odd, if and only if n is of the form $2^k - 1$ for some positive integer k.

We want to show that

$$\binom{n}{m} \equiv 1 \pmod 2 \quad \forall\ 0 \leq m \leq n$$

if and only if $n = 2^k - 1$. (In other words, this tells us excatly which rows of the Pascal triangle have all terms odd).

Suppose that $n = 2^k - 1$. We want to show $\binom{n}{m}$ is always odd. Since k is arbitrary, our first bets should be on induction. Assume the result till $k-1$ and let's prove it for k. Since we want to look at all the binomial coefficients at once, it is best to use the binomial theorem, and the simplest expression is $(X+1)^n$. So

$$\begin{aligned}\sum_{0\leq m\leq n} \binom{n}{m} X^m &= (X+1)^n \\ &= (X+1)^{2^k-1} \\ &= (X+1)^{2\cdot(2^{k-1}-1)+1} \\ &= \left((X+1)^{2^{k-1}-1}\right)^2 \cdot (X+1).\end{aligned}$$

So, if we let $t = 2^{k-1}-1$, then $(X+1)^t = X^t + a_{t-1}X^{t-1} + \cdots + a_1 X + 1$, where $a_1, a_2, \ldots, a_{t-1}$ are all odd (why?). So

$$\left((X+1)^{2^{k-1}+1}\right)^2 \cdot (X+1) = \left(X^t + a_{t-1}X^{t-1} + \cdots + 1\right)^2 (X+1)$$

At this stage, we can simply look at the coefficient of X^m (for any m) in the above expansion and check it will be odd. For instance, the coefficient of $X^{n-1} = X^{2t}$ would be $(1+2a_{t-1})$ (of

course, you would need to elaborate more on why the coefficients would be odd in a proper proof, but I leave the details to the interested reader). However, since $\binom{n}{m}$ was the coefficient of X^m, hence this binomial coefficient is odd.

Thus, we have proven one direction of the problem. The other direction is more tricky, which asks us to show that $\binom{n}{m}$ is always odd for $1 \leq m \leq n$ implies n is of the form $2^k + 1$. So I will just give the theorem's statement:

Theorem 2.14.1 (Lucas's Theorem)**.** *For non-negative integers m and n and a prime p, the following congruence relation holds:*

$$\binom{n}{m} \equiv \prod_{i=0}^{k} \binom{n_i}{m_i} \pmod{p}$$

where

$$n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0$$

and

$$m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0$$

are the base p expansions of m and n respectively. This uses the convention that $\binom{n}{m} = 0$ if $n < m$.

Note that this finishes the problem above easily, since we must have $\binom{n_i}{m_i}$ must always be odd impliying that $n_i = 1$, which corresponds to n be of the form $11\ldots1_{(2)} = 2^k - 1$ for some k.

The cleanest proof for this uses generating functions, with a method slightly similar to the one we found for the previous problem. However, there are some technical details you need to know to fully appreciate the proof, so you can find it in the special section of the chapter: Integer Polynomials.

This theorem is very useful in proving some binomial identities. Here are some problems to try:

Problem 2.14.18. Let $a, b \in \mathbb{N}$ and p be a prime. Prove that

$$\binom{pa}{pb} \equiv \binom{a}{b} \pmod{p}.$$

Problem 2.14.19. Find a formula for the number of entries in the n^{th} row of Pascal's triangle that are not divisible by p, in terms of the base-p expansion of n.

2 Interesting Lemmas

In this part, we talk about two interesting properties related to the binomial coefficients. They give nice formulas for $\binom{p}{k}$ and $\binom{k}{p}$.

Lemma 2.14.1. *Let p be an odd prime. Then*

$$\binom{k}{p} \equiv \left\lfloor \frac{k}{p} \right\rfloor \pmod{p},$$

where $\lfloor \bullet \rfloor$ represents the floor function (aka the greatest integer function).

This is not very tricky to prove, and very easy if you use Lucas's theorem. So the proof is left as an exercise. Another useful property is

Lemma 2.14.2. *Let*

$$\frac{1}{k} \equiv \frac{(-1)^{k-1}}{p}\binom{p}{k} \pmod{p^2}.$$

The proof to this is pretty straightforward too:

$$\begin{aligned}\frac{1}{p}\binom{p}{k} &= \frac{(p-1)(p-2)\dots(p-k+1)}{k(k-1)\dots 1} \\ &\equiv \frac{(-1)(-2)\dots(-k+1)}{k(k-1)\dots 1} \\ &= (-1)^{k-1}\frac{1}{k} \pmod{p}.\end{aligned}$$

Here are two problems using the above lemma (note: they are challenging problems even after using this lemma)

Problem 2.14.20 (ELMO 2009/6). Let p be an odd prime and x be an integer such that $p \mid x^3 - 1$ but $p \nmid x - 1$. Prove that

$$p \mid (p-1)!\left(x - \frac{x^2}{2} + \frac{x^3}{3} - \dots - \frac{x^{p-1}}{p-1}\right).$$

Problem 2.14.21 (IMO Shortlist 2011 N7). Let p be an odd prime number. For every integer a, define the number

$$S_a = \frac{a}{1} + \frac{a^2}{2} + \dots + \frac{a^{p-1}}{p-1}.$$

Let $m, n \in \mathbb{Z}$, such that

$$S_3 + S_4 - 3S_2 = \frac{m}{n}.$$

Prove that p divides m.

Chapter 3

Arithmetic Functions

This chapter is largely about discussion of some common arithmetic functions you will come across in Olympiads, and talks more about multiplicative functions in general too.

But first we ask: what is an arithmetic function? How are they different from normal functions? Well, here's the technical definition:

Definition 3.0.1. *An **arithmetic function**, often called as a **number-theoretic function**, is a function $f : \mathbb{N} \to \mathbb{C}$.*[1]

So the difference really is only in the domain and range. Now here are two things we have defined earlier too:

Definition 3.0.2. *An arithmetic function is called **multiplicative** if*

$$f(mn) = f(m)f(n) \quad \text{for all coprime } m, n.$$

*It is called **completely multiplicative** if*

$$f(mn) = f(m)f(n) \quad \text{for all } m, n.$$

Multiplicative functions are very interesting and have many interesting operations and properties, for instance the Dirichlet Convolution.

There's also the notion of additive functions:

Definition 3.0.3. *An arithmetic function is called **additive** is*

$$f(mn) = f(m) + f(n) \quad \text{for all coprime } m, n.$$

However, this is not so useful for us now. We will largely talk about one additive function in this book, which would be ν_p, the largest exponent function.

Question 3.0.1. *Try and guess the meaning of **completely additive arithmetic functions**.*

Let's now look at some arithmetic functions and start the game.

[1] Hardy & Wright include in their definition the requirement that an arithmetical function "expresses some arithmetical property of n" (source: [17])

3.1 Number of Divisors

I feel that starting this topic without the following classic would be injustice:

Example 3.1.1

The cells in a jail are numbered from 1 to 100 and their doors are activated from a central button. The activation opens a closed door and closes an open door. Starting with all the doors closed the button is pressed 100 times. When it is pressed the k-th time the doors that are multiples of k are activated. Which doors will be open at the end?

Let's make a table to get an idea of the process. A "1" denotes an open door, and a "0" denotes a closed door.

	1	2	3	4	5	6	7	8	...	100
Initial	0	0	0	0	0	0	0	0	...	0
First move	1	1	1	1	1	1	1	1	...	1
Second move	1	0	1	0	1	0	1	0	...	0
Third move	1	0	0	0	1	1	1	0	...	0
Fourth move	1	0	0	1	1	1	1	1	...	1
Fifth move	1	0	0	1	0	1	1	1	...	0
Sixth move	1	0	0	1	0	0	1	1	...	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱	⋮

As of now, we are looking at the rows (each move). Instead, let's now look at the columns[2]. Then we see that, the number 6 for instance, is activated at the kth move if and only if $k \mid 6$. Thus, 6 would be swapped at the $1^{\text{st}}, 2^{\text{nd}}, 3^{\text{rd}}$ and 6^{th} moves. So, it goes $0 \to 1 \to 0 \to 1 \to 0$ and so it's 0 at the end (confirm this from the table).

So, in general, we find that n is operated $d(n)$ times, where $d(n)$ is the number of divisors of n. So if we can know more about the arithmetic function $d(n)$, we might be able to tackle this problem. This is what this section in the book has to offer.

Definition 3.1.1. *Let n be a positive integer. Then the number of divisors of n as a function is denoted by $d(n)$.*

Now divisibility is best dealt with by looking at the prime factors. Let's take an example, say $n = p^3$. Then its divisors will be

$$\{1, p, p^2, p^3\} \implies d(p^3) = 4.$$

Suppose we keep two prime factors this time; $n = p^3q^2$. Then its divisors will be

$$\{1, p, p^2, p^3, q, pq, p^2q, p^3q, q^2, pq^2, p^2q^2, p^3q^2\} \implies d(p^3q^2) = 12.$$

[2]Double Counting anyone?

So in general, a prime divisor is of the form $p^\alpha q^\beta$ where $0 \leq \alpha \leq 3$ and $0 \leq \beta \leq 2$. So there are 4 options for α and 3 options for β. Thus, basic combinatorics[3] tells us that there would be $4 \times 3 = 12$ divisors. Note that this matches with what we wrote above. Generalizing this idea, we obtain the following formula:

Theorem 3.1.1 (Formula for $d(n)$)**.** *Let $n \in \mathbb{N}$ such that its prime factorization is*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

Then

$$d(n) = (1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_k).$$

So, back to the Example 3.1.1, if we want a door to be open at end (meaning a 1 at the end), it must be operated on an odd number of times. So, we would want

$$d(n) = (1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_k)$$

to be odd. This is possible if and only if all of the factors $(1 + \alpha_1), (1 + \alpha_2), \dots (1 + \alpha_k)$ are all odd, which corresponds to $\alpha_1, \alpha_2, \dots, \alpha_k$ all being even. This is the same as saying n is a perfect square (why?). Hence the doors that will be open at the end would be $1, 4, 9, 16, 25, 36, 49, 64, 81, 100$.

Question 3.1.1. *Where was the hypothesis "the button is pressed* 100 *times" used?*

We have thus also shown the following:

Lemma 3.1.1. *The function $d(n)$ is odd if and only if n is a square.*

Is there a formula for $d(n)$ in terms of n? Not really, but we can bound it to get an idea of how large $d(n)$ can really be. For instance, the simplest bound is:

Lemma 3.1.2. *We have*

$$d(n) \leq 2\sqrt{n}.$$

One way to try and do this is directly use the formula. Then we have to prove:

$$\prod (1 + \alpha_i) \leq 2 \prod p_i^{\alpha_i/2}.$$

However, this seems weird to prove. So we try something different, and maybe something simpler. Because of the 2 IN $2\sqrt{n}$, we feel some pairing type argument might be involved in the proof.

Indeed, if $d \mid n$, then $n/d \mid n$. Also, since $d \cdot n/d = n$, hence one of them is smaller than $\sqrt{n}$ (why?). This is sufficient to imply the bound (why?).

Question 3.1.2. *Is $d(n)$ multiplicative?*

[3] The principle of multiplication, to be more specific.

3.2 Sum of Divisors

Suppose now we want the sum of divisors of n. This is often denoted by $\sigma(n)$. Suppose $n = p^3$. Then the sum of its divisors is

$$1 + p + p^2 + p^3 = \frac{p^4 - 1}{p - 1}.$$

Consider $n = p^3q^2$. We mentioned all the divisors of p^3q^2 in the previous section. To add it, we need to be clever with the grouping. So let's make a table for all its divisors:

	1	p	p^2	p^3
1	1	p	p^2	p^3
q	q	pq	p^2q	p^3q
q^2	q^2	pq^2	p^2q^2	p^3q^2

This is much more organized. We now fix a row and add its elements. Then we get

$$(1 + p + p^2 + p^3) + q(1 + p + p^2 + p^3) + q^2(1 + p + p^2 + p^3) = (1 + q + q^2)(1 + p + p^2 + p^3).$$

Thus,

$$\sigma(p^3q^2) = \frac{p^4 - 1}{p - 1} \cdot \frac{q^3 - 1}{q - 1}.$$

If you think carefully, you would realize this is the same as $\sigma(p^3q^2) = \sigma(p^3)\sigma(q^2)$. This raises the question, is σ multiplicative? The answer is yes, and the proof is an argument similar to the one above. We can write prove this in one line: Since all the factors of n are numbers of the form $p_1^{\beta_1} \dots p_k^{\beta_k}$ with $0 \leq \beta_i \leq \alpha_i$ for all i, hence we can use the identity

$$\sigma(n) = \sum_{\substack{0 \leq \beta_i \leq \alpha_i \\ \forall 1 \leq i \leq k.}} p_1^{\beta_1} \dots p_k^{\beta_k} = \left(\sum_{0 \leq \beta_1 \leq \alpha_1} p_1^{\beta_1} \right) \dots \left(\sum_{0 \leq \beta_k \leq \alpha_k} p_k^{\beta_k} \right).$$

Note here that the right side is $\sigma(p_1^{\alpha_1}) \dots \sigma(p_k^{\alpha_k})$, which corresponds to σ being multiplicative.

Question 3.2.1. *Convince yourself the above identity is true. If you can't directly see why, try and take examples, for instance $n = p^3q^2, pq^2, pqr^2$.*

Hence, we obtain the following formula for σ :

Theorem 3.2.1 (Formula for $\sigma(n)$)**.** *Let $n \in \mathbb{N}$ such that its prime factorization is*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

Then

$$\sigma(n) = \frac{p_1^{\alpha_1 + 1} - 1}{p_1 - 1} \dots \frac{p_k^{\alpha_k + 1} - 1}{p_k - 1}.$$

However, more useful than just the formula above is the following fact:

Theorem 3.2.2. *The function σ is multiplicative. Further,*

$$\sigma(p^\alpha) = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.$$

3.3 Euler's Totient Function

We have already discussed this function before, however, I would like to remind you of the very important fact that φ is multiplicative. We will first give the morally right way to prove this

Question 3.3.1. *Show that if* $\gcd(m,n)=1$, *then* $\gcd(x,mn)=1$ *if and only if* $\gcd(x,m)=\gcd(x,n)=1$ *(again, this is an if and only if. You have to show that both* $\implies$ *and* $\impliedby$*).*

Now we look at all the numbers less than mn and pinpoint the ones which are coprime to mn (the idea of looking at the larger picture is quite recurrent, isn't it?). Since we wanna do this in an organized way, we make a table (you should be used to this by now)

$$\begin{array}{cccc} 1 & 2 & \dots & m \\ m+1 & m+2 & \dots & 2m \\ \vdots & \vdots & \ddots & \vdots \\ m(n-1)+1 & m(n-1)+2 & \dots & mn. \end{array}$$

Clearly, each row is a complete residue class modulo m (why?). There are this $\varphi(m)$ numbers in each row coprime to m.

Also, each column is a complete resiude class modulo n (why?). Thus, there are $\varphi(n)$ elements in each column that we have our eyes on. Overall, there are $\varphi(m)\varphi(n)$ elements coprime to mn that are less than it, and so we are done since there are $\varphi(mn)$ such numbers in the list by definition.

We now have the following beautiful result due to Gauss:

Theorem 3.3.1 (Gauss)**.** *For any positive integer* n, *we have*

$$\sum_{d|n}\varphi(d)=n.$$

For instance, if $n=10$, then $\varphi(1)+\varphi(2)+\varphi(5)+\varphi(10)=1+1+4+4=10$. As of now we present a very clever proof, and the idea shown here is very useful.

Proof. Consider the n fractions:

$$\frac{1}{n},\frac{2}{n}\cdots\frac{n}{n}.$$

Reduce each fraction to its lowest form. Then any new denominator d will clearly divide n. Further, the number of fractions with denominator d is $\varphi(d)$ (test this with an example). This is because we get d in the denominator after cancelling the factor n/d and the remaining numerator must be coprime to d (else we can reduce the fraction further). Hence, the number of fractions (which is n) is also the sum $\varphi(d)$ as d varies over all the divisors of n (why?). So we obtain the desired identity. □

Let's hunt for a more direct proof now. So look again at this result for $n=10$. Observe that

$$\varphi(1)+\varphi(2)+\varphi(5)+\varphi(10)=1+\varphi(2)+\varphi(5)+\varphi(2)\varphi(5)=(1+\varphi(2))(1+\varphi(5)).$$

If the result was true for $n = 2, 5$, then we would get $1 + \varphi(2) = 2, 1 + \varphi(5) = 5$. So the right side above becomes $2 \times 5 = 10$. So this seems to resemble "multiplicativeness".

In general, this is true; the left side of Theorem 3.3.1 is multiplicative. Again, this can be expressed neatly using the summation notation (which does exactly what we did above)

$$\sum_{d|n} \varphi(d) = \sum_{\substack{0 \le \beta_i \le \alpha_i \\ \forall 1 \le i \le k.}} \varphi\left(p_1^{\beta_1} \dots p_k^{\beta_k}\right) = \left(\sum_{0 \le \beta_1 \le \alpha_1} \varphi\left(p_1^{\beta_1}\right)\right) \dots \left(\sum_{0 \le \beta_k \le \alpha_k} \varphi\left(p_k^{\beta_k}\right)\right). \tag{3.1}$$

(Note the resemblance of this with the way in which we proved σ is multiplicative).

So, now we just need to show $\varphi(1)+\varphi(p)+\varphi(p^2)+\dots+\varphi(p^\alpha) = p^\alpha$ (which is the theorem for $n = p^\alpha$). However, this is easy to do using $\varphi(p^k) = p^k - p^{k-1}$ (We get a telescoping sum. Try it yourself). So the right side of Equation 3.1 becomes

$$p_1^{\alpha_1} \dots p_k^{\alpha_k} = n.$$

And this proves $\sum_{d|n} \varphi(d) = n$, so we just found another proof!

I hope this was enough to convince you how powerful the idea of a function being multiplicative really is. The next section is now a more general discussion on these functions, which teaches us how to use the above idea in a more general setting and use them to their full power.

Problems for Practice

Problem 3.3.1. Prove that for all composite n

$$\varphi(n) \le n - \sqrt{n}.$$

Prove that for all $n \notin \{2, 6\}$,

$$\varphi(n) \ge \sqrt{n}.$$

The problem below uses basic analysis, so feel free to skip it if needed.

Problem 3.3.2 (The zeta function). The **zeta function** is defined as

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \dots.$$

Note that this is an infinite sum, and does not always converge to a single value. For instance, $\zeta(-1) = 1 + 2 + 3 + 4 + \dots$ clearly diverges.

1. Use basic calculus to show that $\zeta(s)$ converges if and only if $s > 1$. In particular, show that $\zeta(1)$ diverges.

2. Use the Fundamental Theorem of Arithmetic, prove that

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right) = \prod_{p \text{ prime}} \left(\frac{p^s}{p^s - 1}\right).$$

3. (Optional) Use the result above to show that there are an infinite number of primes.

Now, a famous theorem (Basel's problem) states that

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots=\zeta(2)=\frac{\pi^2}{6}.$$

Prove that,

$$\left(\frac{6}{\pi^2}\right)n^2<\sigma(n)\varphi(n)<n^2.$$

Comment 3.3.1: This implies that the product $\sigma(n)\varphi(n)$ behaves like n^2, even though both the terms aren't stable (in the sense that they can be really large at a point and very small all of a sudden. The product somehow balances out each others growth).

3.4 Multiplicative Functions

This section will be slightly harder and technical (considering this chapter is in the "Fundamentals" part of the book) so can be skipped for a first reading. Also, some experience with the sigma notation (especially swapping the order of summations) is highly recommended.

Before we even start, I would highlight the star idea that motivated us to think about multiplicative functions: **It is sufficient to determine a multiplicative function for prime powers.** Now let's generalize the summation idea we used to prove σ and the LHS of Theorem 3.3.1 are multiplicative:

Theorem 3.4.1. *Let f be a multiplicative function. Then*

$$F(n)=\sum_{d|n}f(d)$$

is also multiplicative.

Even though it might seem to "look" different from σ, you can immediately see how this implies that the LHS of Theorem 3.3.1 is multiplicative. The proof of this Theorem has the same idea, which is splitting the sum into product of sums:

Proof. We want to show $F(mn)=F(m)F(n)$. This is possible using the definition of F (note that each divisor of mn can be broken down into a unique divisor of m times a divisor of n since m,n are coprime):

$$F(mn)=\sum_{d|mn}f(mn)=\left(\sum_{d|m}f(m)\right)\left(\sum_{d|n}f(n)\right)=F(m)F(n).$$

So we are done. □

Let's see the power of this. In particular, let's see how is this related to σ. Write

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \mathrm{id}(d).$$

Here, id is the identity function, i.e. $\mathrm{id}(n) = n$ for all n. Clearly id is multiplicative, and hence so is σ using Theorem 3.4.1! That was easy, right? Thus, once we determine σ for prime powers, we basically have determined σ for all integers. The prime power is case is easy to do, so we can prove the formula for σ very easily using this result.

Further, since φ is multiplicative, hence

$$\sum_{d|n} \varphi(n)$$

becomes multiplicative. So we just have to prove Theorem 3.3.1 for prime powers now, which we had shown was very easy!

We can now do much more than just σ. Write

$$d(n) = \sum_{d|n} 1 = \sum_{d|n} \mathbf{1}(d).$$

Here, the function $\mathbf{1}$ is defined as the constant function which always has the value 1. Clearly, $\mathbf{1}$ is multiplicative. Hence, by Theorem 3.4.1, d is multiplicative! Of course, $d(p^\alpha) = \alpha + 1$, so we can directly get the formula for d too.

Now we define something called the Möbius function, which will be very important for our future discussion.

Definition 3.4.1. *The **Möbius function** $\mu(n)$ is defined as:*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^m & \text{if } n \text{ is square-free and has } m \text{ prime divisors} \\ 0 & \text{if } n \text{ is not square-free.} \end{cases}$$

An integer n is called square-free if it is not divisible by any square number (greater than 1), i.e. any prime divisor has exponent at most 1 in n.

For instance, $\mu(1) = 1, \mu(11) = -1, \mu(6) = 1$ and $\mu(12) = 0$. This function is very useful because the following 2 properties:

Theorem 3.4.2. *The Möbius function μ is multiplicative.*

I won't leave everything as an exercise, but if you want you can try to prove it. Anyway, if m or n is not squarefree, then neither is mn so $\mu(mn) = 0 = \mu(m)\mu(n)$. Otherwise since $\gcd(m, n) = 1$, they have no common factors and hence mn is not square free, so $\mu(mn) \neq 0$. Assume $m, n > 1$ (deal with that case separately, it's an easy one). Now clearly $\mu(mn) = \mu(m)\mu(n)$ holds since the number of prime factors get added (use $(-1)^{x+y} = (-1)^x(-1)^y$). That's it, we are done. Another very useful property is the following:

Theorem 3.4.3. *We have*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$$

This is not very hard to prove, and in fact a good combinatorics exercise. I will leave the proof as an exercise. There's a useful notation for the right side:

Definition 3.4.2. *The **Dirichlet Delta Function** δ is an arithmetic function defined by*

$$\delta(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$$

It is not to hard to see that δ is multiplicative. Theorem 3.4.3 thus says

$$\sum_{d|n} \mu(d) = \delta(n).$$

Problems for Practice

Problem 3.4.1. Prove Theorem 3.4.3.

Problem 3.4.2. Let $d(n)$ denote the number of positive divisors of n. For a positive integer n we define $f(n)$ as

$$f(n) = d(k_1) + d(k_2) + \cdots + d(k_m)$$

where $1 = k_1 < k_2 < \cdots < k_m = n$ are all divisors of the number n. Find a formula for $f(n)$ in terms of the prime factorization of n.

3.4.1 Dirichlet Convolution

We observe the sum with indices varying over $d \mid n$ are a common theme in multiplicative function. Based on this idea, we have something called the Dirichlet convolution:

Definition 3.4.3. *Let f, g be two arithmetic functions (not necessarily multiplicative). Then the **Dirichlet Convolution** of f, g, denoted by $f * g$ is defined as*

$$f * g = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

For instance,

$$(f * g)\ (15) = f(1)g(15) + f(3)g(5) + f(5)g(3) + f(15)g(1).$$

Now observe that $\sum_{d|n} f(d) = f * \mathbf{1}$. Further, $f(n) = f * \delta$. Some important examples are the following:

Lemma 3.4.1. *We have the following:*

1. $\mu * \mathbf{1} = \delta$.
2. $\mathbf{1} * \mathbf{1} = d$.
3. $id * \mathbf{1} = \sigma$.
4. $\varphi * \mathbf{1} = id$.
5. $\mu * \mathbf{1} = \delta$.

(Prove these) We have the following properties of $*$ that make it very useful:

Theorem 3.4.4. *Some properties of the binary operation $*$ are*

- ***Commutative**, i.e. $f * g = g * f$;*
- ***Associative**, i.e. $(f * g) * h = f * (g * h)$;*
- ***Identity is δ**[4], i.e. $f * \delta = f$;*
- ***Distributive over Addition**, i.e. $f * (g + h) = f * g + f * h$.*
- ***The convolution of two multiplicative functions is multiplicative.***

(This gives that $(f, *)$ is an abelian group, if you know what it means.) We won't prove these, though it's a good exercise. Note that the last property generalizes Theorem 3.4.1. It is in general very useful to prove a function is multiplicative.

Now consider the following problem:

Example 3.4.1 (Classic)

We say a binary string is *special* if it cannot be expressed as a concatenation of several identical smaller strings. For example, 101101101 is not *special*, but 10101 is. How many *special* strings are there of length n?

Directly approaching to count these is hard. So we take a different route. Firstly, there are 2^n binary strings of length n. Suppose that $f(n)$ is the number of special strings of length n. Clearly, every string of length n is uniquely expressed as a concatenation of a special string of length d (concatenate it n/d times) where d divides n. So we find

$$2^n = \sum_{d|n} f(d) = f * \mathbf{1}.$$

This is useful, however not enough to obtain f. We want a way to "invert" the above. This is exactly what is done by the Möbius Inversion Formula, which we discuss in the next section.

[4]The identity, unlike what you might have expected, is not $\mathbf{1}$.

Problems for Practice

Problem 3.4.3. Prove Lemma 3.4.1 and Theorem 3.4.4.

Problem 3.4.4. Show that

$$\sigma(n) = \sum_{m|n} \varphi(m) d\left(\frac{n}{m}\right).$$

This is an interesting relation between the three functions we have discussed.

3.4.2 Möbius Inversion

We have seen that δ acts as the identity for (arithmetic) functions under Dirichlet's convolution. For a function f, an inverse g would be a function satisfying $f * g = \delta$. Can you think of any one such (f, g) pair?

Recall Theorem 3.4.3. It gives $\mu * \mathbf{1} = \delta$. This is a very useful fact, and can help us find the invert the equation we wanted to! Suppose $f * \mathbf{1} = g$. Then

$$\begin{aligned} g * \mu &= (f * \mathbf{1}) * \mu \\ &= f * (\mathbf{1} * \mu) \\ &= f * \delta = f. \end{aligned}$$

Thus, we have obtained the following:

Theorem 3.4.5 (The Möbius Inversion Formula)**.** *Let f, g be arithmetic functions. Then for all $n \in \mathbb{N}$,*

$$g(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right).$$

Equivalently, we can say that

$$g = f * \mathbf{1} \Leftrightarrow f = g * \mu.$$

We have only proven $f * \mathbf{1} = g \implies f = g * \mu$. We, however, did not show the opposite direction (note that the theorem says the two results are equivalent). I will leave this as an exercise (it will help you get used to Dirichlet's convolution).

Now we are done with Example 3.4.1! Since $2^n = f * \mathbf{1}$, hence we get

$$f(n) = \sum_{d|n} 2^d \mu\left(\frac{n}{d}\right),$$

which is what we wanted to find.

As an application problem, we try and prove a result which is one of my all time favorites; a beautiful result indeed.

Example 3.4.2 (Sum of primitive roots of unity)

For any $n \in \mathbb{N}$, the sum of the nth primitive roots of unity is $\mu(n)$. In other words,

$$\mu(n) = \sum_{\substack{1 \le k \le n \\ (k,n)=1}} \exp\left(\frac{2\pi i k}{n}\right).$$

Firstly, check the result for $n = 1$ and henceforth assume $n > 1$. If you go about trying to tackle it directly, you will have a hard time. However, since sum of all the nth roots of unity is 0, this kind of reminds us of Example 3.4.1. Also, looking at $\mu(n)$ on the left side, we are motivated to try something related to Möbius Inversion. Let $f(n)$ be the function on the right side. We want to prove

$$\mu * \delta = f \Leftrightarrow f * \mathbf{1} = \delta,$$

where the last step used Möbius inversion. This looks much simpler, especially since we don't have μ (which was harder to handle otherwise). We just have to prove

$$\sum_{d|n} \sum_{\substack{1 \le k \le d \\ (k,d)=1}} \exp\left(\frac{2\pi i k}{d}\right) = \delta(n) = 0 \quad \text{(since } n > 1\text{)} \tag{3.2}$$

The left side is a double summation, so hard to think about directly. Let's take an example of $n = 10$ and see how it looks (in fact, we only need to look at the fractions k/d for now):

$$\begin{aligned} d = 1: &\quad \{1/1\} \\ d = 2: &\quad \{1/2\} \\ d = 5: &\quad \{1/5, 2/5, 3/5, 4/5\} \\ d = 10: &\quad \{1/10, 3/10, 7/10, 9/10\} \end{aligned}$$

Since we want the sum to be zero (and we know the sum of all roots of unity is 0), we try to convert these elements into something like that:

$$\begin{aligned} d = 1: &\quad \{1/1\} = \{10/10\} \\ d = 2: &\quad \{1/2\} = \{5/10\} \\ d = 5: &\quad \{1/5, 2/5, 3/5, 4/5\} = \{2/10, 4/10, 6/10, 8/10\} \\ d = 10: &\quad \{1/10, 3/10, 7/10, 9/10\} \end{aligned}$$

We observe that each fraction of the form $n/10$ appears above! This means the sum in Equation 3.2 would be 0 for $n = 10$ (why?) which is what we want to prove!

In general, all the fractions would appear in general in the double sum in Equation 3.2 in general for any n. This is the same idea as in the first proof of Theorem 3.3.1. Do you see now why Equation 3.2 would be true?

Problems for Practice

Problem 3.4.5. Prove the other direction of the Möbius Inversion formula.

Problem 3.4.6. The idea in Example 3.4.2 is the fact the following:

$$\left\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}\right\} = \left\{\left\{\frac{k}{d} : 1 \leq k \leq d\right\} : d \mid n\right\}.$$

Remember this idea and use it to prove for any n,

$$\sum_{d|n} \sum_{\substack{1 \leq k \leq d \\ (k,d)=1}} \mathbf{1} = n.$$

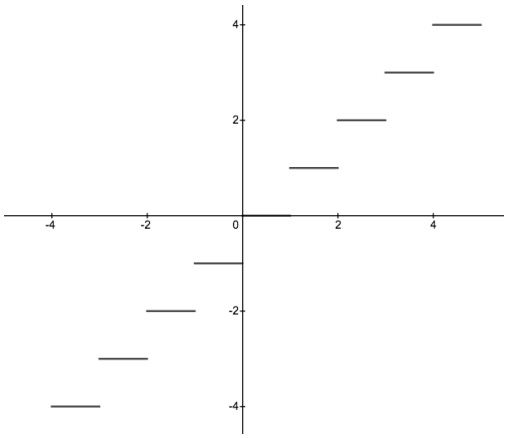
Use the above to show $\varphi * 1 = \mathrm{id}$. Is this the same proof as the one we gave here 3.3.1?

3.5 Floor and Ceiling Functions

Suppose you are given a real number, but we want to deal with integers. What would you do? If it's $r = 2.56$, you might instead consider the integer 2 which is the one just less than it. If it's π, then you might consider 3. This is the idea of the floor function:

Definition 3.5.1. *The **floor function**[5], also called the **greatest integer function**, is a function $\lfloor \bullet \rfloor : \mathbb{R} \to \mathbb{Z}$ such that for every real x, $\lfloor x \rfloor$ is the integer n such that $n \leq x < n+1$.*

Note that the floor function is not an arithmetic function (why?). However, I decided to include it here anyway. This is best understood by examples. For instance, $\lfloor 5 \rfloor = 5$, $\lfloor 2.45 \rfloor = 2$, $\lfloor -3.14159265 \rfloor = -4$ and so on. So basically look at the number line and give the integer just before it. Graphically, it looks like this:



The graph suggests why it is called the "floor function". It is clearly not continuous, and discontinuous at every integer (can you explain this using the definition?).

[5]Technically these aren't Arithmetic Functions since they are $\mathbb{R} \to \mathbb{Z}$. However, I still cover them in this chapter.

This function is widely used, especially in coding and computer science. There is one similar function, called the **ceiling function**, denoted by $\lceil \bullet \rceil$, which gives the integer larger than x. For instance, $\lceil 2.45 \rceil = 3, \lceil -4.5 \rceil = -4$ and $\lceil 5 \rceil = 5$. Lastly, we have something called the fractional part:

Definition 3.5.2. *Let x be a real number. Then the **fractional part** of x, denoted by $\{x\}$ is given by*

$$\{x\} := x - \lfloor x \rfloor .$$

For positive reals, this is simply the decimal part. For instance, $\{4.7\} = 0.7, \{1\} = 0$. For negative, it's not exactly the decimal part, but something similar. For e.g. $\{-2.4\} = 0.6$.

These functions have a lot of properties. Probably the most useful ones are the following (which follow directly from their definitions):

Lemma 3.5.1 (Properties)**.** *The definition gives the following properties:*

1. $x - 1 < \lfloor x \rfloor \leq x$.
2. $x \leq \lceil x \rceil < x + 1$.
3. $0 \leq \{x\} < 1$.

These are very useful in bounding, which is the key idea in equations involving these. An important (yet simple) fact that we will use again and again is the following:

Lemma 3.5.2. *Let x be a real and $n \in \mathbb{Z}$. Then*

1. $\lfloor x + n \rfloor = n + \lfloor x \rfloor$;
2. $\lceil x + n \rceil = n + \lceil x \rceil$;
3. $\{x + n\} = \{x\}$,

Example 3.5.1 (PreRMO 2017[a])

[a] Pre Regional Mathematical Oolympiad (the AMC of India)

Find the maximum value of x such that $\{x\}, \lfloor x \rfloor, x$ form a geometric progression.

Probably the best advice I can give you to solve equations involving the floor function is:

Introduce the Fractional Part.

For instance, the following examples:

Example 3.5.2

Show that $\lfloor 2x \rfloor = 2 \lfloor x \rfloor$ or $2 \lfloor x \rfloor + 1$.

Write $2x = n + f$, where $n = \lfloor 2x \rfloor$ and $f = \{2x\}$. So,

$$\lfloor 2x \rfloor = \lfloor 2n + 2f \rfloor = 2n + \lfloor 2f \rfloor .$$

Now, $0 \leq 2f < 2$ and so $\lfloor 2f \rfloor \in \{0, 1\}$. Hence we are done.

Example 3.5.3 (RMO 2018/5)

Find all natural numbers n such that $1 + \left\lfloor \sqrt{2n} \right\rfloor$ divides $2n$.

Let $k = \left\lfloor \sqrt{2n} \right\rfloor$. This is the same as saying that k is the unique integer such that $k^2 \leq 2n < (k+1)^2$. Let $2n = k^2 + x$, so that $0 \leq x \leq 2k$. Then

$$1 + k \mid k^2 + x \implies 1 + k \mid k^2 + x - (1+k)(k-1) = x + 1.$$

Now, $x + 1 \in \{1, 2, \ldots, 2k+1\}$ and so the only possibility for $k + 1 \mid x + 1$ is when $x = k$. Thus, $2n = k^2 + k$.

Now we substitute back to find which k work. If $2n = k^2 + k$, then $\left\lfloor \sqrt{2n} \right\rfloor = k$ and

$$k + 1 = \left\lfloor \sqrt{2n} \right\rfloor + 1 \mid 2n = k^2 + k$$

holds for all k. Hence, every $k \in \mathbb{N}$ works ($k \in \mathbb{N}$ since $n \in \mathbb{N}$) and the answer is all triangular numbers, i.e. all natural numbers of the form $\frac{k(k+1)}{2}$.

Some problems simply use the definition and a simple idea to solve them. For instance,

Example 3.5.4

Prove that the sum

$$\sum_{i=1}^{n^3} \lfloor \sqrt[3]{x} \rfloor = \frac{(n)(3n^3 - 2n^2 - n + 4)}{4}$$

is true for all $n \in \mathbb{N}$

The key idea is that $\lfloor \sqrt[3]{i^3 + 1} \rfloor = \lfloor \sqrt[3]{i^3 + 2} \rfloor = \cdots = \lfloor \sqrt[3]{i^3 + 3i^2 + 3i} \rfloor = i$. Induction is one way now. Here's a more direct way:

$$\begin{aligned}
\sum_{i=1}^{n^3} \lfloor \sqrt[3]{x} \rfloor &= n + \sum_{i=1}^{n-1} i(3i^2 + 3i + 1) \\
&= n + 3\left(\frac{n(n-1)}{2}\right)^2 + \frac{n(n-1)(2n-1)}{2} + \frac{n(n-1)}{2} \\
&= n + \frac{n(n-1)}{2}\left(\frac{3n(n-1)}{2} + 2n - 1 + 1\right) \\
&= n + \frac{n(n-1)}{2} \cdot \frac{n(3n+1)}{2} \\
&= \frac{n(4 + n(n-1)(3n+1))}{4} \\
&= \frac{n(3n^3 - 2n^2 - n + 4)}{4}
\end{aligned}$$

Problems for Practice

Problem 3.5.1 (Very Useful). One result we will use again and again throughout the book is the following: If $n \in \mathbb{N}$ and $x \in \mathbb{R}$, then

$$n \leq x \implies n \leq \lfloor x \rfloor .$$

This helps to strengthen our bounds. Keep this in mind whenever you have real numbers in integer type inequalities!

3.5.1 Floor Functions of Rational Numbers

The following result is quite useful:

Lemma 3.5.3 (Floor Functions of Rational Numbers)**.** *Let $p, q \in \mathbb{Z}$, $q \neq 0$, and r be the remainder when p is divided by q. Then*

$$\left\lfloor \frac{p}{q} \right\rfloor = \frac{p-r}{q}.$$

The proof is not hard, and left as an exercise. In fact the above is equivalent to the following form of Euclid's Division lemma:

$$p = q \left\lfloor \frac{p}{q} \right\rfloor + r.$$

This is true because the multiple of q just less than p is $q \lfloor p/q \rfloor$.

Let's see this apply to problems.

Example 3.5.5 (All Russian Mathematical Olympiad 2000)

Evaluate the sum $$\left\lfloor \frac{2^0}{3} \right\rfloor + \left\lfloor \frac{2^1}{3} \right\rfloor + \left\lfloor \frac{2^2}{3} \right\rfloor + \cdots + \left\lfloor \frac{2^{1000}}{3} \right\rfloor .$$

Observe that

$$2^i \equiv \begin{cases} 1 \pmod 3 & \text{if } i \text{ is even} \\ 2 \pmod 3 & \text{otherwise.} \end{cases}$$

Hence, the above sum equals

$$\begin{aligned} \frac{2^0-1}{3} + \frac{2^1-2}{3} + \frac{2^2-1}{3} + \cdots + \frac{2^{1000}-1}{3} &= \frac{1}{3}\left(2^0 + 2^1 + \cdots + 2^{1000}\right) - \frac{501 \cdot 1 + 500 \cdot 2}{3} \\ &= \frac{1}{3}(2^{1001} - 2) - 500. \end{aligned}$$

Example 3.5.6 (2002 German Mathematical Olympiad)

Show that for all prime numbers p, we have

$$\sum_{k=1}^{p-1} \left\lfloor \frac{k^3}{p} \right\rfloor = \frac{(p+1)(p-1)(p-2)}{4}$$

Let x_p be the non-negative remainder when x is divided by p. The result holds for $p = 2, 3$. So assume $p \geq 5$. We now claim that for any prime p,

$$\sum_{i=1}^{p-1} i_p^3 = \frac{p(p-1)}{2}$$

Proof. Simply note that

$$2\sum_{i=1}^{p-1} i_p^3 = \sum_{i=1}^{p-1} i_p^3 + (p-i)_p^3 = \sum_{i=1}^{p-1} i_p^3 + \left(p - i_p^3\right) = p(p-1)$$

and we have the lemma. □

Thus, using the lemma we are done, since

$$\begin{aligned}
\sum_{k=1}^{p-1} \left\lfloor \frac{k^3}{p} \right\rfloor &= \sum_{k=1}^{p-1} \frac{k^3 - k_p^3}{p} \\
&= \frac{1}{p}\left(\left(\frac{p(p-1)}{2}\right)^2 - \frac{p(p-1)}{2}\right) \\
&= \frac{(p-1)}{4} \cdot (p^2 - p - 2) \\
&= \frac{(p+1)(p-1)(p-2)}{4}.
\end{aligned}$$

Question 3.5.1. *Was p needed to be a prime? If yes, then where did we use this?*

We can generalize the problem above:

Example 3.5.7

If n is odd, evaluate for any prime $p > 2$ the sum

$$\sum_{k=1}^{p-1} \left\lfloor \frac{k^n}{p} \right\rfloor.$$

A hint to this is given as Problem 3.5.3.

Problem for Practice

Problem 3.5.2. Prove Lemma 3.5.3.

Problem 3.5.3. Prove for odd n

$$\left\lfloor \frac{k^n}{p} \right\rfloor + \left\lfloor \frac{(p-k)^n}{p} \right\rfloor = \frac{k^n + (p-k)^n}{p} - 1.$$

Using this, solve Example 3.5.1.

3.5.2 More Floor Function identities

Let's try the following:

Example 3.5.8

Let x be a real. Prove that

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor = \lfloor 2x \rfloor .$$

Write $x = n + f$, where $n = \lfloor x \rfloor$ and $f = \{x\}$, Then the left side is

$$n + \left\lfloor n + f + \frac{1}{2} \right\rfloor = n + \left(n + \left\lfloor f + \frac{1}{2} \right\rfloor \right) = 2n + \left\lfloor f + \frac{1}{2} \right\rfloor .$$

Now,

$$\lfloor 2x \rfloor = \lfloor 2n + 2f \rfloor = 2n + \lfloor 2f \rfloor .$$

Now, we just have to show

$$\lfloor 2f \rfloor = \left\lfloor f + \frac{1}{2} \right\rfloor .$$

For this, observe that both the sides are 0 when $0 \leq f < 1/2$, and both the sides are 1 when $1/2 \leq f < 1$. So we are done.

We can in fact extend the problem above to

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{3} \right\rfloor + \left\lfloor x + \frac{2}{3} \right\rfloor = \lfloor 3x \rfloor .$$

Again, write $x = n + f$. Then, after some simplification, we just want to prove

$$\left\lfloor f + \frac{1}{3} \right\rfloor + \left\lfloor f + \frac{2}{3} \right\rfloor = \lfloor 3f \rfloor .$$

To prove this, we again employ the same method. Consider the three intervals

$[0, 1/3), [1/3, 2/3), [2/3, 1)$. In the first interval, both the sides are 0. In the second, both the sides are 1. In the last interval, both the sides are 2. Hence, we have a clear generalization now, which is known as Hermite's Identity

Theorem 3.5.1 (Hermite's Identity)**.** *Let x be any real and $m \in \mathbb{N}$. Then*

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{m} \right\rfloor + \cdots + \left\lfloor x + \frac{m-1}{m} \right\rfloor = \lfloor mx \rfloor .$$

We can do this in the same way as above; introduce fractional parts and look at intervals. However, there is another solution (which actually has the same idea, but written differently) which is a much more cooler way of doing this, and a useful trick.

Proof. Define $f(x)$ to be the difference between the left side and the right side. Then

$$\begin{aligned} f\left(x + \frac{1}{m}\right) &= \left\lfloor x + \frac{1}{m} \right\rfloor + \left\lfloor x + \frac{2}{m} \right\rfloor + \cdots + \left\lfloor x + \frac{m}{m} \right\rfloor - \left\lfloor m\left(x + \frac{1}{m}\right) \right\rfloor \\ &= \left\lfloor x + \frac{1}{m} \right\rfloor + \left\lfloor x + \frac{2}{m} \right\rfloor + \cdots + \lfloor x \rfloor + 1 - (\lfloor mx \rfloor + 1) = f(x). \end{aligned}$$

Hence, $f(x)$ is periodic with period $\frac{1}{m}$. Thus, it suffices to find the value of $f(x)$ for $x \in [0, 1/m)$. However, in this interval it is easy to see that $f(x) = 0$ for all x. Hence $f \equiv 0$, which is what we wanted to prove. □

3.5.3 Floor function and Divisors

If you start to solve some of the more challenging problems involving $d(n)$ and the floor function, you would find that the solution of one uses the other.

But how is this possible? Mainly because of this identity:

$$\text{number of multiples of } d, \text{which are} \leq n = \left\lfloor \frac{n}{d} \right\rfloor, n, d \in \mathbb{N}$$

A useful consequence of this is that if $k, n \in \mathbb{N}$, then

$$\left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{n-1}{k} \right\rfloor = \begin{cases} 1, & \text{if } k|n, \\ 0, & \text{otherwise} \end{cases} \tag{3.3}$$

You can see that 3.3 is particularly useful when inducting. One useful lemma we obtain this way is

Let's look at some examples.

Example 3.5.9 (IMO Shortlist 2006 N3)

We define a sequence $(a_1, a_2, a_3, \ldots)$ by

$$a_n = \frac{1}{n}\left(\left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor\right),$$

where $\lfloor x \rfloor$ denotes the integer part of x.

1. Prove that $a_{n+1} > a_n$ infinitely often.
2. Prove that $a_{n+1} < a_n$ infinitely often.

The key idea is to define $b_n = na_n$. Then

$$b_n - b_{n-1} = \sum_{1 \le k \le n} \left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{n-1}{k} \right\rfloor = d(n)$$

The last part follows since a summand in the summation is 1 if and only if k is a divisor of n, and 0 otherwise. Hence,

$$a_n = \frac{d(1) + \cdots + d(n)}{n}.$$

So it suffices to show $d(n+1) > a_n$ and $d(n+1) < a_n$ both hold infinitely often.

But this is easy. Note that $d(n) \ge 2$ for all n with equality if and only if n is a prime. Now $a_6 > 2$ and so $a_n > 2$ for all $n \ge 6$. Thus, set $n = p-1$ for a prime p. Then $d(n+1) = 2 < a_n$ holds true.

Also, note that $d(n)$ is unbounded, as, for instance, $d(2^k) = k+1$. Hence we can find infinitely many $n+1$ such that $d(n+1)$ exceeds all the previous $d(k)$. Hence, $d(n+1) > max\{d(1), \cdots d(n)\} \ge a_n$, as desired.

We proved an interesting result above, which is useful:

Lemma 3.5.4. *For any $n \in \mathbb{N}$,*

$$d(1) + d(2) + \cdots + d(n) = \left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor.$$

There are more interesting ways to prove this. Probably the most interesting one is to double count by making a table. Here, the rows and columns are $1, 2, \ldots, n$, and an element (i, j) is 1 if i is a factor of j, and 0 otherwise (we are basically making an incidence matrix). For instance, for $n = 8$,

	1	2	3	4	5	6	7	8
1	1	0	0	0	0	0	0	0
2	1	1	0	0	0	0	0	0
3	1	0	1	0	0	0	0	0
4	1	1	0	1	0	0	0	0
5	1	0	0	0	1	0	0	0
6	1	1	1	0	0	1	0	0
7	1	0	0	0	0	0	1	0
8	1	1	0	1	0	0	0	1

We will double count the number of 1s in the table. Say there are $\mathcal{T}$ 1s.

Fix a row, say the ith one. Then, the number of 1s here is $\left\lfloor \frac{n}{i} \right\rfloor$, since it denotes how many multiples of i are there that are at most n. Hence, the number of 1s is

$$\mathcal{T} = \left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor.$$

Next, if we fix a column, say the ith one, then the number of 1s here is the number of divisors of i (why?). Hence, there are $d(i)$ 1s. So,

$$\mathcal{T} = d(1) + d(2) + \cdots + d(n).$$

Comparing the two results, we obtain our result. There's a nice and sneaky way to do this double counting using swapping the order of summations:

$$\begin{aligned} d(1) + \cdots + d(n) = \sum_{i=1}^{n} d(i) &= \sum_{i=1}^{n} \sum_{j|i} 1 \\ &= \sum_{j=1}^{n} \sum_{\substack{1 \le k \le n \\ j|k}} 1 \\ &= \sum_{j=1}^{n} \left\lfloor \frac{n}{j} \right\rfloor = \left\lfloor \frac{n}{1} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor. \end{aligned}$$

Now, suppose in our table, instead of writing 1s, we write the multiple. So, the table now is

	1	2	3	4	5	6	7	8
1	1	0	0	0	0	0	0	0
2	2	2	0	0	0	0	0	0
3	3	0	3	0	0	0	0	0
4	4	4	0	4	0	0	0	0
5	5	0	0	0	5	0	0	0
6	6	6	6	0	0	6	0	0
7	6	0	0	0	0	0	7	0
8	8	8	0	8	0	0	0	8

Now, if we try to double count $\mathcal{S}$, the sum of all the elements, we get something interesting. If we fix a row, then the sum of the elements is

$$\mathcal{S} = 1 \left\lfloor \frac{n}{1} \right\rfloor + 2 \left\lfloor \frac{n}{2} \right\rfloor + \cdots + n \left\lfloor \frac{n}{n} \right\rfloor.$$

If we fix a column first, we get

$$\mathcal{S} = \sigma(1) + \sigma(2) + \cdots + \sigma(n).$$

Hence, we have just proven

Lemma 3.5.5. *For any $n \in \mathbb{N}$,*

$$\sigma(1) + \sigma(2) + \cdots + \sigma(n) = 1 \left\lfloor \frac{n}{1} \right\rfloor + 2 \left\lfloor \frac{n}{2} \right\rfloor + \cdots + n \left\lfloor \frac{n}{n} \right\rfloor.$$

Problems for Practice

Problem 3.5.4. The function $d(n)$ doesn't have a nice formula, and is far from continuous. It is very large at some points and very small at just the next input. However, the average function

$$f(n) = \frac{d(1) + d(2) + \cdots + d(n)}{n}$$

is more stable. Show that $f(n) \le \log n$.

Problem 3.5.5. Prove that

$$\sigma(1) + \sigma(2) + \cdots + \sigma(n) \leq n^2.$$

Problem 3.5.6. Prove that $\sigma(n) < n \log n$.

3.6 Example Problems

Example 3.6.1 (Gauss)

Prove that for any coprime integers p, q, we have

$$\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{(q-1)p}{q} \right\rfloor = \frac{(p-1)(q-1)}{2}.$$

The standard way of doing this is to note that $\{p, 2p, \ldots, (q-1)p\}$ forms a complete residue class mod q as p, q are coprime. So, the remainders are exactly $\{1, 2, \ldots, q-1\}$ and the sum evaluates to

$$\frac{p}{q} + \frac{2p}{q} + \cdots + \frac{(q-1)p}{q} - \frac{1}{q}(1 + 2 + \cdots + (q-1)) = \frac{(p-1)(q-1)}{2}.$$

Another elegant argument is the following: Let S be the left side of the equation we have to prove. Consider the triangle formed by $y = 0, x = p$ and $y = \frac{px}{q}$. We double count the number of lattice points[6] inside the triangle.

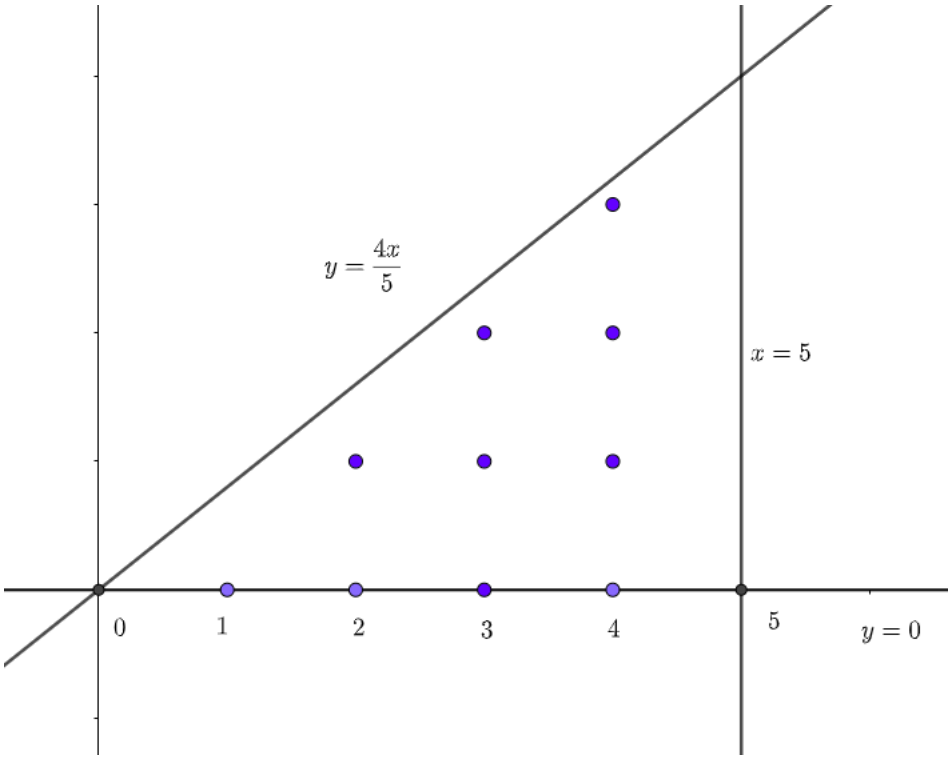


Figure 3.1: Example with $(p, q) = (4, 5)$.

The number of lattice points is clearly the area formed by lattice triangle inside, which is $(p-1)(q-1)/2$ (why?). Further, for every $x \in \mathbb{Z}$ between $0, p$, there are $\lfloor px/q \rfloor$ lattice

[6] A point (x, y) in the Cartesian plane is called a "lattice point" if x, y both are integers.

points above it inside the triangle. Hence, the number of lattice points is S. Hence, we get $S = (p-1)(q-1)/2$.

Question 3.6.1. *In the second proof, where did we use* $\gcd(p,q) = 1$? *Also, why must* $(p-1)(q-1)/2$ *always be an integer?*

The next example is a nice problem.

Example 3.6.2 (Hungarian National Olympiad 1996)

For any positive integer m, denote by $d_i(m)$ the number of positive divisors of m that are congruent to i modulo 2. Prove that if n is a positive integer, then

$$\left|\sum_{k=1}^{n} (d_0(k) - d_1(k))\right| \leq n.$$

For this problem, first we try to think about $d_0(k) - d_1(k)$. Pick a divisor d of k. Notice that if d is even, then it is counted in $d_0(k)$, and if it is odd, it is counted in $d_1(k)$. Hence, the contribution due to d in the difference is $(-1)^d$. So

$$d_0(k) - d_1(k) = \sum_{d|k} (-1)^d.$$

Hence,

$$S = \sum_{k=1}^{n} (d_0(k) - d_1(k)) = \sum_{k=1}^{n} \sum_{d|k} (-1)^d.$$

Now, the key trick is to swap the order of summations. We get

$$\begin{aligned}
\sum_{k=1}^{n} \sum_{d|k} (-1)^d &= \sum_{d=1}^{n} \sum_{\substack{1 \leq k \leq n \\ d|k}} (-1)^d \\
&= \sum_{d=1}^{n} (-1)^d \left\lfloor \frac{n}{d} \right\rfloor \\
&= -\left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{3} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor - \dots.
\end{aligned}$$

We want to show this is at most n in absolute value. This is not hard now, because of the simple observation that

$$n \geq \left\lfloor \frac{n}{1} \right\rfloor \geq \left\lfloor \frac{n}{2} \right\rfloor \geq \dots.$$

Also, it is easy to see that $S \leq 0$. We must thus show $-S \leq n$. This follows since

$$-S = \left\lfloor \frac{n}{1} \right\rfloor - \underbrace{\left(\left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{3} \right\rfloor \right)}_{\geq 0} - \dots \leq n.$$

We finish with a challenging problem related to the σ function!

Example 3.6.3 (St. Petersburg 2011)

Let m, n, k be positive integers with $n > 1$. Show that $\sigma(n)^k = n^m$ is impossible.

The key thing to note here is that $\sigma(n)^k = n^m$ implies $\sigma(n), n$ have the same set of prime factors. Write $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ and $\sigma(n) = p_1^{\beta_1} \dots p_k^{\beta_k}$.

Now since $\sigma(n) > n$, hence $k < m$. Now, $k\beta_i = m\alpha_i$ for each i, so $\beta_i > \alpha_i$ implying $\beta_i \geq \alpha_i + 1$. Hence,

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \leq \frac{p_1^{\beta_1} - 1}{p_1 - 1} \cdots \frac{p_k^{\beta_k} - 1}{p_k - 1} < p_1^{\beta_1} \cdots p_k^{\beta_k} = \sigma(n),$$

and we have a contradiction.

3.7 Practice Problems

Problem 3.7.1. Find all $n \in \mathbb{N}$ such that $\lfloor \sqrt{n} \rfloor$ divides n. **Hints:** 122

Problem 3.7.2. Let a, b, n be positive integers with $\gcd(a, n) = 1$. Prove that

$$\sum_k \left\{ \frac{ak + b}{n} \right\} = \frac{n - 1}{2},$$

where k runs through a complete system of residues modulo n.

Problem 3.7.3. Let $f(x)$ be defined for all rationals $x \in [0, 1]$. If

$$F(n) = \sum_{k=1}^{n} f\left(\frac{k}{n}\right), \quad G(n) = \sum_{k=1,(k,n)=1}^{n} f\left(\frac{k}{n}\right),$$

then prove that $G = \zeta * F$, where $\zeta(n)$ is the sum of the primitive nth roots of unity. **Hints:** 127 410 225

Problem 3.7.4. Show that for all positive integers n,

$$\lfloor \sqrt{n} + \sqrt{n+1} \rfloor = \lfloor \sqrt{4n+1} \rfloor = \lfloor \sqrt{4n+2} \rfloor = \lfloor \sqrt{4n+3} \rfloor.$$

Hints: 95 21

Problem 3.7.5. Prove that for any $n \in \mathbb{N}$,

$$\frac{\sigma(n)}{d(n)} \geq \sqrt{n}.$$

Hints: 58 250

Problem 3.7.6 (IMO 1968/6). Prove that for any positive integer n,

$$\left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n+4}{8} \right\rfloor + \left\lfloor \frac{n+8}{16} \right\rfloor + \cdots = n.$$

Hints: 198 39 351

Problem 3.7.7 (INMO 2014). Let n be a natural number. Prove that

$$\left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor + \lfloor \sqrt{n} \rfloor$$

is even. **Hints:** 409

Problem 3.7.8. Prove that for any integer $n \geq 1$,

$$\sum_{m|n} (d(m))^3 = \left(\sum_{m|n} d(m) \right)^2$$

Hints: 463 414

Problem 3.7.9 (Belarus 1999). For $n \geq 2$,

$$\sigma(n) < n\sqrt{2d(n)}.$$

Hints: 381 11

Problem 3.7.10 (1998 Irish Mathematical Olympiad). Find all positive integers d that have exactly 16 positive integral divisors $d_1, d_2, \ldots, d_{16}$ such that $1 = d_1 < d_2 < \cdots < d_{16} = d$, $d_6 = 18$ and $d_9 - d_8 = 17$. **Hints:** 25 155 213

Problem 3.7.11 (IMO 1991/2). Let $n > 6$ be an integer and $a_1, a_2, \cdots, a_k$ be all the natural numbers less than n and relatively prime to n. If

$$a_2 - a_1 = a_3 - a_2 = \cdots = a_k - a_{k-1} > 0,$$

prove that n must be either a prime number or a power of 2. **Hints:** 437 191 101

Problem 3.7.12 (IMO Shortlist 2016 C2). Find all positive integers n for which all positive divisors of n can be put into the cells of a rectangular table under the following constraints: each cell contains a distinct divisor; the sums of all rows are equal; and the sums of all columns are equal. **Hints:** 259 47 427 **Sol:** pg. 282

Problem 3.7.13 (St. Petersburg City Mathematical Olympiad 1998). Prove that the sequence $d(n^2+1)$ does not become monotonic from any given point onwards. **Hints:** 80 286 **Sol:** pg. 283

Problem 3.7.14 (IMO 1998/3). Determine all positive integers k such that

$$\frac{d(n^2)}{d(n)} = k$$

for some $n \in \mathbb{N}$. **Hints:** 486 339 275 173

Problem 3.7.15 (IMO Shortlist 2004 N2). The function f from the set $\mathbb{N}$ of positive integers into itself is defined by the equality

$$f(n) = \sum_{k=1}^{n} \gcd(k, n), \qquad n \in \mathbb{N}.$$

1. Prove that $f(mn) = f(m)f(n)$ for every two relatively prime $m, n \in \mathbb{N}$.
2. Prove that for each $a \in \mathbb{N}$ the equation $f(x) = ax$ has a solution.
3. Find all $a \in \mathbb{N}$ such that the equation $f(x) = ax$ has a unique solution.

Hints: 113 382 268 293 44 114

Problem 3.7.16 (IMO Shortlist 2011 N1). For any integer $d > 0$, let $f(d)$ be the smallest possible integer that has exactly d positive divisors (so for example we have $f(1) = 1, f(5) = 16$, and $f(6) = 12$). Prove that for every integer $k \geq 0$ the number $f\left(2^k\right)$ divides $f\left(2^{k+1}\right)$. **Hints:** 224 449 140 **Sol:** pg. 283

Problem 3.7.17 (ELMO 2017/4). An integer $n > 2$ is called tasty if for every ordered pair of positive integers (a, b) with $a+b = n$, at least one of $\frac{a}{b}$ and $\frac{b}{a}$ is a terminating decimal. Do there exist infinitely many tasty integers? **Hints:** 297 133 57 324 **Sol:** pg. 284

Problem 3.7.18 (USA TSTST 2016/4). Suppose that n and k are positive integers such that

$$1 = \underbrace{\varphi(\varphi(\ldots\varphi(}_{k \text{ times}} n)\ldots)).$$

Prove that $n \leq 3^k$. **Hints:** 455 203 89 1 289

Problem 3.7.19 (IMO Shortlist 2016 N2). Let $d(n)$ be the number of positive divisors of n. Let $d_1(n)$ be the number of positive divisors of n which have remainders 1 when divided by 3. Find all positive integral values of the fraction $\frac{d(10n)}{d_1(10n)}$. **Hints:** 386 362 236 220 **Sol:** pg. 284

Problem 3.7.20 (China Mathematical Olympiad 2017/5). Let D_n be the set of divisors of n. Find all natural n such that it is possible to split D_n into two disjoint sets A and G, both containing at least three elements each, such that the elements in A form an arithmetic progression while the elements in G form a geometric progression. **Hints:** 149 24 314 111 **Sol:** pg. 285

Problem 3.7.21 (China 2015 TST 3/6). For all natural numbers n, define $f(n) = d(n!) - d((n-1)!)$. Prove that there exist infinitely many composite n, such that for all naturals $m < n$, we have $f(m) < f(n)$. **Hints:** 448 273 109 291 **Sol:** pg. 286

Chapter 4

Diophantine Equations

Roughly speaking, Diophantine equations are equations that ask for integer solutions, which otherwise may be unsolvable in real or complex numbers (or may even have infinitely many solutions there). For instance, the equations $x^2 + y^2 = 2$. This has infinitely many solutions is reals, in fact, any value of x with $|x| \leq \sqrt{2}$ gives a valid real (and of course in complex numbers x can be anything and it would give a valid y). In integers, however, $x = y = 1$ is the only solution.

This was an easy equation, however in general these problems can be very challenging. For instance, Fermat's Last Theorem, which is a very naive looking equation, took over 300 years to be solved!

There have been many advanced techniques developed in modern number theory to solve such equations, for instance elliptic curves. However, in this chapter, we will look at some simpler problems that appear in Olympiads that can be solved using elementary methods. We look at many tricks and types of problems, and each section would contain problems that can largely be solved using that technique only. However, a good problem would be a combination of many techniques and require some ingenuity on its own too. You will find such problems in the problem section.

4.1 Parity

Parity arguments are often useful, especially in problems involving primes.

Example 4.1.1

Let k be an even number. Is it possible to write 1 as the sum of the reciprocals of k odd integers?

Let's suppose

$$1 = \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k}.$$

The given conditions give n_i is odd for all $1 \leq i \leq k$ and k is even. This motivates a parity

type argument. The simplest thing we can do now is cross multiply, which gives

$$n_1n_2n_3\dots n_k = n_2n_3\dots n_k + n_1n_3\dots n_k + \dots + n_1n_2\dots n_{k-1}.$$

The left side is odd, and the right side is a sum of odd terms. There are k terms on the right, so the right side is the sum of an even number of odd numbers, which is even (why?). So we have a contradiction!

4.2 Factoring Equations

Let's look at four very instructive examples, which though easy represent the 4 most fundamental ideas in a lot of Diophantine Equations involving factoring.

Example 4.2.1

Solve over integers:

$$(2x+y)(2y+x) = 7.$$

The key observation here is that $2x+y, 2y+x$ are both integers. So, two integers multiply to give 7. Now, this means they must be one of $(1,7),(7,1),(-1,-7),(-7,-1)$. So you take cases and find your solution set.

$$\begin{cases} 2x+y=1 \\ 2y+x=7 \end{cases} \quad \begin{cases} 2x+y=7 \\ 2y+x=1 \end{cases} \quad \begin{cases} 2x+y=-1 \\ 2y+x=-7 \end{cases} \quad \begin{cases} 2x+y=-7 \\ 2y+x=-1 \end{cases}.$$

Considering each case individually, we find no solutions.

Example 4.2.2

Find $x, y \in \mathbb{Z}$ such that

$$x^2 = 12 + y^2$$

We get $x^2 - y^2 = 12$. Then $(x+y)(x-y) = 12$. So, two integers multiply to give 10, so they can be $\pm(1,12), \pm(2,6), \pm(3,4)$ and it's permutations (for instance if $(3,4)$ is a solution, then so is its permutation $(4,3)$). We take cases now and finish, but there are 12 cases! The key idea here is that if we have $(x+y) = a, (x-y) = b$, then $x = (a+b)/2$, which must be an integer. So, a, b must have the same parity. This is the key idea: $(x+y), (x-y)$ have the same parity.

So, we only consider $(6,2),(2,6),(-6,-2),(-2,-6)$ to get $(x,y) = (4,2),(4,-2),(-4,2),(-4,-2)$.

The key identity is

$$a^2 - b^2 = (a-b)(a+b).$$

So keep your eyes open for even exponents. In particular is the case when $y = 1$ wherein you get $x^2 - 1$.

Example 4.2.3

Find $x, y \in \mathbb{Z}$ such that

$$x^2 + y^2 = x + y + 2.$$

Suppose we had $x^2 + y^2 = 2x + 2y + 2$. Then, we can complete the squares and write $(x-1)^2+(y-1)^2 = 4$. So, $(x-1, y-1) = (0, \pm 2), (\pm 2, 0)$ are the only possibilities. However, completing the square is not so obvious here.

Here's the trick: whenever you have $x^2 \pm x$, multiply both the sides by 4 to complete the square. So, we have

$$4x^2 - 4x + 4y^2 - 4y = 8 \implies (2x-1)^2 + (2y-1)^2 = 10.$$

So, $(2x-1, 2y-1) = \pm(1,3), \pm(3,1)$.

Example 4.2.4

Find $x, y \in \mathbb{Z}$ such that

$$xy = x + y + 3.$$

Whenever you have xy and x, y terms involved, the key identity you should think of is the following:

$$(x+a)(y+b) = xy + xa + yb + ab.$$

In particular, when $a = b = 1$, we get

$$(x+1)(y+1) = xy + x + y + 1.$$

This is often called **Simon's Favorite Factorizing Trick** (SFFT). Who is this Simon is none of our business, but his favorite identity should be our favorite too because this is incredibly useful in a lot of problems. For instance, in our problem we immediately see

$$xy - x - y = 3 \implies (x-1)(y-1) = 4.$$

Ofcourse the above is a variant of simon's identity, however still very useful. In general, if you have $xy + kx + \ell y$, write it as $(x+\ell)(y+k) - k\ell$. When you have $sxy + kx + \ell y$, multiply both the sides by s and then write the above as $(sx+\ell)(sy+k) - k\ell$. So if $2xy - 3x - y = 1$, then write this as

$$2xy - 3x - y = 1 \Leftrightarrow (2x-1)(2y-3) = 5.$$

Let's see some applications.

Example 4.2.5 (British Mathematical Olympiad Round 3, 2005)

The integer n is positive. There are exactly 2005 ordered pairs (x, y) of positive integers satisfying:

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$$

Prove that n is a perfect square.

Write the equation as $nx + ny = xy$. We use Simon's trick and write it as $(x - n)(y - n) = n^2$. We are given that this has 2015 solutions. For any divisor d of n^2, we have $(x - n, y - n) = (d, n^2/d)$ is a valid solution pair. So, the number of solution equals the number of divisors of d. So if $d = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, then

$$(2\alpha_1 + 1) \dots (2\alpha_k + 1) = 2005 = 5 \times 401.$$

Hence, we find either $k = 1$ and $\alpha_1 = 1002$, or $k = 2$ and $(\alpha_1, \alpha_2) = (2, 200)$. In either case, α_i are all even meaning n is a square number.

Example 4.2.6 (INMO)

Determine all non negative integral pairs (x, y) for which

$$(xy - 7)^2 = x^2 + y^2.$$

Write this as

$$\begin{aligned}(xy)^2 - 14xy + 49 = x^2 + y^2 &\iff (xy)^2 - 12xy + 49 = x^2 + y^2 + 2xy \\ &\iff (xy - 6)^2 + 13 = (x + y)^2 \\ &\iff (x + y - xy + 6)(x + y + xy - 6) = 13.\end{aligned}$$

Keeping in mind $x, y \geq 0$, we have the possibilities $(x + y - xy + 6, x + y + xy - 6) = (1, 13), (13, 1)$. Solving these gives $(x, y) = (7, 0), (0, 7), (3, 4), (4, 3)$.

Another useful result is that if $ab = c^2$ with a, b coprime, then a, b are both perfect squares (prove this). In fact, if $\gcd(a, b) = d$, then $a = du^2, b = dv^2$ in general. Here's a nice application:

Example 4.2.7 (Iran 1997)

Let x, y be positive integers such that $3x^2 + x = 4y^2 + y$. Prove that $x - y$ is a perfect square.

Rearrange the terms:

$$3x^2 + x = 4y^2 + y \iff y^2 = (x - y)(3x + 3y + 1) \iff x^2 = (x - y)(4x + 4y + 1).$$

Multiply the second and third equation to get

$$(xy)^2 = (x - y)^2(3x + 3y + 1)(4x + 4y + 1)$$

and so $(3x + 3y + 1)(4x + 4y + 1)$ is a square. However,

$$\gcd(3x + 3y + 1, 4x + 4y + 1) = \gcd(3x + 3y + 1, x + y) = \gcd(1, x + y) = 1.$$

Hence, $3x + 3y + 1, 4x + 4y + 1$ both are squares. Hence, $y^2 = (x - y)(3x + 3y + 1)$ shows $x - y$ is a square.

4.3 Using Inequalities

Inequalities are very useful in Diophantine equations as they help us restrict our attention to certain numbers. This is best seen by examples.

Example 4.3.1

Find all quadruples (x, y, z, w) of positive integers for which

$$x^2 + y^2 + z^2 + 2xy + 2x(z-1) + 2y(z+1) = w^2.$$

Firstly, observe that

$$(x + y + z \pm 1)^2 = x^2 + y^2 + z^2 + 1 + 2xy + 2x(z \pm 1) + 2y(z \pm 1) \pm 2z.$$

The key trick is thus the following bounding:

$$(x + y + z - 1)^2 < w^2 < (x + y + z + 1)^2.$$

Hence, w must equal $x + y + z$. Solving this gives $x = y$. Thus, the solutions are numbers of the form $(x, x, z, 2x + z)$ for any $x, z \in \mathbb{N}$.

Example 4.3.2 (Classic, also Gaussian Gamble 2020/2)

Find all pairs (x, y) of integers such that

$$x^3 + y^3 = (x + y)^2.$$

Suppose $x + y \neq 0$. Then $x^2 - xy + y^2 = x + y$. Clearly, the left side feels to be larger, and this intuition is what makes us believe this will have only a few "small" solutions. Now multiply both the sides by 2 and write this as

$$(x - y)^2 + (x - 1)^2 + (y - 1)^2 = 2.$$

So $(x-1)^2, (y-1)^2 \leq 2$ implies $0 \leq x, y \leq 2$. It is now easy to check the only solutions as $(x, y) = (0, 1), (1, 0), (1, 2), (2, 1), (2, 2)$. Further, we rejected the possibility of $x + y = 0$ above. In fact, any $(k, -k)$ works too.

Example 4.3.3 (PUTNAM)

Find all positive integers $n, k_1, \ldots, k_n$ such that

$$k_1 + k_2 + \cdots + k_n = 5n - 4$$

and

$$\frac{1}{k_1} + \cdots + \frac{1}{k_n} = 1.$$

To anyone who has done enough inequalities, the first thing that the above equations remind one of is the Cauchy-Schwarz (or AM-HM) inequality:

$$(5n-4)(1) = (k_1 + k_2 + \cdots + k_n)\left(\frac{1}{k_1} + \cdots + \frac{1}{k_n}\right) \geq n^2.$$

Hence, $n \leq 4$. The rest of the problem which, although is simple case work, is a good exercise, and hence left to the readers.

Example 4.3.4 (IMO SL 2010 N1)

Find the least positive integer n for which there exists a set $\{s_1, s_2, \ldots, s_n\}$ consisting of n distinct positive integers such that

$$\left(1 - \frac{1}{s_1}\right)\left(1 - \frac{1}{s_2}\right)\cdots\left(1 - \frac{1}{s_n}\right) = \frac{51}{2010}.$$

We can assume $1 < s_1 < s_2 < \cdots < s_n$ (why not $s_1 \geq 1$?). Since s_i are integers, this gives the stronger bounds $2 \leq s_1 \leq s_2 - 1 \leq \cdots \leq s_n - (n-1)$. Thus $s_i \geq i + 1$. Hence

$$\begin{aligned}\frac{51}{2010} &= \left(1 - \frac{1}{s_1}\right)\left(1 - \frac{1}{s_2}\right)\cdots\left(1 - \frac{1}{s_n}\right) \\ &\geq \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\cdots\left(1 - \frac{1}{n+1}\right) \\ &= \frac{1}{2}\cdot\frac{2}{3}\cdots\frac{n}{n+1} = \frac{1}{n+1}.\end{aligned}$$

Hence, $n + 1 \geq (2010)/51 > 39$ meaning $n \geq 39$.

Now if we can show that s_i exist for $n = 39$, we would be done. For this, consider $\{2, 3, \ldots, 33, 35, 36, \ldots, 40, 67\}$. Then

$$\frac{1}{2}\cdot\frac{2}{3}\cdots\frac{32}{32}\cdot\frac{34}{35}\cdots\frac{39}{40}\cdot\frac{66}{67} = \frac{17}{610} = \frac{51}{2010}.$$

4.4 Modular Contradictions

Modular arithmetic is very helpful when dealing with powers. For instance, $a^2 \equiv 0, 1 \pmod 3$ always. We have some more results that are often useful. Modular methods to restraint variables is often a complete solution, but often just an important step. Some useful relations are:

- $a^2 \equiv \{0, 1\} \pmod 3$;
- $(\text{odd})^2 \equiv 1 \pmod 8$
- $a^2 \equiv \{0, 1\} \pmod 4$;

- $a^2 \equiv \{0, \pm 1\} \pmod 5$;
- $a^3 \equiv \{0, \pm 1\} \pmod 7$;
- $a^3 \equiv \{0, \pm 1\} \pmod 9$.

In general, $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$ by Fermat's Little Theorem, and hence we can often try looking for a prime modulus according to the exponent. So if we have terms of the form a^t, and we find $2t+1$ is a prime p, then mod p might help. Further, Euler's theorem comes in handy. For instance above, $6 = \varphi(9)$ and so $a^3 \equiv \{0, \pm 1\} \pmod 9$.

Example 4.4.1 (RMO 2017/2)

Show that the equation

$$a^3 + (a+1)^3 + \cdots + (a+6)^3 = b^4 + (b+1)^4$$

has no solutions in integers a, b.

The key observation here is that $\{a, a+1, \ldots, a+6\}$ are 7 consecutive numbers, hence they are $\{0, 1, \ldots, 6\}$ modulo 7 (in some order). So the left side is congruent to $0^3 + 1^3 + \cdots + 6^3 \pmod 7$, which comes to $0+1+1+(-1)+1+(-1)+(-1) = 0 \pmod 7$. However, $\{0^4, 1^4, \ldots, 6^4\} \in \{0, 1, 2, 4, 4, 2, 1\} \pmod 7$ (in this order) so

$$b^4 + (b+1)^4 \in \{0^4 + 1^4, 1^4 + 2^4, \ldots, 6^4 + 0^4\} \equiv \{1, 3, 6, 1, 6, 3, 1\} \pmod 7.$$

Thus, $b^4 + (b+1)^4 \equiv 0 \pmod 7$ is impossible, and we are done.

Example 4.4.2 (IMO Shortlist 2002 N1)

What is the smallest positive integer t such that there exist integers $x_1, x_2, \cdots, x_t$ with

$${x_1}^3 + {x_2}^3 + \cdots + {x_t}^3 = 2002^{2002} \ ?$$

The x^3 motivates us to try mod 7 or 9. Now, $2002^{2002} \equiv 0 \pmod 7$ and so this isn't very useful. Modulo 9, however, 2002^{2002} is 4. Since $x_i^3 \in \{0, -1, 1\} \pmod 9$, hence we need at least 4 terms, i.e. $t \geq 4$.

Turns out $t = 4$ works. The construction isn't very hard either:

$$\begin{aligned} 2002^{2002} &= 2002 \cdot \left(2002^{667}\right)^3 \\ &= \left(10 \cdot 2002^{667}\right)^3 + \left(10 \cdot 2002^{667}\right)^3 + \left(2002^{667}\right)^3 + \left(2002^{667}\right)^3. \end{aligned}$$

Example 4.4.3 (USAJMO 2013/1)

Are there integers a, b such that $a^5 b + 3$ and $ab^5 + 3$ are perfect cubes?

The answer is no. Assume on the contrary that such a, b exist. Now, each cube is 0 or ± 1 modulo 7. Hence, we must have $a^5b, ab^5 \in \{3, 4, 5\} \pmod 7$. Multiply these two and we get $(ab)^6 \equiv 1, -1, 2, -2, 4 \pmod 7$. By Fermat's Little Theorem, we must have $(ab)^6 \equiv 1 \pmod 7$ and so $(a^5b, ab^5) \equiv (3, 5), (5, 3) \pmod 7$. (note that $7 \nmid a, b$).

Now since $7 \mid 3(3) + 5$, hence we get $7 \mid 3a^5b + ab^5$ or $7 \mid a^5b + 3ab^5$ and so $7 \mid 3a^4 + b^4$ or $7 \mid a^4 + 3b^4$. Assume the first case, as the second one is similar.

As $\gcd(a, 7) = \gcd(b, 7) = 1$, hence on setting $x = a \cdot b^{-1}$, we get $3x^4 \equiv -1 \pmod 7$ and so on checking the possibilities, we find $x \equiv 2 \Leftrightarrow a \equiv 2b \pmod 7$. But then $\{3, 5\} \equiv ab^5 \equiv 2b^6 \equiv \{2, 0\} \pmod 7$, a contradiction.

Note: mod 9 also works.

Example 4.4.4 (USAMTS)

Prove that if m and n are natural numbers, then

$$3^m + 3^n + 1$$

cannot be a perfect square.

Suppose $3^m + 3^n + 1 = x^2$. Clearly, x is odd. Now, mod 4, this means $3^m + 3^n \equiv 0 \pmod 4$. Now, $3^{\text{even}} \equiv 1 \pmod 4$ and $3^{\text{odd}} \equiv 3 \pmod 4$. So, one of m, n must be even, and the other odd.

In fact, we can do better. Every congruence above holds mod 8 too. So $3^m + 3^n \equiv 0 \pmod 8$, and $3^{\text{even}} \equiv 1 \pmod 8, 3^{\text{odd}} \equiv 3 \pmod 8$. Now, we can easily see $3^m + 3^n \in \{1 + 1, 1 + 3, 3 + 1, 3 + 3\} \not\ni 0 \pmod 8$, and we are done.

4.5 Fermat's Last Theorem

Fermat's Last Theorem is a famous theorem of Fermat which despite its innocuous statement is very hard to prove.

Theorem 4.5.1 (Fermat's Last Theorem)**.** *Let $n \geq 3$ be an integer. Then the equation*

$$a^n + b^n = c^n$$

has no solutions in positive integers a, b, c.

Question 4.5.1. *What happens if a, b, c are allowed to be negative?*

The proposition was first stated as a theorem by Fermat around 1637 in the margin of a copy of *Arithmetica*, where he wrote that he had a proof that was too large to fit in the margin. Of course. Other such unproved theorems written off by him were eventually proven, however this one was stuck harder in mathematicians path than others. It was recently proved in 1994 by Andrew Wiles after a shocking 358 years! Of course we don't

discuss the proof in this book; it's the pinnacle of the theory of diophantine equations. We will only look at some variants and fun problems.

Example 4.5.1 (Rejected from ELMO Proposals)

Find all positive integers x, y, z satisfying $xy(x^2 + y^2) = 2z^4$

There are standard albeit boring ways of doing this, however one way stands above all, making it a "troll problem". Note that $(a+b)^2+(a-b)^2 = 2(a^2+b^2)$ and $(a+b)^2-(a-b)^2 = 4ab$. Hence multiply both the sides by 8 and write it as

$$((x+y)^2 - (x-y)^2)((x+y)^2 + (x-y)^2) = (x+y)^4 - (x-y)^4 = (2z)^4$$

which has no solutions by Fermat's last theorem. So we are done.

Of course using Fermat's last theorem here feels like cheating and morally wrong, but it works. In fact, we only used the case $n = 4$ of the big theorem, and it turns out that case isn't very hard to prove. However, we would have to talk more about the case $n = 2$ of the equation (which is not covered in the theorem), which leads us to the discussion of Pythagorean triplets:

4.5.1 Pythagorean Triplets

Definition 4.5.1. *A triplet of three integers (a, b, c) is called a **pythagorean triplet** if*

$$a^2 + b^2 = c^2.$$

The name is obviously inspired from Pythagoras' theorem. Now, it turns out that we can categorize all pythagorean triplets. Firstly, note that if $\gcd(a, b, c) = k$, then we can cancel off a factor of k^2 from both the sides. So assume $\gcd(a, b, c) = 1$. Such pythagorean triplets are called **primitive**.

Theorem 4.5.2. *Let (a, b, c) be a primitive pythagorean triplet. Then there exist integers m, n such that $(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2)$.*

Obviously if a, b, c are of this form, then $a^2 + b^2 = c^2$ is true. However, the amazing part is that this is the only possibility. The proof is a good exercise, so try it yourself before reading it.

Proof. Firstly, note that if a number divides 2 of $\{a, b, c\}$, then it must divide the third, which contradicts our assumption of primitive. So assume every pair is coprime. So one of a, b is odd, suppose a. Then if b is odd, then c is even. But $a^2 + b^2 \equiv 2 \pmod 4$ while $c^2 \equiv 0 \pmod 4$. So suppose b is even, and hence c is odd.

We have $a^2 = c^2-b^2 = (c+b)(c-b)$. Now, we know that if $xy = z^2$, then $x = dm^2, y = dn^2$ where $d = \gcd(x, y)$ and m, n are arbitrary integers. Here,

$$\gcd(c + b, c - b) = \gcd(2c, c + b) = 1,$$

since $c+b$ is odd.

So $c+b=x^2, c-b=y^2$, then $c=(x^2+y^2)/2$ and $b=(x^2-y^2)/2$. Putting this back gives $a=xy$. Since $2 \mid c$, hence $4 \mid x^2+y^2$ which is only possible when x, y are even. Write $x=2m, y=2n$, and you find $c=m^2+n^2, b=m^2-n^2$, and thus $a=2mn$, as deisred. □

You can convert some degree 2 equations into a Pythagorean equation. A prime example is the following:

Example 4.5.2 (INMO 2018/1)

Let ABC be a non-equilateral triangle with integer sides. Let D and E be respectively the mid-points of BC and CA ; let G be the centroid of ΔABC. Suppose, D, C, E, G are concyclic. Find the least possible perimeter of ΔABC.

Using your geometry skills, obtain that the problem is asking you to find $(a,b,c) \in \mathbb{N}^3$ satisfying $a^2+b^2=2c^2$ with $a+b+c$ minimum.

They key trick is that

$$(2c)^2 = 2 \cdot 2c^2 = 2(a^2+b^2) = (a+b)^2 + (a-b)^2.$$

So, $(a-b, a+b, 2c)$ forms a Pythagorean triplet. The smallest Pythagorean triplet is $(3,4,5)$, which doesn't work (why?). The next one is $(6,8,10)$, however note that we look only at primitive Pythagorean triplets if we want them to be the smallest (why?). So we try $(5,7,13)$, and on scaling we find $(a,b,c)=(17,7,13)$. Hence, $17+7+13=36$ is our answer.

4.6 Infinite Descent

Example 4.6.1 (Fermat)

Show that the only solution to the equation

$$x^3+2y^3+4z^3=0$$

in **non-negative integers** is $(0,0,0)$.

The first observation is that $2 \mid x^3$, as $x^3=-2(y^3+2z^3)$. Thus, $2 \mid x$ (as 2 is a prime) so $x=2x^*$. Then $8(x^*)^3+2y^3+4z^3=0$. Dividing by 2 yields $y^3+2z^3+4(x^*)^3=0$. If you have a close eye, you will observe that this is the same format as the equation before! What I mean is, if we have the equation $a^3+2b^3+4c^3=0$, then from the integer solution (x,y,z), we went to the integer solution (y,z,x^*). Further, $x^*<x$ (unless $x=0$) and so, using one solution, we found a smaller solution.

Repeating this process, we can keep getting chains of solutions:

$$(x,y,z) \to (y,z,x^*) \to (z,x^*,y^*) \to (x^*,y^*,z^*) \to (y^*,z^*,(x^*)^*) \to \dots$$

The interesting part is, for each solution we can go to a new solution, and the new solution is "smaller" than the previous one. For instance, if we start with $(16, 4, 12)$, we go

$$(16.4, 12) \to (4, 12, 8) \to (12, 8, 2) \to (8, 2, 6) \to \dots$$

However, since each time we get a solution over non-negative integers, hence we can't go down forever! This is impossible, hence all the numbers originally must have been zero.

Here, we said each triple was getting smaller. However, we can't exactly compare triples (for example, which triple do you think is greater: $(1, 2, 3)$ or $(0, 3, 1)$?), so we need a more formal argument. We can do this by saying $x+y+z$ is decreasing. However, since $x+y+z \geq 0$ always (we always have non-negative integers), hence we cannot keep on decreasing it forever.

Comment 4.6.1: The above problem was solved over non-negative integers. However, we can solve it more generally over integers. Note that if we allow negative integers, our argument fails since we can keep getting smaller and smaller triples and we won't have any issues (earlier we had an issue since the numbers had to be ≥ 0. If we allow negative numbers, we can go down to $-\infty$ without any issue). So how do we solve that problem?

We do this by thinking of $S = |x|+|y|+|z|$. Note that $|x/2| < |x|$ even if x is negative, meaning that S decreases. Clearly, however $S \geq 0$, so it can't go on decreasing forever.

Example 4.6.2 (APMO 2017/1)

We call a 5-tuple of integers arrangeable if its elements can be labeled a, b, c, d, e in some order so that $a - b + c - d + e = 29$. Determine all 2017-tuples of integers $n_1, n_2, \dots, n_{2017}$ such that if we place them in a circle in clockwise order, then any 5-tuple of numbers in consecutive positions on the circle is arrangeable.

The first trick is to note that the given condition is the same as $(a-29)-(b-29)+(c-29)-(d-29)+(e-29) = 0$. So replace each number a_i on the circle by $a_i - 29$.

The next key observation here is that for any i,

$$a_i + a_{i+1} + a_{i+2} + a_{i+3} + a_{i+4} \equiv a_i - a_{i+1} + a_{i+2} - a_{i+3} + a_{i+4} = 29 \equiv 0 \pmod 2.$$

So, $a_i \equiv -(a_{i+1}+a_{i+2}+a_{i+3}+a_{i+4}) \equiv a_{i+5} \pmod 2$. Hence, for every i, a_i, a_{i+5} have the same parity. However, since $\gcd(5, 2017) = 1$, this implies all a_i have the same parity (why?). So, a_i is even for all i (why?). Also, if $a-b+c-d+e = 0$, then so is $a/2-b/2+c/2-d/2+e/2 = 0$.

So, if $(a_1, \dots, a_{2017})$ is a working pair of integers, then so is $(a_1/2, \dots, a_{2017}/2)$. Hence we can keep on decreasing forever, which is impossible (why?). Thus, $a_i = 0$ for all i. Hence, in the problem, all numbers in the circle must equal 29.

A very particular type of infinite descent is the infamous technique "Vieta Jumping". We look at it in the next section.

Problems for Practice

Problem 4.6.1. We solved Example 4.6.1 by showing if (x, y, z) works, then so does $(x/2, y, z)$. The power of 2 in $x/2$ is less than the power of 2 in x. Use this argument to find a second solution to the problem. (take the example of $(16, 4, 12)$ to get an idea)

4.7 Vieta Jumping

Vieta Jumping is a technique

Example 4.7.1 (IMO 1988/6)

Let a and b be positive integers such that $ab + 1$ divides $a^2 + b^2$. Show that

$$\frac{a^2 + b^2}{ab + 1}$$

is the square of an integer.

This is a fascinating result; it says that if $k = \frac{a^2+b^2}{ab+1}$ is an integer, then it is not just any integer, rather a square number!

We could experiment here, maybe try and find explicit values for which $ab + 1 \mid a^2 + b^2$. However, we don't find anything very interesting by these direct methods. Now we try our strongest weapon, the method of contradiction.

Suppose

$$k = \frac{a^2 + b^2}{ab + 1} \in \mathbb{Z}$$

is not a square number. Rearranging, we get an obvious quadratic in a

$$a^2 - kb \cdot a + (b^2 - k) = 0.$$

The interesting part now is if we define $f(t) = t^2 - kbt + (b^2 - k)$, then f has two roots, one of which is a. Are the roots equal?

Question 4.7.1. *Keeping in mind that a, b are positive integers, show that k is a positive integer. Hence, show that the above quadratic cannot have equal roots.*

So, if we let the other root be $x \neq a$, then

$$\frac{x^2 + b^2}{xb + 1} = k.$$

What do we know about x? By Vieta, we know that $x = kb - a$ and $x = \frac{b^2-k}{a}$.

Question 4.7.2. *Show that x is an integer.*

Hence, we went from the pair (a, b) to the pair (x, b). If we can show that (x, b) is "smaller" than (a, b), then we have something like an infinite descent. This is the key idea. We only need to take care of some details now.

We saw that x is an integer. We now show that x is a *positive integer*.

Question 4.7.3. *Use the equation $k = (x^2 + b^2)/(xb + 1)$ and the fact that $k > 0$ to show that $x \geq 0$.*

How do we eliminate the possibility that $x = 0$? Well, $x = (b^2 - k)/a$, hence if $x = 0$, then $k = b^2$ is a perfect square, which contradicts our assumption!

So, from a positive pair (a, b), we went to a positive pair (x, b) (here a positive pair means both elements are positive integers). In order for the new pair to be smaller, we would like $x < a$. This is equivalent to

$$\frac{b^2 - k}{a} < a \Leftrightarrow b^2 - k < a^2.$$

There is no clear reason why this must be true. In fact, this might not even be true!

Question 4.7.4. *Suppose $(a, b) = (8, 30)$. Show that this $ab + 1 \mid a^2 + b^2$ here. Now, show that the process above gives*

$$(8, 30) \to (112, 30).$$

Hence, we got a bigger pair in this case. Show that, however, if $(a, b) = (30, 8)$, then we get

$$(30, 8) \to (2, 8)$$

which is indeed smaller.

Thus, we need the important assumption at the start: without loss of generality, $a > b$ (note that if $a = b$, then it is easy to get $k = 1$, which is a square. So suppose $a \neq b$). In fact, then $b^2 - k < a^2$ becomes obvious. Hence $x < a$. So, from (a, b) we went to (x, b) with $x + b < a + b$.

So, do we have a descent? If we repeat the process of (x, b), we would get a quadratic in x, and we pick the second root. Do you see an issue?

Question 4.7.5. *Revisiting our example, once we get $(30, 8) \to (2, 8)$, what do we get after $(2, 8)$?*

The other root is a, the number we started with! So, if we want a new quadratic, we work with (b, x) now instead of (x, b). This would give a quadratic in b and we get a new pair. However, if we want a smaller pair, we would need $b \geq x$. Is that true? Realizing this is harder than proving it:

$$b \geq \frac{b^2}{a} > \frac{b^2 - k}{a} = x.$$

Thus, we have a descent. Hence, we go from positive pairs to smaller positive pairs, however this process can't go on forever, and so we are done!

As an explicit example, if we start with $(a, b) = (30, 8)$, then we go

$$\dot{(}112, 30) \to (30, 8) \to (2, 8) \to (2, 0).$$

Comment 4.7.1 (Geometric Interpretation): Suppose $k = (x^2 + y^2)/(xy + 1)$. This is the same as $x^2 + y^2 - kxy - k = 0$, which forms a hyperbola $\mathcal{H}$. Assume $x > y$, since if $x = y$ then we can get that k must equal 1[a] (why?). Then, if we have a lattice point $(x, y) \in \mathcal{H}$, then by Vieta the point $(qy - x, y)$ is also a lattice point on $\mathcal{H}$. Further, we can show that $qy - x < x$ and so the x coordinate is lower. Repeating this we get closer and closer the the origin, eventually ending at a point of the form $(x_0, 0)$ or $(0, y_0)$, wherein we get $k = x_0^2$ or y_0^2 respectively.

[a] In that case we get an ellipse.

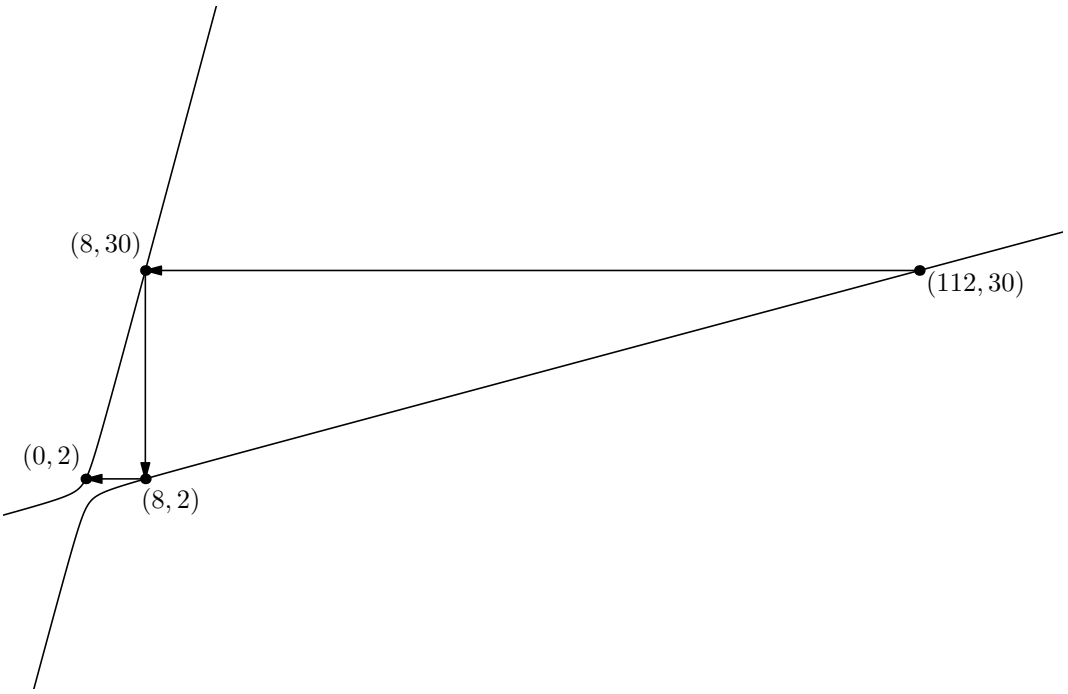


Figure 4.1: Example with $k = 4$

If we retrospect, we realize that we can shorten some of our work. For instance, since we show $x < a$, hence we don't need to show that the quadratic does not have equal roots. Further, there was no need of showing $x < b$, here's why: We have the pair (a, b) with $a > b$. Then we go to (x, b) with $x < a$. If at this point, we have $x > b$, then we repeat everything we just did and get to (a, b) from (x, b), since a is the other roots of the quadratic x forms. However, since everything in the proof would be identical, we can similarly prove (a, b) is smaller than (x, b) meaning $a < x$, which contradicts the fact that $x < a$. So here's a summary of what we did:

1. We assumed on the contrary the result is not true, i.e. $k = (a^2 + b^2)/(ab + 1) \in \mathbb{Z}$ but is not a square.

2. First we showed that if the quadratic in t

$$k = (t^2 + b^2)/(tb + 1)$$

has one positive integer root a, then the second root of the quadratic is also a positive number x. (this part does not require vieta jumping).

3. At this point, we assumed without loss of generality that $a \geq b$.

4. We then showed x is also an integer. Hence x is a positive integer. So we can have a valid descent.

5. Finally, we showed $x < a$. Hence (a, b) gives a smaller pair (x, b). Thus we have a descent.

The best way to tackle all the details is to write down an explicit example. So here's an exercise for you: repeat the process on $(3120, 125)$.

Comment 4.7.2: A neater way of phrasing the above is to use the extremal principle. **Fix k first**, and pick **non-negative integers** (a, b) such that

$$\frac{a^2 + b^2}{ab + 1} = k$$

with $a + b$ **minimum**. For instance, for $k = 4$, both $(2, 0)$ and $(30, 8)$ are valid pairs. So out of all these we pick the one with $a+b$ minimum. Then, once we show $x \leq a$ is a positive integer, so that (x, b) is also a valid pair, we say that $x+b < a+b$ contradicting the minimality. From here on, we will use wither descent or the extremal principle to phrase our argument, depending on which one is easier.

Example 4.7.2

Let a and b be positive integers such that ab divides $a^2 + b^2 + 1$. Show that

$$\frac{a^2 + b^2 + 1}{ab} = 3.$$

The idea is similar here, except that we don't proceed by contradiction. Define k to be the ratio $(a^2 + b^2 + 1) : ab$, so that we want to show $k \in \mathbb{N} \implies k = 3$.

Firstly note that $a = b$ implies $k = 3$ directly. Suppose without loss of generality $a > b$ now. Define the quadratic

$$f(t) = t^2 - kbt + b^2 + 1.$$

One root is a, so say the other one is x. Then by Vieta, $x = kb - a$ which means x is an integer. Also by Vieta, $x = \frac{b^2+1}{a} > 0$, which shows that x is a positive integer. Now, if we want (x, b) to be smaller than (a, b), then we want $x < a$. Since $a > b$, hence

$$x = \frac{b^2+1}{a} < a$$

holds unless $(a, b) = (2, 1)$ (why?). If $(a, b) = (2, 1)$, then $k = 6/2 = 3$, as desired. So suppose not. Hence (x, b) is a smaller pair, i.e. $x < a$. Now, the new x is less than b since

$$x = \frac{b^2+1}{a} < \frac{b^2+1}{b} = b + \frac{1}{b}$$

and if $b > 1$, this means $x \leq \lfloor b + 1/b \rfloor = b$ (why?). In that case, we obtained a smaller pair and can now proceed descent on (b, x) as $b \geq x$. Note again that if $b = x$, then $k = 3$. So we may assume $b > x$.

Hence, the descent must end either when one number becomes 1. In that case if the other number is z, then we have $z \mid z^2 + 2$ which can only happen if $z \in \{1, 2\}$. In either case, we obtain $k = 3$ so we are done.

Now that we have a grip on the basic technique, we can try our hands on some more challenging problems.

Example 4.7.3 (IMO 2007/5)

Let a and b be positive integers. Show that if $4ab - 1$ divides $(4a^2 - 1)^2$, then $a = b$.

First, we start by simplifying $(4a^2-1)^2$ as much as possible by subtracting suitable terms. Since $\gcd(b, 4ab - 1) = 1$, hence

$$4ab - 1 \mid (4a^2 - 1)^2 \Leftrightarrow 4ab - 1 \mid b^2(4a^2 - 1)^2.$$

Now,

$$\begin{aligned} b^2(4a^2 - 1)^2 &= 16a^4b^2 - 8a^2b^2 + b^2 \\ &\equiv a^2 - 2ab + b^2 \\ &= (a - b)^2 \pmod{4ab - 1}. \end{aligned}$$

We stop here, since $(a - b)^2$ is symmetric in a, b and much simpler. The best part is that if we want $a = b$, we want to prove $(a - b)^2 = 0$. So let

$$k = \frac{(a - b)^2}{4ab - 1} \in \mathbb{Z}.$$

We can now use Vieta Jumping! Suppose that (a, b) satisfies $a + b$ is **minimum**.

Assume $a > b$ (if $a = b$ we are done already) and define the quadratic $f(t) = t^2 - 2b(1 + 2k)t + b^2 + k$. One root is a, let the other be x. So, we go

$$(a, b) \to \left(\frac{b^2 + k}{a}, b\right).$$

Clearly, x is a positive integer (why?). Now, we can use descent if $x < a$. This follows since

$$\begin{aligned}\frac{b^2+k}{a} &= \frac{b^2}{a} + \frac{k}{a} \\ &= \frac{b^2}{a} + \frac{(a-b)^2}{a(4ab-1)} \\ &= \frac{4ab^3 - b^2 + a^2 - 2ab + b^2}{a(4ab-1)}.\end{aligned}$$

We want this to be less than a. That is equivalent to

$$4ab^3 + a^2 - 2ab < 4a^3b - a^2 \Leftrightarrow 2a(a-b)(2b(b+a)-1) > 0.$$

This is true since assumed $a > b$. So, we have $0 < x < a$ is a positive integer, and (x, b) is a valid pair. Then $x + b < a + b$ contradicting minimality. So we are done.

Example 4.7.4

Let k be a positive integers not equal to 1 or 3. Prove that the only solution to

$$x^2 + y^2 + z^2 = kxyz$$

over integers is $(0, 0, 0)$.

Vieta jumping can't work here directly, the reason being the fact that x, y, z can be negative. So there is in fact no minimum value of $x + y + z$. So let's try to see if we can make terms positive somehow.

Question 4.7.6. *Show that if one of x, y, z is 0, then so are the rest. Henceforth assume $xyz \neq 0$.*

Now observe that either all x, y, z are all positive, or two of them are negative (why?). Suppose y, z are negative. Note that if we replace $y \mapsto -y, z \mapsto -z$, the equation still holds. Hence, we can assume without loss of generality that x, y, z are all positive. Now we can use Vieta Jumping.

For a given k, pick $(x, y, z) \in \mathbb{N}^3$ [1]. such that $x + y + z$ is minimum. The key claim now is that all x, y, z are distinct.

To see this, observe that if $y = z$, the equation becomes $x^2 + 2y^2 = kxy^2$. Hence, $y \mid x$. Write $x = y\ell$. Then $\ell^2 - ky\ell + 2 = 0$. Since $\ell \in \mathbb{Z}$, we must have $k^2 - 8 = u^2$ for some u. So $(k-u)(k+u) = 8$, and we get $k = 3$ as the only possibility, which we have excluded from the problem.

So now assume without loss of generality $x > y > z$. Define $f(t) = t^2 - kyzt + y^2 + z^2$. One root is x, so say the other root is w. Then $w = kyz - x$ implies $w \in \mathbb{Z}$. To show $w > 0$,

[1] we write $(a, b) \in \mathbb{N}^2$ or $\mathbb{N} \times \mathbb{N}$ if $a \in \mathbb{N}$ and $b \in \mathbb{N}$. In other words, $\mathbb{N}^2$ is the set of all pairs (a, b) where both the elements are from $\mathbb{N}$. Similarly we define $\mathbb{N}^3, \mathbb{N}^4, \ldots$ (we can even define $\mathbb{R}^2, \mathbb{Z}^3, \mathbb{C}^4 \ldots$ similarly). So, in our case we mean x, y, z are all natural numbers.

observe that $w = (y^2 + z^2)/x$. Hence, w is a positive integer. Now, we want to establish a descent. Proving $w < x$ is not easy (try it). The key trick is to compute $f(y)$:

$$f(y) = y^2 - ky^2z + y^2 + z^2 \leq 3y^2 - ky^2z = y^2(3 - kz)$$

For now, say $k \neq 2$, so that $k > 3$. Hence we get $f(y) \leq 0$.. Hence, y lies between the two roots x, w (why?) and since $x > y$, hence $y > w$ implying $x > w$. So, $x + y + z$ has reduced, and we have our contradiction.

So now we just have to deal with the case $k = 2$. This is Problem 4.7.1.

Problems for Practice

Problem 4.7.1 (Korean Mathematical Olympiad). Prove that $x^2 + y^2 + z^2 = 2xyz$ has no solutions in integers x, y, z except $(0, 0, 0)$.

Problem 4.7.2 (Stronger than IMO 1988/6). Show that if $ab + 1$ divides $a^2 + b^2$ for positive integers a, b, then

$$\frac{a^2 + b^2}{ab + 1} = \gcd(a, b)^2.$$

Problem 4.7.3 (Generalization of IMO 1988/6). If a, b, c are positive integers such that

$$0 < a^2 + b^2 - abc \leq c,$$

show that $a^2 + b^2 - abc$ is a perfect square.

Problem 4.7.4. Let $x_1, x_2, \ldots, x_n$ be n integers. If $k > n$ is an integer, prove that the only solution to

$$x_1^2 + x_2^2 + \cdots + x_n^2 = kx_1x_2 \ldots x_n$$

is $x_1 = x_= \cdots = x_n = 0$.

4.8 Pell's Equations

Definition 4.8.1. *The equation $x^2 - dy^2 = 1$ where d is a positive integer which is not a square is called **Pell's Equation**.*

Here, we need d to not be a square, otherwise if $d = c^2$, then this becomes $(x-cy)(x+cy) = 1$. We have the following beautiful theorem:

Theorem 4.8.1. *The Pell's equation always has a solution (x, y).*

In fact, there are infinitely many solutions to the equation! Given that there is 1 solution, we can generate more from it. Let's see how.

Firstly, we need to define something:

Definition 4.8.2. *Define a number $z = x + y\sqrt{d}$. Then, the **conjugate** of z, denoted by $\overline{z}$, is given by $\overline{z} = x - y\sqrt{d}$. Further, the **Norm** of z is given by*

$$\mathrm{N}(z) = z\overline{z} = x^2 - dy^2.$$

Note the resemblance with complex numbers. In fact, in algebraic number theory we study general conjugates and norms, which apply to all these numbers! However, let's not divert now.

One of the most useful property of the Norm is the following:

Theorem 4.8.2. *The Norm is multiplicative, i.e.*

$$\mathrm{N}(z_1 z_2) = \mathrm{N}(z_1)\,\mathrm{N}(z_2).$$

(This also holds for complex numbers). The proof of this isn't very hard, just expand and check:

$$\mathrm{N}(z_1)\,\mathrm{N}(z_2) = (a^2 - db^2)(x^2 - dy^2) = (ax + dby)^2 - d(ay + bx)^2 = \mathrm{N}(z_1 z_2).$$

In fact, the **conjugate is also multiplicative**.

Now, we can see how this is useful: Saying $x^2 - dy^2 = 1$ is the same as saying $z = x + y\sqrt{d}$ satisfies $\mathrm{N}(z) = 1$. Now, note that

$$\mathrm{N}(z^2) = \mathrm{N}(z) \cdot \mathrm{N}(z) = 1.$$

Hence, if z satisfies $\mathrm{N}(z) = 1$, then so does z^2. In fact, $\mathrm{N}(z^k) = 1$ for any natural number k. So from one solution, we can generate infinitely many.

Example 4.8.1

Suppose $d = 3$. Then $(x, y) = (2, 1)$ is a solution. So $z = 2 + \sqrt{3}$ works. Now,

$$z^2 = (2 + \sqrt{3})^2 = 7 + 4\sqrt{3}.$$

Hence, we get another solution $(x, y) = (7, 4)$. Further,

$$z^3 = (2 + \sqrt{3})^3 = 26 + 15\sqrt{3}.$$

This gives the solution $(x, y) = (26, 15)$. We can keep proceeding and generate infinitely many solutions.

Whenever we start with a z, we can generate infinitely many solutions, however we can guarantee that these would be all the solutions to the Pell's equation. For instance in the above example, if we had started with $z = 7 + 4\sqrt{3}$, then no power of z would have given us the solution $26 + 15\sqrt{3}$. So how do we find *all* the solutions to the Pell's equation?

Turns out that there exists one solution z called the **fundamental solution** which generates all the solution to the Pell's equation.

Theorem 4.8.3. *Let d be a positive integer which is not a perfect square. Then there exists $\varepsilon = x_0+y_0\sqrt{d}$ with $x_0, y_0 \in \mathbb{N}$ such that every solution (x, y) to the Pell's equation $x^2-dy^2 = 1$ is found by*

$$x + y\sqrt{d} = \varepsilon^n = (x_0 + y_0\sqrt{d})^n$$

for some integer n.

Note that x_0, y_0 are both positive. The proof is not very hard. They idea is that the fundamental solution (x_0, y_0) is the "smallest".

Proof. Consider α to be the smallest real of the form $x + y\sqrt{d}$ which is greater than 1 and has norm 1. Let $\beta = a + b\sqrt{d}$ be such that (a, b) is another solution to $X^2 - dY^2 = 1$. Let k be such that

$$\alpha^k \leq \beta < \alpha^{k+1}.$$

(since $\alpha < \beta$ and $\alpha^n \to \infty$ as $n \to \infty$ (as $\alpha > 1$) hence by continuity there must exist such a k). Now since $\mathrm{N}(\alpha) = 1$, hence $(x + y\sqrt{d})^{-1} = x - y\sqrt{d}$. So

$$\gamma = \frac{\beta}{\alpha^k} = (a + b\sqrt{d})(x - y\sqrt{d})^k.$$

Now, $\mathrm{N}(\gamma) = 1$, and on expanding γ comes to be something of the form $r + s\sqrt{d}$. Note that $1 \leq \gamma$ means $\overline{\gamma} \leq 1$ (as $\mathrm{N}(\gamma) = 1$). Hence $r - s\sqrt{d} \leq 1 \leq r + s\sqrt{d}$, showing r, s are nonnegative. Since $\gamma < \alpha$, the minimality of α is contradicted unless $\gamma = 1$, which corresponds to $\beta = \alpha^k$, as desired. □

Example 4.8.2 (Kürsák Competition)

Prove that if $m = 2 + 2\sqrt{28n^2 + 1}$ is an integer for some $n \in \mathbb{N}$, then m is a perfect square.

For m to be an integer, we must have $28n^2 + 1 = x^2$ for some x. This is Pell's equation with $d = 28$. If we try to find the fundamental solution, we have a really hard time doing so. Hence we adopt a trick: write the equation as $x^2 - 7(2n)^2 = 1$.

The fundamental solution to $X^2 - 7Y^2 = 1$ is not hard to find, and it is $(8, 3)$. Here, 3 is odd. We generate more solutions from this till we find the second number even (why do we need this?).

$$\left(8 + 3\sqrt{7}\right)^2 = 127 + 48\sqrt{7}.$$

So the second solution is $(127, 48)$. Thus $(127, 24)$ is the fundamental solution to $x^2-28n^2 = 1$ (couldn't have guessed this, could we?). Hence,

$$x + y\sqrt{28} = (127 + 24\sqrt{28})^k$$

for some k. To find x from above, we use another trick: let $z = x+y\sqrt{28}$ and $z_0 = 127+24\sqrt{28}$. Observe that $x = \frac{1}{2}(z + \overline{z})$ and hence

$$x = \frac{1}{2}\left((127 + 24\sqrt{28})^k + (127 - 24\sqrt{28})^k\right)$$

since $\overline{(127+24\sqrt{28})^k} = \left(\overline{127+24\sqrt{28}}\right)^k$ as conjugation is multiplicative. Now,

$$2+2x = (127+24\sqrt{28})^k + (127-24\sqrt{28})^k + 1 = \left((8+3\sqrt{7})^k + (8-3\sqrt{7})^k\right)^2$$

and we are done.

Question 4.8.1. *Why is the part inside the square an integer? That is, why is*

$$(8+3\sqrt{7})^k + (8-3\sqrt{7})^k$$

an integer?

The trick we used before can be generalized to give all solutions of the Pell's equation:

Theorem 4.8.4 (General Solution of Pell's Equation)**.** *Let $x^2-dy^2=1$ be a Pell's equation with fundamental solution (x_0,y_0). Let (x_{n-1},y_{n-1}) be the nth solution. Then*

$$x_{n-1} = \frac{1}{2}\left((x_0+y_0\sqrt{d})^n + (x_0-y_0\sqrt{d})^n\right), \quad y_{n-1} = \frac{1}{2\sqrt{d}}\left((x_0+y_0\sqrt{d})^n - (x_0-y_0\sqrt{d})^n\right).$$

For instance, $x_0 = \frac{1}{2}\left((x_0+y_0\sqrt{d}) + (x_0-y_0\sqrt{d})\right) = x_0$ and $x_1 = x_0^2+dy_0^2$.

You might recognize the above formulas as the solutions of a linear recurrence equation. This is indeed true, and we can find these recurrences:

Theorem 4.8.5 (Recursive Solutions of Pell's Equations)**.** *Let $x^2-dy^2=1$ be a Pell's equation with fundamental solution (x_0,y_0). Let (x_{n-1},y_{n-1}) be the nth solution. Then*

$$x_n = 2x_0x_{n-1} - x_{n-2}, \quad y_n = 2x_0y_{n-1} - y_{n-2}.$$

This is true because $x_n = A\alpha^n + B\beta^n$ satisfies $x_n = (\alpha+\beta)x_{n-1} - (\alpha\beta)x_{n-2}$.

There are some variants of the Pell's equation, the most common being the negative Pell's equation:

Definition 4.8.3. *Let d be a positive integer that is not a perfect square. Then the equation $x^2-dy^2=-1$ is a* ***negative Pell's equation****.*

Unlike the standard one, this equation need not have solutions at all. However, if there exists one solution, then there exist infinitely many. This is done by taking a fundamental solution z_0, and considering the solutions z_0^k where k is odd, and these form all the solutions (as before). In fact, z_0^2 gives the fundamental solution to $x^2-dy^2=1$.

If we consider equations of the form $x^2-ny^2=r$ for $|r|\neq 1$, then we can just consider powers of a fundamental solution. Here, we take one solution and multiply it by solutions of $x^2-ny^2=1$. However, in this case this does not generate all the solutions, unlike before. Luckily, these don't show up a lot in Olympiads.

Here's a great example:

Example 4.8.3 (Vietnam 2016)

Find all n such that

$$\sqrt{\frac{7^n+1}{2}}$$

is a prime.

Suppose this equals p. Squaring and rearranging, we find $7^n - 2p^2 = -1$. This is not Pell's equation if n is odd. We can easily see that $n = 1$ works. So when $n > 1$ small cases suggest that n odd doesn't seem to work. This observation is correct; modulo 8, the equation implies n is even. So we have the negative Pell's equation:

$$(7^m)^2 - 2p^2 = -1$$

where $m = n/2$. So consider the general Pell's equation $x^2 - 2y^2 = -1$. Since $(1, 1)$ is a solution, hence the solutions are generated by $(1+\sqrt{2})^{2k+1}$ for all $k \geq 0$. Hence, the general solution for x_n is

$$x_{n-1} = \frac{1}{2}\left((1+\sqrt{2})^{2k+1} + (1-\sqrt{2})^{2k+1}\right) = \frac{1+\sqrt{2}}{2}\left(3+2\sqrt{2}\right)^k + \frac{1-\sqrt{2}}{2}\left(3-2\sqrt{2}\right)^k.$$

So we obtain the recurrence $x_n = 6x_{n-1} - x_{n-2}$ with $(x_0, x_1) = (1, 7)$. Similarly we get $y_n = 6y_{n-1} - y_{n-2}$ with $(y_0, y_1) = (1, 5)$. Then

$$x_n \equiv -(x_{n-1} + x_{n-2}) \pmod 7, \quad y_n \equiv y_{n-1} - y_{n-2} \pmod 5.$$

Hence, $7 \mid x_n$ if and only if $n \equiv 1 \pmod 3$, which also corresponds to $5 \mid y_n$. Hence, we must have $p = 5$ and so the only other solution we get is $n = 2$.

Problems for Practice

Problem 4.8.1. Show that $\overline{zw} = \overline{zw}$, i.e conjugation is multiplicative.

Problem 4.8.2. Prove Theorem 4.8.4.

Problem 4.8.3. Using the binomial theorem, show that x_n, y_n are integers in Theorem 4.8.4.

4.9 Practice Problems

Problem 4.9.1. Solve in positive integers the equation

$$x^2y + yz^2 + zx^2 = 3xyz.$$

Hints: 128

Problem 4.9.2. Find all triples of positive integers (x, y, z) such that

$$x^3 + y^3 + z^3 - 3xyz = p,$$

Hints: 52

Problem 4.9.3 (USAMTS 2017-18 Round 3 P2). Let q be a real number. Suppose there are three distinct positive integers a, b, c such that $q + a, q + b, q + c$ is a geometric progression. Show that q is rational. **Hints:** 7

Problem 4.9.4 (IMO 2006/4). Determine all pairs (x, y) of integers such that

$$1 + 2^x + 2^{2x+1} = y^2.$$

Hints: 206 411 358

Problem 4.9.5 (INMO 2017/6). Let $n \geq 1$ be an integer and consider the sum

$$x = \sum_{k\geq 0} \binom{n}{2k} 2^{n-2k}3^k = \binom{n}{0}2^n + \binom{n}{2}2^{n-2} \cdot 3 + \binom{n}{4}2^{n-k} \cdot 3^2 + \cdots.$$

Show that $2x - 1, 2x, 2x + 1$ form the sides of a triangle whose area and inradius are also integers. **Hints:** 302 440

Problem 4.9.6 (Indian Mathematical Olympiad 1988). Find all $(x, y, n) \in \mathbb{N}^3$ such that $\gcd(x, n + 1) = 1$ and $x^n + 1 = y^{n+1}$. **Hints:** 81 46 270 199

Problem 4.9.7 (USAMO 1987). Solve the following equation in nonzero integers x, y :

$$(x^2 + y)(x + y^2) = (x - y)^3.$$

Hints: 391 215

Problem 4.9.8. Find all positive integers m and n for which

$$1! + 2! + 3! + \cdots + n! = m^2.$$

Hints: 229 380

Problem 4.9.9 (EGMO 2013/4). Find all positive integers a and b for which there are three consecutive integers at which the polynomial

$$P(n) = \frac{n^5 + a}{b}$$

takes integer values. **Hints:** 6 216 126 **Sol:** pg. 286

Problem 4.9.10 (Leo Moser). Show that the Diophantine equation

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} + \frac{1}{x_1 x_2 \cdots x_n} = 1$$

has at least one solution for every positive integers n. **Hints:** 430

Problem 4.9.11 (IMO 2013 Problem 1). Assume that k and n are two positive integers. Prove that there exist positive integers $m_1, \ldots, m_k$ such that

$$1 + \frac{2^k - 1}{n} = \left(1 + \frac{1}{m_1}\right) \cdots \left(1 + \frac{1}{m_k}\right).$$

Hints: 402 195

Problem 4.9.12. Show that the equation

$$a^2 + b^2 + c^2 + d^2 = abcd$$

has infinitely many solutions in positive integers a, b, c, d. **Hints:** 287 129 484 **Sol:** pg. 287

Problem 4.9.13 (USAMO 2015/1). Solve in integers the equation

$$x^2 + xy + y^2 = \left(\frac{x+y}{3} + 1\right)^3.$$

Hints: 38 369 346 445

Problem 4.9.14 (IMO Shortlist 2012 N2). Find all triples (x, y, z) of positive integers such that $x \leq y \leq z$ and

$$x^3(y^3 + z^3) = 2012(xyz + 2).$$

Hints: 363 93 3 124

Problem 4.9.15 (Vietnam 2002). Find all positive integers n for which the equation

$$a + b + c + d = n\sqrt{abcd}$$

has a solution in positive integers a, b, c and d. **Hints:** 19 453

Problem 4.9.16 (HMMT 2017 A8). Suppose a and b are positive integers such that

$$c = \frac{(a+b)(a+b+1)}{ab}$$

is an integer. Find all possible values of c. **Hints:** 296 167 32

Problem 4.9.17 (IMO 2008 N1). Let n be a positive integer and let p be a prime number. Prove that if a, b, c are integers (not necessarily positive) satisfying the equations

$$a^n + pb = b^n + pc = c^n + pa$$

then $a = b = c$. **Hints:** 14 131 385 99 **Sol:** pg. 287

Problem 4.9.18 (IMO Shortlist 2017 N6). Find the smallest positive integer n or show no such n exists, with the following property: there are infinitely many distinct n-tuples of positive rational numbers $(a_1, a_2, \ldots, a_n)$ such that both

$$a_1 + a_2 + \cdots + a_n \quad \text{and} \quad \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}$$

are integers. **Hints:** 210 332 61 374 **Sol:** pg. 288

Problem 4.9.19 (IMO Shortlist 2019 N8). Let a and b be two positive integers. Prove that the integer

$$a^2 + \left\lceil \frac{4a^2}{b} \right\rceil$$

is not a square. **Hints:** 29 404 251 182 **Sol:** pg. 289

Problem 4.9.20 (China TST 3 2018 Day 3/2). Find all pairs of positive integers (x, y) such that $(xy+1)(xy+x+2)$ be a perfect square. **Hints:** 279 69 429 2 **Sol:** pg. 290

Part II

Advanced Topics

Chapter 5

Modular Arithmetic Advanced

Now that we have a grip on the basics of modular arithmetic, we will discuss some more interesting ideas in this chapter.

5.1 Solving Equations

At the end of the day, solving some sort of equation is one of the key goals of mathematicians. That is what lead them to discover $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$. This is what we have done in the last chapter too. For instance, in solving the equation $ax - b \equiv 0 \pmod{p}$, we were lead to the concept of inverses. We now talk about some other equations.

5.2 Quadratic Residues

One of the equations that lead humanity to discover irrationals was $x^2 = 2$. In general, it was $x^2 = a$ for $a > 0$. So we ask when does the equation

$$x^2 \equiv a \pmod{p}$$

have a solution. Turns out not all a lead to a solution x. So we have 2 terms defined for this purpose:

Definition 5.2.1. *Let p be a prime. A number a is called a **quadratic residue mod** p if there exists an integer x such that $x^2 \equiv a \pmod{p}$. It is called a **quadratic non-residue** otherwise.*

For instance, if $p = 7$, then 2 is a quadratic residue since $3^2 \equiv 2 \pmod{7}$. However, 3 is not a quadratic residue (you can check this by listing all $0^2, 1^2, 2^2, \ldots, 6^2$ and observing that 3 never appears.)

Quadratic residues are very interesting. Hence, I have dedicated a different chapter to them and so won't talk about them anymore for now.

5.3 Square root of -1?

Now let's consider the equation that lead to humans discovering the complex numbers: $x^2 = -1$. However, this time it's modulo p :

$$x^2 \equiv -1 \pmod{p},$$

where p is a prime. So, we basically consider the set of numbers $\{a^2 + 1\}$ where $a \in \{0, 1, \ldots, p-1\}$, and if any element here is 0, we are done. Let's investigate:

1. For $p = 2$, clearly $1^2 \equiv -1 \pmod{2}$, so we ignore this case. Further, we assume $p > 2$ for the rest of the chapter.

2. For $p = 3$,
$$\{a^2 + 1\}_{a=0}^{2} = \{1, 2, 5\} \equiv \{1, 2, 2\} \pmod{3}.$$
So, $x^2 \equiv -1 \pmod{3}$ has no solution.

3. For $p = 5$,
$$\{a^2 + 1\}_{a=0}^{4} = \{1, 2, 5, 10, 17\} \equiv \{1, 2, 0, 0, 2\} \pmod{5}.$$
So, $x^2 \equiv -1 \pmod{5}$ has the solution $x \equiv 3, 4$. These are also the only solutions.

For cases after this, we can ease our work. Firstly, we don't need to consider $a = 0$, since $0^2 + 1 \not\equiv 0 \pmod{p}$ for an prime p. Next, since $a^2 + 1 \equiv (-a)^2 + 1 \pmod{p}$, hence we only need to consider the first half residues mod p.

1. For $p = 7$,
$$\{a^2 + 1\}_{a=1}^{3} = \{2, 5, 10\} \equiv \{2, 5, 3\} \pmod{7}.$$
So, $x^2 \equiv -1 \pmod{7}$ has no solution.

2. For $p = 11$,
$$\{a^2 + 1\}_{a=1}^{5} = \{2, 5, 10, 16, 26\} \equiv \{2, 5, 10, 5, 4\} \pmod{11}.$$
So, $x^2 \equiv -1 \pmod{11}$ has no solution.

3. For $p = 13$,
$$\{a^2 + 1\}_{a=1}^{6} = \{2, 5, 10, 16, 26, 37\} \equiv \{2, 5, 10, 3, 0, 11\} \pmod{13}.$$
So, $x^2 \equiv -1 \pmod{13}$ has the solutions $x \equiv 5, 8$. These are also the only solutions (why?).

So we observe that $x^2 \equiv -1 \pmod{p}$ has solutions for some primes p, but not for the rest.

Question 5.3.1. *Prove that when it has a solution, it has exactly* 2.

Question 5.3.2. *Check that* $x^2 \equiv -1 \pmod{p}$ *has a solution when* $p = 17, 29$ *also. Check that there is no solution when* $p = 19, 23$.

Do you see a pattern? Can you now guess for which primes would it have a solution?

If you guessed it has a solution when $p \equiv 1 \pmod 4$ but does not have a solution when $p \equiv 3 \pmod 4$, then well done. In order to prove our conjecture, we would have to show two things: (1) there is no solution when $p \equiv 3 \pmod 4$, and (2) there is always a solution when $p \equiv 1 \pmod 4$.

Now, also note that any *odd* prime is either 1 (mod 4), or it is 3 (mod 4). Thus our conjecture is that $x^2 \equiv -1 \pmod p$ is equivalent to $p \equiv 1 \pmod 4$. I will spoil it for you, and tell you that this is true. This is often called Fermat's Christmas Theorem[1]:

Theorem 5.3.1 (Fermat's Christmas Theorem)**.** *Let p be a prime. Then there exists an x such that*

$$p \mid x^2 + 1$$

if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

Let's first prove that $p \mid x^2 + 1 \implies p \equiv 1 \pmod 4$, which isn't very hard.

Suppose there exists an x such that $p \mid x^2 + 1$, where $p > 2$. Then

$$\begin{aligned} & x^2 \equiv -1 \pmod p \\ \iff & (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod p \\ \iff & \underbrace{x^{p-1}}_{\equiv 1} \equiv (-1)^{\frac{p-1}{2}} \pmod p \end{aligned}$$

where we wrote $x^{p-1} \equiv 1 \pmod p$ using Fermat's Little Theorem (note that $x \not\equiv 0 \pmod p$, as we already rejected that case). This implies $\frac{p-1}{2}$ is even, which is the same as saying $p \equiv 1 \pmod 4$, as needed. So this part has been proven.

Question 5.3.3. *Where did we use $p > 2$?*

Now we just have to show that for any prime $p \equiv 1 \pmod 4$, there exists an x such that $p \mid x^2 + 1$. For this, we take the following x :

$$x = \left(\frac{p-1}{2}\right)!.$$

This works, since

$$\begin{aligned} x^2 &= \left(\frac{p-1}{2} \cdot \frac{p-3}{2} \dots 1\right) \cdot \left(\frac{p-1}{2} \cdot \frac{p-3}{2} \dots 1\right) \\ &\equiv \left(\frac{p-1}{2} \cdot \frac{p-3}{2} \dots 1\right) \cdot \left(\left(-\frac{p+1}{2}\right) \cdot \left(-\frac{p+3}{2}\right) \dots (-(p-1))\right) \\ &= (-1)^{\frac{p-1}{2}} (p-1)! \equiv -1 \pmod p \end{aligned}$$

by Wilson's Theorem. So, this is a valid construction.

[1] Actually this is not Fermat's Christmas Theorem, the real christmas theorem is Theorem 9.3.1. However in this book, we will use "The Christmas Theorem" for this theorem and "The Two Square Theorem" for Theorem 9.3.1.

Historical note: The proof to that result (two square theorem) was announced by Fermat in a letter to Marin Mersenne dated December 25, 1640, a Christmas Day. Hence the name.

Question 5.3.4. *Where did we use the fact that* $p \equiv 1 \pmod 4$?

Yes, I agree this is a magical construction. But if you keep Wilson's theorem in mind, it's not too hard to come up with. But now, we introduce some theory which would help us prove Theorem 5.3.1 much more naturally.

5.4 Orders

Consider a prime p. We know by Fermat's Little Theorem that $a^{p-1} \equiv 1 \pmod p$ for every $a \not\equiv 0 \pmod p$. Also, $a^{k(p-1)} \equiv 1$ for any k, i.e. a multiple of $(p-1)$ works too. However, does the converse hold? That is, should $a^X \equiv 1 \pmod p$ imply $X = (p-1)$ or a multiple of it?

The answer is no. For instance, when $p = 5$, we have $1^2 \equiv 1, 4^2 \equiv -1 \pmod 5$. However these are trivial examples, since $1^2, (-1)^2 = 1$ is always true (not just modulo p). Let me give you some better examples

$$2^3 \equiv 1 \pmod 7, \quad 3^5 \equiv 1 \pmod{11}, \quad 5^4 \equiv 1 \pmod{13}.$$

So we define something known as the order:

Definition 5.4.1. *Let p be a prime and $a \not\equiv 0 \pmod p$. Then the **order of** a **modulo** p is defined to be the smallest positive integer n such that $a^n \equiv 1 \pmod p$.*

We will denote it by $\text{ord}_p(a)$. Note that we take the order to be positive. It cannot be 0 (because that gives nothing useful).

Question 5.4.1. *Why does the order always exist for every a? That is, why can't we have an a with no finite number n with $a^n \equiv 1$?*

Let me give you a list of orders of a modulo 13 :

a	ord
1	1
2	12
3	3
4	6
5	4
6	12
7	12
8	4
9	3
10	6
11	12
12	2

One thing we can observe is that the order always divides 12.

We can clearly see that if $\text{ord}_p(a) \mid n$ for some n, then $a^n \equiv 1 \pmod p$. However, the converse is also true, which makes the order a very useful concept:

Theorem 5.4.1 (Fundamental Theorem of Orders)**.** *For a prime p and any integer $a \not\equiv 0 \pmod{p}$, we have*

$$a^n \equiv 1 \pmod{p} \iff \mathrm{ord}_p(a) \mid n.$$

Proof. One direction is simple. If $\mathrm{ord}_p(a) \mid n$, then $n = k \cdot \mathrm{ord}_p(a)$ for some k, so $a^n = \left(a^{\mathrm{ord}_p(a)}\right)^k \equiv 1^k \equiv 1 \pmod{p}$. The interesting part is the other direction.

Assume that $a^n \equiv 1 \pmod{p}$, however $\mathrm{ord}_p(a) \nmid n$. Write $n = \mathrm{ord}_p(a)k + r$, where $0 < r < \mathrm{ord}_p(a)$ (why not $0 \leq r$?). So

$$1 \equiv a^n \equiv a^{k \cdot \mathrm{ord}_p(a) + r} = \left(a^{\mathrm{ord}_p(a)}\right)^k \cdot a^r \equiv a^r \pmod{p}.$$

So, $a^r \equiv 1 \pmod{p}$. However, since $0 < r < \mathrm{ord}_p(a)$, we have a contradiction to the fact that $\mathrm{ord}_p(a)$ is the smallest positive integer satisfying $a^X \equiv 1 \pmod{p}$. □

Comment 5.4.1: The above proof is elegant, no doubt (and the same idea which occurred frequently in the first chapter). However another proof which is perhaps easier to come up with is:

$$a^n \equiv 1 \pmod{p} \quad \text{and} \quad a^{\mathrm{ord}_p(a)} \equiv 1 \pmod{p}.$$

So, by Example 2.12.1, we find $a^{\gcd(n, \mathrm{ord}_p(a))} \equiv 1 \pmod{p}$. But if $\mathrm{ord}_p(a) \nmid n$, we will have $\gcd(n, \mathrm{ord}_p(a)) < \mathrm{ord}_p(a)$ (why?), contradicting minimality. Hence, $\mathrm{ord}_p(a) \mid n$.

This gives us a characterization of ALL numbers n such that $a^n \equiv 1 \pmod{p}$! In particular, we have the following:

Corollary 5.4.1 (Order divides $(p-1)$)**.** *We have* $\mathrm{ord}_p(a) \mid p - 1$.

Question 5.4.2. *Prove the above using Fermat's Little Theorem.*

Now let's see the power of this. We have a direct proof of one direction of Theorem 5.3.1:

Proof. Suppose that $x^2 \equiv -1 \pmod{p}$. Then squaring gives $x^4 \equiv 1 \pmod{p}$. Hence, $\mathrm{ord}_p(x) \mid 4 \implies \mathrm{ord}_p(x) \in \{1, 2, 4\}$. Since $x^2 \equiv -1 \pmod{p}$, hence the first two aren't possible (why?). So $\mathrm{ord}_p(x) = 4$.

Hence, we find that $4 \mid p - 1$ by Corollary 5.4.1, which is what we wanted. □

Example 5.4.1 (Classic)

Find all n such that $n \mid 2^n - 1$.

Pick a prime p of n, so that $p \mid 2^n - 1$. Then $2^n \equiv 1 \pmod{p}$, so that $\mathrm{ord}_p(2) \mid n$. But also, $\mathrm{ord}_p(2) \mid p - 1$, hence $\mathrm{ord}_p(2)$ divides $\gcd(p - 1, n)$ (why?). So if we can select p such that we can control $\gcd(p - 1, n)$, then we are good to go.

The idea is this: $\gcd(p-1, n)$ is less than $p-1$, and a divisor of n. So any prime factor of this must be less than p. Hence, if we pick p to be the smallest prime factor of n, then $\gcd(p-1, n) = 1$ and so $\text{ord}_p(2)$ must equal 1 (why?). Hence, $p \mid 2^1 - 1 = 1$, which is impossible as p is a prime.

So is the answer no value of n? If we try $n = 1, 2, 3, \ldots$, then we observe $n = 1$ works.

Question 5.4.3. *Where did we miss the possibility of $n = 1$?*

So, $n = 1$ is the only solution to this equation.

Example 5.4.2

Prove that every prime divisor of $2^p - 1$ is greater than p.

Pick a prime divisor q of $2^p - 1$ (like in the previous problem, why must this have a prime divisor?). Then $2^p \equiv 1 \pmod{q}$ and so $\text{ord}_q(2) \mid p$. What do you notice here?

Yes, since p is a prime, hence $\text{ord}_q(2) \in \{1, p\}$. If $\text{ord}_q(2) = 1$, then $q \mid 2^1 - 1 = 1$, impossible. So $\text{ord}_q(2) = p$. So $p \mid q - 1$, which shows $p \leq q - 1 < q$. Hence we are done!

Example 5.4.3

Prove that any prime factor of $2^{2^n} + 1$ is congruent to 1 modulo 2^{n+1}.

Suppose $p \mid 2^{2^n} + 1$. Then $2^{2^n} \equiv -1 \pmod{p}$, which show $2^{2^{n+1}} \equiv 1 \pmod{p}$. Hence, $\text{ord}_p(2) \mid 2^{n+1}$. What more can we say about the order?

Suppose $\text{ord}_p(2) = 2^k$ with $k \leq n$, Then $2^{2^k} \equiv 1 \pmod{p}$, but since $k < n$, hence this shows $2^{2^n} \equiv 1 \pmod{p}$, which shows $p = 2$ (why?), which is impossible. Hence $\text{ord}_p(2)$ is in fact exactly equal to 2^{n+1} ! Hence, $2^{n+1} \mid p - 1$, which is what we wanted to prove.

5.5 Primitive Roots

Clearly we have seen examples for which the order is less than $p - 1$. The interesting case is when the order is $p - 1$. Suppose g has order $(p - 1)$ modulo p. This means that none of $\{g^1, g^2, g^3 \ldots g^{p-2}\}$ is 1. Further, this means that all these are distinct modulo p, since $g^i \equiv g^j \Leftrightarrow g^{i-j} \equiv 1 \pmod{p}$. However, $0 < i \neq j < p - 1$ implies $0 < i - j < p - 1$, which contradicts the fact that the order of g is $p - 1$. Thus, the powers of g *generate* all the (non-zero) remainders modulo p. Hence we call g a **generator**. Another common name is a **primitive root**. Before saying anything else, let's state the definition and our observation formally:

Definition 5.5.1. *Let p be a prime. Then a residue $g \neq 1$ is called a **primitive root mod p** if g has order $(p - 1)$ modulo p.*

Lemma 5.5.1 (Primitive Roots Generate all Non-zero Residues)**.** *Let g be a primitive root modulo p. Then*

$$\{g^1, g^2, g^3, \ldots, g^{p-1}\} \equiv \{1, 2, 3, \ldots, p - 1\} \pmod{p}.$$

Note that $g^x \equiv 1 \pmod{p}$ does imply $(p-1) \mid x$, unlike what we saw in the previous section.

Before we all fall in the flow of these and blindly start using them, here's a question we did not address: Does a primitive root always exist modulo p? Look at Table 5.4 and see if there exists a primitive root modulo 13.

Question 5.5.1. *List the orders of residues modulo* $7, 11, 17$ *and see if primitive roots exist in each case.*

As you may have guessed by solving the above question, there always does exist a primitive root modulo p. This is true, and it's a very strong result in itself:

Theorem 5.5.1 (Primitive Roots Always Exists modulo p)**.** *Let* $p > 2$ *be a prime. Then there always exists a primitive root modulo* p*.*

We omit the proof for now. This is not very easy to prove, however you can just state this on a contest without proof.

Primitive roots "generate" all the residue and give us a better control over the residues in many scenarios. Let's see it in action now.

Example 5.5.1 (Sum of Powers mod p)

Let $p > 2$ be a prime. Then for any integer x,

$$1^x + 2^x + \cdots + (p-1)^x \equiv \begin{cases} -1 & \text{if } p-1 \mid x \\ 0 & \text{otherwise} \end{cases} \pmod{p}.$$

If $x = 1$, then the left side is $p(p-1)/2$. Since $2 \mid (p-1)$, hence this is $p \times$ some integer and so $0 \pmod{p}$. Use the formula for sum of squares and sum of cubes to confirm the result for $x \in \{2, 3\}$.

But in general, we don't have a (nice) formula for sum of xth powers. So we try something else. We can use Lemma 5.5.1 to get

$$\begin{aligned} 1^x + 2^x + \cdots + (p-1)^x &\equiv g^x + g^{2x} + \cdots + g^{(p-1)x} \\ &= g^x \cdot \frac{g^{(p-1)x} - 1}{g^x - 1} \pmod{p}. \end{aligned}$$

This is true unless the denominator is $0 \pmod{p}$. That happens when $g^x \equiv 1 \pmod{p}$, which is the same as saying $(p-1) \mid x$. So excluding that possibility, $(g^x - 1)^{-1}$ exists and so the sum evaluates to

$$g^x \cdot \frac{g^{(p-1)x} - 1}{g^x - 1} = \frac{g^x}{g^x - 1} \cdot \left(\left(g^{p-1}\right)^x - 1\right) \equiv 0 \pmod{p}.$$

What about the case when $(p-1) \mid x$? Well, in that case Fermat's Little Theorem gives us $a^x \equiv 1 \pmod{p}$ so every term in the sum is 1, so the sum becomes $1+1+\cdots+1 = (p-1) \equiv -1 \pmod{p}$. So done!

This problem was very easy to do using primitive roots, however challenging to do otherwise. Further, this is a very very important result. Always keep this in mind when dealing with sums of powers. Also, this is an important result so remember this.

Problems for Practice

Problem 5.5.1. Let g be a primitive root modulo an odd prime p. If $p = 2m+1$, then show that

$$g^m \equiv -1 \pmod{p}.$$

Problem 5.5.2. Prove that if r is a primitive root modulo m, then so is the inverse of r modulo m.

Problem 5.5.3. Show that there are exactly $\varphi(p-1)$ primitive roots modulo p.

Problem 5.5.4. Show that for any prime p, the quadratic residues mod p are exactly the numbers $g^0, g^2, g^4, \ldots$ for a primitive roots g mod p.

5.6 Some more applications

Now let's see the power of this in proving the other direction of Theorem 5.3.1:

Proof. We want an x such that $x^2 \equiv -1 \pmod{p}$, if $p \equiv 1 \pmod{4}$ is a prime. Instead of finding x, we look for a y such that $(g^y)^2 \equiv -1 \pmod{p}$.

We can now guess a value of y; simply take $y = \frac{p-1}{4}$, since then $g^{2y} = g^{(p-1)/2} \equiv -1 \pmod{p}$ by Problem 5.5.1, and we are home free! □

Question 5.6.1. *Where was the fact that* $4 \mid p-1$ *used?*

Primitive roots are thus very useful in construction type problems too. Also, here's a lemma that you should keep an eye out since it helps to use Fermat's Christmas Theorem:

Lemma 5.6.1. *Let* $x \equiv 3 \pmod{4}$. *Then* x *has at least one prime divisor* $p \equiv 3 \pmod{4}$ *which has an odd exponent.*

Proof. Assume not. Then

$$x = p_1^{\alpha_1} \ldots p_k^{\alpha} \equiv 1 \pmod{4}$$

since $1^u \equiv 1$ and $3^{\text{even}} \equiv 1 \pmod{4}$. □

Example 5.6.1

Prove Wilson's Theorem.

Firstly, the case $p = 2$ is obvious. Now assume p is odd. Clearly we can use Lemma 5.5.1 to get:

$$\begin{aligned}(p-1)! &= (p-1)\cdot(p-2)\ldots 1\\ &\equiv g^1\cdot g^2\ldots g^{p-1}\\ &= g^{p(p-1)/2}\\ &= (g^{p-1/2})^p\\ &\equiv (-1)^p = -1 \pmod p.\end{aligned}$$

Where $g^{(p-1)/2} \equiv -1$ follows by Problem 5.5.1.

Problems for Practice

Problem 5.6.1 (Generating numbers with orders). Let p be a prime and d be any divisor of $p-1$. Show that there exists an integer a such that $\text{ord}_p(a) = d$.

5.7 General Orders and Primitive Roots

We have defined orders modulo a prime. However, they can easily be generalised to orders modulo any number.

Definition 5.7.1. *Let a, m be coprime integers. Then the order of a modulo m is the smallest integer $x > 0$ such that $a^x \equiv 1 \pmod m$.*

The theorem that $a^N \equiv 1 \pmod m$ implies $\text{ord}_m(a) \mid N$ also holds here, and the proof is analogous. In particular, we find that $\text{ord}_m(a) \mid \varphi(m)$.

Time for a very famous example

Example 5.7.1 (Saint Petersburg Mathematical Olympiad)

Prove that for all positive integers $a > 1$ and n we have $n \mid \varphi(a^n - 1)$

The φ function is not easy to deal with, especially $\varphi(a^n - 1)$. However, since we want $n \mid \varphi(a^n - 1)$, we could try to find a number which has order n modulo $a^n - 1$. The most logical guess is a. So if we can show $\text{ord}_{a^n-1}(a) = n$, we are done.

However, this is not too hard. It is easy to see that the smallest integer $d > 0$ such that $a^d \equiv 1 \pmod{a^n - 1}$ is n (why?), and so we are done! What an amazing application of orders.

Similarly, we can define primitive roots in general:

Definition 5.7.2. *A residue g is called a **primitive root modulo** m is the order of g modulo m is $\varphi(m)$.*

However, there is some restriction:

Theorem 5.7.1. *A primitive root modulo m exists if and only if $m \in \{2, 4, p^k, 2p^k\}$ for some integer k and some prime p.*

This means that if, for instance $m = 5^7$, then there does exist a primitive root modulo m. If $m = 2 \cdot 3 \cdot 5$, then there won't exist a primitive root modulo m. We again, omit the proof of this theorem.

The other properties are analogous. For instance, $\{g^1, g^2, \ldots, g^{\varphi(m)}\}$ is the set of residues that are coprime to m (this is the same set $\mathcal{S}$ we had in Theorem 2.9.1.)

Here's a simple problem:

Example 5.7.2

Suppose that m does not have a primitive root. Show that

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$$

for every a relatively prime to m.

The condition is weird, however, looking at the $\phi(m)$ we are obviously reminded of Euler's Totient Function. We have $a^{\varphi(m)} \equiv 1 \pmod{m}$. Hence, if $a^{\varphi(m)/2} = x \pmod{m}$, then $x^2 \equiv 1 \pmod{m}$, i.e.

$$m \mid \left(a^{\frac{\phi(m)}{2}} - 1\right)\left(a^{\frac{\phi(m)}{2}} + 1\right) = (x+1)(x-1).$$

At this point, we can now make more sense of the weird condition in the problem. Clearly if p were a prime, then the above would imply $m \mid (x-1)$ or $m \mid (x+1)$, the former being the one we would want.

Now if $m = xy$ with x, y coprime and $x, y > 2$, then

$$a^{\frac{\varphi(m)}{2}} = a^{\varphi(x)\cdot\frac{\varphi(y)}{2}} \equiv 1 \pmod{x}.$$

Similarly it is $\equiv 1 \pmod{y}$. Combining, we get $a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{xy}$. The case $m = 2^k$ with $k > 2$ is left to reader.

Problems for Practice

Problem 5.7.1. Complete the proof above.

Problem 5.7.2. Show that there are $\varphi(\varphi(n))$ primitive roots.

5.8 Example Problems

Our first example is a long one, although there aren't a lot of clever steps involved. It's straightforward in the sense that each step gives a conclusion, and that conclusion gives the next step, eventually leading us to a solution. However, this is an instructive problem and an excellent practice for using orders.

Example 5.8.1 (USA TST 2003)

Find all ordered prime triples (p, q, r) such that $p \mid q^r + 1, q \mid r^p + 1$, and $r \mid p^q + 1$.

First of all, let's analyze only the condition $p \mid q^r + 1$ (since the others are symmetric). Now, this gives $q^r \equiv -1 \pmod{p}$. Hence, $q^{2r} \equiv 1 \pmod{p}$ and so $\text{ord}_p(q) \mid 2r$. Since r is a prime, hence $\text{ord}_p(q) \in \{1, 2, r, 2r\}$. Not too shabby. Let's deal with each case properly:

1. Suppose $\text{ord}_p(q) = 1$. Then $p \mid q - 1$. However, then $q^r \equiv 1 \pmod{p}$ combined with $p \mid q^r + 1$ implies $1 \equiv -1 \pmod{p}$, i.e. $p = 2$.

2. Suppose $\text{ord}_p(q) = 2$. Then $p \mid q^2 - 1 = (q-1)(q+1)$. As before $p \mid q - 1$ is impossible (unless $p = 2$). So $p \mid q + 1$.

3. Suppose $\text{ord}_p(q) = r$. Then $q^r \equiv 1 \pmod{p}$. This as before implies $p = 2$ (why?)

4. Suppose $\text{ord}_p(q) = 2r$. Then $2r \mid p - 1$. In particular, p is an odd prime and $r \mid p - 1$.

The rest of the problem is smart casework now. For now, suppose all p, q, r are odd. So, we have obtained the following result:

Lemma 5.8.1. *For odd primes x, y, z,*

$$x \mid y^z - 1 \implies \begin{cases} \text{ord}_x(y) = 2 \implies x \mid y + 1 \\ \text{ord}_x(y) = 2z \implies 2z \mid x - 1 \end{cases}$$

Suppose $\text{ord}_p(q) = 2r$, which gives $r \mid p - 1$. This means $r \mid p^q - 1$ (why?). However, then $r \mid p^q + 1$ is impossible, since r is odd. Similarly, $\text{ord}_q(r) = 2p$ of $\text{ord}_r(p) = 2q$ are not possible.

So $\text{ord}_p(q), \text{ord}_q(r), \text{ord}_r(p) = 2$ implying $p \mid q+1, q \mid r+1, r \mid p+1$. However, this doesn't feel to be possible for primes, because the chain seems to be "too close". This intuition is formalized by using inequalities, since these three give $p \leq q + 1, q \leq r + 1, r \leq p + 1$ and we can't find such primes.

At the end of all this discussion, we can conclude that our assumption that p, q, r are all odd gives no solution. So, one of p, q, r is even, say $p = 2$. Then $2 \mid q^r + 1$ implies q is odd (and nothing more, so this condition is useless now, i.e. we can't extract anymore information from here). Also, $q \mid r^2 + 1$ implies $\text{ord}_q(r) = 4$ (why?) implying $4 \mid q - 1$. Lastly $r \mid 2^q + 1$ implies r is odd. So using the lemma we obtain either $r \mid 2 + 1 = 3$, or $2q \mid r + 1$.

If $r = 3$, then $q \mid 3^2 + 1 = 10$ and so $q = 5$ (since we obtained q is odd). If $2q \mid r + 1$, then we try to combine it with $q \mid r^2 + 1$. We get $q \mid r + 1, r^2 + 1$ which implies $q \mid r^2 + 1 - (r + 1)(r - 1) = 2$, which is again impossible since q was odd. So if $p = 2$, then $(r, q) = (3, 5)$. Similarly we have two more solutions for the cases when $q = 2$ or $r = 2$. Hence the solutions are:

$$(p, q, r) = (2, 5, 3), (3, 2, 5), (5, 3, 2).$$

Example 5.8.2 (Schinzel)

Find all integers $n \geq 1$ such that n divides $2^{n-1} + 1$

This has a very short solution, however is hard to come up with. Assume on the contrary that for some $n > 1$ we have $n|2^{n-1} + 1$. Let $p_1 < p_2 < \cdots < p_k$ be the prime divisors of n. Write $p_i = 2^{r_i} m_i + 1$ with m_i odd for all $1 \leq i \leq k$. Let $t = r_j$ be the minimum of all r_i. The advantage of doing this is

$$n = \prod_i (2^{r_i} m_i + 1) \equiv 1 \pmod{2^t}.$$

So we can write $n = 2^t m + 1$ with m odd. Since $p_j = 2^t m_j + 1$, hence

$$-1 \equiv (-1)^{m_j} \equiv \left(2^{n-1}\right)^{m_j} = 2^{(2^t m) m_j} \equiv \left(2^{2^t m_j}\right)^m \equiv \left(2^{p_j - 1}\right)^m \equiv 1 \pmod{p_j}.$$

Hence $p_j = 2$, which is clearly impossible.

Example 5.8.3 (Chinese TST 2005)

Prove that for any $n > 2$, the greatest prime factor of $2^{2^n} + 1$ is greater than or equal to $n \cdot 2^{n+2} + 1$.

This problem, just like the previous one, is tricky despite having a simple solutions. In fact our solution will prove a stronger bound (try to point out how and where). Suppose $2^{2^n} + 1 = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. Now a standard order argument shows $p_i \equiv 1 \pmod{2^{n+1}}$ (we saw this in Example 5.4.3).

Hence write $p_i = 2^{n+1} x_i + 1$ for each i. Now firstly since $p_i \geq 2^{n+1} + 1$, hence

$$2^{2^n} + 1 \geq (2^{n+1} + 1)^{\alpha_1 + \cdots + \alpha_k} > 2^{(n+1)(\alpha_1 + \cdots + \alpha_k)}.$$

Hence, $\alpha_1 + \cdots + \alpha_k < \frac{2^n}{n+1}$.

Now if we can show $x_i \geq 2(n + 1)$ for some i, then we are done. For this, it is enough to show that $x_i(\alpha_1 + \cdots + \alpha_k) \geq 2^{n+1}$. How do we get terms of the form $x_i \alpha_i$? The answer is binomial theorem. We get the following:

$$p_i^{\alpha_i} = (2^{n+1} x_i + 1)^{\alpha_i} \equiv 2^{n+1} \alpha_i x_i + 1 \pmod{2^{2n+2}}.$$

(since $2^n \geq 2n+2$ for $n \geq 3$. The cases $n \leq 2$ can be checked manually). Thus

$$2^{2^n} = \prod p_i^{\alpha_i} \equiv (2^{n+1}\alpha_i x_i + 1) \pmod{2^{2n+2}}$$

and so $2^{n+1}(x_1\alpha_1 + \cdots + x_k\alpha_k) \equiv 0 \pmod{2^{2n+2}}$. So if x_r is the largest from all of x_i, then

$$x_r(\alpha_1 + \cdots + \alpha_k) \geq x_1\alpha_1 + \cdots + x_k\alpha_k \geq 2^{n+1}$$

which gives the desired bound.

Lastly, we (again) conclude with a problem which is intertwined between Number Theory and Combinatorics:

Example 5.8.4 (ELMO 2010/5)

2010 MOPpers are assigned numbers 1 through 2010. Each one is given a red slip and a blue slip of paper. Two positive integers, A and B, each less than or equal to 2010 are chosen. On the red slip of paper, each MOPper writes the remainder when the product of A and his or her number is divided by 2011. On the blue slip of paper, he or she writes the remainder when the product of B and his or her number is divided by 2011. The MOPpers may then perform either of the following two operations:

1. Each MOPper gives his or her red slip to the MOPper whose number is written on his or her blue slip.
2. Each MOPper gives his or her blue slip to the MOPper whose number is written on his or her red slip.

Show that it is always possible to perform some number of these operations such that each MOPper is holding a red slip with his or her number written on it.

We generalize the result by replacing 2011 by p for any odd prime p. It is best done by experimenting yourself, so do that before reading the solution. Firstly, we define a few terms for convenience:

1. Let M denote the ordered set $\{1, 2, \cdots p-1\}$. For any real constant $0 < c < p$, define $cM := \{c, 2c, \cdots c(p-1)\}$. Note that cM is a complete residue class modulo p. But for any two $0 < a \neq b < p$, the sequences aM, bM are different permutations of M.
2. Call a permutation π of M *good* if there exists a constant C such that $\pi(M) = CM$. (Note that not every permutation of M is *good*.)
3. Next, if we perform the first move (Each MOPper gives his or her red slip to the MOPper whose number is written on his or her blue slip), then say that we *fix* blue and *move* red. Similar terms exist for the second move.

We have the following claim:

Claim. *At any moment, if we have two good permutations, then fixing any one of them and moving the other will also result in a good permutation.*

Proof. Let's suppose the permutations are xM, yM. Suppose we fix yM and move xM. Then, by definition, the number k at the ith spot in xM will move to jth spot, where j is the number written at the ith spot in yM.

But clearly $j \equiv i \cdot y \pmod{p}$ and $k = i \cdot x \pmod{p}$. Hence the new number at the jth spot is $k = x \cdot i = x \cdot (jy^{-1}) = j \cdot (xy^{-1})$. Hence if set $t = xy^{-1}$, then $k = tj$ is the new number at the jth spot.

Hence, the new sequence obtained is tM, which is clearly *good*. □

Also, as proved above, if we have the sequences xM, yM, then we can get to $(x \cdot y^{-1})M$ in the next move by fixing yM.

Claim. *Let g be a primitive root modulo p. Then from the original sequences AM, BM, we can get to BM, gM.*

Proof. Set $A = g^k$ and $B = g^\ell$. Let $gcd(k-1, \ell) = d$ and write $\ell = d\ell'$ and $p - 1 = dz$.

Then consider the following moves by fixing BM:

$$A = g^k \mapsto g^k \cdot g^{-l} \mapsto g^k \cdot g^{-2\ell} \cdots g^k \cdot g^{-dz\ell'}$$

Here, since $g^{-dz\ell'} = \left(g^{p-1}\right)^{\ell'} \equiv g^{\ell'}$, hence we have obtained the sequence $(g^k \cdot g^{\ell'})M$.

By repeating this process, we can further reduce ℓ' to $\frac{\ell'}{gcd(p-1,\ell')}$ and so on until we get reach a number L such that $gcd(L, p-1) = 1$.

Then again by fixing BM, we can get to $g^k \cdot g^{-L}, \cdots g^k \cdot g^{-Ln} \equiv g$, where $k - Ln \equiv 1$ modulo $p-1$ (note that this number n exists since $gcd(L, p-1) = 1$). Hence we have reached gM without disturbing B and we are done. □

To finish it, we have the two sequences BM, gM. Now fix BM and perform moves to get these $p-1$ sequences: $BM, (Bg^{-1})M, (Bg^{-2})M \cdots (Bg^{-(p-1)})M$.

Note that $\{B, Bg^{-1}, Bg^{-2}, \cdots Bg^{-(p-1)}\}$ forms a complete residue class modulo p, hence there will exist the sequence $1M$ in the sequences listed above, and we are done.

5.9 Practice Problems

Problem 5.9.1. Find all n such that $3^n + 1$ is divisibly by n^2.

Problem 5.9.2. Show than any prime factor q of $p^p - 1$ is $\equiv 1 \pmod{p}$.

Problem 5.9.3 (Fermat). Let $p > 3$ be a prime. Prove that any positive divisor of $\frac{2^p+1}{3}$ is of the form $2kp + 1$.

Problem 5.9.4 (IMO Shortlist 2006 N2). For $x \in (0, 1)$ let $y \in (0, 1)$ be the number whose n-th digit after the decimal point is the 2^n-th digit after the decimal point of x. Show that if x is rational then so is y.

Problem 5.9.5. Suppose that $k \geq 2$ and $n_1, n_2, \cdots, n_k \geq 1$ be natural numbers having the property

$$n_2 \mid 2^{n_1} - 1, n_3 \mid 2^{n_2} - 1, \cdots, n_k \mid 2^{n_{k-1}} - 1, n_1 \mid 2^{n_k} - 1.$$

Show that $n_1 = n_2 = \cdots = n_k = 1$. **Hints:** 408 16

Problem 5.9.6 (Iran 3rd round 2017 Numbers theory final exam P1). Let x and y be integers and let p be a prime number. Suppose that there exist relatively prime positive integers m and n such that

$$x^m \equiv y^n \pmod{p}$$

Prove that there exists an unique integer z modulo p such that

$$x \equiv z^n \pmod{p} \quad \text{and} \quad y \equiv z^m \pmod{p}.$$

Hints: 193

Problem 5.9.7 (China TST 2006). Find all positive integers a and n such that

$$\frac{(a+1)^n - a^n}{n}$$

is an integer. **Hints:** 415

Problem 5.9.8. Let g be a Fibonacci primitive root $\pmod{p}$. i.e. g is a primitive root $\pmod{p}$ satisfying $g^2 \equiv g + 1 \pmod{p}$. Prove that

1. $g - 1$ is also a primitive root $\pmod{p}$.
2. Show that if $p \equiv 3 \pmod{4}$, then $g - 2$ is also a primitive root $\pmod{p}$.

Hints: 219 354

Problem 5.9.9 (PUTNAM 1976 B6). Prove that if n is an integer such that $\sigma(n) = 2n + 1$, then n is the square of an odd integer. **Hints:** 106 86 388 278

Problem 5.9.10 (China 2009). Find all prime numbers p, q such that $pq \mid 5^p + 5^q$. **Hints:** 163 476 176 88

Problem 5.9.11. Suppose that $p > 3$ is prime. Prove that the products of the primitive roots of p between 1 and $p-1$ is congruent to 1 modulo p. **Hints:** 50 461

Problem 5.9.12 (Bulgaria National Olympiad). Find all positive integers m and n such that

$$\left(2^{2^m}+1\right)\left(2^{2^n}+1\right)$$

is divisible by mn. **Hints:** 322

Problem 5.9.13. Determine all the pairs (p, n) of a prime number p and a positive integer n for which

$$\frac{n^p+1}{p^n+1} \in \mathbb{Z}.$$

Hints: 141 396

Problem 5.9.14 (Iran MO 3rd round 2016 finals Number Theory P1). Let p and q be prime numbers (q is odd). Prove that there exists an integer x such that

$$q \mid (x+1)^p - x^p$$

if and only if

$$q \equiv 1 \pmod{p}.$$

Hints: 331 320 56 **Sol:** pg. 290

Problem 5.9.15 (China TST 4 2018 Day 2 Q4). Let p be a prime and k be a positive integer. Set S contains all positive integers a satisfying $1 \le a \le p-1$, and there exists positive integer x such that $x^k \equiv a \pmod{p}$.

Suppose that $3 \le |S| \le p-2$. Prove that the elements of S, when arranged in increasing order, does not form an arithmetic progression. **Hints:** 257 179

Problem 5.9.16 (IMO Shortlist 1998 N5). Determine all positive integers n for which there exists an integer m such that $2^n - 1$ is a divisor of $m^2 + 9$. **Hints:** 102 368 143 183

Problem 5.9.17 (USA TST for EGMO 2019, Problem 3). Let n be a positive integer such that the number

$$\frac{1^k + 2^k + \cdots + n^k}{n}$$

is an integer for any $k \in \{1, 2, \ldots, 99\}$. Prove that n has no divisors between 2 and 100, inclusive. **Hints:** 28 338 376 387 335 **Sol:** pg. 291

Problem 5.9.18 (IMO Shortlist 2014 N6). Let $a_1 < a_2 < \cdots < a_n$ be pairwise coprime positive integers with a_1 being prime and $a_1 \ge n+2$. On the segment $I = [0, a_1 a_2 \cdots a_n]$ of

the real line, mark all integers that are divisible by at least one of the numbers $a_1, \ldots, a_n$. These points split I into a number of smaller segments. Prove that the sum of the squares of the lengths of these segments is divisible by a_1. **Hints:** 375 170 256 26 4 242 222 62 **Sol:** pg. 291

✠ Identical Polynomials in $\mathbb{F}_p[X]$

By $\mathbb{F}_p[X]$, we denote the set of polynomials with coefficients modulo p. The key idea here is that X has no meaning of its own, i.e. it is just a way to write the polynomial. The coefficients are the ones that interest us (just like in generating functions). We say that X is just a "formal variable" here.

So, if we are given two polynomials f, g, then we could have $f = g$ in $\mathbb{F}_p$, or we could have $f = g$ in $\mathbb{F}_p[X]$, and these are two different things. For example, $f = g$ in $\mathbb{F}_p$ means $f(x) \equiv g(x) \pmod{p}$ for all values of $x \in \mathbb{F}_p$. For instance, $x^p \equiv x \pmod{p}$ is true by Fermat's little Theorem, and so x^p, x are the same in $\mathbb{F}_p$.

In $\mathbb{F}_p[X]$, we need to look at the coefficients only. So x^2+5x+2, x^2+2x+2 and x^2-x-1 are all the same in $\mathbb{F}_3[X]$. Also, $x^p \neq x$ in $\mathbb{F}_p[X]$ (since one has degree p and the other has degree 1). So, $f = g$ in $\mathbb{F}_p$ means they are equal value-wise (modulo p), but $f = g$ in $\mathbb{F}_p[X]$ means they are the same polynomials (coefficients modulo p).

Problem 5.9.19. Show that if $f = g$ in $\mathbb{F}_p[X]$, then $f = g$ in $\mathbb{F}_p$ holds too.

Comment 5.9.1: We often use $f \equiv g$ to denote they are identical polynomials. So if f, g are polynomials in $\mathbb{F}_p[X]$, then $f \equiv g$ would mean the coefficients are same modulo p.

Now that you have understood this, we can discuss the following:

Freshman's Dream

We stated and proved Freshman's dream in Example 2.12.3, where we said $(a+b)^p \equiv a^p + b^p \pmod{p}$. There's a more useful way of writing this:

$$(X+1)^p \equiv X^p + 1 \pmod{p}$$

for any X (I think you can see where I am going with this). So we know that the polynomials $(X+1)^p$ and X^p+1 are equal in $\mathbb{F}_p$. However, this is stupid, since Fermat's Little Theorem gives $(X+1)^p \equiv X+1 \equiv X^p+1 \pmod{p}$ anyway. So why is this any useful?

Here's the reason. Go back and take a look at the proof we had given while discussing this originally in Example 2.12.3. If we write the proof here again, then it's

$$(X+1)^p = X^p + \binom{p}{1}X^{p-1} + \binom{p}{2}X^{p-1} + \cdots + \binom{p}{p-1}X + 1 \equiv X^p + 1 \pmod{p}.$$

The fact used here in the proof treats X as a formal variable and doesn't need it's value, and we only worked with coefficients! What this means is the stronger fact that $(X+1)^p$ and X^p+1 are equal polynomials in $\mathbb{F}_p[X]$ (why is this stronger?). So, we have the following:

Theorem 5.9.1 (Freshman's Dream)**.** *For any prime p, we have*

$$(X+1)^p \equiv X^p + 1$$

in $\mathbb{F}_p[X]$. We can generalize this to

$$(X+1)^{p^i} \equiv X^{p^i} + 1$$

in $\mathbb{F}_p[X]$.

This is very useful, much more useful than the earlier Freshman's dream (which followed from Fermat's Little Theorem directly). Let's see an application, which we had promised earlier:

Proof of Lucas's Theorem

Before we skip to the general proof, it is better to work with an example first. Suppose $n = 66$ and $m = 13$. Also, let $p = 5$. Write $n = 231_{(3)}$ and $m = 23_{(3)}$. The key idea again is to use generating functions since it covers all the coefficients at once. So

$$\begin{aligned}(X+1)^{66} &= (X+1)^{2\cdot 5^2 + 3\cdot 5^1 + 1\cdot 5^0} \\ &= \left((X+1)^{5^2}\right)^2 \left((X+1)^{5^1}\right)^3 \left((X+1)^{5^0}\right)^1 \\ &\equiv \left(X^{5^2}+1\right)^2 \left(X^{5^1}+1\right)^3 \left(X^{5^0}+1\right)^1,\end{aligned}$$

where the last equality is in $\mathbb{F}_5[X]$. Further, this equals

$$= \left(\binom{2}{0}X^{2\cdot 5^2} + \binom{2}{1}X^{1\cdot 5^2} + \binom{2}{2}X^{0\cdot 5^2}\right)\left(\binom{3}{0}X^{3\cdot 5^1} + \binom{3}{1}X^{2\cdot 5^1} + \binom{3}{2}X^{1\cdot 5^1} + \binom{3}{3}X^{0\cdot 5^1}\right)\left(\binom{1}{0}X^{1\cdot 5^0} + \binom{1}{1}X^{0\cdot 5^0}\right).$$

We want the coefficient of X^{13} here (why?). Note that each exponent is of the form $X^{a\cdot 5^b}$. So, on multiplying out all the brackets, the power of X would be something of the form $a_1 5^{b_1} + a_2 5^{b_2} + \ldots$, so a base 5 number. Since $13 = 0\cdot 5^2 + 2\cdot 5^1 + 3\cdot 5^0$, hence we have to choose the right terms from each bracket. Doing this, we would get

$$\binom{66}{13} \equiv \binom{2}{2}\binom{3}{1}\binom{1}{3} \pmod 5$$

(note that we chose $\binom{1}{3}$ from the third bracket since there weren't enough terms). So, we proved Lucas's theorem for this case. Let's look at the general case now.

Write

$$n = n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0$$

and

$$m = m_k p^k + m_{k-1}p^{k-1} + \cdots + m_1 p + m_0$$

as the base p expansions of m and n respectively. Then (we work in $\mathbb{F}_p[X]$)

$$\begin{aligned}\sum_{0\leq m\leq n}\binom{n}{m}X^m &= (X+1)^n \\ &= (X+1)^{n_kp^k+n_{k-1}p^{k-1}+\cdots+n_0} \\ &= \prod_{i=0}^{k}\left((X+1)^{p^i}\right)^{n_i}\end{aligned}$$

Now, we use Freshman's dream on each bracket to get

$$\begin{aligned}&\equiv \prod_{i=0}^{k}\left(X^{p^i}+1\right)^{n_i} \\ &= \prod_{i=0}^{k}\sum_{m_i=0}^{n_i}\binom{n_i}{m_i}X^{p^im_i}.\end{aligned}$$

At this point, note that we can change the upper index of the sum to $(p-1)$ since $\binom{x}{y}=0$ if $y>x$ (why must we do this? Look back at our proof for the $n=66$ example and point out where we did this). Then, to obtain the coefficient of X^m, we collect the right terms from each sum to multiply so that we get $m=m_kp^k+m_{k-1}p^{k-1}+\cdots+m_1p+m_0$ (we can do this since the base p representation of m is unique). So we write

$$\begin{aligned}&= \prod_{i=0}^{k}\sum_{m_i=0}^{p-1}\binom{n_i}{m_i}X^{p^im_i}. \\ &= \sum_{m=1}^{n}\prod_{i=0}^{k}\binom{n_i}{m_i}X^m.\end{aligned}$$

And so, by comparing the coefficients of X^m on both the sides, we are done!

We can nicely summarize this as:

$$\begin{aligned}\sum_{0\leq m\leq n}\binom{n}{m}X^m &= (X+1)^n = (X+1)^{n_kp^k+n_{k-1}p^{k-1}+\cdots+n_0} \\ &= \prod_{i=0}^{k}\left((X+1)^{p^i}\right)^{n_i} \equiv \prod_{i=0}^{k}\left(X^{p^i}+1\right)^{n_i} \\ &= \prod_{i=0}^{k}\sum_{m_i=0}^{n_i}\binom{n_i}{m_i}X^{p^im_i} = \prod_{i=0}^{k}\sum_{m_i=0}^{p-1}\binom{n_i}{m_i}X^{p^im_i}. \\ &= \sum_{m=1}^{n}\prod_{i=0}^{k}\binom{n_i}{m_i}X^m.\end{aligned}$$

Lagrange's Theorem

Define the polynomials $f, g \in \mathbb{F}_p[X]$ by

$$f(x) = x^p - x, g(x) = x(x-1)(x-2)\dots(x-(p-1)).$$

We saw in Example 2.12.4 that $f(x)$ and $g(x)$ are equal in $\mathbb{F}_p$, i.e. always give the same value modulo p. The question we promised to answer was if they are equal as polynomials too, i.e., equal in $\mathbb{F}_p[X]$.

Turns out the answer is yes, and it goes by the name Lagrange's Theorem.

Theorem 5.9.2 (Lagrange's Theorem)**.** *Let p be a prime. Then the polynomials*

$$x^p - x \equiv x(x-1)\dots(x-(p-1))$$

holds in $\mathbb{F}_p[X]$.

The sharp-eyed reader might say that this follows by the factor theorem; i.e., $f(x)$ has the roots $0, 1, 2, \dots, p-1$ in $\mathbb{F}_p$ and is monic, so $f(x) = x(x-1)\dots(x-(p-1))$ in $\mathbb{F}_p[X]$. This is a perfect argument, however as a technical issue: we know that the factor theorem holds in $\mathbb{C}[X]$. Does it also hold in $\mathbb{F}_p[X]$?

The answer is yes, and it depends on two key properties of $\mathbb{F}_p[X]$ which distinguishes it from other sets that don't have factor theorem:

1. If $fg = 0$ for two polynomials $f, g \in \mathbb{F}_p[X]$, then one of f, g must be 0.
2. Euclid's Division Algorithm holds in $\mathbb{F}_p[X]$ (see Comment 7.1.3.)

A number a is called a **zero divisor** if there is a non-zero number x such that $ax = 0$. Hence, the first property says that $\mathbb{F}_p[X]$ has no zero divisors. In fact, for this to hold, the hypothesis that p is a prime is essential. For instance, $2 \cdot 5 \equiv 0 \pmod{10}$ even though both are non-zero in $\mathbb{Z}/10\mathbb{Z}$.

The second property says that if $f, g \in \mathbb{F}_p[X]$ are two polynomials, then there exist polynomials $q, r \in \mathbb{F}_p[X]$ such that

$$f(x) = g(x)q(x) + r(x), \quad \deg r < \deg q.$$

We need to take some care with deg here. For instance, $\deg(5x^2+2x+1) = 1$ in $\mathbb{F}_5[X]$ since $5x^2$ is just 0 in $\mathbb{F}_5[X]$. However, $\deg(5x^2 + 2x + 1) = 2$ in $\mathbb{F}_2[X]$.

Question 5.9.1. *Convince yourself that Euclid's algorithm holds in $\mathbb{F}_p[X]$. Take a few examples, if needed (hint: polynomial division, see Comment 7.1.3.)*

Now, we can prove the factor theorem:

Theorem 5.9.3 (Factor Theorem)**.** *Let $f \in \mathbb{F}_p[X]$ have n distinct roots $x_1, \dots, x_m$, where $\deg f = n$. Then there exists a polynomial $g(x)$ such that $\deg g = n - m$ and*

$$f(x) = (x - x_1)\dots(x - x_m)g(x)$$

holds identically in $\mathbb{F}_p[X]$.

Proof. Say f is non-constant (else there is nothing to prove). Write

$$f(x) = (x - x_1)q(x) + r(x).$$

Since $\deg r < \deg(x - x_1)$, hence r must be a constant. Further, $f(x_1) = 0$ implies $r = 0$ in $\mathbb{F}_p$. If $n = 1$, then we are done. Otherwise there is a second root x_2. Then $f(x_2) = 0$ implies $(x_2 - x_1)q(x_2) = 0$ in $\mathbb{F}_p[X]$. We have seen earlier that this means either $x_2 - x_1 = 0$, or $q(x_2) = 0$. The first one is not possible (since we assume roots to be distinct.) Hence $q(x_2) = 0$. Now since $\deg q < \deg f$, hence we can finish by induction now. □

Question 5.9.2. *In $\mathbb{Z}/6\mathbb{Z}[X]$, consider $x^2 - 5x$. It has the roots $x = 0, 2, 3, 5$. However, $x^2 - 5x \neq (x - 0)(x - 2)(x - 3)(x - 5)$ for degree reasons. Why do we face this issue here?*

Hence, we have the following corollary (by looking at the degree)

Corollary 5.9.1. *Let $f \in \mathbb{F}_p[X]$ have n distinct roots $x_1, \ldots, x_n$, where $\deg f = n$. Let $c \neq 0$ be the leading coefficient of f. Then*

$$f(x) = c(x - x_1) \ldots (x - x_n)$$

holds identically in $\mathbb{F}_p[X]$.

This corollary proves Lagrange's theorem. Lagrange's theorem has many amazing applications. For instance:

Problem 5.9.20. Prove Wilson's Theorem by comparing coefficients.

Problem 5.9.21. Using Newton's sum identities, prove the result in Example 5.5.1.

Roots of Polynomials in $\mathbb{F}_p[X]$

Now that we are discussing polynomials and their roots, let's talk about them properly. A natural question is how many roots does a polynomial have mod m? If $\deg f = d$, then does it have d roots (like polynomials in $\mathbb{C}[X]$)? Turns out the answer isn't very simple. Consider the following two polynomials:

$$f(x) = x^p - x + 1 \in \mathbb{F}_p[X], \quad g(x) = x^2 - 5x \in \mathbb{Z}/6\mathbb{Z}[X], \quad h(x) = 5x^2 + 10x \in \mathbb{F}_5[X].$$

In the first example, we see that modulo p, the polynomial has 0 roots (why?) despite having degree p. In the second example (which we have seen before), we find 4 roots modulo 6, which is more than the degree. In the last example, we see that every number is a root of the polynomial. So is there any good result?

The answer is yes, but only when m is a prime. We have the following analogue of the Fundamental Theorem of Algebra (before presenting it, recall that if $\deg f = n$ for a polynomial $f \in \mathbb{F}_p[X]$, then the coefficient of x^n is not 0 in $\mathbb{F}_p$, i.e. not divisible by p. So the degree of $h(x)$ above is not defined).

Theorem 5.9.4 (Lagrange's Theorem)**.** *Let $f \in \mathbb{F}_p[X]$ be a polynomial with $\deg f = n$. Then, f has at most n distinct roots in $\mathbb{F}_p$.*

One proof directly follows from the factor theorem above. We present a second proof:

Proof. We prove this by induction on $\deg f$. The base case is clear, so suppose we have the result till some $\deg f = k-1$. Now consider a polynomial f of degree k, and suppose it has more than k roots mod p, say $x_1, \ldots, x_\ell$ with $\ell > k$. Let $c \neq 0$ be the leading coefficient of f. Then define

$$g(x) = f(x) - c(x - x_1)\ldots(x - x_k).$$

Now if $\deg g$ is not identically 0 in $\mathbb{F}_p[X]$, then $\deg g < k$ and hence it has at most $\deg g < k$ roots by the induction hypothesis. However, $x_1, \ldots, x_k$ are all its roots, and we have a contradiction.

So it must be identically zero in $\mathbb{F}_p[X]$. However, this is impossible as $\deg f > k = \deg\left(c(x - x_1)\ldots(x - x_k)\right)$, and so we are done. □

This gives the following important corollary:

Corollary 5.9.2. *Let $f \in \mathbb{F}_p[X]$ be a polynomial with more than $\deg f$ roots. Then f is identically zero in $\mathbb{F}_p[X]$.*

When does a polynomial have exactly $\deg f$ roots? The answer to this question is in the following theorem:

Theorem 5.9.5. *Let $f \in \mathbb{F}_p[X]$ be a polynomial. Then f has exactly $\deg f$ roots if and only if $f(x)$ divides $x^p - x$.*

Proof. Suppose f has $\deg f$ roots. Write $x^p - x = f(x)q(x) + r(x)$ with $\deg r < \deg f$. Now since each root of f is also a root of $x^p - x$, we find that $r(x) = 0$ for $\deg f$ values. However, since $\deg f > \deg r$, hence by Corollary 5.9.2 we find $r \equiv 0$, and so $f(x) \mid x^p - x$.

Conversely, suppose $f(x)$ divides $x^p - x$. Write $x^p - x = f(x)q(x) + pr(x)$ in $\mathbb{Z}[X]$. Here, $\deg f = n$ and $\deg g = p - n$, and so by Theorem 5.9.4, f has at most n roots, and g has at most $p - n$ roots, implying that $f(x)g(x)$ has at most $n + (p - n) = p$ roots. However, we see that for all p numbers in $\mathbb{F}_p$, $x^p - x$ vanishes. Hence, $f(x)g(x) = 0$ for all $x \in \mathbb{F}_p$. Thus, equality holds above, showing that f has n roots. □

Chapter 6

Largest Exponent

This chapter is based on the whole idea of looking at prime factors to think of a number, an idea we hinted to in the first chapter.

Definition 6.0.1. *Let p be a prime and n be an integer. Then the **p-adic valuation** or **p-adic order** of n is defined to be the largest integer t such that $p^t \mid n$.*

The are two[1] common notations for this. The one we will use is $\nu_p(n)$.

So, $\nu_2(48) = 4$ and $\nu_5(10) = 1$. We can also have $\nu_p = 0$, for instance $\nu_2(3) = 0$. By convention, we set $\nu_p(0) = +\infty$. Thus, if we let $2 = p_1 < p_2 < p_3 < \dots$ be all the primes, then we can write any integer n as

$$n = \prod_{i \geq 0} p_i^{\nu_{p_i}(n)} = p_1^{\nu_{p_1}(n)} p_1^{\nu_{p_1}(n)} \dots .$$

For instance $36 = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^0 \dots$. Let's now present one property which is going to be most important result related to ν_p :

Lemma 6.0.1 (Divisibility)**.** *Let x, y be integers. Then*

$$x \mid y \iff \nu_p(x) \leq \nu_p(y) \quad \textit{for all primes } p.$$

As a corollary, $x = y$ if and only if $\nu_p(x) = \nu_p(y)$ for all primes p.

The key part here is that we must have $\nu_p(x) \leq \nu_p(y)$ for **all primes** p. Can you see why this lemma is true?

This lemma can be used to interchange divisibility with ν_p, which is very useful at times. For instance, here is a classic example which is hard to do otherwise but easy using this lemma. We give a walkthrough to it

Example 6.0.1

Let a, b be integers such that $a \mid b^2 \mid a^3 \mid b^4 \mid a^5 \dots$. Show that $a = b$.

The idea is to use ν_p to remove the divisibility. Also, to show $a = b$, we must show $\nu_p(a) = \nu_p(b)$ for all primes p. So take any prime p.

[1]The other is $\text{ord}_p(n)$. However, that clashes with the notation we used for order. So we don't use that.

(a) Use $a \mid b^2$ to get $\nu_p(a) \leq 2\nu_p(b)$. Use $b^2 \mid a^3$ to get $2\nu_p(b) \leq 3\nu_p(a)$. Continue the pattern to get

$$n\nu_p(a) \leq (n+1)\nu_p(b) \leq (n+2)\nu_p(a) \quad \text{for all } n \in \mathbb{N}.$$

(b) Choose n large to conclude that $\nu_p(b)/\nu_p(a) = 1$ (In other words, take $n \to \infty$). Conclude.

6.1 Arithmetic properties

Consider two integers x, y. Suppose $\nu_p(x) = m, \nu_p(y) = n$. So $x = p^m a, y = p^n b$ where a, b are coprime to p. Then

$$xy = (p^m a)(p^n b) = p^{m+n} ab.$$

Since $\gcd(ab, p) = 1$, hence we find $\nu_p(xy) = m + n$. We can similarly get $\nu_p(x \div y) = m - n$. So,

Lemma 6.1.1 (Product)**.** *Let x, y be integers and p be a prime. Then*

$$\nu_p(xy) = \nu_p(x) + \nu_p(y).$$

Thus, ν_p is an additive function. As a corollary, we find:

Corollary 6.1.1 (Exponentation)**.** *Let x be an integer and $n \in \mathbb{N}$. Let p be a prime. Then*

$$\nu_p(x^n) = n\nu_p(x).$$

You might observe the resemblance of this property with logarithms; we have $\log(xy) = \log(x) + \log y$ and $\log(x^n) = n \log x$.

Just like $\log(x/y) = \log x - \log y$, we can similarly get that

$$\nu_p\left(\frac{x}{y}\right) = \nu_p(x) - \nu_p(y) \quad \text{if } y \mid x.$$

However note that we must have $y \mid x$ for the division property (otherwise $\frac{x}{y}$ won't be an integer). This is kind of annoying. To overcome this, we generalize p-adic numbers:

Definition 6.1.1. *Let $q = m/n$ be a rational number, where $m, n \in \mathbb{Z}$. Let p be a prime. We define the **p-adic valuation** of q as*

$$\nu_p(q) = \nu_p(m) - \nu_p(n).$$

So now ν_p can take rational inputs too. For instance, $\nu_7(49/10) = 2, \nu_5(20/15) = 0$ and $\nu_2(3/4) = -2$. Note that ν_p can be positive, 0 or even negative. We can now ignore the $y \mid x$ condition to get:

Lemma 6.1.2 (Quotient)**.** *Let x, y be integers and p be a prime. Then*

$$\nu_p\left(\frac{x}{y}\right) = \nu_p(x) - \nu_p(y).$$

We can also replace x, y integers to x, y rational in Lemma 6.1.1 and n to any integer in Corollary 6.1.1.

Now consider $x+y$. As before, we have $x = p^m a, y = p^n b$ with a, b coprime to p. Suppose $m > n$. Then

$$x + y = p^m a + p^n b = p^n(p^{m-n}a + b) \tag{6.1}$$

Since $m - n > 0$, hence $p \mid p^{m-n}a$. So the bracket term is coprime to p. Hence $\nu_p(x+y) = n$. In general $\nu_p(m+n) = \min\{\nu_p(m), \nu_p(n)\}$.

For instance, if $m = 30$ and $n = 162$, then $\nu_3(30 + 162) = \nu_3(192) = 1 = \nu_3(30)$.

Question 6.1.1. *Take $m = 30$ and $n = 6$. What is $\nu_3(m+n)$? Does it match with the formula we got?*

If you did the above question, you would realize something is fishy. Can you find the mistake in our proof?

If you noticed that we did not deal with the case $m = n$, then well done. When $m = n$, we find $p^{m-n} = 1$, and so the bracket term in Equation 6.1 is $(a + b)$. Now $\gcd(a, p) = 1 = \gcd(b, p)$ does not guarantee $\gcd(a + b, p) = 1$. So it is possible the $(a + b)$ term also contributes a power of p, and so $\nu_p(x + y) > \min\{\nu_p(x), \nu_p(y)\}$. So in general we have the following lemma:

Lemma 6.1.3 (Sum)**.** *Let x, y be integers and p a prime. Then*

$$\nu_p(x + y) \geq \min\{\nu_p(x), \nu_p(y)\},$$

and equality holds if $\nu_p(x) \neq \nu_p(y)$.

Note a subtle detail here. We have said "equality holds if" not if and only if. Can you reason out why?

Let's try an example problem now:

Example 6.1.1 (IMO Shortlist 2007 N2)

Let $b, n > 1$ be integers. Suppose that for each $k > 1$ there exists an integer a_k such that $b - a_k^n$ is divisible by k. Prove that $b = A^n$ for some integer A.

Clearly, if $b = A^n$, then the constant sequence $a_k = A$ works. So this is one of those problems where the obvious solution is the only one.

Now, we can write the divisibility as $\nu_p(b - a_k^n) \geq \nu_p(k)$ for all k and primes p. Now, $\nu_p(b - a_k^n) \geq \min\{\nu_p(b), n\nu_p(a_k)\}$. If we can strategically choose k such that $\nu_p(b) \neq \nu_p(a_k^n) = n\nu_p(a_k)$, then we will know for sure that $\nu_p(b - a_k^n) = \min\{\nu_p(b), n\nu_p(a_k)\}$. So this is our key idea.

At this point, note that $\nu_p(b) = n\nu_p(a_k) \implies n \mid \nu_p(b)$. So if we suppose a prime p exists such that $n \nmid \nu_p(b)$, then we can pick that prime p and we would get

$$\nu_p(k) \leq \nu_p(b - a_k^n) = \min\{\nu_p(b), n\nu_p(a_k)\} \leq \nu_p(b) \quad \forall\ k > 1.$$

However, the right side is a constant (since b is fixed) but we can pick $\nu_p(k)$ on the left side to be as large as we want, meaning that the above is a contradiction.

This means that for every prime p we have $n \mid \nu_p(b)$. This precisely means $b = A^n$ for some A (since b becomes a product of nth power primes) which is what we wanted!

The motivation I gave might seem slightly hard to some of you. So here's a nicely written solution which is different (even though the idea is exactly the same).

Proof. Assume on the contrary that b is not a perfect nth power, which is the same as saying there is a prime p with $n \nmid \nu_p(b)$. Then write

$$b = p^{xn+y}\ell, \quad 1 \leq y \leq x - 1.$$

Now pick $k = p^{(x+1)n}$. Then $xn + y = \nu_p(b - a_k^n) \geq \nu_p(k) = (x + 1)n$, a contradiction. □

Comment 6.1.1: Note that we could have chosen k to be any very large power of p so that $xn + y > \nu_p(k)$. The key part in the problem is that $n \nmid \nu_p(b) \implies \nu_p(a_k^n) \neq \nu_p(b)$ and so $\nu_p(b - a_k^n) = \nu_p(b)$.

Problems for Practice

Problem 6.1.1. Show that a rational number q is an integer if and only if $\nu_p(q) \geq 0$ for every prime p.

6.2 Legendre's Formula

Apart from Wilson's theorem, we haven't talked much about factorials. One of the most useful properties is the following, which is surprisingly ubiquitous:

Theorem 6.2.1 (Legendre's Formula)**.** *Let n be an integer and p a prime. Then*

$$\nu_p(n!) = \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots.$$

Question 6.2.1. *The right side is an infinite sum. The left side, however is finite obviously. How is this possible?*

For instance,

$$\nu_2(6!) = \left\lfloor \frac{6}{2} \right\rfloor + \left\lfloor \frac{6}{2^2} \right\rfloor + \left\lfloor \frac{6}{2^3} \right\rfloor + \left\lfloor \frac{6}{2^4} \right\rfloor + \dots = 3 + 1 + 0 + 0 + \dots = 4.$$

Also, $6! = 720 = 2^4 \times 45$. So our formula works well.

Question 6.2.2. *Use the formula to show $\nu_3(8!) = \nu_3(7!) = \nu_3(6!)$. Then explain why is this true (without using the formula).*

Let's try and see why this is true. Write

$$n! = n(n-1)(n-2)(n-3)\dots 1.$$

First let's see how many terms are divisible by p. It's clearly $\lfloor n/p \rfloor$ since there are these many multiples of p atmost n.

Now any term which is divisible by p^2 has more contribution than just one factor of p. There are $\lfloor n/p^2 \rfloor$ terms divisible by p^2 that are atmost n. These have a contribution of 2. However, we counted them once before so we only need to count them once now. So we add $\lfloor n/p^2 \rfloor$.

Similarly we account for terms divisible by p^3 by adding $\lfloor n/p^3 \rfloor$ and so on. A diagram representation of this proof for $n = 12$ and $p = 2$ is shown:

	1	2	3	4	5	6	7	8	9	10	11	12	
$\nu_2 \geq 1$		1		1		1		1		1		1	$\lfloor 12/2 \rfloor$
$\nu_2 \geq 2$				1				1				1	$\lfloor 12/4 \rfloor$
$\nu_2 \geq 3$								1					$\lfloor 12/8 \rfloor$
$\nu_2 \geq 4$													$\lfloor 12/16 \rfloor$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\nu_p(9!)$	$=$ 1	$+$ 2	$+$ 1	$+$ 3	$+$ 1	$+$ 2							$= \lfloor 12/2 \rfloor + \lfloor 12/4 \rfloor + \lfloor 12/8 \rfloor + \lfloor 12/16 \rfloor + \dots$

Let's try a simple problem now:

Example 6.2.1

Show that for any positive integer n,

$$\binom{2n}{n} \mid \operatorname{lcm}\{1, 2, \dots, 2n\}.$$

Pick a prime p. Then we have to prove $\nu_p\left(\binom{2n}{n}\right) \leq \nu_p\left(\operatorname{lcm}\{1, 2, \dots, 2n\}\right)$. The right side is $\max\{\nu_p(1), \nu_p(2), \dots, \nu_p(2n)\}$ (why?). We can write the left side as $(2n)!/(n!)^2$ and use Legendre to evaluate its ν_p. So we just have to prove

$$\max\{\nu_p(1), \nu_p(2), \dots, \nu_p(2n)\} \geq \nu_p((2n)!) - 2\nu_p(n!) = \sum_{i \geq 1} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor.$$

At this point, note that each term in the summand on the right is of the from $\lfloor 2x \rfloor - 2\lfloor x \rfloor$. We would like to bound this. We do this by writing $x = \lfloor x \rfloor + \{x\}$ to get $\lfloor 2x \rfloor - 2\lfloor x \rfloor = \lfloor 2\{x\} \rfloor \in \{0, 1\}$. Also, note that the right side becomes 0 for $i > \lfloor \log_p(2n) \rfloor$. So, we find

$$\sum_{i \geq 1} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor \leq \lfloor \log_p(2n) \rfloor.$$

At this point we are done, since $\lfloor \log_p(2n) \rfloor$ is the maximum power of p that occurs in a number $\leq 2n$, which is precisely the same as $\max\{\nu_p(1), \nu_p(2), \ldots, \nu_p(2n)\}$. So we are done.

Turns out there's another formula for $\nu_p(n!)$, which is useful for simple bounding:

Theorem 6.2.2. *For any prime p and integer n, if $s_p(n)$ denotes the sum of digits of n when written in base p, then*

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1}.$$

This is not very hard to prove, and is left as an exercise. For $p = 2$, this gives $\nu_2(n!) = n - s_2(n)$, which is quite useful. For instance, it trivializes the following problem:

Problem 6.2.1 (Canada). Find all n such that 2^{n-1} divides $n!$.

For a much more interesting example using this $\nu_2(n!)$ formula, see Example 6.6.1. For now, here's a nice and challenging example:

Example 6.2.2

Prove that for all positive integers n, $n!$ divides

$$P = \prod_{k=0}^{n-1} (2^n - 2^k).$$

Firstly, take out 2^k from every bracket $(2^n - 2^k)$. Thus $\nu_2(P) = 0+1+\cdots+(n-1) = \frac{n(n-1)}{2}$. This is clearly larger than $\nu_2(n!) = n - s_2(n) \leq n - 1$. Now, write

$$Q = (2^n - 1)(2^{n-1} - 1)(2^{n-2} - 1)\ldots(2 - 1).$$

We need to show that $\nu_p(n!) \leq \nu_p(Q)$ for all odd primes p (why?). We first estimate $\nu_p(Q)$. For that, we need to look at how many terms of the form $2^x - 1$ are divisible by p. Now, $p \mid 2^{p-1} - 1$ by Fermat's Little Theorem, so $p \mid 2^{k(p-1)} - 1$ for all k. So the weakest estimate on $\nu_p(Q)$ is the number of k for which $k(p-1) \leq n$, i.e. the number of multiples of $(p-1)$ that are less than n. This is clearly $\left\lfloor \frac{n}{p-1} \right\rfloor$. So,

$$\nu_p(Q) \geq \left\lfloor \frac{n}{p-1} \right\rfloor.$$

This is a weak and naive estimate (since even if $p \mid 2^{k(p-1)} - 1$, the power of p in $2^{k(p-1)} - 1$ might be more than 1) and so we have no guarantee if it would work. However, there is no harm in trying.

Let's try to see if we can show $\nu_p(n!) \leq \left\lfloor \frac{n}{p-1} \right\rfloor$. Looking at the $p-1$, we are motivated to try Theorem 6.2.2. So,

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1} < \frac{n}{p-1}.$$

However, since $\nu_p(n!)$ is an integer, hence this gives

$$\nu_p(n!) \leq \left\lfloor \frac{n}{p-1} \right\rfloor \leq \nu_p(Q),$$

and we are done.

Problems for Practice

Problem 6.2.2. Prove Theorem 6.2.2 by writing the base p representation of n as $n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_0$.

6.3 Revisiting GCD and LCM

This notation provides us with a very convenient way of writing the GCD and LCM formula given as Lemma 1.6.3:

Lemma 6.3.1. *Let m, n be integers. Then for every prime p, we have*

$$\nu_p(\gcd(m,n)) = \min\{\nu_p(m), \nu_p(n)\}$$
$$\nu_p(\operatorname{lcm}(m,n)) = \max\{\nu_p(m), \nu_p(n)\}.$$

This lemma makes problems related to GCD and LCM both easier to manage, especially easier to write (and explain).

Example 6.3.1

Prove that $\operatorname{lcm}(a,b,c)^2 \mid \operatorname{lcm}(a,b)\operatorname{lcm}(b,c)\operatorname{lcm}(c,a)$ for any positive integers a, b, c.

Pick any prime p and let $x = \nu_p(a), y = \nu_p(b), z = \nu_p(c)$. The problem is equivalent to showing

$$2\nu_p(\operatorname{lcm}(a,b,c)) \leq \nu_p(\operatorname{lcm}(a,b)) + \nu_p(\operatorname{lcm}(b,c)) + \nu_p(\operatorname{lcm}(c,a)),$$

which is equivalent to $2\max\{x,y,z\} \leq \max\{x,y\} + \max\{y,z\} + \max\{z,x\}$. But this is clear (for instance, assume without loss of generality that $x \geq y \geq z$).

6.4 Lifting The Exponent (LTE)

Multiplication is fine, when we want to think of the valuation of the product. However, sum of two quantities can get weird, especially in the case when $\nu_p(a) = \nu_p(b)$. In this section we look at a particular type of sums whose ν_p we can calculate. Suppose, for instance, we want to find

$$\nu_3\left(4^{3^n} - 1\right).$$

We try and guess the answer for various values of n :

$$\begin{aligned}
&\nu_3\left(4^1-1\right)=\nu_3(3)=1\\
&\nu_3\left(4^3-1\right)=\nu_3(63)=\nu_2(3^2\times 7)=2\\
&\nu_3\left(4^9-1\right)=\nu_3(262143)=\nu_3(3^3\times 9709)=3
\end{aligned}$$

We do see a pattern, and conjecture that $\nu_3\left(4^{3^n}-1\right)=n+1$. It's better if we take more examples and confirm this. Instead of actually calculating the value of $4^{3^n}-1$, let's act smart and factorize in terms of previous expressions:

$$4^{27}-1=(4^9-1)(4^{18}+4^9+1).$$

If we can show that the second bracket has $\nu_3=1$, we will have $\nu_3(4^{27}-1)=4$, which is what we would like. To show it's divisible by 3 is easy:

$$4^{18}+4^9+1\equiv 1+1+1\equiv 0 \pmod 3.$$

This shows its $\nu_3\geq 1$. But, how to show it's equal to 1? Here's the idea; we show it's not divisible by 9. So let's find it modulo 9. Calculate (in any way you like) to get:

$$4^{18}+4^9+1\equiv 1+1+1=3\not\equiv 0 \pmod 9.$$

Boom! Exactly what we wanted.

How do we show $\nu_3\left(4^{3^n}-1\right)=n+1$ in general though? The idea is exactly what we did above. Just iterate that (or you can say use induction). It would look something like

$$4^{3^{n+1}}-1=\left(4^{3^n}-1\right)\left(4^{2\cdot 3^n}+4^{3^n}+1\right),\quad 4^{2\cdot 3^n}+4^{3^n}+1\equiv 1+1+1\not\equiv 0 \pmod{3^{n+1}}.$$

Here, we used $4^{3^n}\equiv 1 \pmod{3^{n+1}}$ by the induction hypothesis.

I won't trouble you anymore and give you the statement of LTE:

Lemma 6.4.1 (Lifting The Exponent (LTE)[2])**.** *Let $p>2$ be a prime and $a,b\in\mathbb{Z}$ be coprime to p such that $p\mid a-b$. Suppose n is a positive integer.*

$$\nu_p(a^n-b^n)=\nu_p(a-b)+\nu_p(n).$$

Using this, can you get a one line proof of the result we derived above?

[2]Note that I used "Lemma" instead of "Theorem". Whenever you use LTE on an Olympiad, it is highly advisable that you first state the result, then give a short sketch of the proof. Don't assume this to be a famous formula that you can use just by stating it.

Comment 6.4.1: Before we move on, I would like to lay stress on three particular conditions in the lemma that are very easy to miss:

1. p must be odd, i.e. $p = 2$ is not allowed.
2. $\gcd(p, a) = \gcd(p, b) = 1$. In other words, $p \nmid a, b$.
3. p divides $a - b$. So in the formula if you see that the $\nu_p(a - b)$ term is 0, you probably need to take a step back and rethink your plan.

Everyone forgets one or the other condition sometime in their life. So learn from their mistakes, and please don't repeat them, because there's nothing worse than feeling proud about a wrong solution.

This is a very useful result! Let's prove it. The idea is to use induction. However, just like the example we did, instead of the case when $n = 1$ (which is obvious), we first establish the case $n = p$. So we want $\nu_p(a^p - b^p) = \nu_p(a - b) + 1$. Write

$$\frac{a^p - b^p}{a - b} = a^{p-1} + a^{p-2}b + \cdots + b^{p-1}.$$

It suffices to show the right side has $\nu_p = 1$. Firstly, $p \mid a - b$ by the hypothesis so $a \equiv b \pmod{p}$. So

$$a^{p-1} + a^{p-2}b + \cdots + b^{p-1} \equiv a^{p-1} + a^{p-1} + \cdots + a^{p-1} = pa^{p-1} \equiv 0 \pmod{p}.$$

Next, as before, we show this quantity isn't divisible by p^2. For this, write $b = a + pk$ for an integer k (why?). For any $\ell \geq 1$, we have

$$b^\ell = (a + pk)^\ell = a^\ell + \ell a^{\ell-1}pk + \binom{\ell}{2}a^{\ell-2}(pk)^2 + \cdots + (pk)^\ell \equiv a^\ell + a^{\ell-1}\ell pk \pmod{p^2}.$$

Then

$$\begin{aligned} a^{p-1} + a^{p-2}b + \cdots + b^{p-1} &\equiv a^{p-1} + a^{p-2}(a + pk) + a^{p-3}(a^2 + 2apk) + \cdots + a^{p-2}(a + (p-1)pk) \\ &= pa^{p-1} + pa^{p-2}k(1 + 2 + \cdots + (p-1)) \\ &\equiv pa^{p-1} \not\equiv 0 \pmod{p^2}, \end{aligned}$$

where the last step follows since $pa^{p-2}k(1 + 2 + \cdots + (p-1)) = p^2a^{p-2}k \cdot \frac{p-1}{2} \equiv 0 \pmod{p^2}$ since $\frac{p-1}{2} \in \mathbb{Z}$ (why?). Hence, we have proven this result and derive as corollary the following lemma:

Lemma 6.4.2 (Case $n = p$ of LTE)**.** *Let $a, b \in \mathbb{Z}$ and $p > 2$ a prime so that $p \nmid a, b$ and $p \mid a - b$. Then*

$$\nu_p(a^p - b^p) = \nu_p(a - b) + 1.$$

Comment 6.4.2: Point out in the proof where we used the three important conditions: $p > 2, p \nmid a, b$ and $p \mid a - b$.

Now, for the general result, we induct on $\nu_p(n) = k$ (kind of like what we did in the problem). The case $n = 0$ is not hard (left as an exercise). Assume the result till some k, and we want to prove it for $k + 1$.

We simply use the lemma to get (first verify the three conditions)

$$\begin{aligned}\nu_p(a^n - b^n) &= \nu_p\left(\left(a^{n/p}\right)^p - \left(b^{n/p}\right)^p\right) \\ &= \nu_p(a^{n/p} - b^{n/p}) + 1 \\ &= \nu_p(a - b) + \nu_p(n/p) + 1 = \nu_p(a - b) + \nu_p(n).\end{aligned}$$

So we are done (point out where we used the induction hypothesis.).

Let's take a look at some examples:

Example 6.4.1

Prove that for any natural n,

$$\nu_3(2^{3^n} + 1) = n.$$

This is similar to LTE, with a plus instead of a minus. If n is odd, we can change b to $-b$ to obtain the following form of LTE:

Lemma 6.4.3. *LTE for addition Let $p > 2$ be a prime and $a, b \in \mathbb{Z}$ be coprime to p such that $p \mid a - b$. Suppose n is an odd positive integer.*

$$\nu_p(a^n + b^n) = \nu_p(a + b) + \nu_p(n).$$

Now let's look at some real examples:

Example 6.4.2 (Iran 2008 Round 2 Day 2/1)

Let a be a natural number. Suppose that $4(a^n + 1)$ is a perfect cube for every natural number n. Prove that $a = 1$

If an odd prime p divides $a^n + 1$ for some n, then $\nu_p(a^n + 1)$ must be divisible by 3, since $\gcd(p, 4) = 1$. This is the key insight.

Now, we are clearly motivated to try LTE by looking at $\nu_p(a^n + 1)$. So, we want the 3 conditions. By assumption, $p > 2$. Also, $p \nmid a$ (why?). We just want $p \mid a + 1$ and n odd. So let's start by this assumption. Pick an odd prime p divisor of $a + 1$, if it exists (when does it not exist?). Then by Fermat's Little Theorem, $p \mid a + 1 \mid a^{pk} + 1$ for all k. So, by LTE

$$\nu_p(a^{pk} + 1) = \nu_p(a + 1) + \nu_p(k) + 1 \quad \forall \text{ odd } k.$$

We know this is divisible by 3 for all odd k (why do we need odd k?). However, since $\nu_p(a+1)+1$ is fixed, hence we can choose (odd) k such that $\nu_p(a+1)+\nu_p(k)+1 \not\equiv 0 \pmod 3$, which is a contradiction. Hence, our assumption that $a+1$ has an odd prime factor was false. So $a+1$ can't have an odd prime factor.

Write $a+1=2^k$. Here's the clever trick now: since $\gcd(a^2+1, a+1) = \gcd(a+1, 2) = 2$, hence a^2+1 will have an odd prime factor p if $k>1$ (why?). So, you can repeat the process above with a^2 instead of a and still get a contradiction (convince yourself that this argument works). Hence, $k=1$, meaning $a+1=2$, i.e. $a=1$, as needed.

Comment 6.4.3: In problems like these (involving find all solutions, or prove this is the solution), when we write a proper proof, we must show two things: the solution works, and second this is the only solution. Most people often miss the first, thinking it's trivial, and lose marks on an actual Olympiad. So, the starting line of our solution to this problem would be: "Clearly, $a=1$ works since then $4(1^n+1)=8$ for all n, which is a cube. Now, we will show this is the only possibility." The proof we gave follows after this. Don't miss this "obvious" statement and lose marks!

Example 6.4.3 (AMM)

Let a, b, c be positive integers such that $c \mid a^c - b^c$. Prove that $c \mid \frac{a^c-b^c}{a-b}$.

This problem calls for LTE. So we first establish the 3 conditions. Suppose $c \geq 3$. Pick an odd prime $p \mid c$ (that's why we need $c \geq 3$). If $p \nmid a-b$, the result is obviously true. So suppose $p \mid a-b$.

If p divides one of a or b, then p must divide the other (why?). Write $\nu_p(a)=x, \nu_p(b)=y, \nu_p(c)=z$. Suppose $x>y$. Then we just need $z \leq y(c-1)$. However, since $c \geq p^z > z+1$ (why?) hence $z \leq yz \leq y(c-1)$ holds true. If $x=y$, then take p^{cx} out and ignore it. We prove the result for the leftover part only, in which case $p \nmid a^*, b^*$, where a^*, b^* are the leftovers from a, b respectively. So now assume $p \nmid a, b$.

Upto this point we have just established the conditions for LTE. Now, using LTE,

$$\nu_p(a^c-b^c) = \nu_p(a-b)+\nu_p(c) \implies \nu_p(c) \leq \nu_p\left(\frac{a^c-b^c}{a-b}\right).$$

This is what we needed. Now, we just need the result for $p=2$. For this case, we can't apply LTE. So we need something new:

6.5 The sad case when $p=2$

We particularly asked you to remember that the formula does not work with $p=2$. But what if we want ν_2? We have the following result in this case:

Lemma 6.5.1 (LTE for $p = 2$)**.** *Let x, y be odd integers such that $2 \mid x - y$. Let n be an even integer. Then*

$$\nu_2(x^n - y^n) = \nu_2(x^2 - y^2) + \nu_2(n/2) = \nu_2(x - y) + \nu_2(x + y) + \nu_2(n) - 1.$$

Note here that n must be even, We have another result for $p = 2$, wherein we don't need $2 \mid n$ (however we need $4 \mid x - y$) :

Lemma 6.5.2. *Let x, y be odd integers such that $4 \mid x - y$. Then*

$$\nu_2(x^n - y^n) = \nu_2(x - y) + \nu_2(n).$$

The proof for these 2 are not very different, just some care is needed with the base case. The full proof is left to the interested readers.

6.6 Example Problems

Example 6.6.1 (Paul Erdos)

Prove that there exists a constant c such that for any positve integers a, b and $n > 1$ satisfying $a! \cdot b! \mid n!$, we have $a + b < n + c \log n$.

This is an analytic kind of problem. A common theme in many of these is to make use of simple number theoretic facts and estimates. Often the simplest estimates give very good (at times, optimal) bounds.

In this problem, the given condition gives $\nu_p(a!) + \nu_p(b!) \leq \nu_p(n!)$ for any prime p. The key trick at this point is to consider $p = 2$, to get $a - s_2(a) + b - s_2(b) \leq n - s_2(n)$ (since the problem wants us to prove something involving a, b, n not $a!, b!, n!$, hence making use of $\nu_2(x!) = x - s_2(x)$ is slightly motivated). So, we get

$$a + b - n \leq s_2(a) + s_2(b) - s_2(n).$$

If we can show the right side is at most $c \log n$ for some constant c, we are done. At this point, we need upper bounds on $s_2(a), s_2(b)$. The simplest upper bound is obtained by considering the case when all of the digits of a, b in base 2 are 1. Thus, $s_2(a) \leq \lfloor \log_2(a) \rfloor + 1$ (why?) and so

$$a + b - n \leq \log_2(a) + \log_2(b) + 2 - s_2(n) \leq \log_2(ab) + 2 \leq 2 \log_2(n) + 2,$$

where, we used $ab < n \times n = n^2$ and $s_2(n) > 0$. The result is now immediate, since the right side is $2 \log_2(n) + 2 \leq 4 \log_2(n) = \left(\frac{4}{\log 2}\right) \log n$. (these are just rough estimates. The key point is that $\log_2(n) + 2 = \mathcal{O}(\log n)$).

The next is a great example showing how simple uses of ν_p can be really powerful.

Example 6.6.2 (APMO 2017/4)

Call a rational number r powerful if r can be expressed in the form p^k/q for some relatively prime positive integers p, q and some integer $k > 1$. Let a, b, c be positive rational numbers such that $abc = 1$. Suppose there exist positive integers x, y, z such that $a^x + b^y + c^z$ is an integer. Prove that a, b, c are all powerful.

We need to consider a prime p and show that if $\nu_p(a) > 0$, then it is divisible by some fixed $k > 1$, which is independent of p (why?). Firstly, the condition $abc = 1$ translates to

$$\nu_p(a) + \nu_p(b) + \nu_p(c) = 0.$$

Assume that $\nu_p(a) > 0$. By the above, at least one is negative. If $\nu_p(b) > 0$ while $\nu_p(c) < 0$, then $\nu_p(a^x + b^y + c^z) < 0$, which is impossible since it's an integer.

Comment 6.6.1: Before we move on, here's a tip on how to think about ν_p in such problems. If $\nu_p(x) = y$, think of y as p^x, not as cp^x, This makes it easier to think about operations. So, for instance the above argument can be thought of as

$$a^x + b^y + c^z = p^\bullet + p^\bullet + \frac{1}{p^\bullet} = \frac{p^\bullet + p^\bullet + 1}{p^\bullet}.$$

Of course, there would be a constant in place of 1s, but the idea is that it won't be divisible by p. So the numerator above isn't divisible by p while the denominator is, giving $\nu_p(a^x + b^y + c^z) < 0$.

Even when we think about $\nu_p(a + b) \geq \min\{\nu_p(a), \nu_p(b)\}$, it is easiest to think of $a = p^x, b = p^y$. So if $x > y$, then $a + b = p^y(p^{x-y} + 1)$ and so the bracket is coprime to p implying $\nu_p(a + b) = y$. However, if $x = y$, the bracket becomes $1 + 1$, which means some constant+constant which *might* be divisible by p.

Hence, we obtain $\nu_p(b), \nu_p(c) < 0$. In this case, if $\nu_p(a^x + b^y + c^z) \geq 0$, we must have that $\nu_p(b^x) = \nu_p(c^z)$ (confirm this both by giving a formula argument (by writing $\nu_p(a) = u, \dots$), and by convincing yourself by the way described in the comments above).

Hence, $x\nu_p(b) = y\nu_p(c)$. If $\gcd(x, y) = d$ and $x = x^*d, y = y^*d$, then we must have $\nu_p(b) = kx^*$ and $\nu_p(c) = ky^*$ for some k. Hence,

$$\nu_p(a) = -(\nu_p(b) + \nu_p(c)) = -k(x^* + y^*).$$

Hence $\nu_p(a)$ is always divisible by $x^* + y^*$ which is independent of p. So we are done.

Comment 6.6.2: The most reasonable way to motivate the last step is to take an example. If $4\nu_p(b) = 6\nu_p(c)$, then $(\nu_p(b), \nu_p(c))$ can be $(3, 2), (6, 4), (9, 6), \dots$. It is now easy to see that $\nu_p(b)$ must be of the form $3k = \frac{6k}{\gcd(4,6)}$ and $\nu_p(c)$ must be of the form $2k = \frac{4k}{\gcd(4,6)}$.

The next problem is again analytic in nature, and again shows how simple ideas work when used properly.

Example 6.6.3 (China TST 2009 Quiz 6/1)

Let $a > b > 1$ be positive integers and b be an odd number, let n be a positive integer. If $b^n \mid a^n - 1$, prove that $a^b > \frac{3^n}{n}$.

Since b is odd, it has a prime factor p. So $a^n \equiv 1 \pmod{p}$ implying $d = \text{ord}_p(a) \mid n$. Further, $\nu_p(a^n - 1) \geq n\nu_p(b)$. We can use LTE as

$$n \leq n\nu_p(b) \leq \nu_p((a^d)^{n/d} - 1) = \nu_p(a^d - 1) + \nu_p\left(\frac{n}{d}\right) = \nu_p(a^d - 1) + \nu_p(n).$$

Here, we used $\nu_p(d) = 0$ since $1 < d \leq p - 1$. This gives

$$p^n \leq p^{\nu_p(a^d-1)} p^{\nu_p(n)} \leq (a^d - 1)n \leq a^b n \implies a^b > \frac{p^n}{n} \geq \frac{3^n}{n}. \qquad \square$$

6.7 Practice Problems

Problem 6.7.1. Show that if $n \geq 6$ is composite, then n divides $(n-1)!$.

Problem 6.7.2. Let p be an odd prime. For any $t \geq 1$, define

$$S_t = \sum_{k=1}^{p-1} k^{p^t}.$$

Then prove that $\nu_p(S_t) \geq t+1$. In particular,

$$p^2 \mid 1^p + 2^p + \cdots + p^p.$$

Hints: 419 412

Problem 6.7.3. Show that $\binom{2n}{n} \mid \operatorname{lcm}(1, 2, \ldots, 2n)$ for all positive integers n. **Hints:** 295 217

Problem 6.7.4 (USAMO 1975/1). Prove that

$$\lfloor 5x \rfloor + \lfloor 5y \rfloor \geq \lfloor 3x + y \rfloor + \lfloor 3y + x \rfloor,$$

where $x, y \geq 0$. Using this or otherwise, prove that

$$\frac{(5m)!(5n)!}{m!n!(3m+n)!(3n+m)!}$$

is integral for all positive integral m and n. **Hints:** 325 187

Problem 6.7.5. Prove that for all integers $n \geq 1$,

$$C_n = \frac{1}{n+1}\binom{2n}{n} \in \mathbb{Z}.$$

(The number C_n is called the n**th Catalan Number.** It is an interesting object of study in enumerative combinatorics)

Problem 6.7.6. Find all positive integers n such that $3^n - 1$ is divisible by 2^n. **Hints:** 434

Problem 6.7.7 (Austria National Competition Final Round). Let $a, b,$ and c be integers such that

$$\frac{ab}{c} + \frac{ac}{b} + \frac{bc}{a}$$

is an integer. Prove that each of the numbers

$$\frac{ab}{c}, \frac{ac}{b}, \text{ and } \frac{bc}{a}$$

is an integer. **Hints:** 399 334 185

Problem 6.7.8. Prove that if the odd prime p divides $a^b - 1$, where a and b are positive integers, then p appears to the same power in the prime factorization of $b(a^d - 1)$, where $d = \gcd(b, p-1)$. **Hints:** 355 244

Problem 6.7.9 (PUTNAM). Show that for each positive integer n,

$$n! = \prod_{i=1}^{n} \operatorname{lcm}\left\{1, 2, \ldots, \left\lfloor \frac{n}{i} \right\rfloor\right\}.$$

Hints: 121

Problem 6.7.10. Let n be a positive integer with $n > 1$.

1. Prove that the nth Harmonic number defined by

$$\mathbb{H}_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

is not an integer. **Hints:** 318 55 315

2. Prove that

$$1 + \frac{1}{3} + \cdots + \frac{1}{2n-1}$$

is not an integer. **Hints:** 161 107

Problem 6.7.11 (IMO 1990/3). Find all natural n such that $\frac{2^n+1}{n^2}$ is an integer. **Hints:** 452 214 300

Problem 6.7.12 (IMO 1999/4). Find all pairs of positive integers (x, p) such that p is prime, $x \leq 2p$, and $x^{p-1} \mid (p-1)^x + 1$. **Hints:** 238 470 474 373

Problem 6.7.13 (Taiwan TST 2018 Round 2 Quiz 3/1). Given a square-free positive integer n. Show that there do not exist coprime positive integers x, y such that $x^n + y^n$ is a multiple of $(x+y)^3$. **Hints:** 98 169 189

Problem 6.7.14 (China TST 1 2019/4). Call a sequence of positive integers $\{a_n\}$ good if for any distinct positive integers m, n, one has

$$\gcd(m, n) \mid a_m^2 + a_n^2 \text{ and } \gcd(a_m, a_n) \mid m^2 + n^2.$$

Call a positive integer a to be k-good if there exists a good sequence such that $a_k = a$. Does there exists a k such that there are exactly 2019 k-good positive integers? **Hints:** 432 348 74

Problem 6.7.15 (Indian TST 2018 Day 2/1). For a natural number $k > 1$, define S_k to be the set of all triplets (n, a, b) of natural numbers, with n odd and $\gcd(a, b) = 1$, such that $a + b = k$ and n divides $a^n + b^n$. Find all values of k for which S_k is finite. **Hints:** 298 151 361 290

Problem 6.7.16 (Gabriel Dospinescu). Let a, b be two distinct positive rational numbers such that for infinitely many integers n, $a^n - b^n$ is an integer. Prove that a, b are also integers. **Hints:** 79 347 443

Problem 6.7.17 (Iran 3rd round 2017 Number theory first exam P1). Let n be a positive integer. Consider prime numbers $p_1, \ldots, p_k$. Let $a_1, \ldots, a_m$ be all positive integers less than n such that are not divisible by p_i for all $1 \leq i \leq n$. Prove that if $m \geq 2$ then

$$\frac{1}{a_1} + \cdots + \frac{1}{a_m}$$

is not an integer. **Hints:** 153 488 356 433 **Sol:** pg. 293

Problem 6.7.18 (China TST 2 2019/4). Set positive integer $m = 2^k \cdot t$, where k is a non-negative integer, t is an odd number, and let $f(m) = t^{1-k}$. Prove that for any positive integer n and for any positive odd number $a \leq n$, $f(1)f(2)\ldots f(m)$ is a multiple of a. **Hints:** 178 247 342 **Sol:** pg. 293

Problem 6.7.19 (IMO Shortlist 2014 N5). Find all primes p and positive integers (x, y) such that $x^{p-1} + y$ and $y^{p-1} + x$ are powers of p. **Hints:** 134 60 31

Problem 6.7.20 (Tuymaada Olympiad). Prove that the equation

$$\frac{1}{10^n} = \frac{1}{n_1!} + \frac{1}{n_2!} + \cdots + \frac{1}{n_k!}$$

does not have integer solutions such that $1 \leq n_1 < \cdots < n_k$. **Hints:** 117 441 473 92 274 **Sol:** pg. 294

Problem 6.7.21 (USAMO 2009/6). Let $s_1, s_2, s_3, \ldots$ be an infinite, nonconstant sequence of rational numbers, meaning it is not the case that $s_1 = s_2 = s_3 = \ldots$. Suppose that $t_1, t_2, t_3, \ldots$ is also an infinite, nonconstant sequence of rational numbers with the property that $(s_i - s_j)(t_i - t_j)$ is an integer for all i and j. Prove that there exists a rational number r such that $(s_i - s_j)r$ and $(t_i - t_j)/r$ are integers for all i and j. **Hints:** 12 201 249 367

Problem 6.7.22 (India TST 2019 Day 1/2). Show that there do no exist natural numbers $a_1, a_2, \ldots a_{2018}$ such that all

$$(a_1)^{2018} + a_2, (a_2)^{2018} + a_3, \ldots, (a_{2018})^{2018} + a_1$$

are powers of 5. **Hints:** 70 478 280 303

Problem 6.7.23 (USA TSTST 2014/6). Suppose we have distinct positive integers a, b, c, d, and an odd prime p not dividing any of them, and an integer M such that if

one considers the infinite sequence

$$\begin{aligned} ca - db \\ ca^2 - db^2 \\ ca^3 - db^3 \\ ca^4 - db^4 \\ \vdots \end{aligned}$$

and looks at the highest power of p that divides each of them, these powers are not all zero, and are all at most M. Prove that there exists some T (which may depend on a, b, c, d, p, M) such that whenever p divides an element of this sequence, the maximum power of p that divides that element is exactly p^T. **Hints:** 313 146 267 317 **Sol:** pg. 294

Problem 6.7.24 (ELMO Shortlist 2017 N3). For each integer $C > 1$ decide whether there exist pairwise distinct positive integers $a_1, a_2, a_3, \ldots$ such that for every $k \geq 1$, a_{k+1}^k divides $C^k a_1 a_2, \ldots, a_k$. **Hints:** 337 72 456 359 **Sol:** pg. 295

I know I promised no functional equations in this book. However this problem is one of my all time favorites:

Problem 6.7.25 (USA TSTST 2019 Day 3/1). Let $f : \mathbb{Z} \to \{1, 2, \ldots, 10^{100}\}$ be a function satisfying

$$\gcd(f(x), f(y)) = \gcd(f(x), x - y)$$

for all integers x and y. Show that there exist positive integers m and n such that $f(x) = \gcd(m + x, n)$ for all integers x.

✠ Zsigmondy's Theorem

We have seen expressions of the form $a^k - b^k$ occur a lot in many problems. There is one theorem in particular that is very useful in such expressions:

Theorem 6.7.1 (Zsigmondy's Theorem)**.** *Let a, b be coprime positive integers. Then for any integer $n > 1$, $a^n - b^n$ has a prime factor that does not divide $a^k - b^k$ for any $k < n$, except in the following cases:*

- $2^6 - 1^6$
- *$n = 2$ and $a + b$ is a power of 2.*

Such a prime divisor is called a ***primitive*** *prime divisor of $a^n - b^n$.*

So $a^n - b^n$ always (except a few cases) has a new prime factor. This theorem is very hard to prove despite having an elementary proof (unlike say, Dirichlet's Theorem). The proofs dwells a lot upon many properties of Cyclotomic Polynomials, a topic we avoid in this book.

This theorem is delicate, and is not allowed to be used in all Olympiads. So be careful before using it on an exam. For now, however, let's nuke some problems using this!

Example 6.7.1 (Polish MO 2010 Round 1)

Let p and q be prime numbers with $q > p > 2$. Prove that $2^{pq} - 1$ has at least three distinct prime factors.

Observe that $2^p - 1$ and $2^q - 1$ both divide $2^{pq} - 1$. Now, since $q, p > 2$, hence by Zsigmondy, both $2^{pq} - 1$ has a prime factor that does not divide $2^p - 1, 2^q - 1$. Further, $q > p > 2$, so $2^q - 1$ has a prime factor that does not divide $2^p - 1$. So we are done.

Example 6.7.2 (1994 Romanian Team Selection Test)

Prove that the sequence $a_n = 3^n - 2^n$ contains no three terms in geometric progression

Say $a_i a_j = a_k^2$ with $i < k < j$. However, a_j has a prime factor that a_k does not by Zsigmondy's theorem, hence we already have a contradiction.

Example 6.7.3

Let a be an integer. Prove that for any d, there exist infinitely many primes p such that $d \mid \text{ord}_p(a)$.

Consider numbers of the form $a^{dn} - 1$. For any n (such that we avoid an exception), by Zsigmondy, there would exist a primitive prime factor p of $a^{dn} - 1$. Then $\text{ord}_p(a) = dn$. So Zsigmondy trivialized a very hard problem.

Example 6.7.4 (IMO Shortlist 2000 N4)

Find all triplets of positive integers (a, m, n) such that $a^m + 1 \mid (a+1)^n$.

Over here, any prime divisor of $a^m + 1$ must divide $a + 1$. We can't use Zsigmondy here, since it involves a $-$ sign instead of a $+$. This need calls for a second version of the theorem:

Theorem 6.7.2 (Zsigmondy's Variant)**.** *Let a, b be positive coprime integers. Then for any integer $n > 1$, there exists a prime factor of $a^n + b^n$ that does not divide $a^k + b^k$ for any $k < n$, except for the case:*

- $2^3 + 1^3$.

Proof. Consider a primitive divisor of $a^{2n} - b^{2n}$ (excluding the exceptions). Then $p \mid a^n + b^n$ or $p \mid a^n - b^n$, the latter being rejected since p is primitive. This p works.

As for the exceptions, the case $2^6 - 1^6$ is reflected in $2^3 + 1^3$. The second exception of $n = 2$ and $a + b$ a power of 2 is ignored since we only consider $n > 1$ in the theorem. □

As for our problem, if $m > 1$, then $a^m + 1$ has a prime factor that $a + 1$ doesn't unless $(a, m) = (2, 3)$. Hence, the only solutions are $(a, m, n) = (a, 1, n), (2, 3, n)$.

Example 6.7.5 (IMO Shortlist 2002 N3)

Let $p_1, p_2, \ldots, p_n$ be distinct primes greater than 3. Show that $2^{p_1 p_2 \cdots p_n} + 1$ has at least 4^n divisors.

Let $e = p_1 p_2 \ldots p_n$. Then e has 2^n divisors. Also, $3 \nmid e$, and so by Zsigmondy, $2^e + 1$ has at least 2^n prime factors. So, a total of $2^{2^n} > 2^{2n} = 4^n$ divisors.

Let's try two challenging problems that aren't directly trivialized by Zsigmondy's Theorem.

Example 6.7.6 (IMO Shortlist 2000/5)

Does there exist a positive integer n such that n has exactly 2000 prime divisors and n divides $2^n + 1$?

The answer is yes, and we prove it for any k instead of just 2000. They key idea is to add primes one by one. Suppose we have n such that $n \mid 2^n + 1$ and n has k prime factors. We want to find a prime p such that $np \mid 2^{np} + 1$ and $p \nmid n$.

To have $p \mid 2^{np} + 1$, we would take a prime $p \mid 2^n + 1$. Now we need to ensure $p \nmid n$. Since $n \mid 2^{\varphi(n)} - 1$, hence we are done if we can ensure $p \nmid 2^{\varphi(n)} - 1$.

Here's how we do this: By Zsigmondy, pick a primitive prime factor p of $2^{2n} - 1$. Then $p \nmid 2^n - 1$, so $p \nmid 2^n + 1$. Further, $p \nmid 2^{\varphi(n)} - 1$ as $\varphi(n) < 2n$, so $p \nmid n$. Hence, $np \mid 2^{np} - 1$ and we are done.

Example 6.7.7 (Iran third round 2018 NT/4 (weaker version))

Prove that for any natural numbers a, b there exist infinity many prime numbers p so that $\text{ord}_p(a) \geq \text{ord}_p(b)$.

The proof I present is quite magical. Take a prime q and pick a primitive prime factor p of $a^q - b^q$ using Zsigmondy's Theorem. It is not hard to check that $\text{ord}_p(ab^{-1}) = q$. The key claim is the following:

Claim. *One of* $\text{ord}_p(a), \text{ord}_p(b)$ *is divisible by* q.

We first show how this claim finishes the problem: Suppose $q \mid \text{ord}_p(a)$, and write $\text{ord}_p(a) = qx$. Then $1 \equiv a^{qx} \equiv b^{qx} \pmod{p}$ implies $\text{ord}_p(b) \mid qx$, which gives $\text{ord}_p(a) \geq \text{ord}_p(b)$ as desired. Now we prove the claim:

Proof. Since $\text{ord}_p(ab^{-1}) = q$, we get $q \mid p - 1$. Write $p = qk + 1$.

We also know that $\text{ord}_p(a), \text{ord}_p(b) \mid p - 1 = kq$. So if the claim isn't true, then $\text{ord}_p(a), \text{ord}_p(b) \mid k$. Then

$$a^k \equiv 1 \equiv b^k \pmod{p} \implies \left(a \cdot b^{-1}\right)^k \equiv 1 \pmod{p}.$$

Hence, $q = \text{ord}_p(ab^{-1}) \mid k$. So write $k = qk^*$, so $p = q^2k^* + 1$.

Now, the finishing argument is that we can repeat the above process and show $q \mid k^*$, and keep going on forever, which is a contradiction. □

Some problems for you to try:

Problem 6.7.26 (IMO Shortlist 1997, Q14). Let b, m, n be positive integers such that $b > 1$ and $m \neq n$. Prove that if $b^m - 1$ and $b^n - 1$ have the same prime divisors, then $b + 1$ is a power of 2.

Problem 6.7.27. Let $a \in N$ prove that the set

$$\left\{ \frac{p-1}{\text{ord}_p(a)} : \gcd(p, a) = 1, p \text{ prime} \right\}$$

is unbounded.

Problem 6.7.28 (USA TSTST 2018/8). For which positive integers $b > 2$ do there exist infinitely many positive integers n such that n^2 divides $b^n + 1$?

Chapter 7

Integer Polynomials

This chapter is largely about discussion of integer polynomials, which are polynomials with integer coefficients. Just like integers, these have a lot of interesting properties, and a lot of analogous identities. However, this is a highly delicate topic too, and a good conceptual approach is needed to truly appreciate it. So I have included a section on basics of polynomials which covers almost all these important topics you need to know to build your base.

After enough experience, you would start to see patterns in the arguments we give in Olympiad problems, and develop a strong intuition. This would be the day you would start to solve such problems with ease.

7.1 Basics of Polynomials

We would deal with single variable polynomials in the theory. I would expect some basic knowledge from your side, but I would anyway give a brief discussion of some of the most important properties of polynomials.

7.1.1 Definitions

Just for the sake of completeness, let me define some common terms related to polynomials:

Definition 7.1.1. *A **polynomial** of degree n is an algebraic expression of the form*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

*where x is a variable and $a_n, a_{n-1}, \ldots, a_0$ are numbers. It is called an **integer polynomial** if the coefficients are integers. It is called **monic** if the leading coefficient, i.e. a_n, equals 1.*

We know that $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ denote integers, rationals, reals and complex numbers respectively. There are analogous expressions for polynomials: $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{R}[X], \mathbb{C}[X]$.

Comment 7.1.1: Note that we did not define $\mathbb{N}[X]$. For now just keep in mind that $\mathbb{N}[X]$ is not correct. If you wanna know the reason really bad, then it's because $\mathbb{N}$ is not a "commutative ring"(A "structure" from abstract algebra. So ignore if you haven't heard this before.)

So, if p is an integer polynomial, we write $p \in \mathbb{Z}[X]$. If p has real coefficients, we would write $p \in \mathbb{R}[X]$.

7.1.2 Fundamental Theorem of Algebra

This is a beautiful result which says:

Theorem 7.1.1 (Fundamental Theorem of Algebra)**.** *Let $p \in \mathbb{C}[X]$ be a **non-zero** polynomial of degree n. Then $p(x)$ has exactly n complex roots, not necessarily distinct.*

Comment 7.1.2 (Degree of 0): You can notice that $P(x) = 0$ has infinitely many roots (since it is always zero). However, the degree of the zero polynomial is not defined. As we will soon see in the next section, in Euclid's division lemma $f(x) = g(x)q(x) + r(x)$, we want $\deg r < \deg g$. So a convention often used is to set the degree of the zero polynomial to be $-\infty$, so that it's consistent with Euclid's division lemma.

This is not as easy to prove as you might think. It, however, is incredibly useful, and finds applications outside maths For instance:

Problem 7.1.1. Consider an equilateral triangle and place three charges $+q$ on the vertices. Find the number of null points (of the electric field) in the plane.

The answer to this is 4. Firstly, you guess and find the 4 points. To show there are no more, imagine setting up an equation for a general point. The equation would be a polynomial of degree 4, so you will have atmost 4 points!

Another important and useful fact is that complex roots come in pairs; if z is a root, then so is $\overline{z}$. In particular odd degree polynomials always have a real root. Keep this in mind!

7.1.3 Euclidean Division Lemma and GCD

This section creates analogues of some normal divisibility properties of integers in Polynomials. Firstly, we define division:

Definition 7.1.2. *A polynomial $F(x)$ is said to be **divisible** by a polynomial $G(x)$ if there exists a polynomial $Q(x)$ such that*

$$F(x) = G(x)Q(x).$$

For instance consider $x^2 + \frac{2}{3}x$. This is divisible by x and $x + \frac{2}{3}$. This is also divisible by every constant, for instance

$$5 \times \left(\frac{1}{5}x^2 + \frac{2}{15}x\right) = x^2 + \frac{2}{3}x.$$

More interesting is divisibility **over** $\mathbb{Q}$. The only difference here is that we must have $Q \in \mathbb{Q}[X]$. [1] Similarly we can define division **over** $\mathbb{Z}$, which is the most restrictive since you want $Q \in \mathbb{Z}[X]$. So this time a polynomial need not be divisible by every constant. For instance $f(x) = x^2 + 4x + 2$ is not divisible by any constant, but $f(x) = 2x^2 + 4$ is divisible be 2.

Just like in the chapter on divisibility, once we discuss divisibility, it is almost natural to talk about remainders and hence Euclid's Division Lemma:

Theorem 7.1.2 (Polynomial Division)**.** *For every pair of polynomials F, G, there correspond **unique** polynomials Q, R such that*

$$F(x) = G(X)Q(X) + R(X),$$

where R is the zero polynomial or $\deg R < \deg G$.

The process of finding Q, R (called the **quotient**,**remainder** respectively) is by polynomial long division. Now we are dealing with integer polynomials, so answer the following question:

Question 7.1.1. *If F, G are integer polynomials, do Q, R have to be integer polynomials too?*

While you might feel like the answer is yes, it actually is no:

$$X^3 + 4X^2 + 1 = (5X^2 + 2)\left(\frac{1}{5}X + \frac{4}{5}\right) + \left(\frac{-2}{5}X + \frac{-3}{5}\right).$$

This example makes it quite clear; we might need rational numbers to adjust the coefficients. However it is always true that Q, R would have rational coefficients. Hence we get

Theorem 7.1.3 (Euclid's Division Lemma for Polynomials)**.** *For every pair of polynomials $F, G \in \mathbb{Q}[X]$ there correspond **unique** polynomials $Q, R \in \mathbb{Q}[X]$ such that*

$$F(x) = G(X)Q(X) + R(X),$$

where R is the zero polynomial or $\deg R < \deg G$.

The proof of this is to look at the long division algorithm; when worse comes to worst we would have to divide by rationals, which would still give rationals. Irrational numbers don't just randomly pop up.

Comment 7.1.3 (Euclid's Division Lemma in $\mathbb{F}_p[X]$): The only fact used in the argument above is the fact that we can divide by non-zero rationals and still get rationals. This is precisely the reason why Euclid's division lemma doesn't hold in $\mathbb{Z}[X]$: we can't divide by a non-zero integer an always expect to get an integer.

This property of rationals is also seen in $\mathbb{F}_p$; if we divide two non-zero elements of $\mathbb{F}_p$ and still get an element in $\mathbb{F}_p$. Thus, Euclid's Division Lemma also holds true in $\mathbb{F}_p[X]$. This was used in the special section of the chapter Modular Arithmetic.

At this point we must take a minute to define the GCD:

[1] We generally also want $F, G \in \mathbb{Q}[X]$, but well, we can say $\sqrt{2}$ divides $4\sqrt{2}$ since the ratio is an integer.

Definition 7.1.3. *For two polynomials $F, G \in \mathbb{Q}[X]$, the **GCD over** $\mathbb{Q}$ of F, G is the polynomial $D \in \mathbb{Q}[X]$ of largest degree satisfying $D(x) \mid F(x)$ and $D(x) \mid G(x)$.*

Note that this is the GCD of polynomials, which has to be a polynomial dividing both. So saying $\gcd(X^2+1, X+1) = \gcd(2X, X+1) = 2$ when X is odd is wrong, since we want a polynomial identity which is true for all X. So saying $\gcd(X^2+1, X+1) = 1$ since they have no common polynomial is correct.

What is the GCD of x^2+2, x^3+2x? It is x^2+2. Well, we can also say it is $2(X^2+2)$ since each constant divides a polynomial in $\mathbb{Q}[X]$. So the GCD is not unique. However, it turns out that only constants cause any disturbance:

Lemma 7.1.1 (GCD of Polynomials is not unique)**.** *For two polynomial $F, G \in \mathbb{Q}[X]$, the GCD of F is not unique. However, if D_1, D_2 are two GCDs, then $D_1 = qD_2$ for a non-zero rational q.*

So by convention if we treat all constants as 1, then we consider constant GCDs to be 1 as well. So $2(x+1)$ and $2(x^2+1)$ are actually considered coprime. For integers, the best way to identify the GCD of two polynomials is by looking at their prime factors. What are prime factors for polynomials? We discuss this in the section on irreducibility.

Now we have the two theorems carried over directly from the first chapter:

Lemma 7.1.2 (Euclid's Lemma for Polynomials)**.** *Let $F, G \in \mathbb{Q}[X]$. Write $F = GQ + R$ with $\deg R < \deg F$. then*

$$\gcd(F(x), G(x)) = \gcd(R(X), G(X)).$$

Lemma 7.1.3 (Bézout's Lemma for Polynomials)**.** *Let $F, G \in \mathbb{Q}[X]$ be two polynomials with $\gcd = D$. Then there exist polynomials $A, B \in \mathbb{Q}[X]$ such that*

$$F(x)A(x) + G(x)B(x) = D(x).$$

The second theorem is particularly useful when we have two coprime polynomials. In that case, we have $A, B \in \mathbb{Q}[X]$ such that $F(x)A(x) + G(x)B(x) = 1$. The best part is that by multiplying throughout by the denominators, we can convert A, B into integer polynomials and then the above becomes $F(x)A(x) + G(x)B(x) = c$ for some constant c. The benefit here is that $A, B \in \mathbb{Z}[X]$. This is a very effecting way of dealing with coprime polynomials that we will soon see in problems.

7.1.4 Remainder and Factor Theorem

Suppose you have a polynomial $p(x)$ that you want to factor. Then we have the following theorem:

Theorem 7.1.4 (Factor Theorem)**.** *Let $p(x)$ be a polynomial. If $p(a) = 0$ for some a, then $(x-a)$ is a factor of $p(x)$.*

Proof. Use Euclid's division lemma: Write $p(x) = (x-a)q(x) + r(x)$ for polynomials $q(x), r(x)$. We must have $\deg r < \deg(x-a)$ which means r is a constant, say c. Now, $p(a) = (a-a)q(a)+c = c$. But we are given that $p(a) = 0$. Hence $c = 0$, which means $(x-a)$ divides $p(x)$. □

Suppose we want to factor $p(x) = x^3 + x^2 - x - 1$. We can guess that $p(1) = 0$ so $(x-1)$ is a factor. So divide $p(x)$ by $(x-1)$ (using long division or in whichever way you prefer) to get

$$p(x) = (x-1)(x^2+2x+1).$$

The bracket part factors to $(x+1)^2$ so $p(x) = (x-1)(x+1)^2$. In general, there's another theorem you would find useful in guessing which value to try:

Theorem 7.1.5 (Rational Root Theorem)**.** *For a monic polynomial $p(x)$ with integer coefficients, $p(a) = 0$ implies a divides the constant term of $p(x)$.*

So suppose you had $p(x) = x^3 - 7x^2 + 16x - 12$. This is monic. Now, to find an a such that $p(a) = 0$, we try factors of -12, which are $\{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$. We find that $p(2) = 0$, so $(x-2)$ is a factor. On long division, we then get:

$$p(x) = (x-2)(x^2-5x+6).$$

The second bracket is easy to factorize. However, you can also factorize it using the factor theorem. Since $(2)^2 - 5(2) + 6 = 0$, hence $(x-2)$ divides it. So $p(x) = (x-2)(x-2)(x-3)$.

It's also useful to point out the remainder theorem:

Theorem 7.1.6 (Remainder Theorem)**.** *Let $p(x)$ be a polynomial. The remainder on dividing $p(x)$ by $(x-a)$ is $p(a)$.*

The proof is exactly the same as the one for Factor Theorem.

Probably the most used implication of the Factor Theorem that we would use a lot is that if $\alpha_1, \ldots, \alpha_n$ are the roots of the polynomial P, then we can write

$$P(x) = c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n),$$

where c is the leading coefficient of P.

7.1.5 Vieta's Theorem

Suppose that $p(x)$ has roots $\alpha_1, \ldots, \alpha_n$, then

$$\begin{aligned}
\sum_i \alpha_i &= -\frac{a_{n-1}}{a_n} \\
\sum_{i<j} \alpha_i\alpha_j &= \frac{a_{n-2}}{a_n} \\
\sum_{i<j<k} \alpha_i\alpha_j\alpha_k &= -\frac{a_{n-3}}{a_n} \\
&\vdots \\
\alpha_1 \ldots \alpha_n &= (-1)^n \frac{a_0}{a_n}.
\end{aligned}$$

I hope you have seen applications of this in algebra and are comfortable with these. You may also read them from some other algebra sources.

Let's look at a simple example:

Example 7.1.1 (PUTNAM)

Find all polynomials $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ such that $a_n \in \{\pm 1\}$ for all $0 \leq i \leq n-1$ satisfying the condition that all roots of $P(x)$ are real.

Let $\alpha_1, \ldots, \alpha_n$ be the roots. Then by Vieta,

$$\sum_i \alpha_i = -a_{n-1}, \quad \sum_{i<j} \alpha_i \alpha_j = a_{n-2}.$$

This means

$$0 \leq \sum_i \alpha_i^2 = \left(\sum_i \alpha_i\right)^2 - 2\left(\sum_{i<j} \alpha_i \alpha_j\right) = a_{n-1}^2 - 2a_{n-2} \leq 3.$$

This shows $0 \leq a_{n-1}^2 - 2a_{n-2} \leq 3$, hence $a_{n-2} = -1$. Vieta also gives $\alpha_1 \ldots \alpha_n = \pm 1$. Thus, by the AM-GM inequality, $3 \geq \alpha_1^2 + \cdots + \alpha_n^2 \geq n$. Now we can directly find the polynomials to be $x \pm 1, x^2 \pm x - 1$ and $x^3 - x \pm (x^2 - 1)$.

7.1.6 Irreducibility

Irreducibility is a very natural concept; it is an analogue of prime numbers. For instance, the number 10 reduces to 2×5. The number 7, however is "irreducible" and cannot be broken into the product of two numbers, unless one of them is 1. In a similar way we define irreducible polynomials. However, first I must define something known as a **unit**:

Definition 7.1.4. *Let* $\mathbf{R}$ *denote any one of* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. *Then an element in* $\mathbf{R}$ *is called a* ***unit*** *if it has an inverse in* $\mathbf{R}$. *i.e. an element* $y \in \mathbf{R}$ *such that* $xy = 1$.

Here, $\mathbf{R}$ can also be $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{R}[X]$ or $\mathbb{C}[X]$. The units of $\mathbb{Z}$ are ± 1. Every element of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, however, are units (why?). Now an element of $\mathbf{R}$ is called irreducible if it cannot be expressed as a product of two non-units. So $2x + 2 = 2(x + 1)$ is reducible in $\mathbb{Z}[X]$ since 2 is not a unit. However, in $\mathbb{Q}[X]$ it is irreducible since 2 is a unit.

Definition 7.1.5. *Let* $\mathbf{R}$ *denote any one of* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. *Then a non-constant polynomial* $p \in \mathbf{R}[X]$ *is called* ***irreducible over*** $\mathbf{R}$ *if it cannot be expressed as a product of two* ***non-units*** *in* $\mathbf{R}$.

For instance, $x^2+5x+6 = (x+2)(x+3)$ is reducible. However, $f(x) = x^2-2$ is irreducible over $\mathbb{Z}[X]$. On the other hand, $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$, and since $x \pm \sqrt{2} \in \mathbb{R}[X]$, hence this polynomial is reducible over $\mathbb{R}$. Also note the non-constant part. So $5x^2 - 10 = 5(x^2 - 2)$ is still considered irreducible.

An interesting idea is that if a polynomial has a root $\alpha \in \mathbf{R}$, then it is reducible over $\mathbf{R}$, since $(x-\alpha) \in \mathbf{R}[X]$ becomes a factor. However, being reducible need not mean it has a root. For instance,

$$x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1).$$

Hence the polynomial is reducible over $\mathbb{Z}[X]$, however does not have any root in $\mathbb{Z}$.

Let's talk about the simplest case; irreducibility over $\mathbb{C}[X]$. This follows from the fundamental theorem of Algebra:

Theorem 7.1.7 (Fundamental Theorem of Algebra)**.** *Every polynomial of degree at least* 2 *in* $\mathbb{C}[X]$ *is reducible into linear factors over* $\mathbb{C}[X]$.

Note the above says reducible into linear factors. This is much stronger than just reducible, since this tell us that it has complex roots. So

Lemma 7.1.4 (GCD of real polynomials)**.** *Let* $f(x) = c(x-\alpha_1)\dots(x-\alpha_k)$ *and* $g(x) = C(x-\beta_1)\dots(x-\beta_\ell)$. *Then the GCD of* f, g *over* $\mathbb{C}[X]$ *is the set of common factors of the form* $(x-\gamma)$ *that are common in both.*

This is because terms of the form $(x-\gamma)$ are irreducible factors themselves and behave as primes. Now do you see an analogy with the gcd of integers?

What about $\mathbb{R}[X]$ now? We know that complex roots come in pairs, i.e. if $P(z) = 0$, then $P(\bar{z}) = 0$ too. Also, $(x-z)(x-\bar{z}) = x^2 - (z+\bar{z}) + z\bar{z} = x^2 - \Re(z)x + |z| \in \mathbb{R}[X]$. Hence

Theorem 7.1.8 (Fundamental Theorem of Algebra)**.** *Every polynomial of degree at least* 2 *in* $\mathbb{C}[X]$ *is reducible into linear and quadratic factors in* $\mathbb{R}[X]$.

The most interesting case is irreducibility over rational or integer polynomials. There is no general answer for this, only certain criterion that work at times. Irreducibility of integer polynomials form very hard questions at times and need ingenious approaches. We won't discuss these criterion in this book, and you may read about them from some other source, for instance [19]. We will, however, discuss one of them which is important:

Theorem 7.1.9 (Gauss's Irreducibility Lemma)**.** *Suppose* $f \in \mathbb{Z}[X]$ *be a* ***monic*** *polynomial that is reducible into* $g(x)h(x)$ *where* $g, h \in \mathbb{Q}[X]$ *are* ***monic*** *polynomials. Then* g, h *have integer coefficients.*

So if we say f is reducible (which we generally say over $\mathbb{Q}$), we can assume this is over $\mathbb{Z}$.

Proof. Assume on the contrary that $f(x) = g(x)h(x)$ with $g, h \in \mathbb{Q}[X]$, such that at least one of them is not in $\mathbb{Z}[X]$. Take c_1 to be the *least integer* such that $c_1 g(x)$ has integer coefficients. Clearly then the coefficients of $c_1 g$ are coprime (why?). Similarly take c_2 so that $c_2 h \in \mathbb{Z}[X]$. Then

$$(c_1 c_2) f = (c_1 g)(c_2 h).$$

Now write $c_1 g(x) = a_n x^n + \dots + a_0$ and $c_2 h(x) = b_m x^m + \dots + b_0$ and $c_1 c_2 f(x) = k_{n+m} x^{n+m} + \dots + k_0$. Now since at least one of c_1, c_2 is greater than 1 (why?), hence there is a prime p dividing $c_1 C_2$. So p divides k_i for all i.

Now p does not divide all the coefficients of $c_1 g$ and $c_2 h$ (why?). So pick the smallest $0 \leq i \leq n$ and $0 \leq j \leq m$ such that $p \nmid a_i, b_j$. Thus $p \mid a_k$ for all $k > i$ and $p \mid b_k$ for all $k > j$. Then compare the coefficients of x^{i+j} on both the sides.

$$k_{i+j} = a_n b_{m-i-j} + \cdots + a_i b_j + \cdots + a_{n-i-j} b_m.$$

Here if the index of a or b is negative, set it to be 0 (why?). Now it is easy to check that the only term not divisible by p on the right is $a_i b_j$. But the left side is divisible by p, hence $p \mid a_i b_j$, but this is a contradiction. □

There's another way to state this result. Firstly, we define something known as a primitive polynomial:

Definition 7.1.6. *A polynomial $f \in \mathbb{Z}[X]$ is called **primitive** if the coefficients of f are coprime.*

Then the alternative way of stating Gauss's lemma is:

Theorem 7.1.10 (Gauss's Lemma (primitivity))**.** *The product of two primitive polynomials is primitive.*

Why are these two the same? I will let you answer this question.

7.1.7 Identical Polynomials

Definition 7.1.7. *Two polynomials P, Q are called **identical** if they have the same coefficient for same degree terms. That is, $\deg P = \deg Q$ and coefficient of x^i is the same in P, Q for any $0 \leq i \leq \deg P = \deg Q$. When two polynomials are identical, we write $P \equiv Q$.*

So, identical polynomials means "exactly the same", i.e. carbon copies. The important point in the definition is that it says the coefficients are same, and says nothing about the values. We say that are "formally" equal ("formal" in context of polynomial is used for coefficients)

Being equal in values is different. Having $P(1) = Q(1), P(2) = Q(2), \ldots$ means that have the same values. However, this doesn't mean they have the same coefficients. Being identical is *conceptually* different.

Now clearly, if two polynomials are identical, then they are always equal value wise. The interesting (and non-trivial part is the following):

Theorem 7.1.11. *If two polynomials f, g are equal value-wise for more than $\max\{\deg f, \deg g\}$ times, then they are identical.*

Please note that this is not obvious. For instance, this isn't true for polynomials in $\mathbb{F}_p[X]$ (see the special section of Modular Arithmetic Advanced). A **non-zero** polynomial P has at most $\deg P$ roots. This is more useful and fundamental than you think. The proof of the above lemma completely depends on this fact:

Proof. Define the polynomial $p(x) := f(x) - g(x)$. It has degree at most $d = \max\{\deg f, \deg g\}$. Now, by the hypothesis, it is zero for more than d values, that is has more than d roots. Hence, it must be the zero polynomial. So $f \equiv g$. □

Here's a simple corollary:

Corollary 7.1.1. *Let f be a polynomial such that $f(x) = 0$ for infinitely many x. Then $f \equiv 0$. Alternatively if $f(x) = g(x)$ for infinitely many x, then $f \equiv g$.*

This is very useful. For instance:

Example 7.1.2

Find all polynomials P with real coefficients such that $P(x^2 + x) = (x + 1)P(x)$ for all x and $P(1) = 1$.

Here, if we put $x = 1$, we get $P(2) = 2P(1) = 2$. Put $x = 2$ to get $P(6) = 3P(2) = 6$. Similarly proceeding we find $P(n) = n$ for any integer n of the form $x^2 + x$. So we guess $P(x) \equiv x$, but we only have this for integers, and that too only a small subset of them.

Here's the key argument: since the polynomials $P(x)$ and x are equal for infinitely many values, hence they are identically equal. So $P(x) \equiv x$ is true!

7.2 Lagrange Interpolation

Consider the following classic example:

Example 7.2.1

Let P be a degree 3 polynomial such that $P(1) = 2, P(2) = 3, P(3) = 4, P(4) = 5$. Find $P(5)$.

Firstly, note that we can write $P(x) = c(x-\alpha)(x-\beta)(x-\gamma)$ since it has degree 3. Using the given data, we can set up the equations and find 4 equations for the 4 variables c, α, β, γ. So, $P(x)$ is unique.

The idea now is to forcefully create a polynomial of degree 3 which gives these values. We start by writing the following:

$$P(x) = (x-2)(x-3)(x-4)+(x-3)(x-4)(x-1)+(x-4)(x-1)(x-2)+(x-1)(x-2)(x-3).$$

Each term serves as an "indicator term". For instance, when we put $x = 1$, all except the first term vanish. The first term gives $(1-2)(1-3)(1-4) = -6$. However, since we want $P(1) = 2$, hence we multiply this by $2/(-6)$. We do the same thing and refine our polynomial to the following:

$$P(x) = 3 \cdot \frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} + 4 \cdot \frac{(x-3)(x-4)(x-1)}{(2-3)(2-4)(2-1)} + 5 \cdot \frac{(x-4)(x-1)(x-2)}{(3-4)(3-1)(3-2)} + 2 \cdot \frac{(x-1)(x-2)(x-3)}{(4-1)(4-2)(4-3)}.$$

Do you see how clever this construction is? It is degree 3 clearly. It satisfies the given conditions. For instance, when we put $x = 2$, only the second term remains (the other vanish) and we get

$$P(2) = 0 + 0 + 4 \cdot \frac{(2-3)(2-4)(2-1)}{(2-3)(2-4)(2-1)} + 0 = 4.$$

This is the idea behind Lagrange Interpolation:

Theorem 7.2.1 (Lagrange Interpolation)**.** *A polynomial of degree n is uniquely determined by $n+1$ values. Further, if $P(x_i) = y_i$ for $i = 0, 2, \ldots, n$, then*

$$P(x) = \sum_{i=0}^{n} y_i \prod_{0 \le j \ne i \le n} \frac{x - x_j}{x_i - x_j}.$$

This theorem is the analogue of the Chinese Remainder Theorem in Algebra. It can be viewed as a generalization of the facts that two points uniquely determine a straight line, three points uniquely determine a plane, and so on. More important than the formula is the idea, the one we used to solve Example 7.2.1. Here's a nice application:

Example 7.2.2 (IMO Shortlist 1997)

Let p be a prime number and f an integer polynomial such that $f(0) = 0, f(1) = 1$ and $f(n)$ is congruent to 0 or 1 modulo p for every integer n. Prove that $\deg f \ge p-1$.

Firstly rule out $p = 2$, and so say $p > 2$ now. Assume on the contrary that $\deg f \le p-2$. Now we have information of f at $0, 1, 2, \ldots, p-1$, so it is only natural to use Lagrange Interpolation. We get

$$f(x) = \sum_{j=0}^{p-1} f(j) \prod_{i \ne j} \frac{x - i}{j - i}.$$

The above polynomial is obviously a degree $p-1$ polynomial, which is impossible. So the leading coefficient must be 0. This gives:

$$0 = \sum_{j=0}^{p-1} f(j) \prod_{i \ne j} \frac{1}{j - i} = \sum_{j=0}^{p-1} f(j) \cdot \frac{(-1)^{p-1-j}}{j!(p-j-1)!}.$$

However, this shows (why?)

$$\sum_{j=0}^{p-1} (-1)^j \binom{p-1}{j} f(j) = 0.$$

Now we consider this modulo p. Firstly,

$$\binom{p-1}{j} = \frac{(p-1)(p-2)\ldots(p-j)}{j(j-1)\ldots 1} \equiv \frac{(-1)(-2)\ldots(-j)}{j!} \equiv (-1)^j \pmod{p}.$$

(This result was Problem 2.14.2). So we find

$$f(0) + f(1) + \cdots + f(p-1) \equiv 0 \pmod{p}.$$

However since $f(i) \in \{0, 1\} \pmod{p}$, this is impossible unless all $f(i)$ are 0, which is false since $f(1) = 1$. Hence we are done.

Question 7.2.1. *Why did we treat $p = 2$ individually?*

Example 7.2.3 (ELMO 2014 Shortlist N3)

Let t and n be fixed integers each at least 2. Find the largest positive integer m for which there exists a polynomial P, of degree n and with rational coefficients, such that the following property holds: exactly one of

$$\frac{P(k)}{t^k} \text{ and } \frac{P(k)}{t^{k+1}}$$

is an integer for each $k = 0, 1, \ldots, m$.

We want $P \in \mathbb{Q}[X]$, and want to work with the values of P rather than the polynomial (i.e. coefficients) itself (and hence want to treat it like an arbitrary function). Hence, Lagrange Interpolation is useful here; we can do whatever we want with $P(0), P(1), \ldots, P(m)$, but we would still be able to ensure such a polynomial with rational coefficients exist.

In this spirit, clearly $m = n$ works: just set $P(k) = t^k$ for all $k = 0, 1, \ldots, n$. Now suppose $m > n$ exists. Write $P(k) = a_k t^k$ with $\gcd(a_k, t) = 1$ and $k = 0, 1, \ldots, m$. If $\deg P = n$, then the formula of P we get by Lagrange Interpolation should have the coefficient of x^m to be zero. But this is

$$0 = \sum_{j=0}^{m} P(j) \prod_{i \neq j} \frac{1}{j-i} = \sum_{j=0}^{m} t^j a_j \frac{(-1)^{m-j}}{j!(m-j)!}.$$

Hence,

$$\sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} t^j a_j = 0.$$

But modulo t this evaluates to $(-1)^m a_0$, hence $t \mid a_0$, a contradiction.

We now do a simple problem, which is surprisingly useful in a lot of scenarios:

Example 7.2.4

Prove that if for a polynomial p, we have $p(\mathbb{Q}) \subset \mathbb{Q}$ (i.e. a rational input always gives a rational output), then p has rational coefficients.

The proof is simple. Just take any $\deg P + 1$ rational points. Then look at the interpolation formula which everywhere involves only rational numbers, showing the coefficients are rational.

A natural extension of this result is the following problem:

Example 7.2.5

Find all polynomials $f(x)$ with real coefficients such that $x \in \mathbb{Q} \iff f(x) \in \mathbb{Q}$

In other words rational inputs give rational values, whereas irrational ones give irrational values. Firstly by our result above, we get that $f \in \mathbb{Q}[X]$. Now clearly if f satisfies the conditions, then so does cf for any integer c. Hence we can multiply by a suitable constant and so assume without loss of generality that $f \in \mathbb{Z}[X]$. Further multiply by -1 if needed to make the leading coefficient positive.

Our intuition tells us that $\deg f = 1$ should be the only possibility. So let's assume that $\deg f > 1$ and try to see if we can find a contradiction. The key difference in polynomials of degree greater than 1 from linear ones is the following

Lemma 7.2.1. *Let ε be fixed. Then for any polynomial $f : \mathbb{R} \to \mathbb{R}$ with $\deg f > 1$ and leading coefficient positive, the difference $f(x+\varepsilon) - f(x)$ grows arbitrarily large.*

So we would like to create an interval $\mathcal{I}$ of length ε such that for any rational $x \in \mathcal{I}$, $f(x)$ is not an integer. But $f(x+\varepsilon) - f(x)$ grows very large, hence some $x \in \mathcal{I}$ must satisfy $f(x) \in \mathbb{Z}$ (since polynomials are continuous. Just visualize the graph), which would be our desired contradiction. This is our plan of action.

This is however easy. Suppose f has leading coefficient a. Then if $f(q)$ is an integer, then the denominator of q must be divisible by a (why?) So take an interval $\mathcal{I}$ of length less than $\frac{1}{a}$ so that I does not contain any multiple of $\frac{1}{a}$. This works.

Problems for Practice

Problem 7.2.1. Using Lagrange Interpolation, prove that if a polynomial $p(x)$ has roots $x_1, \ldots, x_n$ and has leading coefficient c, then

$$p(x) = c(x - x_1) \ldots (x - x_n).$$

Problem 7.2.2. Prove Lemma 7.2.1.

7.3 A Periodicity lemma

One of the, if not the most useful lemma related to integer polynomials is the following:

Lemma 7.3.1. *Let $P \in \mathbb{Z}[X]$ be an integer polynomial. Then for any integers a, b,*

$$a - b \mid P(a) - P(b).$$

Proving this is not too hard if we know the key lemma: For any integers a, b we have $a - b \mid a^n - b^n$ for any positive integer n.

Now write $P(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$. Then

$$P(a) - P(b) = c_n(a^n - b^n) + c_{n-1}(a^{n-1} - b^{n-1}) + \cdots + c_1(a-b) + c_0 - c_0$$

Each bracket here is of the form $a^k - b^k$, which is divisible by $(a-b)$. Hence, the entire expression on the right side becomes divisible by $(a-b)$, hence we are done.

Comment 7.3.1: Alternatively, since $a \equiv b \pmod{(a-b)}$, hence

$P(a)-P(b) = c_n(a^n-b^n)+c_{n-1}(a^{n-1}-b^{n-1})+\cdots+c_1(a-b)+c_0-c_0 \equiv 0 \pmod{(a-b)}$.

So, even if you forgot the $a-b \mid a^k-b^k$ result, modular arithmetic is here to save you!

One special form in which this lemma can be represented is the following:

Lemma 7.3.2 (Periodicity)**.** *Let $P \in \mathbb{Z}[X]$ be an integer polynomial. If $m \equiv n \pmod{a}$, then*

$$P(m) \equiv P(m) \pmod{a}.$$

What this means is that $\{P(0), P(1), P(2), \ldots, P(a-1)\}$ are the only values we honestly care about modulo a, just like in normal modular arithmetic of integers. A natural question now is, when is $\{P(0), P(1), \ldots, P(a-1)\}$ a complete residue class? Example 7.4.2 is inspired from this.

Let's look at some simple applications first.

Example 7.3.1 (USAMO 1974)

Let a, b, c be three distinct integers, and let P be a polynomial with integer coefficients. Show that in this case the conditions $P(a) = b, P(b) = c, P(c) = a$ cannot be satisfied simultaneously

We simply use the lemma which gives $a - b \mid P(a) - P(b) = b - c$. We similarly get $b - c \mid c - a$ and $c - a \mid a - b$. However then $|a-b| \leq |b-c| \leq |c-a| \leq |a-b|$, so equality hold everywhere. So if we assume without loss of generality that $a = \max\{a, b, c\}$ (note that we can't assume an ordering here since this is cyclic not symmetric). But then $a-b = |a-b| = |c-a| = a-c$ implies $b = c$, contradicting the fact that a, b, c were distinct.

Let's look at another interesting example.

Example 7.3.2

Find all integer polynomials f such that for all $n \in \mathbb{N}$, we have $f(n)$ and $f(2^n)$ are relatively prime.

On some simple guess work you can conjecture that no polynomial works, non-constant ones at least. It's useful to keep the solution set in mind while solving such problems.

Take a prime $p \mid f(2^t)$ for some t. What we do is let $n = 2^t$ for simplicity. Then, $p \mid f(n)$ implies $p \mid f(n + kp)$. So, $p \nmid f(2^{n+kp})$. However, if we can get $n + kp \equiv t \pmod{p-1}$, then $f(2^{n+kp}) \equiv f(2^t) \equiv 0 \pmod{p}$. And luckily this is possible, by choosing $k \equiv (t-n) \cdot p^{-1} \pmod{p-1}$. So, we have a contradiction.

What does this mean? Does it mean no polynomial exists? No, it basically means $f(2^r)$ can't have a prime factor, i.e. it will always be ± 1. Hence, f must be identically ± 1 (why?). So, $f(x) = 1$ for all x or $f(x) = -1$ for all x works.

Comment 7.3.2: Once we took a prime $p \mid f(t)$, we had $p \nmid f(t)$ and $p \nmid f(2^{2^t})$. However, our lemma tell us that we can reduce things inside $f(\bullet)$ modulo p. So, if 2^{2^t} reduces to 2^t modulo p, we would have a contradiction. However, this is not always true.

Now that we have our goal in mind, we try to add in a variable that we can adjust so that $f(\bullet)$ does reduce to $f(2^t)$. So, what we did was use $p \mid f(n + kp)$, where k was a variable. We basically used the periodic property to add a "degree of freedom", which is always very helpful. While this might sound weird, it is a common albeit very useful trick. You will see this often in many problems, so keep it in mind. Try to point it out wherever you see it.

7.4 Some Arithmetic Properties

We first define two terms for notational ease:

Definition 7.4.1. *For any polynomial $p \in \mathbb{Z}[X]$, we denote by $\mathcal{F}(P)$ the set $\{p(n) : n \in \mathbb{Z}\}$, and call this the **value set of** p.*

Then we have the following interesting result we present as a problem:

Example 7.4.1 (Value Sets miss an AP)

Let $p \in \mathbb{Z}[X]$ be such that $\deg p > 1$. Then there exists an infinite arithmetic sequence none of who terms can be expressed as $p(x)$ for some $x \in \mathbb{Z}$.

Proof. Assume on the contrary, and then for any n and $d > 2$, we can find an x such that $p(x) \equiv n \pmod{d}$. Thus, $p(n), p(n+1), \ldots, p(n+d-1)$ form a residue class modulo d for all n. However, since $\deg p > 1$ and hence we can choose an N such that $D = p(N+1) - p(N) > 2$. Then taking $(n, d) = (N, D)$ gives a contradiction. □

Before we introduce the next theorem, consider the following term:

Definition 7.4.2. *For any polynomial $p \in \mathbb{Z}[X]$, the set of primes dividing any element of $\mathcal{F}(p)$ is denoted by $\mathfrak{P}(p)$ and call it the **prime set of** p.*

Theorem 7.4.1 (Schur's Theorem)**.** *The prime set of any non-constant polynomial is infinite.*

Proof. Roughly the idea is the same as Euclid's proof for the infinitude of primes. Let f be the polynomial.

- Suppose $f(0) = 0$. Then $n \mid f(n)$ and so the result is obvious here.
- Suppose $f(0) \neq 0$. We would like $f(0) = 1$. But direct scaling doesn't work because we want integer coefficients. So we force this by defining $g(x) := \frac{f(xf(0))}{f(0)}$, so that $g \in \mathbb{Z}[X]$ and $g(0) = 1$.

  Now, for large n, $g(n)$ is non zero always. Then $g(n) \equiv 1 \pmod{n}$ for all $n \in \mathbb{N}$. So if $\mathfrak{P}(g) = \{p_1, \ldots, p_\ell\}$, then pick $n = p_1 \cdots p_\ell$ and so $g(n) = kn + 1$ for some k, hence has a new prime factor, the desired contradiction

Hence, $\mathfrak{P}(f)$ is infinite. □

Let's look at a few applications:

Example 7.4.2

For which polynomials $f \in \mathbb{Z}[X]$ do $\{f(0), f(1), \ldots, f(p-1)\}$ form a complete residue class modulo p for all sufficiently large primes p?

Proof. In other words, which polynomials are surjective modulo large primes. Clearly linear polynomials work. We show that these are the only ones. The idea in this problem is too look at common differences (which if often useful if you wanna show a polynomial is linear). So define $Q(x) := P(x+1) - P(x)$. Then for large enough primes, $Q(x)$ is non-zero modulo p by the problem statement. This means $\mathfrak{P}(Q)$ is finite, which by Schur's Theorem means $\deg Q = 0$. Hence $P(x)$ must be linear, and we are done. □

Example 7.4.3 (Taiwan 2014 TST 1, Problem 2)

For a fixed integer k, determine all polynomials $f(x)$ with integer coefficients such that $f(n)$ divides $(n!)^k$ for every positive integer n

Proof. The idea here is that any prime divisor of $n!$ is $\leq n$. So if we pick p such that $p \mid f(n)$, then clearly we can assume $1 \leq n \leq p$ (by the periodicity lemma). However then $p \mid n!$ implies $p \leq n$. Hence, $p \mid f(p)$ implying $p \mid a_0$, the constant coefficient.

However by Schur's Theorem, if f is non-constant there exist infinitely many such primes p. Hence a_0 must be 0. So define the polynomial $g(x) = \frac{f(x)}{x} \in \mathbb{Z}[X]$. Now $\deg g < \deg f$ so we can keep on reducing the degree till we get a constant polynomial (why do we end here?). In other words, $f(x)$ was originally of the form cx^w for some w. Putting back we see that we must have $f(x) = \pm x^a$ with $0 \leq a \leq k$, which indeed works. □

For a generalization of Schur's theorem, see Problem 9.6.11. For now, we discuss another lemma which is extremely useful:

Lemma 7.4.1. *Let $f \in \mathbb{Z}[X]$ be a polynomial. Then for any $n, k \in \mathbb{Z}$,*

$$f(n) \mid f(n + kf(n)).$$

In particular, $f(n) \mid f(n + f(n))$.

The proof is a fun application that I leave as an exercise. Let's look at some examples:

Example 7.4.4 (Polish)

Find all polynomials with integer coefficients such that for all positive integers n, $f(n) \mid 2^n - 1$.

We can guess that $\deg f > 0$ doesn't seem possible, and the only constant polynomials that work are ± 1. Let's try to see if we can prove there is no other solution.

Note that if f is a solution, then so is $-f$. So assume without loss of generality that the leading coefficient of f is positive. So we can assume $f(n) > 0$ for n large.

So $f(n) \mid f(n + f(n)) \mid 2^{n+f(n)} - 1$. Hence, $f(n) \mid 2^{f(n)} - 1$ (why?). Now, does $x \mid 2^x - 1$ remind you of something?

Comment 7.4.1: For a nice generalization of this, see Problem 7.7.10. Also, here's a much more challenging problem which is stronger than this Polish problem too:

Find all polynomials with integer coefficients such that for all primes p, $f(p) \mid 2^p - 2$.

I suggest you do it after doing the Constructions chapter, as tools like Dirichlet's theorem are likely to be helpful.

Example 7.4.5 (Problems from The Book)

Find all polynomials $f \in \mathbb{Z}[X]$ such that for any relatively prime positive integers a, b the sequence $(f(an + b))_{n \geq 0}$ contains an infinite number of terms, any two of which are relatively prime.

Firstly, observe that the f is non-constant. Since $f, -f$ both work, hence assume the leading term is positive in f. Now, pick N such that $f(n) > 2$ for all $n > N$.

Thus by the identity $f(n) \mid f(n + kf(n))$ for all $k \in \mathbb{Z}$, we find $\gcd(n, f(n)) \neq 1$ for $n > N$ (why?). In particular when $n = p > N$ is a prime, we must have $p \mid f(p)$ (why?). Thus, $p \mid f(0)$ for all primes $> N$, and hence $f(0) = 0$. Write $f(x) = xg(x)$ with $g \in \mathbb{Z}[X]$.

Now $\deg g < \deg f$ and g also satisfies the problem's property. Hence we can keep on going down till a constant polynomial, and so $f(n) = cx^n$ with $c > 0$ (recall that the leading coefficient was assumed to be positive). But then $c = +1$ otherwise c always becomes an obvious common factor. Hence $f(X) = \pm X^n$, which indeed all work for any n.

Problems for Practice

Problem 7.4.1. Prove Lemma 7.4.1.

7.5 Gauss's Lemma

In this final section, I would like to point out an interesting result:

Theorem 7.5.1 (Gauss's Lemma)**.** *Let $P \in \mathbb{Z}[X]$ be a monic polynomial with integer coefficients. Suppose that $P(q) = 0$ for a rational number q. Then q must be an integer.*

The important thing to keep in mind is that the polynomial must be monic. Proving this is not too hard, and I suggest you try it yourself before seeing it below.

Proof. Let $q = u/v$, where $\gcd(u, v) = 1$. We want to show $v = 1$. Suppose $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then

$$\left(\frac{u}{v}\right)^n + a_{n-1}\left(\frac{u}{v}\right)^{n-1} + \cdots + a_0 = 0 \Leftrightarrow -u^n = v(a_{n-1}u^{n-1} + \cdots + a_0 v^{n-1}).$$

Hence, $v \mid u^n$. However, we know that $\gcd(u, v) = 1$, so this implies $v = 1$, as desired. □

Question 7.5.1. *Where did we use the fact that $P(x)$ is monic? What goes wrong if it isn't monic? Give an example of a non-monic polynomial with a rational root that is not an integer.*

This lemma basically follows from the Rational Root Theorem too. It has many equivalent forms, for instance it says that any real root of a monic integer polynomial is either an integer, or an irrational number. Another equivalent form is that any rational algebraic integer must be an integer (see the special section of this chapter).

Question 7.5.2. *Is there any relation between this Gauss's Lemma and the Gauss's irreducibility lemma we did earlier?*

Example 7.5.1

Let a, b, c be integers such that $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ and $\frac{b}{a} + \frac{c}{b} + \frac{a}{c}$ are both integers. Prove that $|a| = |b| = |c|$.

Clearly, if $|a| = |b| = |c|$, then the two expressions are integers. The interesting part is that if these two are integers, then this is the only possibility. This is an example of the situation when the obvious guess is the only solution.

To prove this, the first trick is to let $u = a/b, v = b/c, w = c/a$. Then u, v, w are rational numbers. We basically want to show that these are integers, and then we would be done (why?). Does this ring a bell? Attempting to show a rational number is an integer should

always remind you of Gauss's lemma. So keep this at the back of your mind while attempting this problem. Now the given condition is

$$u+v+w, \frac{1}{u}+\frac{1}{v}+\frac{1}{w} \in \mathbb{Z}.$$

Clearly $uvw = 1$ (why?), hence the second term implies $vw + wu + uv \in \mathbb{Z}$. Now we have two term $u + v + w$ and $vw + wu + uv$. Do these remind you of something?

If you said Vieta, then your thought is spot on. We create the polynomial with roots u, v, w :

$$P(x) = x^3 - (u+v+w)x^2 + (vw+wu+uv)x - uvw.$$

Everything comes together now! We needed a polynomial for Gauss's lemma, and this polynomial seems good, since it has the roots u, v, w! So if we can show P has integer coefficients (it is already monic), then the roots u, v, w which are currenty rational numbers must be integers, which is what we want to prove. However, $u + v + w, vw + wu + uv \in \mathbb{Z}$ is given, and $uvw = 1 \in \mathbb{Z}$. So we are done! Here's a properly written proof:

Proof. Let $u = a/b, v = b/c, w = c/a$. Clearly $u, v, w \in \mathbb{Q}$. Define the polynomial

$$P(x) = (x-u)(x-v)(x-w) = x^3 - (u+v+w)x^2 + (vw+wu+uv)x - uvw.$$

We claim that this has integer coefficients. Indeed, $u + v + w \in \mathbb{Z}$ is given, $uvw = \frac{a}{b} \cdot \frac{b}{c} \cdot \frac{c}{a} = 1 \in \mathbb{Z}$, and finally

$$vw + wu + uv = uvw(\tfrac{1}{u} + \tfrac{1}{v} + \tfrac{1}{w}) = (\tfrac{1}{u} + \tfrac{1}{v} + \tfrac{1}{w}) \in \mathbb{Z}$$

is given. Thus, P is a monic polynomial with integer coefficients such that the three rational numbers u, v, w are its roots. By Gauss's Lemma, $u, v, w \in \mathbb{Z}$. Hence $a \mid b, b \mid c, c \mid a$, which respectively imply $|a| \leq |b|, |b| \leq |c|, |c| \leq |a|$. Hence $|a| = |b| = |c|$, which is what we wanted to prove. □

7.6 Example Problems

We start of by an easy problem and give a fascinating proof to it:

Example 7.6.1 (Israel November TST 2 P1)

Find all polynomials $P(x) \in \mathbb{Z}[x]$ such that for all $x \in \mathbb{Z}$ and $n \in \mathbb{N}$

$$n \mid P^n(x) - x.$$

Here, P^n is the composition of P n times.

Suppose $f(x) = P(x) - x$ is non-constant. Hence $\mathfrak{P}(f)$ is infinite, so pick a prime $p \mid f(n)$ for some n. So now we know P^p is identity in $\mathbb{F}_p$. If we view P has a function in $\mathbb{F}_p$, then the cycle length is either 1 or p as p is a prime. However, since it has one fixed point n, hence it must be identity in $\mathbb{F}_p$. This is true for infinitely many primes and hence $P(x) \equiv x$.

If however f is constant, then $P(x) = x + c$, which also works. □

Example 7.6.2 (Indian TST 2019 Day 4 P1)

Determine all non-constant monic polynomials $f(x)$ with integer coefficients for which there exists a natural number M such that for all $n \geq M$, $f(n)$ divides $f(2^n) - 2^{f(n)}$

Proof. Firstly, pick a prime $p \in \mathfrak{P}(f)$. Then (note again how we add a degree of freedom k) pick k large enough so that $n + pk > M$. Then

$$p \mid f(n+pk) \mid f(2^{n+pk}) - 2^{f(n+pk)} \equiv f(2^{n+k}) - 2^{f(n+k)} \pmod{p}$$

where we used Fermat's Little Theorem and Lemma 7.3.2. Now pick a k such that $n + k \equiv r \pmod{p}$ for any r. Thus $p \mid f(2^r) - 2^{f(r)}$. Now fix r and pick a large prime p (since $\mathfrak{P}(f)$ is infinite) so that $p > f(2^r) - 2^{f(r)}$. This shows $f(2^r) = 2^{f(r)}$ for any r.

Now $2^{f(n)} = f(2^n) \equiv f(0) \pmod{2^k}$ for any $k < n$. Now we can assume without loss of generality that the leading coefficient of f is positive. Then we can pick a large n such that $f(n) > k$ for a fixed k. Hence, $2^k \mid 2^{f(n)}$ and so $2^k \mid f(0)$. Since this is true for all k, hence we must have $f(0) = 0$.

Finally, $f(2^n) = 2^{f(n)}$ by putting $n = 0$ gives $f(1) = 1$. Putting $n = 1$ thus gives $f(2) = 2$. Putting $n = 2$ would give $f(4) = 4$. Similarly we get $f(2^k) = 2^k$ for all k. Hence $f(x) = x$ holds for infinitely many x, which shows $f(x) = x$ for all x. Considering we assume the leading coefficient of f was positive, we now get that $f(x) = \pm x$ are the only possibilities. □

The next problem will test your concepts of general polynomials (the basics we did at the start)!

Example 7.6.3 (Romania TST 6 2009, Problem 2)

Let n and k be positive integers. Find all monic polynomials $f \in \mathbb{Z}[X]$, of degree n, such that $f(a)$ divides $f(2a^k)$ for $a \in \mathbb{Z}$ with $f(a) \neq 0$.

(In this solution, just to avoid confusion, you should note that $f(a)$ is talking about an integer only, whereas $f(x)$ is talking about a polynomial and hence all values of x at once).

Proof. Since f is monic, hence $f \equiv 0$ is rejected. Now clearly $f(2x^k)$ is a polynomial in x with integer coefficients. Hence, using Euclid's Division Lemma, we can write $f(2x^k) = f(x)q(x) + r(x)$ where $q, r \in \mathbb{Q}[X]$ with $\deg r < \deg f$. We would like to work with integer polynomials instead of rational ones. What do we do?

We can find an integer N such that Ng, Nr both are in $\mathbb{Z}[X]$. Now since $f(x) = 0$ only for finitely many x, hence $f(a) \mid Nr(a)$ for all large a. However, this is impossible since $\frac{Nr(x)}{f(x)}$ tends to 0 as x tends to infinity (why?) so it can't always be an integer.

Thus, we find $f(x) \mid Nf(2x^k)$ holds as a polynomial identity in $\mathbb{Z}[X]$. Let α be a root of $f(x)$. Then this shows that $Nf(2\alpha^k) = 0$, so that $2\alpha^k$ is another root. So for every root α, we can find a new root $2\alpha^k$. If $|\alpha| \geq 2$, then $|2\alpha^k| > |\alpha|$, and so f has infinitely many roots, which is impossible unless $f \equiv 0$ (which is not possible as said before). However why must such a root with absolute values at least 1 always exist?

Question 7.6.1. *Consider $f(x) = 2x - 1, 2x^2 - 1, 5x^3 - 1$. All these have no roots with absolute values at least 1. Which hypothesis in the problem prevents these situations?*

The key hypothesis now is that f is monic. So if the constant term of f is c, then product of roots has magnitude $|c| \geq |1|$ (unless $c = 0$). Hence there exists at least one root with absolute value at least 1, which gives us a contradiction.

So we must have $c = 0$, so that $x \mid f(x)$.

Now replace $f(x)$ by $g(x) = \frac{f(x)}{x} \in \mathbb{Z}[X]$ and repeat the process (repeat the steps to check each step is still valid). We can keep on doing this and we find that the only factor of $f(x)$ is x, so that $f(x) = x^n$. Clearly this and $f \equiv 0$ work, and hence are the only solutions. □

We conclude this chapter with two amazing and very challenging problems.

Example 7.6.4 (APMO 2018/5)

Find all polynomials $P(x)$ with integer coefficients such that for all real numbers s and t, if $P(s)$ and $P(t)$ are both integers, then $P(st)$ is also an integer.

Proof. Our first step should be guessing the answer. Clearly, $P(x) = \pm x^d + b$ works. Let's try the problem now:

Call a number x *good* if $P(x) \in \mathbb{Z}$. So we are given that if s, t are good, then so is their product. We make a few observations first. Suppose x is good.

- For any $n \in \mathbb{Z}$, nx is good.
- For any $n \in \mathbb{N}$, x^n is good.

Now suppose x is rational, then say $P(x) = r$. Suppose the denominator of x is q. Then multiplying both sides by $q^{\deg P}$ shows $q^{\deg P} \mid a_0$, where a_0 is the leading coefficient of P. In fact, we can do the same with x^k (which is also rational) to find $q^{k \deg P} \mid a_0$ for all k, which shows $q = 1$ or $a_0 = 0$, the latter being impossible. Hence, $q = 1$ so that $x \in \mathbb{Z}$. Hence we have shown the following:

Claim. *Any good rational number is an integer.*

Now suppose r is good. Then $P(kr) = a_k \in \mathbb{Z}$ for all k. Hence we can use these to determine $P(x)$ using Lagrange Interpolation (we set $\deg P = d$):

$$P(x) = \sum_{k=0}^{d} a_k \prod_{i \neq k} \frac{x - ir}{kr - ir}.$$

Hence, the leading coefficient of P is $\frac{1}{r^d} q \in \mathbb{Z}$ for some $q \in \mathbb{Q}$. So $r^d \in \mathbb{Q}$. But since r was good, hence so is r^d. So by our claim we find $r^d \in \mathbb{Z}$. Hence we have proved the following:

Claim. *For any good r, we have $r^{d-1} \in \mathbb{Z}$ for all n.*

The finish is not very hard now. Define $f(x) = P(x) - Ax^d$ where A is the leading coefficient of A. It is easy to see that this satisfies the problem conditions too. Hence, □

Example 7.6.5 (Iranian 2015 Round 3 number theory P4)

a, b, c, d, k, ℓ are positive integers such that for every natural number n the set of prime factors of $n^k + a^n + c, n^\ell + b^n + d$ are same. prove that $k = l, a = b, c = d$.

Proof. We first choose which n to work with (which make our job easier). Suppose we fix constants α. Let n satisfy $n \equiv \alpha \pmod{p-1}$, i.e. $n = (p-1)t + \alpha$ for any t. The advantage of this is that $n^k + a^n + c \equiv n^k + a^\alpha + c \pmod{p}$, and so the exponent of a is fixed now.

Now since p divides both $n^k + a^\alpha + c, n^\ell + b^\alpha + d$, hence

$$(-a^\alpha - c)^\ell \equiv \left(n^k\right)^\ell = \left(n^\ell\right)^k \equiv (-b^\alpha - d)^k \pmod{p}.$$

Hence $p \mid (-a^\alpha - c)^\ell - (-b^\alpha - d)^k$. So unless this quantity is 0, this shows p is bounded. But since p divides $n^k + a^\alpha + c = ((p-1)t + \alpha)^k + a^\alpha + c = P(t)$, i.e. a polynomial in t, hence by Schur's theorem this is a contradiction.

Hence $(-a^\alpha - c)^\ell = (-b^\alpha - d)^k$. The best part is that the identity is true for all α. The problem is not too hard now. This shows $(a^\alpha + c)^\ell = (b^\alpha + d)^k$. Let $\gcd(k, \ell) = g$. Then $a^\alpha + c$ becomes a perfect k/gth power. So pick $\alpha = kx/g$ for some x. Then a^α is a perfect power k/gth power, and so is $a^\alpha + c$. However, two perfect k/gth powers cannot always differ by c, and we have a contradiction. □

7.7 Practice Problems

Problem 7.7.1 (USAMO 1975/3). If $P(x)$ denotes a polynomial of degree n such that $P(k) = \frac{k}{k+1}$ for $k = 0, 1, 2, \ldots, n$, determine $P(n+1)$.

Problem 7.7.2 (AoPS). Let $a_1, a_2, ..., a_n$ be n distinct positive integers. Let $p_i = P'(a_i)$, where

$$P(x) = \prod_{i=1}^{n}(x - a_i)$$

Prove that $\sum_{i=1}^{n} \frac{Q(a_i)}{p_i}$ is a integer for all positive integer k and polynomials Q with integer coefficients.

Problem 7.7.3 (AoPS). Find all polynomials P with integer coefficients such that for any reals a, b such that $P(a+b)$ is integer if and only if $P(a) + P(b)$ if an integer. **Hints:** 112

Problem 7.7.4 (IMO Shortlist 2005 N3). Let a, b, c, d, e and f be positive integers. Suppose that the sum $S = a + b + c + d + e + f$ divides both $abc + def$ and $ab + bc + ca - de - ef - fd$. Prove that S is composite. **Hints:** 370 43

Problem 7.7.5 (IMO 2006/5). Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients and let k be a positive integer. Consider the polynomial $Q(x) = P(P(\ldots P(P(x))\ldots))$, where P occurs k times. Prove that there are at most n integers t such that $Q(t) = t$. **Hints:** 41 123 311

Problem 7.7.6. Find all polynomials $P \in \mathbb{R}[X]$ such that if $P(a)+P(b)$ is rational whenever $a + b$ is rational for any $a, b \in \mathbb{R}$. **Hints:** 164 272 166

Problem 7.7.7 (ELMO 2016/4). Big Bird has a polynomial P with integer coefficients such that n divides $P(2^n)$ for every positive integer n. Prove that Big Bird's polynomial must be the zero polynomial. **Hints:** 383 285

Problem 7.7.8 (ELMO 2019/1). Let $P(x)$ be a polynomial with integer coefficients such that $P(0) = 1$, and let $c > 1$ be an integer. Define $x_0 = 0$ and $x_{i+1} = P(x_i)$ for all integers $i \geq 0$. Show that there are infinitely many positive integers n such that $\gcd(x_n, n + c) = 1$. **Hints:** 459 8 36

Problem 7.7.9 (USAMO 1995/4). Suppose $q_0, q_1, q_2, \ldots$ is an infinite sequence of integers satisfying the following two conditions:

1. $m - n$ divides $q_m - q_n$, for $m > n \geq 0$,
2. there is a polynomial P, such that $|q_n| < P(n)$ for all n.

Prove that there is a polynomial Q such that $q_n = Q(n)$ for all n. **Hints:** 292 51 422 460

Problem 7.7.10 (Iran MO 3rd round 2016 finals Number Theory P2). We call a function g special if $g(x) = a^{f(x)}$ (for all x) where a is a positive integer and f is polynomial with integer coefficients such that $f(n) > 0$ for all positive integers n.

A function is called an exponential polynomial if it is obtained from the product or sum of special functions. For instance, $2^x 3^{x^2+x-1} + 5^{2x}$ is an exponential polynomial.

Prove that there does not exist a non-zero exponential polynomial $f(x)$ and a non-constant polynomial $P(x)$ with integer coefficients such that

$$P(n)|f(n)$$

for all positive integers n. **Hints:** 172 202 360 158 **Sol:** pg. 297

Problem 7.7.11 (USA TSTST 2018/1). Find all functions $\theta : \mathbb{Z}[x] \to \mathbb{Z}$ such that for any polynomials $p, q \in \mathbb{Z}[x]$,

1. $\theta(p+1) = \theta(p) + 1$, and
2. If $\theta(p) \neq 0$ then $\theta(p)$ divides $\theta(p \cdot q)$.

Hints: 125 157 82

Problem 7.7.12 (IMO Shortlist 2002 N6). Find all pairs of positive integers $m, n \geq 3$ for which there exist infinitely many positive integers a such that

$$\frac{a^m + a - 1}{a^n + a^2 - 1}$$

is itself an integer. **Hints:** 400 64 309 464

Problem 7.7.13 (Problems from The Book). Find all polynomials f with integer coefficient such that $f(n) \mid n^{n-1} - 1$ for all sufficiently large n. **Hints:** 190 420 447 27 319 53

Problem 7.7.14 (USAMO 2006/3). For integral m, let $p(m)$ be the greatest prime divisor of m. By convention, we set $p(\pm 1) = 1$ and $p(0) = \infty$. Find all polynomials f with integer coefficients such that the sequence

$$\{p\left(f\left(n^2\right)\right) - 2n\}_{n \geq 0}$$

is bounded above. (In particular, this requires $f\left(n^2\right) \neq 0$ for $n \geq 0$.) **Hints:** 145 395 405 253 246

Problem 7.7.15 (USA TST 2020/5). Find all integers $n \geq 2$ for which there exists an integer m and a polynomial $P(x)$ with integer coefficients satisfying the following three conditions:

1. $m > 1$ and $\gcd(m, n) = 1$;
2. the numbers $P(0)$, $P^2(0)$, ..., $P^{m-1}(0)$ are not divisible by n; and

3. $P^m(0)$ is divisible by n.

Here P^k means P applied k times, so $P^1(0) = P(0)$, $P^2(0) = P(P(0))$, etc.

Problem 7.7.16 (IMO Shortlist 2011 N6). Let $P(x)$ and $Q(x)$ be two polynomials with integer coefficients, such that no nonconstant polynomial with rational coefficients divides both $P(x)$ and $Q(x)$. Suppose that for every positive integer n the integers $P(n)$ and $Q(n)$ are positive, and $2^{Q(n)}-1$ divides $3^{P(n)}-1$. Prove that $Q(x)$ is a constant polynomial. **Hints:** 413 205 451 271 13 258 **Sol:** pg. 297

Problem 7.7.17 (2020 Korean MO winter camp Test 1 P3). Find all integer coefficient polynomials Q such that $Q(n) \geq 1$ $\forall n \in \mathbb{Z}_+$. $Q(mn)$ and $Q(m)Q(n)$ have the same number of prime divisors $\forall m, n \in \mathbb{Z}_+$. **Hints:** 120 245 384 22 148 **Sol:** pg. 298

✠ Algebraic Numbers

At this point, we take a small dive into algebraic number theory and discuss algebraic numbers and integers, which work as a bridge between olympiad number theory and algebraic number theory.

Introduction

Number Theory is generally studied as being about Numbers, and at most Rational Numbers. But what about real numbers, what about complex numbers? Do they have any connection with integers? Where do these irrational numbers come up? Consider some special irrational number like $\sqrt{2}$. Why was it invented? Why was $i = \sqrt{-1}$ invented?

Yes, solving equations. $\sqrt{2}$ is **a** number[2] number which satisfies

$$x^2 = 2.$$

$i = \sqrt{-1}$ is **a** number which satisfies

$$x^2 = -1.$$

In fact, consider the polynomial

$$f(x) = X^3 - 2.$$

This polynomial is used to define $\sqrt[3]{2}$. But this polynomial has other roots. What are they?

They are $\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ where ω is a cube root of unity.

So we see that the weird numbers too appear in such equations with coefficients only in integers. Let us study them more.

Definition 7.7.1. *A complex number α is called an **algebraic integer** if it is the root of some **monic** polynomial $f \in \mathbb{Z}[X]$. The set of algebraic integers is denoted by $\overline{\mathbb{Z}}$.*

So, $5, \sqrt{2}, \sqrt[5]{5}, e^{2\pi i/17}$ are all algebraic integers (why?).

Question 7.7.1. *Is $\frac{1}{2}$ an algebraic integer?*

We saw in the previous problem that $\frac{1}{2}$ is not an algebraic integer. However, seeing how algebraic integers are so vast, it is annoying that such a simple rational number is not such an algebraic integer. So here comes the general idea:

Definition 7.7.2. *A complex number α is called an **algebraic number** if it is the root of some polynomial $f \in \mathbb{Q}[X]$. The set of algebraic integers is denoted by $\overline{\mathbb{Q}}$.*

So now $\frac{1}{2}, \frac{3}{17}, \frac{1}{\sqrt{2}}$ are all algebraic numbers. Yay.

Question 7.7.2. *Show that the above numbers are actually algebraic numbers. In particular, show that $\frac{1}{\sqrt{2}}$ is an algebraic number but not an algebraic integer.*

[2] not "the number"

Minimal Polynomials

Remember how we talked about the "defining polynomial" of $\sqrt{2}$ as $f(x) = x^2 - 2$? What's so special about it?

Consider the two polynomials

$$p_1(x) = x^3 + x^2 - 2x - 2$$
$$p_2(x) = x^4 - 4x^2 + 4.$$

Check that $\sqrt{2}$ is a root of both the polynomials. However, neither of $p_1(x)$ or $p_2(x)$ is the **defining** polynomial of $\sqrt{2}$. No ancient mathematician thought of some number like $\sqrt{2}$ by looking at something weird like $p_1(x)$ or $p_2(x)$. So $f(x) = x^2 - 2$ is special for $\sqrt{2}$. How do we make the idea of *special* rigorous?

Here's the ingenious trick: For each algebraic integer α, we consider **monic** polynomial $f \in \mathbb{Z}[X]$ with **minimal degree** such that $f(\alpha) = 0$. Call this the **minimal polynomial** of α.

What's the advantage of the two words in bold? Consider $p(x) = 20x^2 - 40 = 20(x^2 - 2)$. It is almost same as $x^2 - 2$ but still different. To avoid this dumb situation, we keep the "defining" polynomial monic (another reason is that we want $f(x)$ to be irreducible as we will soon see). Yet another reason is that non-monic polynomials with integer coefficients are actually disguised monic polynomials with rational coefficients (for instance $3x + 2$ is actually $3\left(x + \frac{2}{3}\right)$). So seeing $f(x) = 2x - 1$ might trick you into thinking $\frac{1}{2}$ is an algebraic integer, which we know is false.

But why Minimal Degree? The answer to the question is explained by our intuition of the "smallest defining polynomial"[3]. So the reason is: consider $f(x) = x - \sqrt{2}$. This does not have integer coefficient. So we add in another factor and hope that it has integer coefficients.

So, the golden factor here is $x + \sqrt{2}$, since then

$$(x - \sqrt{2})(x + \sqrt{2}) = x^2 - 2 \in \mathbb{Z}[X].$$

For $\sqrt[3]{2}$, we have to add in both $(x - \sqrt[3]{2}\omega)$ and $(x - \sqrt[3]{2}\omega^2)$ to get

$$(x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2) = X^3 - 2.$$

The idea is to add the least number of factors, and hence we choose *minimal degree*, which leads us to the first time after adding some factors that we get a polynomial $\in \mathbb{Z}[X]$.

Again, we define minimal polynomials for algebraic numbers too.

Definition 7.7.3. *The **minimal polynomial** of an algebraic number α is the **monic** polynomial $f \in \mathbb{Q}[X]$ with the **least degree** which has α as a root.*

Question 7.7.3. *Convince yourself again why the monic part is useful.*

[3] Recall that the polynomial analogue of Euclid's Division lemma involves $\deg r < \deg q$, not $r < q$. Thus, we use the degree of the polynomials to think of them being small or large.

Question 7.7.4. *Why is minimal polynomial never defined with real coefficients? What's wrong in that?*

Some examples are:

1. The minimal polynomial of $\frac{1}{2}$ is
$$f(x) = x - 1/2.$$
2. The minimal polynomial of $\omega = e^{2\pi i/3}$ is
$$f(x) = x^2 + x + 1 = \tfrac{x^3-1}{x-1}.$$
3. The minimal polynomial of $\zeta_p = e^{2\pi i/p}$ for p prime is
$$f(x) = x^{p-1} + x^{p-2} + \cdots + 1 = \tfrac{x^p-1}{x-1}.$$
4. The minimal polynomial of $\zeta_6 = e^{2\pi i/6}$ is
$$f(x) = x^2 - x + 1.$$

Question 7.7.5. *Why is the minimal polynomial of ω not $x^3 - 1$? Why is the minimal polynomial of ζ_p not $x^p - 1$?*

Question 7.7.6. *Why is the minimal polynomial of ζ_6 not $\frac{x^6-1}{x-1}$?*

Here's a fun fact: The minimal polynomial of ζ_n equal to $\Phi_n(x)$, i.e. the nth cyclotomic polynomial (if you know what they are).

You might have heard that π is *transcedental*. This means that there is no polynomial with rational coefficients which has π as a root. So, sadly π is not an algebraic number.

Here's a nice problem:

Problem 7.7.18. Let α be an algebraic number. Show that for large enough integer n, the number $n\alpha$ is an algebraic integer.

Hence, the relation between algebraic numbers and algebraic integer is kind of similar to the relation between rationals and integers. (why?)

Properties of Minimal Polynomials

Minimal polynomials have some exciting properties.

Theorem 7.7.1. *The following are true for the minimal polynomial f of any algebraic integer α :*

- *The polynomial is irreducible.*

- $g(\alpha) = 0$ *for some polynomial* $g \in \mathbb{Z}[X]$ *if and only if* $f \mid g$.

This explains why $x^2 - 2$ is irreducible, and why $p(x) = x^3 + x^2 - 2x - 2$ also has the root $\sqrt{2}$; since $p(x) = (x^2 - 2)(x + 1)$ and $(x^2 - 2) \mid p(x)$.

Proof. Suppose f is reducible, say $f(x) = g(x)h(x)$, where $g, h \in \mathbb{Q}[X]$. By Gauss's Irreducibility lemma, we find $g, h \in \mathbb{Z}[X]$. Since f is monic, hence neither of g, h can be a constant, and they both are monic (why?). Then $f(\alpha) = 0$ implies $g(\alpha) = 0$ or $h(\alpha) = 0$. However, since $\deg g, \deg h < \deg f$, hence this contradicts the definition of minimal polynomial.

Next, write $g(x) = f(x)q(x) + r(x)$ with $\deg r < \deg f$ and $q, r \in \mathbb{Z}[X]$. But then $x = \alpha$ implies $r(\alpha) = 0$. However this again is a contradiction. (why?) □

Question 7.7.7. *Using Gauss's irreducibility lemma, show that* f *is also irreducible in* $\mathbb{Q}[X]$.

We have already seen an application of the second result here: the special section of the first chapter which basically says that if $f(\zeta_p) = 0$, then $f(x)$ is divisible by $x^{p-1} + \cdots + x^0$.

Normal Polynomials vs Minimal Polynomials

At this point, I would like to point out something important. A number α is an algebraic integer if it is the root of **any** monic integer polynomial. However, there is one special monic integer polynomial called the minimal polynomial which has the lowest degree out of all these.

So if you want to prove that α is an algebraic integer, you have to show it is the root of *some* monic integer polynomial, not necessarily the minimal one. For instance ζ_6 is an algebraic integer because it is the root of $X^6 - 1$, which is not actually its minimal polynomial, but that doesn't matter.

So suppose $f(\alpha) = 0$ for some monic $f \in \mathbb{Z}[X]$. How do we know if f is its minimal polynomial?

Theorem 7.7.2. *Any monic polynomial* $f \in \mathbb{Z}[X]$ *with root* α *is its minimal polynomial if and only if* f *is irreducible.*

You should get an intuitive feel for this if you understood everything till here, and hence be able to prove it. Nevertheless here's the proof:

Proof. If f is the minimal polynomial, then we have shown before that it is irreducible. Now if $f(\alpha) = 0$ and it is irreducible, then let g be the minimal polynomial. We have seen before that $g \mid f$. But this contradicts the fact that f is irreducible. □

Hence, irreducible is interchangeable with minimal.

Properties of Algebraic Numbers

There are two main properties that make these very useful in Olympiads.

Theorem 7.7.3. *If you add or multiply two algebraic integers, you get an algebraic integer. Same for algebraic numbers. Further, you can divide in algebraic numbers too.*

So $\sqrt{2}+\sqrt{3}$ is also an algebraic integer! In fact, its minimal polynomial is

$$f(x) = (x^2-5)^2 - 4\cdot 6^2.$$

Now, $\sqrt{2}\times i$ is also an algebraic integer! So just by this simple property, we can now tell something like $\sqrt{2+\sqrt{2}}+i\zeta_{15}$ is also the root of some nice integer polynomial!

Question 7.7.8. *Why can't we divide in algebraic integers? Give an example.*

We don't prove this property, but it is really helpful. The second property is

Theorem 7.7.4. *Any algebraic integer which is a rational number must be a an integer, i.e.*

$$\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}.$$

What this means is that if you can show an algebraic integer is a rational number, then it must in fact be an integer. This is precisely the Gauss's lemma we have discussed before (do you see how?). This lemma is very useful in problems.

Practice Examples

Example 7.7.1 (China TST 2005)

Prove that the number

$$\sqrt{1001^2+1}+\sqrt{1002^2+1}+\cdots+\sqrt{2000^2+1}$$

is irrational.

This is a hard problem, especially because there's no particular approach we could try here. Let's try our new machinery on this.

Clearly the number is an algebraic integer, since it is the sum of algebraic integers. Assume on the contrary that it is rational. However, an algebraic integer is rational only if it is an integer. So we just want to show this isn't an integer! This is much simpler, we just bound it between two consecutive integers. For this observe that

$$\sqrt{k^2+1}-k = \frac{1}{\sqrt{k^2+1}+k} < \frac{1}{2k}.$$

Thus,

$$\begin{aligned} 0 &< \left(\sqrt{1001^2+1}-1001\right)+\cdots+\left(\sqrt{2000^2+1}-2000\right) \\ &< \frac{1}{2}\left(\frac{1}{1001}+\cdots+\frac{1}{2000}\right) < \frac{1}{2}\cdot\frac{1000}{1001} < 1. \end{aligned}$$

Hence the sum cannot be an integer.

Next we prove a very interesting result. Clearly $\cos x$ takes every rational number between $-1, 1$ since it is a continuous function. However, the values of cos we commonly learn are $\cos(\pi/6), \cos(\pi/4)$ and so on, so basically x is a rational times π. In which cases are these rationals? Turns out they are rational only in the few cases we can guess: $\cos(0) = 1, \cos(\pi/3) = 1/2, \cos(\pi/2) = 0$.

Example 7.7.2 (Useful Lemma)

Let $q \in \mathbb{Q}$. Show that $\cos(q\pi) \in \mathbb{Q}$ if and only if $\cos(q\pi) \in \{0, \pm\frac{1}{2}, \pm 1\}$.

What's the best algebraic way to deal with trigonometric functions? Complex numbers! Let $z = \cos(q\pi) + i\sin(q\pi) = e^{q\pi i}$. Then $z + z^{-1} = 2\cos(q\pi)$, which we are given to be rational. Now if we can show that $z + z^{-1}$ is an algebraic integer, then this would show $2\cos(q\pi) \in \mathbb{Z}$, in which case we would be done (why?).

Now since q is rational, hence some n satisfies $nq \in \mathbb{Z}$ (set n to be the denominator of q). Hence $z = e^{q\pi i}$ becomes a root $z^{2n} - 1$. Hence, z becomes an algebraic integer. Similarly z^{-1} is an algebraic integer so $z + z^{-1}$ is an algebraic integer!

Question 7.7.9. *Where does the proof fail if q is not rational?*

Example 7.7.3 (Useful Result)

Let p be a prime and $a_0, a_1, \ldots, a_{p-1}$ be rational numbers satisfying

$$a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1} = 0$$

where ζ is a pth root of unity. Then $a_0 = a_1 = \cdots = a_{p-1}$.

Since the minimal polynomial of ζ is $f(X) = X^{p-1} + \cdots + X + 1$, hence if ζ is a root of $g(X) = a_{p-1}X^{p-1} + \cdots + a_1X + a_0$, then $f(x)$ divides $g(x)$ (why?). It is not easy to see that this happens if and only if $a_0 = \cdots = a_{p-1}$, as desired.

A definition:

Definition 7.7.4. *Let α be an algebraic number and f be its minimal polynomial. Then the* ***Galois conjugates*** *(or just conjugates) are the roots of f except α.*

So practically the conjugates of α are the numbers used to complete α to find the minimal polynomial. Also, our earlier theorem translates to:

Theorem 7.7.5. *Whenever you have have $g \in \mathbb{Z}[X]$ such that $g(\alpha) = 0$, then every conjugate of α is also a root of g.*

Before we proceed with more problems, here's a result for sanity:

Example 7.7.4 (Galois Conjugates don't repeat)

Prove that an irreducible polynomial in $\mathbb{Q}[X]$ does not have repeated roots.

The proof is simple. If g has a repeated root α, then $g(\alpha) = g'(\alpha) = 0$. However then the minimal polynomial of α divides both g, g', which is impossible.

We know that $\zeta_k = e^{2\pi ik}$ has magnitude 1 for any k. So a natural question is which algebraic integers have magnitude 1, i.e. lie on the unit circle in the complex plane. Turns out there are some nasty algebraic integers on the unit circle that aren't roots of unity. However, the following amazing result due to Kronecker is true:

Theorem 7.7.6 (Kronecker's Theorem)**.** *Let α be an algebraic integer of magnitude 1. Suppose that all the galois conjugates of α are also on the unit circle. Then α is a root of unity.*

This has an amazing elementary proof:

We finish by solving a challenging problem from the famous Miklós Schweitzer Competition:

Example 7.7.5 (Miklós Schweitzer Competition 2015/5)

Let $n \geq 4$ be a positive integer. Let P, Q be two polynomials with complex coefficients such that

$$P(Q(x)) = x^n + x^{n-1} + \cdots + 2016.$$

Show that one of $\deg P, \deg Q$ is 1.

Assume that $\deg P = k > 1$ and $\deg Q = \ell > 1$. Clearly P, Q are monic. The key idea is to think of the coefficient of $x^{\ell-1}$ in $Q(x)$. It not to hard to see that x^{n-1} is found in the $Q(x)^k$ term in $P(Q(x))$, and further is obtained by

$$\underbrace{x^\ell \cdot x^\ell \dots x^\ell}_{k-1} \cdot x^{\ell-1} = x^{n-1}.$$

However, each term above occurs $\binom{k}{k-1,1,0,\dots,0} = k$ times, so the coefficient of $x^{\ell-1}$ is $1/k$.

Now let $\alpha_1, \dots, \alpha_m$ be all the roots of $P(x)$ (which might include repeated roots) Then

$$P(Q(x)) = \prod_{i=1}^{m} (Q(x) - \alpha_i).$$

For each $Q(x) - \alpha_i$, the sum of roots is $-1/k$. However, each root is a root of $x^n + \cdots + 2016$, and hence an algebraic integer. Thus, the sum should also be an algebraic integer, which we know is $-1/k \in \mathbb{Q}$. Hence $-1/k$ is an integer, showing $k = 1$, a contradiction.

Chapter 8

Quadratic Residues

We have introduced quadratic residues in an earlier chapter, and defined them (see Definition 5.2.1). However, I would give the definition again for completeness:

Definition 8.0.1. *Let p be a prime. A number a is called a **quadratic residue mod** p if there exists an integer x such that $x^2 \equiv a \pmod{p}$. It is called a **quadratic nonresidue** otherwise. We use the shorthand **QR** to denote a quadratic residue and **NQR** for a qudratic nonresidue.*

For instance, if $p = 7$, then 2 is a quadratic residue since $3^2 \equiv 2 \pmod{7}$. However, 3 is not a quadratic residue (you can check this by listing all $0^2, 1^2, 2^2, \ldots, 6^2$ and observing that 3 never appears.) Also, we can extend the definition to non-prime moduli easily:

Definition 8.0.2. *Let $m > 1$ be an integer. An integer a coprime to m is called a **quadratic residue mod** m if there exists an x such that $x^2 \equiv a \pmod{m}$. If no such x exists, we call it a **quadratic nonresidue**.*

A lot of properties that we discuss below apply when we are dealing modulo a prime number p. They don't apply for composite numbers, however. But for a composite number, we can deal with each of its prime factors individually.

In this chapter we will try and study properties of quadratic residues. Before we move on, I would like to remind you of Fermat's Christmas Theorem (see Theorem 5.3.1) which tells us that -1 is a quadratic residue mod p if and only if $p \equiv 1 \pmod{4}$. Also, keep in mind that we would be dealing with **non-zero residues** mod p everywhere.

Comment 8.0.1: Some texts don't consider 0 as a quadratic residue! We won't do this, since it's confusing. However, the reason behind their assumption is important to us as well (which largely is the fact that 0 does not have an inverse). So for sanity, make it a habit to check the case 0 individually whenever we talk about a theorem on quadratic residues.

8.1 How to find them?

This is the first question we try to answer. The naive answer is to find all the elements $\{1^2, 2^2, 3^2, \ldots, (p-1)^2\} \pmod p$. Instead of first writing all the elements of this set, then removing repetitions, let's try to directly do this.

Suppose $0 < i, j < p$ such that $i^2 \equiv j^2 \pmod p$. Then $p \mid (i-j)(i+j)$, so that $p \mid i-j$ or $p \mid i+j$. The latter case corresponds to $i \equiv -j \pmod p$. The first case is not possible. Thus, if we consider the following set X

$$X = \left\{1^2, 2^2, \ldots, \left(\tfrac{p-1}{2}\right)^2\right\} \pmod p,$$

then we find that any two elements in X are distinct. Further, for any number $i > (p-1)/2$, we have $i^2 \equiv (p-i)^2$, and $p - i < (p-1)/2$. So, X is the set of ALL the quadratic residues mod p. This gives us the following:

Lemma 8.1.1 (Number of Quadratic Residues)**.** *For any prime p, there are exactly $\frac{p-1}{2}$ non-zero quadratic residues. Further, they are given by the set*

$$\left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\} \pmod p.$$

This also implies that there are $(p-1)/2$ quadratic nonresidues.

This simple fact alone can help us solve the following problem:

Example 8.1.1

Let p be a prime. Show that the congruence $x^2 + y^2 + 1 \equiv 0 \pmod p$ always has a solution (x, y).

Assume p odd, since this is clear for $p = 2$. Now, we know that there are $\frac{p+1}{2}$ elements in the set $\{0, 1, 2, \ldots, p-1\}$ that can be written as x^2 for some x. Further, by the same logic there are $\frac{p+1}{2}$ elements in the set $\{0, 1, 2, \ldots, p-1\}$ that can be written as $-1 - y^2$ for some y. Since these add to $p+1$ while $\{0, 1, \ldots, p-1\}$ only has p elements, some two must overlap, which is what we wanted (why?).

Problems for Practice

Problem 8.1.1. Prove that the sum of quadratic residues mod p is congruent to 0, if $p > 3$.

Problem 8.1.2. Show that the product of quadratic residues mod p is $+1$ if $p \equiv 1 \pmod 4$, and -1 otherwise.[1]

[1] Does this seem familiar? This was used in the first proof of Fermat's Christmas Theorem (the one without primitive roots), where we directly put $x = ((p-1)/2)!$ and showed $x^2 \equiv -1$.

8.2 Multiplication

This is the first non-trivial question we try to answer. This will motivate a genius notation which will form the base of the theory of quadratic residues. Suppose you have two squares. Then their product is obviously a square. So, the product of two QRs is a QR.

What about QR $\times$ NQR? Well, intuitively it doesn't feel right for this to be a square. Indeed, if $x^2y \equiv z^2 \pmod{p}$, then $y \equiv (z \cdot x^{-1})^2 \pmod{p}$, contradicting the fact that y is a NQR (note here that we are dealing with quadratic residues).

Finally, what is a NQR $\times$ NQR? Try and guess the answer (maybe take a few examples). For instance, if n is a NQR, then $n \times n = n^2$ is a QR. Turns out that in general the product will always be a QR! Here's one ingenious proof:

Suppose n is a NQR. Let $q = (p-1)/2$ and $X = \{x_1, x_2, \ldots, x_q\}$ be the set of QRs and $Y = \{y_1, y_2, \ldots, y_q\}$ be the set of NQRs. Then

$$X \cup Y = \{1, 2, 3, \ldots, p-1\} = \mathcal{S},$$

where $\mathcal{S}$ is the set of all non-zero residues modulo p. Now, by Theorem 2.5.1, $n\mathcal{S} \equiv \mathcal{S} \pmod{p}$. However, since a NQR times a QR is a NQR, hence nX must be the set of NQRs (since it has q elements). This means that nY must be the set of QRs, and so n times any NQR is a QR, which is what we wanted to prove! Thus we have the following:

Lemma 8.2.1. *We have the following (remember that we are dealing with non-zero residues)*

1. $QR \times QR = QR$;
2. $QR \times NQR = NQR$;
3. $NQR \times NQR = QR$.

So the same category objects give QR, and opposite category gives NQR. Does this remind of you something?

This should ring a bell and motivate you to think of $+1, -1$, since the "same category idea" is everywhere; multiplication by negative integers, labelling of positive and negative charges, magnetic poles, dipoles, rotation etc. This idea motivates giving a $+1$ to a QR, and a -1 to a NQR. This is how we do it:

Definition 8.2.1. *Let p be a prime, and x be an integer. Then we define the* ***Legendre's notation*** *as*

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a } QR \\ 0 & \text{if } x \equiv 0 \pmod{p} \\ -1 & \text{otherwise} \end{cases}$$

Thus, Lemma 8.2.1 gives us the following very useful property:

Theorem 8.2.1 (Legendre's Symbol is completely multiplicative)**.** *Let a, b be integers and p a prime. Then*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Using the Legendre's symbol, we basically have converted the English question "is x a quadratic residue" to a mathematical expression. For instance, we have the following lemma, that English couldn't have allowed us to write:

Theorem 8.2.2 (Euler's criterion)**.** *Let p be a prime. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

For instance, if $a = x^2$ is a QR, then the left side is 1 and the right side is $(x^2)^{(p-1)/2} = x^{p-1} \equiv 1 \pmod{p}$. The interesting case is when a is a NQR. The easiest way to prove this is use the following:

Lemma 8.2.2 (Primitive Roots and Quadratic Residues)**.** *Let g be a primitive root modulo p. Then for any $a \not\equiv 0 \pmod{p}$, write $a = g^k$. Then a is a quadratic residue if and only if k is even.*

This is easy to prove, and I leave it as an exercise (this was also Problem 5.5.4). Back to Euler's Criterion, write $a = g^k$ with k odd. Then $a^{(p-1)/2} \equiv g^{k(p-1)/2} \equiv -1 \pmod{p}$ (why?). Hence we are done.

Comment 8.2.1: We know that every non-zero number is a root of the polynomial $x^{p-1} - 1$ in $\mathbb{F}_p$. So,

$$p \mid x^{\frac{p-1}{2}} - 1 \text{ or } p \mid x^{\frac{p-1}{2}} + 1.$$

We know that every number of the form $1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ is a root of $x^{\frac{p-1}{2}} - 1$. By Lagrange's Theorem (Theorem 5.9.4), we know that this polynomial has at most deg $= \frac{p-1}{2}$ roots in $\mathbb{F}_p[X]$. Hence, these all are the only roots of this polynomial (why?) and so every quadratic nonresidue satisfies

$$x^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Hence we have given an alternate proof of Euler's Criterion.

Lemma 8.2.1 is very useful, and is sufficient to solve a lot of problems. An amazing example is the following:

Example 8.2.1

Prove that for a prime $p > 3$, the smallest quadratic nonresidue is less than $\sqrt{p}$.

The idea is simple, pick the smallest quadratic nonresidue r, and try to show $r < \sqrt{p}$. The first thing we can do is to use the definition of r to get that $\{1, \ldots, r-1\}$ are all quadratic residues.

Now, since r is a NQR, hence ra is a NQR for any QR a. In particular, $\{r \cdot 1, \ldots, r \cdot (r-1)\}$ are all NQRs. Now, if $r > \sqrt{p}$ (note that r cannot equal $\sqrt{p}$) then $r^2 > p$. This means r^2

"crosses" p. Here's the idea: If r^2 lands on a number in $\{1, \ldots, r-1\}$, we have something interesting. However, we can't control where r^2 lands. But this is a good idea.

If we try to mend this idea, we look at numbers of the form $r, 2r, \ldots, (r-1)r$. Consider the **first** number that crosses p, say ra.[2] Hence, by definition,

$$ra > p > r(a-1).$$

(why not $\geq$?). Hence, we get $p + r > ra > p$. Hence, $ra \mod p$ lies in $\{1, 2, \ldots, r-1\}$, which means it must be a QR, a contradiction!

We will see a generalization of this result in the chapter "Constructions."

Problems for Practice

Problem 8.2.1. Give an example of two nonresidues that don't multiply to give a residue mod 12. Hence conclude that Lemma 8.2.1 doesn't always hold in no-prime moduli.

Problem 8.2.2. Prove that any quadratic residue can't be a primitive root modulo p.

Problem 8.2.3. Prove Lemma 8.2.2.

Problem 8.2.4. Use Euler's Criterion to prove that the Legendre's symbol is completely multiplicative.

Problem 8.2.5. Show that for any prime p,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

8.3 The Law of Quadratic Reciprocity

We now try to investigate if there's a nice formula to find the Legendre's symbol. For this purpose, we have the following beautiful theorem:

Theorem 8.3.1 (Quadratic Reciprocity Law)**.** *Let $p \neq q$ be odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

This is a very powerful theorem, and is amazing in its own right. If you want to find (p/q), you can instead calculate (q/p).

Question 8.3.1. *Explain the significance of "reciprocity" in the theorem's name.*

[2] Why must such an a exist? This is the idea of *discrete continuity*. Since $r \cdot 1 < p$ but $r \cdot r > p$, hence there must exist an $a \in (1, p)$ such that $ra > p$ but $r(a-1) < p$. Despite being extremely useful and ubiquitous, it is quite a simple idea.

For instance, $q = 3$ implies

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}}.$$

Thus, 3 is a quadratic residue mod p if and only if $p \equiv \pm 1 \pmod{12}$ (why?). If $q = 5$, then

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

Thus, 5 is a quadratic residue mod p if and only if $p \equiv \pm 1 \pmod{5}$. Interesting right?

Let's use this to evaluate something scary like $\left(\frac{21}{61}\right)$. We have

$$\begin{aligned}\left(\frac{21}{61}\right) = \left(\frac{3}{61}\right)\left(\frac{7}{61}\right) &\overset{\text{QR}}{=} (-1)^{\frac{3-1}{2}\cdot\frac{61-1}{2}}\left(\frac{61}{3}\right)(-1)^{\frac{7-1}{2}\cdot\frac{61-1}{2}}\left(\frac{61}{7}\right) \\ &= \left(\frac{1}{3}\right)\left(\frac{5}{7}\right) \\ &\overset{\text{QR}}{=} (-1)^{\frac{5-1}{2}\cdot\frac{7-1}{2}}\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1.\end{aligned}$$

So 21 is not a quadratic residue mod 61.

Again, we left out the case $p = 2$. The poor case always gets left out from all the big theorems, but is never ignored; here's the result with $p = 2$:

Theorem 8.3.2 (Criterion for 2)**.** *For any odd prime p,*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

In other words, 2 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod{8}$.

We don't prove Quadratic Reciprocity for now. There's a classic proof that we won't discuss. We do, however, present a special and non-standard proof in the special section at the end.

Comment 8.3.1: There's a very beautiful theorem which states that if a number is a quadratic residue mod p for all but finitely many prime numbers, then it is square number. This is not just an amazing result, but useful too. You can find some applications of this in the book [14]. This, however, is not very easy to prove. It is given as an exercise problem (with solution) in the chapter "Constructions".

Let's try some simple examples now.

Example 8.3.1

Prove that if a prime p is a quadratic residue of an odd prime q, and p is of the form $4k + 1$, then q is a quadratic residue of p.

This is a direct application of quadratic reciprocity:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right) = (-1)^{2k\cdot\frac{q-1}{2}}\cdot 1 = 1.$$

Question 8.3.2. *Where did we use the fact that q is odd?*

Example 8.3.2

The last digit of the number x^2+xy+y^2 is zero (where x and y are positive integers). Prove that two last digits of this numbers are zeros.

The problem statement in itself is very interesting. We basically want to show if $10 \mid x^2+xy+y^2$, then 10^2 also divides this. Firstly, if $2 \mid x^2+xy+y^2$, then one can easily check that we must have $x \equiv y \equiv 0 \pmod 2$. Hence, $4 \mid x^2+xy+y^2$.

Now suppose $5 \mid x^2+xy+y^2$. Again, if $5 \mid x, y$, we are done like before. Also, if 5 divides one of x, y, it divides both. So assume 5 divides neither. Hence,

$$5 \mid 4(x^2+xy+y^2) \implies (2x+y)^2 \equiv -3y^2 \pmod 5.$$

So, $-3 = (2x\cdot y^{-1}+1)^2 \pmod 5$ is a quadratic residue (since $5 \nmid y$). Hence,

$$\begin{aligned} 1 = \left(\frac{-3}{5}\right) &= \left(\frac{-1}{5}\right)\left(\frac{3}{5}\right) \\ &= (-1)^{\frac{5-1}{2}}\cdot(-1)^{\frac{3-1}{2}\cdot\frac{5-1}{2}}\left(\frac{5}{3}\right) \\ &= \left(\frac{2}{3}\right) = -1. \end{aligned}$$

So we have a contradiction. Hence $5 \mid y \implies 5 \mid x$, and so $5^2 \mid x^2+xy+y^2$, and we are done.

Problems for Practice

Problem 8.3.1. If a is a quadratic nonresidue of each of the odd primes p and q, is $x^2 \equiv a \pmod{pq}$ solvable?

8.4 Legendre Symbol Manipulation

This section is better understood by examples than words. Let's try to prove the following:

Lemma 8.4.1. *If* $\gcd(a,p)=1$ *and* p *is an odd prime, then*

$$\sum_{n=1}^{p}\left(\frac{an+b}{p}\right) = 0.$$

Just recall that $\{an+b\}$ forms the complete residue class mod p if $\gcd(a,p)=1$. So

$$\sum_{n=1}^{p}\left(\frac{an+b}{p}\right)=\sum_{n=1}^{p}\left(\frac{n}{p}\right)=0,$$

since there are an equal number of QRs and NQRs.

This was a simple example. However, what if we had a quadratic in place of $an+b$? This method fails there. We need a more general method. So let's try to find a more general method. Since we can't exactly pin-point when $an+b$ would be a QR, our best bet would be to try something algebraic. Which identity can convert the Legendre symbol into something algebraic?

Yes, Euler's criterion. So $\left(\frac{an+b}{p}\right)\equiv(an+b)^{\frac{p-1}{2}} \pmod p$. This is something we could try, however there is a cost: we would be able to find the value $\pmod p$ but not the exact value. But let's try this anyway for now. Also, a thing we can do is

$$\left(\frac{an+b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{n+c}{p}\right)$$

where $c\equiv b\cdot a^{-1} \pmod p$ (we used $p\nmid a$ here). Now, we just evaluate the sum $\left(\frac{n+c}{p}\right)$. We have (let $w=\frac{p-1}{2}$)

$$\begin{aligned}\sum_{n=1}^{p}\left(\frac{n+c}{p}\right)&\equiv\sum_{n=1}^{p}(n+c)^w\\&\equiv\sum_{n=1}^{p}\left(n^w+\binom{w}{1}n^{w-1}c+\cdots+c^w\right)\pmod p\end{aligned}$$

How do we evaluate the above sum? Firstly, write this as:

$$\sum_{n=1}^{p}\left(n^w+\binom{w}{1}n^{w-1}c+\cdots+c^w\right)=\left(\sum_{n=1}^{p}n^w\right)+\binom{w}{1}c\left(\sum_{n=1}^{p}n^{w-1}\right)+\cdots+c^w\left(\sum_{n=1}^{p}n^0\right).\tag{8.1}$$

So now we just need sums of the form $1^i+2^i+\cdots+p^i$. Does this ring a bell? Recall:

Lemma 8.4.2 (Sum of Powers mod p)**.** *Let $p>2$ be a prime. Then for any integer x,*

$$1^x+2^x+\cdots+(p-1)^x\equiv\begin{cases}-1 & \text{if } p-1\mid x\\ 0 & \text{otherwise}\end{cases}\pmod p.$$

Using this, we see that each sum in Equation 8.1 is 0, and hence the original sum is 0. Thus,

$$\sum_{n=1}^{p}\left(\frac{an+b}{p}\right)\equiv 0 \pmod p.$$

Now we have to deal with the issue we mentioned earlier: how do we find the exact value? Here's the trick. If $\mathcal{S}$ is the sum we want, then $\mathcal{S} \equiv 0 \pmod{p}$. Also, it involves the sum of p Legendre symbols, each of which is atmost 1 and at least -1. Hence,

$$-p \leq \mathcal{S} \leq p.$$

So, $\mathcal{S} \in \{-p, 0, p\}$. We have to eliminate the possibilities $\mathcal{S} = p$ and $\mathcal{S} = -p$. Note that $\mathcal{S} = p$ if all $\left(\frac{an+b}{p}\right) = 1$, which means all $an+b$ are quadratic residues. However, since $p > 2$, this is impossible. Similarly $\mathcal{S} \neq -p$ and we are done.

This seemingly long method has a merit: it can be generalized more easily. Try to prove the following yourself first, as the method is the same.

Lemma 8.4.3. *Let p be an odd prime and a be an integer with $\gcd(a, p) = 1$. Then*

$$\sum_{n=1}^{p} \left(\frac{n^2 + a}{p}\right) = -1.$$

We again employ the same method, however this time write it without explaining each step.

$$\begin{aligned}
\mathcal{S} = \sum_{n=1}^{p} \left(\frac{n^2 + a}{p}\right) &\equiv \sum_{n=1}^{p} (n^2 + a)^{\frac{p-1}{2}} \\
&= \sum_{n=1}^{p} \left(n^{p-1} + \binom{(p-1)/2}{1} n^{p-2} a + \cdots + a^{\frac{p-1}{2}}\right) \\
&= \left(\sum_{n=1}^{p} n^{p-1}\right) + \binom{(p-1)/2}{1} a \left(\sum_{n=1}^{p} n^{p-3}\right) + \cdots + a^{\frac{p-1}{2}} \left(\sum_{n=1}^{p} n^0\right) \\
&\equiv -1 \pmod{p}
\end{aligned}$$

So, $\mathcal{S} \equiv -1 \pmod{p}$. However, we can see that $|\mathcal{S}| \leq p - 1$. Hence, $\mathcal{S} \in \{-1, p-1\}$.

We have to eliminate the possibility that $\mathcal{S} = p-1$. Note that $\mathcal{S} = p-1$ if all $\left(\frac{n^2+a}{p}\right) = 1$, which means n^2+a is quadratic residues for all $1 \leq n \leq p$. Thus, $\{0^2+a, 1^2+a, \ldots, \left(\frac{p-1}{2}\right)^2+a\}$ is precisely the set of all quadratic residues including 0 (why?), i.e.

$$\left\{0^2 + a, 1^2 + a, 2^2 + a, \ldots, \left(\tfrac{p-1}{2}\right)^2 + a\right\} \equiv \left\{0^2, 1^2, 2^2, \ldots, \left(\tfrac{p-1}{2}\right)^2\right\} \pmod{p}.$$

We need to somehow show this is not possible. What's the first thing we do for equal sets? Yes, add and equate the elements. We get

$$0^2 + 1^2 + \cdots + \left(\tfrac{p-1}{2}\right)^2 \equiv (0^2 + a) + (1^2 + a) + \cdots + \left(\left(\tfrac{p-1}{2}\right)^2 + a\right) \pmod{p}.$$

Hence, $\left(\frac{p+1}{2}\right) a \equiv 0 \pmod{p}$, which means $a \equiv 0 \pmod{p}$. However the statement includes $\gcd(a, p) = 1$, and so this is impossible! Hence $\mathcal{S} \neq p - 1$ and so $\mathcal{S} = -1$, and we are done.

Question 8.4.1. *As usual, where did we need $p > 2$? Why did we consider 0 along with the quadratic residues here? Also, what happens if $\gcd(a, p) \neq 1$? What does the sum evaluate to in that case?*

Using this, we can obtain the following:

Corollary 8.4.1. *Let p be an odd prime and a, b be integers both coprime to p. Then*

$$\sum_{n=1}^{p} \left(\frac{an^2 + b}{p} \right) = \left(\frac{a}{p} \right).$$

To prove this, just multiply our previous lemma by $\left(\frac{a}{p}\right)$. Also think why we need a, b both coprime to p.

Problems for Practice

Problem 8.4.1. Show that

$$\sum_{n=1}^{p} \left(\frac{n^2 + a}{p} \right) = (p - 1)$$

if $p \mid a$.

Problem 8.4.2. Use Corollary 8.4.1 and a suitable transformation to prove:

Let a, b, c be integers and let p be an odd prime with $p \nmid a$. Then

$$\sum_{n=1}^{p} \left(\frac{an^2 + bn + c}{p} \right) = (p - 1) \left(\frac{a}{p} \right) \quad \text{if } p \mid b^2 - 4ac.$$

$$\sum_{n=1}^{p} \left(\frac{an^2 + bn + c}{p} \right) = - \left(\frac{a}{p} \right) \quad \text{otherwise.}$$

This is the most general form of quadratic and hence the most useful result. Keep this in mind. There's another form which is often useful: If a, b are not congruent, then

$$\sum_{n=1}^{p} \left(\frac{(n + a)(n + b)}{p} \right) = -1.$$

8.5 Points on the circle $x^2 + y^2 \equiv 1$ in $\mathbb{F}_p$

The title is self-explanatory; we try to solve the following equation:

$$x^2 + y^2 \equiv 1 \pmod{p}.$$

Problem 8.5.1. Use the method from Example 8.1.1 to sow that $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ always has a solution $x, y \in \mathbb{F}_p$.

Does this mean the end of our discussion? Certainly not. Suppose $p = 7$ so that the QRs are $\{0, 1, 2, 4\}$. Hence, we can list all possible values of $x^2 + y^2 \pmod 7$ as:

	0^2	1^2	2^2	3^2	4^2	5^2	6^2
0^2	0	1	4	2	2	4	1
1^2	1	2	5	3	3	5	2
2^2	4	5	1	6	6	1	5
3^2	2	3	5	4	4	5	3
4^2	2	3	5	4	4	5	3
5^2	4	5	1	6	6	1	5
6^2	1	2	5	3	3	5	2

We see that there are 8 solutions to $x^2 + y^2 \equiv 1 \pmod 7$. So, now we ask: how many solutions does $x^2 + y^2 \equiv 1 \pmod p$ have?

Directly counting with two variables is hard. So, we count the number of 1s in each row and add all of them. That is, we fix $y = c$, and see how many x exist. So, our question is how many solutions does $x^2 \equiv 1 - c^2 \pmod p$ have. Once we answer this (in terms of c), we sum the number of solutions as c goes from 0 to $p - 1$.

Since we have fixed c, we have $1 - c^2 = a$ is a constant. So we ask: how many solution does $x^2 \equiv a \pmod p$ have? Clearly it's 2 when a is a QR and 0 when a is a NQR (and 1 if $a = 0$). There's a nice algebraic way to write this:

Lemma 8.5.1. *The number of solutions to $x^2 \equiv a \pmod p$ for a fixed a is*

$$1 + \left(\frac{a}{p}\right).$$

Hence, the number of solutions to $x^2 \equiv 1 - c^2 \pmod p$ is

$$1 + \left(\frac{1 - c^2}{p}\right).$$

Thus, the number of solutions to $x^2 + y^2 \equiv 1 \pmod p$ is

$$\sum_{c=0}^{p-1} 1 + \left(\frac{1 - c^2}{p}\right) = p + \left(\frac{-1}{p}\right) \sum_{c=0}^{p-1} \left(\frac{c^2 - 1}{p}\right) = p + (-1)^{\frac{p-1}{2}} \cdot (-1).$$

Hence, $x^2 + y^2 \equiv 1 \pmod p$ has $p - (-1)^{\frac{p-1}{2}}$ solutions. So, we have shown

Lemma 8.5.2. *The number of solutions to $x^2 + y^2 \equiv 1 \pmod p$ for an odd prime p and $x, y \in \mathbb{F}_p$ is*

$$p - (-1)^{\frac{p-1}{2}}.$$

For instance, when $p = 7$, this gives $7 - (-1)^3 = 8$, exactly what we had before. This also implies something interesting: the equation $x^2 + y^2 \equiv 1 \pmod p$ always has a solution, and at least $p - 1$ of them.

We can generalize the above result to get

Theorem 8.5.1. *Let p be an odd prime. Let N be number of solutions to $x^2 + y^2 \equiv a \pmod{p}$ with $x, y \in \mathbb{F}_p$. Then*

$$N = \begin{cases} p + (p-1)(-1)^{\frac{p-1}{2}} & \text{if } a \equiv 0 \pmod{p} \\ p - (-1)^{\frac{p-1}{2}} & \text{otherwise} \end{cases}$$

Problems for Practice

Problem 8.5.2. Prove Theorem 8.5.1.

Problem 8.5.3. Show that the number of solutions to $x^2 - y^2 \equiv a \pmod{p}$ for $x, y \in \mathbb{F}_p$ is $p - 1$. This represent the number of points on the hyperbola $x^2 - y^2 = a$ in $\mathbb{F}_p$.

8.6 Example Problems

Quadratic residues are really powerful in problems, especially Olympiad problems. Let's start by a classic example

Example 8.6.1

Prove that $2^n + 1$ has no prime factor of the form $8k - 1$.

Suppose $p \mid 2^n + 1$, so that $2^n \equiv -1 \pmod{p}$. Now, clearly $p \neq 2$ and so this gives $\text{ord}_p(2) = 2n$ (why?).

If n is even, then $2^n \equiv -1 \pmod{p}$ above implies that -1 is a quadratic residue and so $p \equiv 1 \pmod{4}$, meaning p cannot be of the form $8k - 1$.

If n is odd, then $2^{n+1} \equiv -2 \pmod{p}$ implying -2 is a QR. However,

$$1 = \left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}}.$$

So if $p \equiv -1 \pmod{8}$, then the above is impossible. So we are done.

Now a problem which has a surprisingly simple solution, but is not easy by any means.

Example 8.6.2 (Iran TST 2013)

Prove that for positive integers x, y, z, the number $x^2 + y^2 + z^2$ is not divisible by $2013(xy + yz + zx)$.

The 2013 is sitting there just because of the exam year. Now $2013 = 3 \times 11 \times 61$. We only need the factor of 3.

Assume on the contrary. Clearly we can assume that $\gcd(a, b, c) = 1$. Now write $x^2 + y^2 + z^2 = 3k(xy + yz + zx)$ so that

$$(x + y + z)^2 = (3k + 2)(xy + yz + zx).$$

Here is the key idea: Since $3k + 2 \equiv 2 \pmod{3}$, hence there exists at least one prime factor p of $3k + 2$ so that $p \equiv 2 \pmod{3}$ and it has an odd exponent in $3k + 2$, otherwise the prime factors multiply to give a number which is $\equiv 1 \pmod{3}$.

So, there exists a prime $p \equiv 2 \pmod{3}$ such that $\nu_p(3k+2)$ is odd. But then $p \mid x+y+z$ and so $p \mid xy + yz + zx$ as $\nu_p(3k + 2)$ is odd. So

$$p \mid xy + z(x + y) \equiv xy - (x + y)^2 \implies p \mid x^2 + xy + y^2.$$

This in particular means that if $p \mid y$, then $p \mid z, x$ too contradicting the gcd assumption. So $p \nmid y$.

This means $(2x \cdot y^{-1} + 1)^2 \equiv -3$ and so -3 is a quadratic residue. However, since $p \equiv 2 \pmod 3$,

$$1 = \left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = -1.$$

This is a contradiction.

Now we do a challenging problem, which is a great example problem involving quadratic residues.

Example 8.6.3 (Taiwan TST?)

Suppose that $\varphi(5^m - 1) = 5^n - 1$ for a pair (m, n) of positive integers. Prove that $\gcd(m, n) > 1$.

Assume on the contrary, and assume $m > 2$. Then note that

$$\gcd(5^m - 1, 5^n - 1) = 5^{\gcd(m,n)} - 1 = 4.$$

In particular, $5^m - 1$ is square free, and $\min\{\nu_2(5^m - 1), \nu_2(5^n - 1)\} = 2$. Write $5^m - 1 = 2^e p_1 p_2 \dots p_k$ with p_i pairwise distinct odd primes. Clearly $k > 0$ for $m > 2$ (by Zsigmondy, say). Then $\nu_2(5^n - 1) \geq (e - 1) + k \geq e$ and so $e = 2$. In particular, m is odd. Thus, we can write

$$5^n - 1 = 2(p_1 - 1)(p_2 - 1) \dots (p_k - 1). \tag{8.2}$$

Now, consider the following crucial claim:

Claim. *Suppose $p \mid 5^m - 1$ for some odd prime $p \neq 5$, where $m > 2$ is odd. Then $p \equiv \pm 1 \pmod 5$.*

Proof. Assume $p \equiv \pm 2 \pmod 5$. Then

$$\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{5-1}{2}} \cdot \left(\frac{p}{5}\right) = -1.$$

So $5 = g^\ell$ for some primitive root g (modulo 5) and non-negative odd integer ℓ. But then $2 \mid p - 1 \mid m\ell$, a contradiction since m, ℓ are odd. □

Thus, $p_i \equiv \pm 1 \pmod 5$ for all i. However, by taking Equation (8.2) modulo 5, we must have $p_i \equiv -1 \pmod 5$ for all i. Then

$$\begin{aligned} -1 \equiv 5^m - 1 = 4p_1 p_2 \dots p_k &\equiv 4(-1)^k \pmod 5 \\ -1 \equiv 5^n - 1 = 2(p_1 - 1) \dots (p_k - 1) &\equiv 2(-2)^k \pmod 5. \end{aligned}$$

However, it is easy to see these two equations can't hold simultaneously. So we are done.

Last, we solve a challenging problem with a surprising application of quadratic residues.

Example 8.6.4 (AOPS 2019 IMOTC Thread)

If $p > 3$ is a prime such that $\varphi(p-1) > \frac{p-1}{3}$, then there are two consecutive primitive roots modulo p.

Assume not. Let g be a primitive root, which means g^{-1} is also a primitive root. Now, by our assumption, neither of $g+1, g^{-1}+1$ is a primitive root. However,

$$g \cdot (g^{-1}+1) \equiv g+1 \pmod{p}.$$

Now, since a primitive root is always a quadratic nonresidue, hence g is a quadratic nonresidue and so the above implies that exactly one of $g+1, g^{-1}+1$ is a quadratic nonresidue (why?), say $g+1$. Then the set $\{g, g^{-1}, g+1\}$ is a set of three quadratic nonresidues. Associate this (that is, create a map) from g to this set.

Now note that $g \not\equiv g^{-1} \pmod{p}$ for any primitive root g, Also, g, g^{-1} map to the same set, and no two primitive roots map to the same set unless they are the same or inverses. So, the image set of this map is half of the number of primitive roots, which is $\varphi(p-1)/2$.

Since each set haS 3 quadratic nonresidues, hence there are at least

$$3 \cdot \frac{\varphi(p-1)}{2} > \frac{p-1}{2}$$

quadratic nonresidues by the given hypothesis. However, this is a contradiction, and we are done.

8.7 Practice Problems

Problem 8.7.1. For a given prime $p > 3$, define $\mathcal{S} = \{0^3, 1^3, 2^3, \cdots (p-1)^3\}$. Then prove that $\mathcal{S}$ is a complete residue class mod p if and only if $p \equiv 2 \pmod 3$.

Problem 8.7.2 (Iran third round number theory exam 2015/3). Let $p > 5$ be a prime number and $A = \{b_1, b_2, \ldots, b_{\frac{p-1}{2}}\}$ be the set of all quadratic residues modulo p, excluding zero. Prove that there doesn't exist any natural a, c satisfying $(ac, p) = 1$ such that set $B = \{ab_1 + c, ab_2 + c, \ldots, ab_{\frac{p-1}{2}} + c\}$ and set A are disjoint modulo p. **Hints:** 442

Problem 8.7.3 (Indian TST). Suppose that p is an odd prime and that A and B are two different non-empty subsets of $\{1, 2, \ldots, p-1\}$ for which

1. $A \cup B = \{1, 2, \ldots, p-1\}$;
2. If a, b are both in A or both in B, then $ab \pmod p \in A$;
3. If $a \in A, b \in B$, then $ab \pmod p \in B$.

Find all such subsets A and B.

Problem 8.7.4. A prime p is called a **Sophie-Germain prime** if $2p + 1$ is also a prime. Show that if $p \equiv 1 \pmod 4$, then 2 is a primitive root mod $2p + 1$. **Hints:** 96 228

Problem 8.7.5 (Iranian Third round Number theory exam 2015/5). $p > 5$ is a prime number. Prove that one of the following numbers is in form of $x^2 + y^2$.

$$p + 1, 2p + 1, 3p + 1, \ldots, (p-3)p + 1.$$

Hints: 475 283

Problem 8.7.6 (IMO Shortlist 1991). Let $p > 3$ be a prime and let a, b, c be integers with $a \neq 0$. Suppose that $ax^2 + bx + c$ is a perfect square for $2p - 1$ consecutive integers x. Prove that p divides $b^2 - 4ac$. **Hints:** 393

Problem 8.7.7 (Vietnam TST 2005/5 Part a). Let p be a prime number of the form $4k + 1$. Show that

$$\sum_{i=1}^{p-1} \left(\left\lfloor \frac{2i^2}{p} \right\rfloor - 2 \left\lfloor \frac{i^2}{p} \right\rfloor \right) = \frac{p-1}{2}.$$

Hints: 340

Problem 8.7.8 (RMM 2013/1). For a positive integer a, define a sequence of integers $x_1, x_2, \ldots$ by letting $x_1 = a$ and $x_{n+1} = 2x_n + 1$ for $n \geq 1$. Let $y_n = 2^{x_n} - 1$. Determine the largest possible k such that, for some positive integer a, the numbers $y_1, \ldots, y_k$ are all prime. **Hints:** 42 364 150

Problem 8.7.9 (Romania TST 2008). Let a and b be positive integers such that $2^a - 1$ divides $3^b - 1$. Prove that either $a = 1$ or b is even. **Hints:** 17 33

Problem 8.7.10 (Gabriel Dospinescu). Prove that for any positive integer n, the number $2^{3^n} + 1$ has at least n prime divisors of the form $8k + 3$. **Hints:** 282 68 54

Problem 8.7.11 (IMO 1996/4). The positive integers a and b are such that the numbers $15a + 16b$ and $16a - 15b$ are both squares of positive integers. What is the least possible value that can be taken on by the smaller of these two squares? **Hints:** 160 466 142

Problem 8.7.12. Let p be a prime number of the form $4k + 1$. Prove that

$$\sum_{j=1}^{\frac{p-1}{4}} \left\lfloor \sqrt{jp} \right\rfloor = \frac{p^2 - 1}{12}.$$

Hints: 446 431 269

Problem 8.7.13 (AMM). Find all positive integers n such that $2^n - 1 \mid 3^n - 1$. **Hints:** 165 65 **Sol:** pg. 299

Problem 8.7.14 (Taiwan 1997). Let n be a positive integer and let $k = 2^{2^n} + 1$. Show that k is a prime if and only if k divides $3^{\frac{k-1}{2}} + 1$. **Hints:** 352 118 174 **Sol:** pg. 299

Problem 8.7.15 (ELMO 2011/5). Let $p > 13$ be a prime of the form $2q + 1$, where q is prime. Find the number of ordered pairs of integers (m, n) such that $0 \leq m < n < p - 1$ and

$$3^m + (-12)^m \equiv 3^n + (-12)^n \pmod{p}.$$

Hints: 97 175 266 344 **Sol:** pg. 299

Problem 8.7.16 (Iran TST 2020/6). p is an odd prime number and $n = \frac{p-1}{2}$. Find all n-tuples $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_p^n$ such that

$$\sum_{i=1}^{n} x_i \equiv \sum_{i=1}^{n} x_i^2 \equiv \cdots \equiv \sum_{i=1}^{n} x_i^n \pmod{p}.$$

Hints: 212 333 263 208 232 **Sol:** pg. 300

Problem 8.7.17 (USA TST 2014/2). Let $a_1, a_2, a_3, \ldots$ be a sequence of integers, with the property that every consecutive group of a_i's averages to a perfect square. More precisely, for every positive integers n and k, the quantity

$$\frac{a_n + a_{n+1} + \cdots + a_{n+k-1}}{k}$$

is always the square of an integer. Prove that the sequence must be constant (all a_i are equal to the same perfect square). **Hints:** 211 326 371 **Sol:** pg. 301

Problem 8.7.18 (USOMO 2020/3). Denote by A the set of all integers a such that $1 \leq a < p$, and both a and $4 - a$ are quadratic nonresidues. Calculate the remainder when the product of the elements of A is divided by p. **Hints:** 239 171 35 139 **Sol:** pg. 302

✠ A Proof of The Quadratic Reciprocity Law

There are over a 100 different proofs of the quadratic reciprocity law, and the most common that you find in book uses a lemma of Gauss. We, however, present a different proof through a completely different route. We first try to generalize our result on the number of solutions to $x^2 + y^2 \equiv 1 \pmod{p}$. Here's the result:

Theorem 8.7.1 (V. Lebesgue)**.** *Let $p > 2$ be a prime and let n be an odd integer. The number of solutions to the congruence $x_1^2 + \cdots + x_n^2 \equiv 1 \pmod{p}$ for $x_i \in \mathbb{F}_p$ is*

$$p^{n-1} + \left((-1)^{\frac{p-1}{2}} p\right)^{\frac{n-1}{2}}.$$

Note that we have n odd in the hypothesis.

Proof. To prove it, we look more generally at the equation $x_1^2 + \cdots + x_n^2 = a$ and let the number of solutions be $N(a, n)$. Then we write this equation as

$$x_1^2 + \cdots + x_{n-2}^2 = a - (x_{n-1}^2 + x_n^2).$$

So,

$$N(a, n) = \sum_{x_{n-1}, x_n \in \mathbb{F}_p} N(a - x_{n-1}^2 - x_n^2, n-2).$$

Now, by Theorem 8.5.1, we know that $a - x_{n-1}^2 - x_n^2$ takes each residue different from a $p - (-1)^{\frac{p-1}{2}}$ many times, and the residue a $p + (p-1)(-1)^{\frac{p-1}{2}}$ times. So

$$\begin{aligned} N(a, n) &= \left(p - (-1)^{\frac{p-1}{2}}\right) \sum_{b \neq a} N(b, n-2) + \left(p + (p-1)(-1)^{\frac{p-1}{2}}\right) N(a, n-2) \\ &= \left(p - (-1)^{\frac{p-1}{2}}\right) \sum_{b=0}^{p-1} N(b, n-2) + p(-1)^{\frac{p-1}{2}} N(a, n-2). \end{aligned}$$

Now, it is easy to see that (why?)

$$\sum_{b=0}^{p-1} N(b, n-2) = p^{n-2}.$$

Hence, we get

$$N(a, n) = p^{n-2}\left(p - (-1)^{\frac{p-1}{2}}\right) + p(-1)^{\frac{p-1}{2}} N(a, n-2).$$

Now, we have a recursion formula, and so we can just finish by induction. □

Question 8.7.1. *Where do we use the fact that n is odd?*

The recursion we obtained is the important result, and we can use it to find a formula for n even as well. However, for our purposes n odd suffices. Now let's try to prove the qudratic reciprocity law using this.

Suppose we want the number of solutions to $x_1^2 + \cdots + x_q^2 \equiv 1 \pmod{p}$ for odd primes p, q. By Lebesgue's result, this is

$$N = p^{q-1} + \left((-1)^{\frac{p-1}{2}} p\right)^{\frac{q-1}{2}} = p^{q-1} + (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}} \equiv 1 + (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right) \pmod{q}.$$

Do some terms feel familiar? If we can show

$$N \equiv 1 + \left(\frac{q}{p}\right) \pmod{q}, \tag{8.3}$$

then we would get

$$\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right) \pmod{q}.$$

Since both the sides are in $\{1, -1\}$ and $q > 2$, hence their difference would be at most 2 which would be divisible by q. So they must be equal, which is precisely the Quadratic Reciprocity law!

So now we must only show Equation 8.3. The proof of this is combinatorial. Observe that if $(x_1, x_2, \ldots, x_q)$ is a solution, then so are $(x_2, x_3, \ldots, x_1), \ldots, (x_q, x_1, \ldots, x_{q-1})$. So, we can obtain groups of q solutions of this equation, obtained by permuting $x_1, \ldots, x_q$ cyclically. Since q is a prime, the only possibility for two solutions in a group to be equal is to have $x_1 = \cdots = x_q$ (think why). So, if M is the number of solutions to $x_1 = \cdots = x_q$, then

$$N \equiv M \pmod{q}.$$

Now to find M, we only have to solve the equation $qx_i^2 \equiv 1 \pmod{p}$. This is the same as $(qx_i)^2 \equiv q \pmod{p}$ which has

$$M = 1 + \left(\frac{q}{p}\right)$$

solutions. And so, we are done!

Comment 8.7.1: Quadratic Residues are very interesting, and studying their properties we dive deep really fast. We define something known as the Gauss sum and study its properties. Gauss sums give a very short proof of both Lebesgue's result and the quadratic reciprocity law. Manipulations involving these give fascinating results. For instance, the following is Jacobi's conjecture, proven by Dirichlet:

If p is a prime of the form $4k+3$, then there are more quadratic residues in the first half. This is the same as saying there are more quadratic residues in between $1, (p-1)/2$ than quadratic nonresidues.

Comment 8.7.2 (Continued): When $p = 4k + 1$, then QRs are equally distributed in both the halves, because for each quadratic residue a, we find $-a$ to also be a quadratic residue. However, for $p = 4k + 3$ there are more QRs in the first half. An algebraic way of writing this is

$$\sum_{k=1}^{\frac{p-1}{2}} \left(\frac{k}{p}\right) > 0.$$

This is a beautiful result, with a non-elementary proof using something known as Dirichlet's L-function (although the proof can be derived using Gauss sums).

Chapter 9

Constructions

Existence type problems are very common, not just in Number Theory, but all fields of maths. When you are asked to show the existence of something, you might either explicitly give a construction, or somehow show its existence implicitly, for instance a probabilistic proof of existence.

Constructions don't always occur as problems, often as ideas in other problems too, especially where you have a lot of freedom with variables. Choosing the right variables to work with is the main task in these. Hence, this chapter is valuable in all sorts of problems

In this chapter, we will focus on two main ideas:

1. **Existence:** Use methods to show the existence directly instead of explicitly writing down the object. This would (could) involve the use Chinese Remainder Theorem, Dirichlet's Theorem and Thue's Lemma[1].

2. **Hands-on Constructions:** These would involve writing down the object manually and showing it works. These problems belong more to the combinatorial family which makes them hard, since there aren't a lot of fixed techniques that can work. You have to get your hands dirty on a lot of approaches and see which one works the best. You might have to use some theorems (like the Chinese Remainder Theorem) to guarantee existence, but the way in which you use it would require a construction type logic.

Just as an advice: Often problems of the form "Do(es) there exist" are harder than simple "prove this" ones, because you don't know the answer. Hence, you should rely on your intuition, but still have an open heart to both possibilities. At times, there might be an obscure construction, to which believing its existence is harder than actually constructing it. Assuming that no construction exists in these problems can lead you to a death trap. Hence, a good idea is to start constructing, see if what you tried fails, see if you can fix it. By this approach you might even find a convincing reason as to why no construction is possible, and

[1]It can argued that these are actually hands-on construction methods, since you are explicitly setting up congruence relations. However, it really depends on the problem, and these methods could be either. For instance, in a problem asking you to show there exists a prime $\equiv 2 \pmod 7$, the use of Dirichlet's theorem works as an existence type proof. However, in a problem in which you show $p \equiv 2 \pmod 7$ satisfies the desired condition and just use Dirichlet to guarantee its existence, the argument is a hands-down construction.

hence this is safer than crossing out the possibility of a construction existing/not-existing altogether.

9.1 Dirichlet's Theorem

In this section, we will discuss a beautiful theorem due to Dirichlet. Let $\mathcal{P}$ denote the set of *odd* primes, which is infinite. Pick a number, say 4. Then any prime in $\mathcal{P}$ is of the form $4n+1$ or $4n+3$. By symmetry, it would make sense if there are an equal number of primes of the form $4n+1$ and $4n+3$. Turns out this is true, however "symmetry" is not the right argument (remember that primes don't behave nicely and have no good patterns). In particular, the number of primes of the form $4n+1$ is infinite, and the same holds for primes of the form $4n+3$.

Suppose now we consider $\mathcal{P}$ modulo 6. Then clearly any prime is either $6n+1$ or $6n+5$ (why?). Again, primes, despite not having any pattern, are equally distributed in the sets $\{6n+1\}$ and $\{6n+5\}$. In particular, there are infinitely many primes of the form $6n+1$.

In general, we have the following beautiful theorem:

Theorem 9.1.1 (Dirichlet's Theorem)**.** *Let a, b be coprime integers. Then the arithmetic progression $\{an+b\}_{n\geq 0}$ contains infinitely many primes.*

Question 9.1.1. *Why do a, b have to be coprime?*

Comment 9.1.1: In fact, Dirichlet's theorem is stronger than this. It says that the primes are equally distributed over the $\varphi(a)$ arithmetic progressions of the form $\{an+x\}$ where x varies over the $\varphi(a)$ integers less than a that are coprime to it. So, the "density" of primes in $\{an+b\}$ is

$$\frac{1}{\varphi(a)}.$$

You can think of this by imagining prime numbers as points being distributed equally over the $\varphi(a)$ sets $\{an+x\}$, where x varies over positive integers coprime to a. You can also think of this as the probability that a randomly chosen prime is of the form $an+b$, i.e. $\equiv b \pmod{a}$. For example, a randomly chosen prime has the probability $1/\varphi(4) = 1/2$ of being of the form $4n+1$.
Density is a formal term in Number Theory, and even though is pretty much what you think it is, we won't dwell much on that side of analytic number theory. For our purposes, the fact that the number of primes are infinite in each AP is sufficient.

This theorem is amazing, since it not only says a prime $p \equiv a \pmod{b}$ will exist, but also that there will be infinitely many such primes! The proof of this theorem is way beyond the scope of the book and uses something known as Dirichlet's L-function, which is an extensive topic for study in itself.

This theorem is very useful. Let's look at one simple application.

Example 9.1.1

Show that there are infinitely many positive numbers n that cannot be written as $3ab + a + b$ for any $a, b \in \mathbb{N}$.

For instance, $10 = 3ab + a + b$ has no solution in positive integers (check this). We need to show there are infinitely(!) many more.

One of the first things we try in these problems is factorization. So write $n = 3ab + a + b$ for some a, b, n. Trying to factor the right side doesn't yield anything useful. However, if we multiply both the sides by 3 and add 1 to both the sides (Simon's trick) we get

$$n = 3ab + a + b \iff 3n + 1 = 9ab + 3a + 3b + 1 = (3a + 1)(3b + 1).$$

Nice! This tells us that $3n+1$ is composite. So, if we want to find n such that $n = 3ab+a+b$ does not have a solution, one thing we can *try* is to keep $3n+1$ a prime. For example, when $n = 10$, $3n + 1 = 31$ and so $31 = (3a + 1)(3b + 1)$ will have no solution pair (a, b).

Now we just want infinitely many such n such that $3n + 1$ is a prime. However, this directly follows from Dirichlet's Theorem!

9.2 Chinese Remainder Theorem

Suppose we want an x such that $x \equiv 2 \pmod 7$. Then we can pick anything from the set $\{\dots, -5\ , 2, 9, 16, \dots\}$. Suppose now we want an x such that

$$\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 1 \pmod 7 \end{cases}$$

Clearly, there is no solution to this system. Let's look at something more interesting.

$$\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 1 \pmod 3 \end{cases} \tag{9.1}$$

Any x satisfying the first congruence lies in the set

$$A = \{\dots, -19, -12, -5, 2, 9, 16, 23, 30, 37, 44, 51 \dots\}.$$

Any number satisfying the second congruence lies in the set

$$B = \{\dots, -8, -5, -2, 1, 4, 7, 10, 13, 16, 19, 23, 26, 29, 32, 37, 40, 43, \dots\}.$$

Then a solution x to the two equations must be in $A \cap B$, which we can check is the set

$$A \cap B = \{\dots, -5, 16, 37, \dots\}.$$

If you look closely, you will realize this is an AP with common difference 21, which means it is the set of integers x such that $x \equiv 16 \pmod{21}$. We can quickly check if our guess is true. If $x = 21k + 16$, then $x \equiv 16 \equiv 2 \pmod{7}$ and $x \equiv 16 \equiv 1 \pmod{3}$. Hence, any number 16 modulo 21 satisfies Equation 9.1!

However, does any other integer satisfy Equation 9.1?

Question 9.2.1. *Check (prove) that any other number does not satisfy the system in Equation 9.1 by taking an x with $x \not\equiv 16 \pmod{21}$. So basically the pattern we observed is good enough.*

Let's now look at a different system.

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{6} \end{cases}$$

Again, you can check that the solution set is:

$$\{\dots, -5, -2, 1, 4, 7, 10, 13, 16, 19, 22, \dots\} \cap \{\dots, -5, 1, 7, 13, 19, \dots\} = \{\dots, -5, 1, 7, 13, 19, \dots\}.$$

So in this case, the solution set is $x \equiv 1 \pmod{6}$. If we think about it now, it's obvious why this is true; if $x = 6k + 1$, then x is automatically $1 \pmod{3}$ as $3 \mid 6$.

One last example:

$$\begin{cases} x \equiv 1 \pmod{6} \\ x \equiv 2 \pmod{9} \end{cases}$$

Here, the set satisfying $x \equiv 1 \pmod{6}$ is

$$\{\dots, -5, 1, 7, 13, 19, \dots\}.$$

The set satisfying $x \equiv 2 \pmod{9}$ is

$$\{\dots, -16, -7, 2, 11, 20, 29, \dots\}.$$

Try as hard as you want, but you won't find a common element. Why is this true?

If x satisfies both, then there exist k, ℓ such that $6k + 1 = x = 9\ell + 2$. However, both sides don't match modulo 3.

So, we can our summarize our idea: the classes obtained for two numbers that have a common factor are not completely independent of each other. However, if they are coprime, we do sense an independence. This is the intuition behind the Chinese Remainder Theorem:

Theorem 9.2.1 (Chinese Remainder Theorem)**.** *Let $a_1, a_2, \dots, a_n$ be integers, and $b_1, b_2, \dots, b_n$ be pairwise coprime integers, i.e. $\gcd(b_i, b_j) = 1$ for any $i \neq j$. Then the system of equations*

$$\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \\ \vdots \\ x \equiv a_n \pmod{b_n} \end{cases}$$

has a unique solution $\pmod{b_1 b_2 \dots b_n}$.

We developed the intuition for the case $n = 2$. The general case is quite similar, and the proof is just by induction with the base case $n = 2$. I leave it as an exercise for the interested readers.

Let's see an example on how to find the x :

Example 9.2.1

Solve the system of linear congurences:

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 8 \end{cases}$$

To solve this, we first use the fact that there must exist k, ℓ such that $x = 5k + 3$ and $x = 8\ell + 4$. Equating them, we find $5k + 3 = 8\ell + 4$, i.e. $5k = 8\ell + 1$. Modulo 5, this implies $3\ell + 1 \equiv 0 \pmod 5$, so $\ell \equiv -3^{-1} \equiv 3 \pmod 5$. So write $\ell = 5n + 3$ to get $x = 8(5n + 3) + 4 = 40n + 28$. Note that this satisfies both the congrunces.

Question 9.2.2. *Where was the fact that* $\gcd(8, 5) = 1$ *used?*

This theorem is incredibly useful in constructing an x when we want it to satisfy many properties. Cleverly picking these conditions can help solve some very challenging construction based problems.

Example 9.2.2

Show that for $c \in \mathbb{Z}$ and a prime p, the congruence $x^x \equiv c \pmod p$ has a solution.

We are working modulo p, so the exponents can be handled using Fermat's Little Theorem. In particular, since $z^{p-1} \equiv 1 \pmod p$, hence the exponent cycles mod $(p - 1)$. We use this to our advantage.

Suppose we set the exponent to be 1, then $x^x = x = 1$. if $c = 1$ this is enough. However, if we set the x somehow such that $x^x \equiv x$, then we can set $x \equiv c \mod p$ and be done. This is how we do it: consider the system

$$\begin{cases} x \equiv 1 \pmod{p-1} \\ x \equiv c \pmod p \end{cases}$$

This has a solution by CRT as $\gcd(p, p - 1) = 1$. Then this works! Here's a properly written proof:

Proof. Consider the system

$$\begin{cases} x \equiv 1 \pmod{p-1} \\ x \equiv c \pmod p \end{cases}$$

This has a solution by CRT as $\gcd(p, p - 1) = 1$. We claim that any such x works. Indeed, we have

$$x^x \equiv x^{x \pmod{p-1}} \equiv x^1 \equiv c \pmod p,$$

where the first step follows by Fermat's Little Theorem. Hence, our claim is true and we are done. □

Comment 9.2.1: If you try and follow the main theme of the book here, which is to look at the larger picture, you would write all the values of $x^x \bmod p$. You can ease your work using Fermat's Little Theorem to get $x^{p-1} \equiv x^0$. So the set of values of x^x looks like:

$$\begin{array}{cccc} 0^0 & 1^1 & \dots & (p-1)^0 \\ p^1 & (p+1)^2 & \dots & (2p-1)^{p-2} \\ (2p)^0 & (2p+1)^1 & \dots & (3p-1)^{p-3} \\ (3p)^{p-2} & (3p+1)^0 & \dots & (4p-1)^{p-4} \\ \vdots & \vdots & \ddots & \vdots \end{array}$$

You observe that the bases and the powers move along different periods, and differ just by 1. Also, the numbers with exponent 1 in the list are $p^1, (2p+1)^1, (3p+2)^1, \dots$ Note that the bases cover all the residues mod p so eventually we will also get $c^1 \equiv c \pmod p$, which is what we want. So we basically found a new proof to this problem!

This argument is perfect. However, the beauty of the Chinese Remainder Theorem is that we don't have to explicitly make this table; the theorem contains it without having to explicitly write it down!

The best way to use CRT in a lot of construction type problems is the following:

Add as many conditions as you want, and combine them using CRT.

9.3 Thue's Lemma

Thue's lemma is an amazing result in modular arithmetic, and is very useful in constructions especially related to squares. Let me first give the statement, and then discuss it further:

Lemma 9.3.1 (Thue's Lemma)**.** *Let $n > 1$ be an integer and a be an integer coprime to n. Then there exist integers x, y with $0 < |x|, |y| < \sqrt{n}$ so that*

$$ay \equiv x \pmod n.$$

Basically, we have $a \equiv \frac{x}{y} \pmod n$, where x, y are "small". Let's prove this first. It's a good exercise so be sure to try it yourself first before reading the proof:

Proof. Let $r = \lfloor \sqrt{n} \rfloor$, which is the unique integer satisfying $r^2 \leq n < (r+1)^2$. Now, consider number of the form $ay - x$ with $0 \leq x, y \leq r$. There are $(r+1)^2 > n$ such numbers, so two would be the same by the Pigeonhole Principle. So, for some $(x_1, y_1), (x_2, y_2)$, we have

$$ay_1 - x_1 \equiv ay_2 - x_2 \iff (y_1 - y_2)a \equiv (x_1 - x_2) \pmod n.$$

So, if we set $y = y_1 - y_2$ and $x = x_1 - x_2$, we get $ay \equiv x \pmod n$, which is what we need. We just need to show $0 < |x|, |y| < r$. The right inequality is clear. However, we could have

$x = 0$. If $x = 0$, then $ax \equiv y$ implies $y \equiv 0$. This means the pairs (x_1, y_1) and (x_2, y_2) were the same, which is not true. Hence we have $0 < |x|, |y| < r$ and the show's over. □

Let's look at some famous applications

9.3.1 Fermat's Two Square Theorem

Let's investigate a question raised by Fermat: which primes can be expresses as sums of squares? Let's test (the ones left blank indicate no solution to $p = x^2 + y^2$)

p	x^2+y^2		p	x^2+y^2		p	x^2+y^2
2	1^2+1^2		23			59	
3			29	5^2+2^2		61	6^2+5^2
5	2^1+1^2		31			67	
7			37	6^2+1^2		71	
11			41	5^2+4^2		73	8^2+3^2
13	3^2+2^2		43			79	
17	4^2+1^2		47			83	
19			53	7^2+2^2		89	8^2+5^2

At this point, do you observe any pattern? Test your pattern with more values.

If you guessed precisely the primes of the form $p \equiv 1 \pmod 4$ (apart from 2) then you are correct. This observation contains two things, the first being the fact that no prime $p \equiv 3 \pmod 4$ can be written as $x^2 + y^2$. The second fact is that any prime $p \equiv 1 \pmod 4$ can be written as $x^2 + y^2$. This is Fermat's two square theorem[2]

Theorem 9.3.1 (Fermat's Two Square Theorem)**.** *Let p be an odd prime. Then there exist integers x, y such that $p = x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$.*

Looking at the $x^2 + y^2$ appearing, you should think of Fermat's Christmas Theorem. According to it, there exists x such that $p \mid x^2 + 1$ if and only if $p \equiv 1 \pmod 4$. Interestingly enough, the condition here is the same too! Clearly, Fermat's Christmas theorem implies the first part of our observation above (why?). However, the second part of our observation above is actually stronger than Fermat's Christmas Theorem. So we need something stronger.

The key idea is to use Thue's Lemma as follows: Suppose we have some a coprime to p. Then we can find $0 < |x|, |y| < \sqrt{p}$ with $ay \equiv x \pmod p$. Then $p \mid x^2 - a^2y^2$. So, if we pick a such that $a^2 \equiv -1 \pmod p$ using Fermat's Christmas Theorem, then $p \mid x^2 + y^2$. The amazing part now is that $0 < x^2 + y^2 < 2p$ (why?). However, the only multiple of p between $0, 2p$ is p, so we must have $p = x^2 + y^2$ and we are done! By a similar method, you can try the following problem

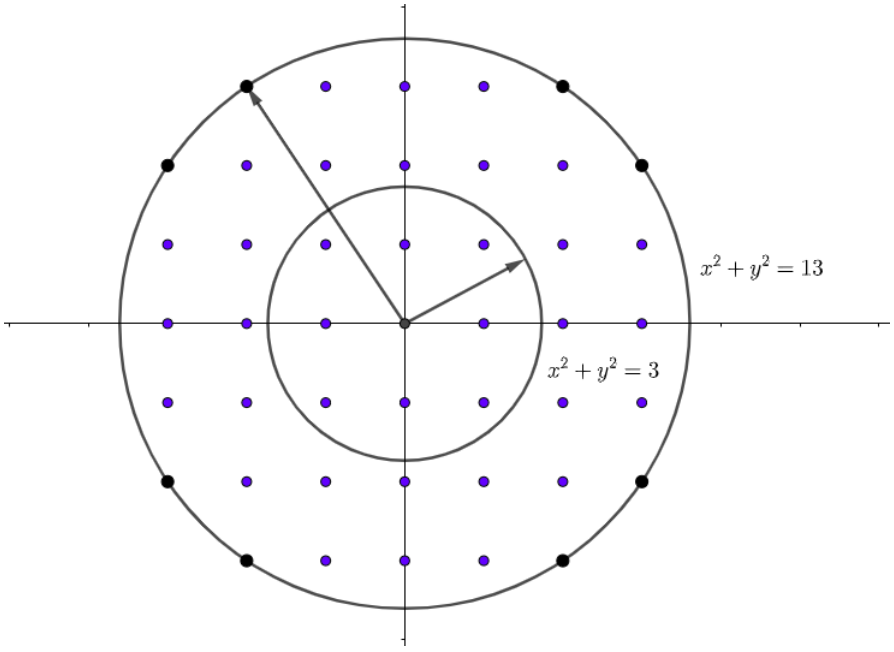
Problem 9.3.1. Let $n \in \{-1, -2, -3\}$. If n is a quadratic residue modulo a prime p, then there are integers a, b such that $p = a^2 - nb^2$.

[2]This is the real "Fermat's Christmas Theorem", not the one we did earlier (in fact this is a generalization of that)

At this point, we can try and answer the more general question: which numbers can be expressed as sum of squares of two integers? Call a number n *good* if it can be written as a sum of squares. Let's investigate properties of *good* numbers.

Comment 9.3.1: Consider the circle centered at the origin with radius $\sqrt{n}$, where $n \in \mathbb{N}$. Then there is a lattice point, i.e. a point with integer coordinates, on the circumference if n is *good*. Hence, this question of ours has geometric significance.

More than this, there's another useful appearance. A complex number $x+iy$ is called a **Gaussian Integer** if $x, y \in \mathbb{Z}$. Thus, the problem of asking which integer values can $|z|$ take for a gaussian integer z is the same as asking which integers are *good*.



Suppose $n = x^2+y^2$, and n has one prime factor $p \equiv 3 \pmod 4$. Then $p \mid x^2+y^2$ implies $p \mid x, y$ by Fermat's Christmas Theorem (again). So, $p^2 \mid n$.

Now, also note that $p \mid x, y$ implies $x = px^*, y = py^*$. So $n = p^2((x^*)^2 + (y^*)^2)$. Hence, if $p^3 \mid n$, then $p \mid (x^*)^2 + (y^*)^2$, again implying $p \mid x^*, y^*$. So, $p^4 \mid n$. In this way, we can show that $\nu_p(n)$ must be even. This is a necessary condition. You can check that this approach fails if $p \equiv 1 \pmod 4$, in which case these primes cause no issue. So is $\nu_p(n)$ even for $p \equiv 3 \pmod 4$ primes a sufficient condition?

Question 9.3.1. *Show that if $n = x^2+y^2$ is good, then so is $2n$ by expressing it as the sum of two squares. In other words we can have any power of 2 and it won't affect n's "goodness".*

Suppose m, n are good. Then what about their product mn? If we can show mn will also be good, then we our condition above would indeed by sufficient (since every prime $p \equiv 1 \pmod 4$ and $p = 2$ are good).

So we want to express $(a^2+b^2)(c^2+d^2)$ as a sum of squares. An elegant approach is to write $z=a+ib, w=c+id$ where $i=\sqrt{-1}$. Then

$$(a^2+b^2)(c^2+d^2)=|z|^2|w|^2=|zw|^2=(ac-bd)^2+(ad+bc)^2.$$

Hence, if m,n are *good*, then so is their product. So now using Fermat's two square theorem, we know that every prime $p\equiv 1 \pmod 4$ is good. Further, 2 is clearly good. So any number who prime factors are only 2 or $\equiv 1 \pmod 4$. Further, if $n=x^2+y^2$ is good, then $p^2n=(px)^2+(py)^2$ is good. So if we have an even power of a prime $\equiv 3 \pmod 4$, we don't lose the "goodness". Hence, we obtain

Lemma 9.3.2. *A number n can be expressed as a sum of squares of integers if and only if for any prime $p\equiv 3 \pmod 4$, we have $\nu_p(n)$ is even (possibly 0).*

Comment 9.3.2 (Some extra information on Brahmagupta's Identity): The identity

$$(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2=(ac-bd)^2+(ad+bc)^2.$$

is called **Brahmagupta's Identity**. It can be derived by directly expanding both the LHS and RHS, however the complex numbers' approach is an elegant one.

This identity can be used to prove the Cauchy-Schwarz inequality for the 2 variable case. Also, it can be used to generate quadruples (x,y,z,w) with $x^2+y^2=z^2+w^2$. For instance, this is done by first picking a Pythagorean triplet (k,ℓ,m), and then any x,y. They are then combined using

$$(mx)^2+(my)^2=m^2(x^2+y^2)=(k^2+\ell^2)(x^2+y^2)=(kx-y\ell)^2+(ky+\ell x)^2.$$

So $(mx,my,kx-y\ell,ky+\ell x)$ is a working quadruple.

Let's look at another amazing application of Thue's lemma:

Example 9.3.1

Let p be a prime. There exist integers a,b such that $p=a^2+ab+b^2$ if and only if $p=3$ or $p\equiv 1 \pmod 3$.

Firslty, we prove that if $p\equiv 2 \pmod 3$, then we can't find such a,b (which is the non-constructive and easy part of the problem). Suppose on the contrary that $p=a^2+ab+b^2$. A better way of writing this is $4p=4(a^2+ab+b^2)=(2a+b)^2+3b^2$. Then

$$(2a+b)^2\equiv -3b^2 \pmod p.$$

Hence, -3 is a quadratic residue modulo p unless $p\mid b$. However, using quadratic reciprocity,

$$-1=\left(\frac{-3}{p}\right)\left(\frac{p}{3}\right)=\left(\frac{-1}{p}\right)\cdot(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}=1,$$

a contradiction. So $p \mid b$, meaning $p \mid a$ too. But then $p^2 \mid a^2 + ab + b^2 = p$, which is impossible.

Now comes the interesting part. Ignore $p = 3$, since $(1, 1)$ works then. Now note that the above method can be modified to find an x for which $p \mid x^2 + x + 1$, when $p \equiv 1 \pmod 3$ (try it). Then, using Thue's lemma, find a, b such that $ax \equiv b \pmod p$ with $0 < |a|, |b| < \sqrt{p}$. Then

$$\begin{aligned} a^2 + ab + b^2 &\equiv a^2 + a(ax) + (ax)^2 \\ &\equiv a^2(x^2 + x + 1) \equiv 0 \pmod p. \end{aligned}$$

Now, $p \mid a^2 + ab + b^2$ and $0 < a^2 + ab + b^2 < 3p$. Hence, $a^2 + ab + b^2 \in \{p, 2p\}$. We are close, but not there. What if $a^2 + ab + b^2 = 2p$? Well, then both (a, b) must be even (check this). Hence, $4 \mid a^2 + ab + b^2 = 2p$, which is impossible. So this possibility is rejected altogether. Hence, $a^2 + ab + b^2 = p$, and we are through.

9.4 Hands-On Constructions

Upto this point we have talked of methods that are more existence type, in which you know the number exists using CRT, or you found a prime using Dirichlet. This section is dedicated to problems where we manually and explicitly construct objects. (Also, just as a note, this section would be more about small tricks rather than just a collection of examples.)

Solutions of this type to construction problems are often "magical" and out of the blue, and roughly take the form "take $P(x) = 24x^3 - 4xy^2 + 1$. This works now deal with it". For instance, here is a prime example:

Example 9.4.1 (Kvant)

Is there an infinite set of positive integers such that no matter how we choose some elements of this set, their sum is not a perfect power?

Proof. The answer is yes. Consider the set $A = \{2^n \cdot 3^{n+1} : n \geq 1\}$. If we add some elements from this, it would be of the form $2^x 3^{x+1} y$ for some y coprime to 6. This clearly isn't a perfect power. □

This was not an easy problem by any standard. The proof, on the other hand, is a one line solution with no back story given, which probably involved pages and pages of rough work and trials.

In general, what makes these problems hard is their combinatorial nature, which means you will have to try a lot of things and there are no fixed approaches you could try. In this section, I would try to give some small ideas which could work at times, but more so focus on examples, including slight motivations for them (because each solution takes a lot of trial and error and there is no one fixed motivation that can dig a path through). I will try and give some strategies and hopefully you would be able to approach such problems better by the end of this chapter.

9.4.1 Restrictions

The general idea is to experiment with possibilities. At times, you can try to add restrictions and see if they work. For instance, if you want to find odd working n, you only look at which primes values of n work. If you can find a prime that works, you are good to go. Otherwise go back a step and try something else. It's always a leap of faith. The key part is to ask the question: "why did my restriction fail?" If you can answer it, you should be able to mend it.

Enough of general talks, let's look at some examples now. The first one shows how even the slightest pattern is worth considering:

Example 9.4.2

1. Find infinitely many pairs of integers a and b with $1 < a < b$, so that ab exactly divides $a^2 + b^2 - 1$.
2. With a and b as above, what are the possible values of
$$\frac{a^2 + b^2 - 1}{ab}?$$

With no idea on how to start with (2), we start with (1). Naturally, we first set $a = 2$ to get $3b|b^2 - 8$. It is clear that $b = 3$ works.

At this point, we ask: does every solution of the form $(a, a+1)$ work? Substitute it, and we get

$$E = \frac{a^2 + b^2 - 1}{ab} = \frac{a^2 + a^2 + 2a + (1 - 1)}{a(a+1)} = \frac{2a(a+1)}{a(a+1)} = 2$$

That's how some wishful thinking can come in handy!

For the part (2), we guess that every natural number is possible, for which all that was needed was to make a (clever) construction. It's logical to try to extend the above construction to $(a, b) = (a, a + k)$. If you try this, you would realize it doesn't work. What is it that is not working here, but worked for $k = 1$?

After some thought, we realize that it is the 1 that gets canceled by the (annoying) -1! So we try $(a, b) = (a, ka - 1)$ instead. We then get

$$E = \frac{a^2 + (ka - 1)^2 - 1}{a(ka - 1)} = \frac{(k^2 + 1)a - 2k}{ka - 1} = k + \frac{a - k}{ka - 1}$$

So we want $ka - 1|a - k$. The simplest thing that we can do is to make $a - k = 0$ by setting $a = k$. That's it, it works! So we have the working construction $(a, b) = (k, k^2 - 1)$ showing every integer k is possible.

Example 9.4.3 (IMO Shortlist 2014 N4)

Let $n > 1$ be an integer. Prove that there are infinitely many integers $k \geq 1$ such that

$$\left\lfloor \frac{n^k}{k} \right\rfloor$$

is odd.

If n is odd, then this isn't very hard. Just take $k = n^t$ for any t. This works.

The interesting part is n even. Suppose $n = 2$. On experimenting $k = 1, 2, 3, \ldots, 12$, we find that 12 is the smallest integer for k that works. Now $12 = 2^2 \times 3$. This motivates $k = n^2(n+1)$. Does it work?

$$\left\lfloor \frac{n^{n^2(n+1)}}{n^2(n+1)} \right\rfloor = \left\lfloor \frac{n^{n^2(n+1)-2}}{n+1} \right\rfloor = \frac{n^{n^2(n+1)-2} - 1}{n+1},$$

which is odd since the numerator and denominator are both odd (here, we used the observation that $n^{n^2(n+1)-2} \equiv 1 \pmod{n+1}$).

So, for each even n, we have working number. How do we get infinitely many? Well, in our proof we used the fact that $n^{n^2(n+1)-2} \equiv 1 \pmod{n+1}$ since $n^2(n+1) - 2$ is even. This remains true if we replace 2 by any even number. So, if we try $k = n^{2t}(n+1)$ for any t, we find

$$\left\lfloor \frac{n^{n^{2t}(n+1)}}{n^{2t}(n+1)} \right\rfloor = \left\lfloor \frac{n^{n^{2t}(n+1)-2t}}{n+1} \right\rfloor = \frac{n^{n^{2t}(n+1)-2t} - 1}{n+1},$$

which is still odd. So, for even n, we have found the construction $k = n^{2t}(n+1)$.

Example 9.4.4 (APMO 1997)

Find a number n between 100 and 1997 such that $n \mid 2^n + 2$.

This expression should remind you of Example 5.8.2. What the result there tells us is that n cannot be odd. So we only try to find even n. Suppose we restrict it to $n = 2p$. But then $p \mid 2^{2p-1} + 1$, which fails because of Fermat's Little Theorem.

Suppose we restrict our attention to $n = 2pq$. So we want $pq \mid 2^{2pq-1} + 1$, which means -2 is a quadratic residue mod p, q. Further Fermat's Little Theorem gives us

$$pq \mid 2^{pq} - 1 \iff p \mid 2^{2q-1} - 1 \text{ and } q \mid 2^{2p-1} - 1.$$

We have enough restrictions on our search now, so we manually start to find values. Since we want -2 to be a quadratic residue, we must have $q \equiv \{1, 3\} \pmod 8$. Now 3 gives $p \mid 31$, so $p = 31$. But then $31 \equiv 7 \pmod 8$. So take $q = 11$. It shows $p \mid 2^{21} - 1 = (2^7 + 1)(2^{14} - 2^7 + 1)$. So if $p \mid 129$, then $p = 43$ since $p \neq 3$. This works, since $11 \mid 2^{2(43)-1} - 1 = 2^{85} - 1$ (why?). Hence $n = 2 \cdot 11 \cdot 43$ works.

9.4.2 Wishful Thinking

Yes, wishful thinking is very common in all kinds of problems. It is highly involved in any problem, and mostly used more than once in a challenging one. However, in this section I present some problems which are short and cute, depicting purely the idea of wishful thinking.

Example 9.4.5

Prove that for any n, there exist n consecutive composite numbers.

This shows how prime numbers are so sparsely placed. The key idea is to think factorials, since they basically contain n consecutive numbers. So, $n! + i$ would have i as a common factor, which would mean this can't be prime. So if we pick $n! + 1, n! + 2, \ldots, n! + n$, then we are done... or are we? Well, $n! + 1$ could be a prime, we can't guarantee anything here. How do we fix this? We start from $n! + 2$. However, this gives us $n - 1$ consecutive numbers. To get n consecutive numbers, we pick $(n + 1)! + 2, (n + 1)! + 3, \ldots, (n + 1)! + (n + 1)$, and this works.

Example 9.4.6 (RMM 2015/1)

Does there exist an infinite sequence of positive integers $a_1, a_2, a_3, \ldots$ such that a_m and a_n are coprime if and only if $|m - n| = 1$?

The key idea here is to think in terms of numbers in terms of its prime factors, since then we can easily handle the coprime condition as having no common numbers. So, looking at numbers as multisets (chapter 1 anyone?), we want sets $A_1, A_2, \ldots$ such that $A_m \cap A_n = \phi$ if and only if m, n are consecutive.

Suppose we set $A_1 = \{2\}$. Then we can set $A_2 = \{3\}$. Then A_3 must contains A, and so must be A_4. Hence both contain $\{2\}$, and so they can't be disjoint. So we start with two elements. In fact, we try and keep 2 "new" elements, i.e. elements which haven't occurred before).

So set $A_1 = \{2, 3\}$. Then set $A_2 = \{5, 7\}$. Write $A_3 = \{2, 11, 13\}$, and1 $A_4 = \{3, 5, 17, 19\}$. Now for A_5, we choose 2 from A_1, and we are lucky since $2 \notin A_4$. Similarly, we choose 7 from A_2 since $7 \notin A_4$. So we set $A_5 = \{2, 7, 11, 23, 29\}$. And this idea of ours works, we alternatively add elements of A_1 into sets after A_3, and similarly alternatively add elements from A_2 into sets beyond A_4. We can express this in the following table:

A_i	$\{2,3\}$	$\{5,7\}$	$\{11,13\}$	$\{17,19\}$	$\{23,29\}$	$\{31,37\}$	$\{41,43\}$	$\{47,53\}$	
From A_1			2	3	2	3	2	3	
From A_2				5	7	5	7	5	
From A_3					11	13	11	13	...
From A_4						17	19	17	
From A_5							23	29	
From A_6								31	

Then let the sets S_i to be $A_i \cup$ the ith column works, for instance $S_1 = \{2, 3\}$ and $S_4 = \{17, 19, 3, 5\}$.

9.4.3 Pell's Equations

Recall the

$$a^2 - db^2 = 1$$

is the Pell's equation in (a, b) for a given square-free d. We know that this has infinitely many solutions. Occasionally, this fact is useful in constructions. For instance, let's look at the following problems:

Example 9.4.7

Find infinitely many triples (a, b, c) of positive integers such that a, b, c are in arithmetic progression and such that $ab + 1$, $bc + 1$, and $ca + 1$ are perfect squares.

Firstly, to utilize the AP condition, we make the standard substitution $(a, b, c) \mapsto (a - v, a, a + v)$, an then we have that

$$\begin{cases} a^2 - av + 1 = A^2 \\ a^2 + av + 1 = B^2 \\ a^2 - v^2 + 1 = C^2 \end{cases}$$

Now, remember the trick of multiplying $a^2 + ab + b^2$ by 4 to complete the square? We apply something similar, but a slight variation. Since we have to choose a, we set $a = 2u$ for some u. Then some wishful thinking gives

$$\begin{cases} 4u^2 - 2uv + 1 = (u - v)^2 + 3u^2 - v^2 + 1 \\ 4u^2 + 2uv + 1 = (u + v)^2 + 3u^2 - v^2 + 1 \\ 4u^2 - v^2 + 1 = u^2 + 3u^2 - v^2 + 1 \end{cases}$$

where motivated by the $2uv$, we wrote the first expression in the form $(u - v)^2 + \cdots$ and similarly for the second one, and seeing carefully, we find that the annoying (common) component in the first 2 expressions also appears in the last expression! So, we act wishfully and try to set $3u^2 - v^2 + 1 = 0$. If we can have this for infinitely many (u, v), we are done. However, this is precisely Pell's equation!

So, our construction is to pick any (u, v) with $v^2 - 3u^2 = 1$, and then set $(a, b, c) = (2u - v, 2u, 2u + v)$. These can be checked to work manually too.

Example 9.4.8

Show that there exist infinitely many positive integers n such that $n^2 + 1$ divides $n!$.

Here's the key idea: if we can select $n^2 + 1 = dm^2$ and ensure $dm^2 \mid n!$, we are done. The equation we seek is $n^2 - dm^2 = -1$, which is negative Pell's equation. Recall the this

has infinitely many solutions if we can find one solution. So, we choose d selectively. Since $2^2 - 5(1)^2 = -1$, hence $d = 5$ is good.

Now, if we want $5m^2 \mid n!$, we first try to prove $n > 5m^2$, since then this would be clear. However, this is not true (why?). We would be done however if two multiples of m are less than n, since then $m^2 \mid n!$, and we can ensure $n > 5$ (how?). Clearly, $m, 2m < \sqrt{5}m = \sqrt{n^2+1} < n+1$ implies $m, 2m \leq n$, and so our construction works.

Example 9.4.9

Prove that there exists infinitely many positive integers n such that $n^2 + 1$ has two divisors whose difference is n.

Suppose one divisor is a and the other is $n + a$. The simplest thing for us would be $a(n + a) = n^2 + 1$, i.e. $n^2 + 1 = a^2 + an$. We try to complete the square now, for which we multiply both the sides by 4. Then this becomes $(2a+n)^2 - 5n^2 = 4$. This is Pell's equation! However, this is not so easy to solve because of the 4 instead of 1. But if we set $n = 2k$ for some k, then this becomes $(a+k)^2 - 5k^2 = 1$. This is Pell's equation and hence has infinitely many solutions, and hence works.

9.4.4 Fermat's Little Theorem

Fermat's Little Theorem is very useful in polynomial constructions. There are two particular uses I would talk about:

1. Every number $x \in \mathbb{F}_p$ is a root of the polynomial $x^p - x$.
2. $x^{p-1} \equiv 1 \pmod{p}$ iff $p \nmid x$.

The second one can be used to set up "indicator variables". For instance, let's try to prove the following two results on polynomials in $\mathbb{F}_p[X]$ (the names are made-up)

Example 9.4.10 (Degree Reduction)

If $f \in \mathbb{Z}[X]$ is a polynomial so that $\deg f > p$, where p is a prime, then either

- Every integer is a solution of $p \mid f(x)$; or
- There exists a monic polynomial $g \in \mathbb{Z}[X]$ with $\deg g < p$ and the roots of $p \mid g(x)$ are the same as that of $p \mid f(x)$.

The key idea is to notice that every integer is a root of $x^p - x$ in $\mathbb{F}_p$. So, we find polynomial $q, r \in \mathbb{F}_p[X]$ so that $f(x) = (x^p - x)q(x) + r(x)$. If r is identically zero (recall it's coefficient are in $\mathbb{F}_p$), then $p \mid f(x)$ for all x.

Otherwise, we find that $r(x)$ is also zero whenever $f(x)$ is 0 modulo p. This works, except it might not be monic. So write bx^m to be the leading coefficient of r with $b \neq 0$. Then consider $g \in \mathbb{F}_p[X]$ that satisfies

$$g(x) = b^{-1}r(x)$$

This works, and so we are done.

Example 9.4.11 (Functions to small polynomials)

Let $h : \mathbb{F}_p \to \mathbb{F}_p$ be a function. Then there exists a polynomial f with $\deg f \leq p-1$ such that $h(x) \equiv f(x) \pmod{p}$ for all $x \in \mathbb{F}_p$.

The proof is constructive in nature. We define the indicator function $\varepsilon_a(x) : \mathbb{F}_p \to \{0, 1\}$ such that $\varepsilon_a(x) = 1$ if and only if $x \equiv a \pmod{p}$, for some a. Then defining $f(x) = h(0)\varepsilon_0(x) + h(1)\varepsilon_1(x) + \cdots + h(p-1)\varepsilon_{p-1}(x)$ works.

So if we find an indicator function which is a polynomial, then we are done. The following function

$$\varepsilon_a(x) = 1 - (x-a)^{p-1}$$

works.

9.5 Example Problems

This section contains many example problems, which serve as a finale. The problems here meander through many ideas discussed in this chapter, and hence are quite illustrative.

Example 9.5.1

Let n be a positive integer. Prove that the following two statements are equivalent.

1. n is not divisible by 4
2. There exist $a, b \in \mathbb{Z}$ such that $a^2 + b^2 + 1$ is divisible by n.

We first do the easy direction, which is $n \mid a^2 + b^2 + 1$ implies $4 \nmid n$. if 4 did divide n, then we would get $a^2 + b^2 \equiv -1 \pmod 4$. I will leave it upto you to show this is not possible (hint: what values can $x^2 \pmod 4$ take?).

Now comes the interesting part: showing that if $4 \nmid n$, then there exist a, b such that $n \mid a^2 + b^2 + 1$. Looking at the "$a^2 + b^2$", we think of Fermat's two square theorem. If $p \equiv 1 \pmod 4$ is a prime, then there would exist a, b such that $p = a^2 + b^2$. So we would want $n \mid p + 1$. Now comes the interesting part, since $\gcd(n, 4) = 1$, hence the following system would have a solution:

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv -1 \pmod n \end{cases}$$

The above system would have a solution of the form $p \equiv (\bullet) \pmod{4n}$. Such a p would satisfy both our conditions. However, how do we ensure we can find a prime p satisfying? Yes, by using Dirichlet's theorem.

Next we do a problem which can be done by other methods, especially non-constructive (which are more natural solutions). However, a constructive solution is quite fascinating so it would be a shame to not include it. The key idea is again to be greedy and keep on adding as many conditions as needed, and use CRT to combine them.

Example 9.5.2 (All-Russian Mathematics Olympiad 2018 Grade 10/6)

Let a and b be given positive integers. Prove that there are infinitely many positive integers n such that $n^b + 1$ doesn't divide $a^n + 1$.

We use the simplest idea for construction: find a prime p dividing $n^b + 1$ that doesn't divide $a^n + 1$. So we want to construct an n such that $p \mid n^b + 1$, i.e. $n^b \equiv -1 \pmod p$. This can be done if we find an n such that $\text{ord}_p(n) = 2b$. How do we do this though?

Here's the idea: use a primitive root. They are our best tool to control orders, so why not. So we can let $n \equiv g^{\frac{p-1}{2b}}$ and that would work... if $\frac{p-1}{2b}$ is an integer. So we would want $2b \mid p - 1$. Add that to the list of conditions we want.

Next, we want $p \nmid a^n + 1$. For this, we can pick $p - 1 \mid n$ so that $a^n \equiv 1 \pmod{p}$ by Fermat's little theorem. So we have the system:

$$\begin{cases} n \equiv z & (\text{mod } p) \\ n \equiv 0 & (\text{mod } p-1) \end{cases}$$

We pick such a n. What about p? We want a p such that $p \equiv 1 \pmod{2b}$. And of course, we can choose any of the infinitely many primes satisfying this (by Dirichlet). So we are done.

Next, we take a look at a beautiful problem. Even though the statement might seem weird, it is quite intriguing. The solution is also purely wishful thinking, which makes you like the problem even more after reading the solution.

Example 9.5.3 (USAMTS 2017-18 Round 3 P4)

A positive integer is called uphill if the digits in its decimal representation form an increasing sequence from left to right. That is, a number $\overline{a_1 a_2 \dots a_n}$ is uphill if $a_i \leq a_{i+1}$ for all i. For example, 123 and 114 are both uphill. Suppose a polynomial $P(x)$ with rational coefficients takes on an integer value for each uphill positive integer x. Is it necessarily true that $P(x)$ takes on an integer value for each integer x?

If the answer is no, then we must show that there exists a polynomial $P(x) \in \mathbb{Q}[X]$, either indirectly or explicitly, such that P sends uphill integers to integers, but some non-uphill integers to non-integers. If the answer is yes, then we would need to somehow show uphill numbers are strong enough to define P over all integers. It is not too hard to see that proving the latter would be much harder, so we first try to see if no is a possibility.

The first thing we try is to find a good way to think about uphill numbers. After some thought we can find that $123 = 111 + 11 + 1, 1245 = 1111 + 111 + 11 + 11 + 1$. So, if we define $b_1 = 1, b_2 = 11, b_3 = 111, \dots$, then each uphill number can be expressed as a sum of b_i. A key observation here is that each uphill number is the sum of at most 9 b_i because each digit is atmost 9.

Now, the b_i motivate us to think modulo 11. Clearly, $b_i \equiv 0 \pmod{11}$ if i is even and $b_i \equiv 1 \pmod{11}$ if i is odd. So any uphill number is at most 9 modulo 11. Hence, if $x \equiv 10 \pmod{11}$, then x cannot be an uphill integer. So we have found that uphill numbers belong to a class of numbers (numbers which are at most 9 mod 11), and this class is much easier to deal with. So, if we can construct $P \in \mathbb{Q}[X]$ such that $P(x) \in \mathbb{Z}$ iff $x \not\equiv 10 \pmod{11}$ for an integer x, then we may celebrate.

We are now done with the hard part, and is just like Example 9.4.11. Note that $x^{10} \equiv 1 \pmod{11}$ iff $x \not\equiv 0 \pmod{11}$ by Fermat's Little Theorem. So, the polynomial

$$P(x) = \frac{(x-10)^{10} - 1}{11}$$

works.

I would like to conclude by sharing a difficult problem given to me by my friend Samuel Goodman. The solution I present here was also communicated to me by him.

Example 9.5.4

Let p be a prime that is 1 modulo 4. Let x denote the number of non-quadratic residues less than or equal to $\sqrt{p}$, modulo p. Then

$$|2x - \sqrt{p}| \leq \sqrt{\frac{p+1}{2}}.$$

Comment 9.5.1: In the chapter of quadratic residues, we showed that the smallest quadratic non-residue is less than $\sqrt{p}$, i.e. we showed $x > 0$. Here, we are asked to prove the much stronger result that

$$\frac{1}{2}\left(\sqrt{p} - \sqrt{\frac{p+1}{2}}\right) \leq x \leq \frac{1}{2}\left(\sqrt{p} + \sqrt{\frac{p+1}{2}}\right).$$

The task of showing $x > 0$ was in itself a good challenge, hence you can expect this to be a delight too.

Here's the beautiful proof:

Proof. There are $(p-1)/2$ quadratic non-residues. Select any one, say r. Then, using Thue's lemma, we find $0 < |a|, |b| < \sqrt{p}$ such that $ar \equiv b \pmod{p}$. Call the pair (a, b) *good*. Now, the key observation is that exactly one of a, b must be a non-quadratic residue, and the other is a residue.

Now, $p \equiv 1 \pmod{4}$ implies -1 is a quadratic residue. So if (a, b) is a good pair, so are $(-a, b), (a, -b)$ and $(-a, -b)$ (note the condition for Thue's lemma involves $|a|, |b| < \sqrt{p}$ not just a, b). At least one of these has both its elements less than $\sqrt{p}$. Call such a pair *special*. Noting that no two good pairs can be equal (why?), we conclude that there are at least $\frac{1}{4}\left(\frac{p-1}{2}\right) = \frac{p-1}{8}$ special pairs.

The final trick is to consider all ordered pairs (k, ℓ) with $0 < k, \ell < \sqrt{p}$ and exactly one of k, ℓ is a quadratic residue, the other being a quadratic non-residue. Clearly, there are $x(\sqrt{p} - x)$ such pairs. However, since every special pair belongs to this category, hence

$$x(\sqrt{p} - x) \geq \frac{p-1}{8}.$$

This can be solved to get the desired bound. □

9.6 Practice Problems

Problem 9.6.1. The integers a and b have the property that for every nonnegative integer n the number of $2^n a + b$ is the square of an integer. Show that $a = 0$. **Hints:** 100

Problem 9.6.2 (USAMO 2011/4). Consider the assertion that for each positive integer $n \geq 2$, the remainder upon dividing 2^{2^n} by $2^n - 1$ is a power of 4. Either prove the assertion or find (with proof) a counterexample. **Hints:** 221 444 252

Problem 9.6.3 (USAMO 2017/1). Prove that there are infinitely many distinct pairs (a, b) of relatively prime integers $a > 1$ and $b > 1$ such that $a^b + b^a$ is divisible by $a + b$. **Hints:** 327 230

Problem 9.6.4 (IMO 1989/5). Prove that for each positive integer n there exist n consecutive positive integers none of which is an integral power of a prime number. **Hints:** 181 87 372

Problem 9.6.5 (USA TSTST 2018 Problem 4). For an integer $n > 0$, denote by $\mathcal{F}(n)$ the set of integers $m > 0$ for which the polynomial $p(x) = x^2 + mx + n$ has an integer root.

1. Let S denote the set of integers $n > 0$ for which $\mathcal{F}(n)$ contains two consecutive integers. Show that S is infinite but
$$\sum_{n \in S} \frac{1}{n} \leq 1.$$
2. Prove that there are infinitely many positive integers n such that $\mathcal{F}(n)$ contains three consecutive integers.

Hints: 394 71 479

Problem 9.6.6 (USAJMO 2016/2). Prove that there exists a positive integer $n < 10^6$ such that 5^n has six consecutive zeros in its decimal representation. **Hints:** 406 135 105

Problem 9.6.7 (AoPS Mock Olympiad "SORY" P2[3]). Determine whether there exists an infinite set S of positive integers such that for every real number $t \in (0, \frac{1}{2})$, we have
$$|x - my| > ty$$
for every pair of different elements x, y of S and every positive integer m. **Hints:** 77 18

Problem 9.6.8 (RMM 2011/1). Prove that there exist two functions $f, g \colon \mathbb{R} \to \mathbb{R}$, such that $f \circ g$ is strictly decreasing and $g \circ f$ is strictly increasing. **Hints:** 294 240 45 483

Problem 9.6.9. Prove that the equation $a^2 + b^2 = c^2 + 3$ has infinitely many integer solutions (a, b, c). **Hints:** 254 330 15

[3] See [9]

Problem 9.6.10 (APMO 2009/4). Prove that for any positive integer k, there exists an arithmetic sequence

$$\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \ldots, \frac{a_k}{b_k}$$

of rational numbers, where a_i, b_i are relatively prime positive integers for each $i = 1, 2, \ldots, k$ such that the positive integers $a_1, b_1, a_2, b_2, \ldots, a_k, b_k$ are all distinct. **Hints:** 94 227 184 **Sol:** pg. 302

Problem 9.6.11 (Bulgarian Olympiad). Let $f \in \mathbb{Z}[X]$ be a non-constant polynomial and let n, k be positive integers. Prove that there exists a positive integer a such that each of the numbers $f(a), f(a+1), \ldots, f(a+n-1)$ has at least k distinct prime divisors. **Hints:** 255 299

Problem 9.6.12 (China TST 2006 Day 6/2). Prove that for any given positive integer n and m, there is always a positive integer k so that $2^k - n$ has at least m different prime divisors. **Hints:** 366 416 353 138

Problem 9.6.13. Prove that if a number is a quadratic residue modulo all but finitely many primes, then it is a square. **Hints:** 450 40 **Sol:** pg. 303

Problem 9.6.14 (USAMO 2008/1). Prove that for each positive integer n, there are pairwise relatively prime integers $k_0, k_1, \ldots, k_n$, all strictly greater than 1, such that $k_0 k_1 \ldots k_n - 1$ is the product of two consecutive integers. **Hints:** 132 262 234

Problem 9.6.15 (IMO Shortlist 2005 N6). Let a, b be positive integers such that $b^n + n$ is a multiple of $a^n + n$ for all positive integers n. Prove that $a = b$. **Hints:** 154 425 316 **Sol:** pg. 303

Problem 9.6.16 (EGMO 2018/6).

1. Prove that for every real number t such that $0 < t < \frac{1}{2}$ there exists a positive integer n with the following property: for every set S of n positive integers there exist two different elements x and y of S, and a non-negative integer m (i.e. $m \geq 0$), such that

$$|x - my| \leq ty.$$

2. Determine whether for every real number t such that $0 < t < \frac{1}{2}$ there exists an infinite set S of positive integers such that

$$|x - my| > ty$$

for every pair of different elements x and y of S and every positive integer m (i.e. $m > 0$).

Hints: 428 76 439 23 **Sol:** pg. 304

Problem 9.6.17 (USA TST 2 2017/3). Prove that there are infinitely many triples (a, b, p) of positive integers with p prime, $a < p$, and $b < p$, such that $(a + b)^p - a^p - b^p$ is a multiple of p^3. **Hints:** 481 482 426 188

Problem 9.6.18 (IMO Shortlist 2013 N3). Prove that there exist infinitely many positive integers n such that the largest prime divisor of $n^4 + n^2 + 1$ is equal to the largest prime divisor of $(n + 1)^4 + (n + 1)^2 + 1$. **Hints:** 248 454 307 438

Problem 9.6.19 (China TST 1 2019/2). Fix a positive integer $n \geq 3$. Do there exist infinitely many sets S of positive integers $\{a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n\}$, such that $\gcd(a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n) = 1$, $\{a_i\}_{i=1}^n$, $\{b_i\}_{i=1}^n$ are arithmetic progressions, and $\prod_{i=1}^n a_i = \prod_{i=1}^n b_i$? **Hints:** 152 63 159 **Sol:** pg. 304

Problem 9.6.20 (Tuymaada 2004, also INMO 2019/4). Let n and M be positive integers such that $M > n^{n-1}$. Prove that there are n distinct primes $p_1, p_2, p_3 \cdots, p_n$ such that p_j divides $M + j$ for all $1 \leq j \leq n$. **Hints:** 110 472 462 336 **Sol:** pg. 305

Problem 9.6.21 (USA TSTST 2015/5). Let $\varphi(n)$ denote the number of positive integers less than n that are relatively prime to n. Prove that there exists a positive integer m for which the equation $\varphi(n) = m$ has at least 2015 solutions in n. **Hints:** 119 345 260 75 147 465 **Sol:** pg. 305

Problem 9.6.22 (APMO 2020/4). Find all polynomials $P(x)$ with integer coefficients that satisfy the following property:

For any infinite sequence a_1, a_2, ... of integers in which each integer in $\mathbb{Z}$ appears exactly once, there exist indices $i < j$ and an integer k such that $a_i + a_{i+1} + \cdots + a_j = P(k)$. **Hints:** 398 144 48 469 186 **Sol:** pg. 306

Problem 9.6.23 (USA TSTST 2016/3). Decide whether or not there exists a nonconstant polynomial $Q(x)$ with integer coefficients with the following property: for every positive integer $n > 2$, the numbers

$$Q(0),\ Q(1), Q(2),\ \ldots,\ Q(n-1)$$

produce at most $0.499n$ distinct residues when taken modulo n. **Hints:** 417 162 485 243 423 323 **Sol:** pg. 307

✠ Linear Independence among $\sqrt{n_i}$

This section is about a very elegant proof of a particular result, and is taken from [18]. Unlike some of the other special sections, this is not a section to teach you a particular theorem or some theory. However, this is the final section of the book, so presenting a beautiful proof that has ideas interlinked from our work so far and advanced number theory would be a great way to end our journey.

We build up the key idea through examples and eventually present the full formal proof by the end of the discussion.

Motivation

- Let $i = \sqrt{-1}$, and suppose $a, b \in \mathbb{Z}$ with
$$a + bi = 0.$$
Then $a = b = 0$.
- Suppose $a, b \in \mathbb{Z}$ and
$$a + b\sqrt{2} = 0.$$
Then $a = b = 0$.
- Suppose $a, b, c \in \mathbb{Z}$ and
$$a + b\sqrt[3]{2} + c\sqrt[3]{4} = 0$$
Then $a = b = c = 0$.

The first example implies that simple integer operations like scaling and translating by integers can't reduce i to 0, or even some irrational number like $\sqrt{2}$ to 0.

What about rational numbers? Here's an exercise for you:

Problem 9.6.24. Show that if $q \in \mathbb{Q}$, then $a + bq = 0$ has a non-trivial solution in integers a, b

What's so special about non-rational numbers? Do all irrational numbers follow this? (Hint: No, take $1 \cdot (2\sqrt{2}) + (-2) \cdot \sqrt{2} = 0$.)

Our goal is to present some special tuples of irrational numbers that do satisfy this. First, we introduce a term.

Definition 9.6.1. *A set of numbers $\{x_1, x_2, \ldots, x_n\} \in \mathbb{C}^n$ is said to be **linearly independent** over integers if the only solution $\{a_1, a_2, \ldots, a_n\} \in \mathbb{Z}^n$ to the equation*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$$

is the trivial solutions $a_1 = a_2 = \cdots = a_n = 0$.

Example 9.6.1

The numbers $\{1, i\}$ are independent, and so is $\{1, \sqrt{3}\}$. Here's an exercise: Show that $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ is independent.

Our main goal in the talk would be to to prove:

Theorem 9.6.1. *Let $\{n_1, n_2, \ldots, n_\ell\}$ be distinct square-free integers. Then*

$$\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_\ell}$$

are all linearly independent.

Note here that taking $n_\ell = 1$, this implies that any linear combination of non-integer square roots is irrational! This generalizes the classic problem about proving $\sqrt{2} + \sqrt{3}$ is irrational. But how do we prove this theorem?

Raw Idea

Firstly, suppose want to prove $\{1, \sqrt{2}\}$ are linearly independent, which is equivalent to showing $\sqrt{2}$ is irrational. The classic proof of that is the "reductio-ad absurdum" method. However, that method won't work in our problem. So we need to find a different method.

Here's the nice idea: **look at things locally**. Since 2 is not a quadratic residue mod 3, hence it can't be a square! Neat way of showing $\sqrt{2}$ is irrational, right?

So now suppose we want to show $\sqrt{2} + \sqrt{3} = k$ is irrational. We try a similar method. In fact, the prime 7 works, $\sqrt{2} \equiv \pm 3 \pmod 7$ and so we must have $3 \equiv (k \pm 3)^2 \pmod 7$, but 3 is not a quadratic residue! So here's an overview of our approach:

We would like to find a prime p in general, such that modulo p, every term in

$$a_1\sqrt{n_1} + a_2\sqrt{n_2} + \cdots + a_\ell\sqrt{n_\ell}$$

except the last one becomes an integer. So, we would love to have:

Lemma 9.6.1. *Suppose we have primes $q_1, q_2, \ldots, q_\ell$. Then there exists an **arbitrarily large** prime p such that $q_1, \ldots, q_{\ell-1}$ are quadratic residues modulo p, however, q_ℓ isn't.*

The arbitrarily large part is needed since we would not want $p \mid a_\ell$, otherwise that would make $a_\ell\sqrt{n_\ell} \equiv 0$ an integer mod p, ruining our plan.

Spolier Alert: The Lemma is indeed true, and we prove it at the end, since it is a bit technical. Now, we just formalize a finish using this lemma.

Finishing using the Lemma

The proof would be induction on the number of prime factors in $n_1 n_2 \dots n_\ell$. The base case is clearly true.

Assume on the contrary, and suppose there does exist $(a_1, \dots, a_\ell)$. Say the set of prime factors currently is $q_1, q_2 \dots, q_k$. Notice that we can view the $n_1, n_2, \dots$ terms as polynomial in $q_1, q_2, \dots, q_k$. So we can write

$$0 = a_1\sqrt{n_1} + \dots + a_\ell\sqrt{n_\ell} = A + B\sqrt{q_k},$$

where A, B are linear combinations of products of $\sqrt{q_1}, \dots, \sqrt{q_{k-1}}$.

Example 9.6.2

For instance, if $(q_1, q_2, q_3, q_4) = (2, 3, 5, 7)$, we can write

$$2\sqrt{6} - \sqrt{10} + 5\sqrt{42} + 7\sqrt{7} = \underbrace{(2\sqrt{6} - \sqrt{10})}_{A} + \underbrace{(5\sqrt{6} + 7)}_{B}\sqrt{7}.$$

So now we can find prime p by the lemma such that $A, B \in \mathbb{F}_p$ giving

$$q_k \equiv \left(-\frac{A}{B}\right)^2 \pmod{p}.$$

So q_k is also a QR. However, this contradicts the choice of p, so we are done!

Or are we...

Loophole

There's a tricky point that B^{-1} might not exist modulo p, so we can't divide by B.

To fix this, we would like to choose a prime p such that $B \not\equiv 0 \pmod{p}$. Since surds modulo p keep changing on changing p, there is no direct way to do this.

Example 9.6.3

Like $\sqrt{2} \equiv \pm 3 \pmod{7}$ but $\sqrt{2} \equiv \pm 6 \pmod{17}$, and even $\sqrt{2} \equiv \pm 8 \pmod{31}$.

The trick now is slightly technical. Note that B is a sum of algebraic integer, and hence itself an algebraic integer. So its minimal polynomial $P(x)$ has integer coefficients. Also, the other roots of $P(x)$ (the conjugates of B) are also integer mod p by the lemma, and is non-zero by the induction hypothesis.

In particular, the constant term $c \in \mathbb{Z}$ [4] of $P(x)$ is fixed and non-zero, and is an integer multiple of B modulo p. So if we pick $p > c$, then $p \nmid c$ and so $B \not\equiv 0 \pmod{p}$. So done! □

[4] This is called the **norm** of B. The fact about it we use here is that even though B can keep changing mod p, the constant integer c won't.

Proof of the Lemma

Of course, some of you might not be satisfied with the key lemma left hanging. So here's the proof, which is quite similar to Problem 9.6.13.

Proof. It is quite logical to think of the chinese remainder theorem here. However, we would need mod q_i instead of mod p. So we must invert the order using Quadratic reciprocity.

$$\left(\frac{q_i}{p}\right) = 1 \Leftrightarrow \left(\frac{p}{q_i}\right) = (-1)^{(p-1)(q_i-1)/4}$$

for $q_i > 2$. For simplicity, we may take $4 \mid (p-1)$ so that we want $(p/q_i) = 1$. In fact, to have $(2/p) = 1$ if $q_i = 2$, we might as well choose $p \equiv 1 \pmod 8$.

Now, just greedily use the Chinese remainder theorem: Let s be a non-quadratic residue mod q_ℓ. Then the system

$$\begin{cases} p \equiv 1 \pmod 8 \\ p \equiv 1 \pmod{q_i} \quad \text{for all } i < \ell, q_i \neq 2 \\ p \equiv s \pmod{q_\ell}. \end{cases}$$

has a solution by CRT. But we want p to be a prime. How to ensure that? Dirichlet's Theorem of course! So we are done. □

Hints

1. Show that $f(ab) = f(a) + f(b) + 1$ if both a, b are even and $f(ab) = f(a) + f(b)$ otherwise.
2. Vieta Jump to finish.
3. When $x = 1$, do some bounding and parity work to show $y + z \in \{503 \cdot 2, 503 \cdot 4\}$.
4. You should now get a formula for how many times a segment of length ℓ appears. So find a formula for the desired sum.
5. Try to force a telescoping sum.
6. Consider algebraic combinations of $P(n-1), P(n), P(n+1)$ to get simpler terms.
7. You get $(a + c - 2b)q = b^2 - ac$. When does this imply q is rational?
8. Make $n + c = p^2$. Combine your results.
9. Write $d = 4k + 1$ and finish.
10. Show that $n = 1$.
11. Prove $\sigma(n) < n\sqrt{d(n)}$ for all p^α except one p, where you use the factor of $\sqrt{2}$.
12. Why can we shift and scale terms? If we do this to set $s_1 = t_1 = 0$ and $s_2 = 1$, then what do we get?
13. If $p^M \nmid Q(n)$, show that $M < \alpha t$ for some constant α. Why does this imply M is bounded by a constant?
14. You get $a^n - b^n = p(b - c), \ldots$ In order to pair up $(a - b)$ with $(a^n - b^n)$, what do you do?
15. $(2\ell, 2\ell^2 - 2, 2\ell^2 - 1)$ works.
16. Use the fact that $2^{n_i} - 1 \mid 2^x - 1$ and combine all the divisibility relations.
17. If b is odd, then 3 is a quadratic residue mod any divisor of $3^b - 1$.
18. Show $\nu_2(a_{i+1}) < \nu_2(a_i)$.
19. Did you know Vieta Jumping is also known as Root Flipping?
20. Suppose a z exists. How do you show uniqueness?
21. Now show $4n + 1 < (\sqrt{n} + \sqrt{n+1})^2 < 4n + 3$.
22. Show that $R(m^c)$ have the same set of prime divisors.
23. Pick p_2 so that $p_2 \equiv \frac{p_1 - 1}{2} \pmod{p_1}$ and $p_2 > 2p_1$. Continue adding elements like this.

24. In which set would n be?
25. How many factors does 18 have?
26. Each point in I is uniquely defined by its value mod a_i for all i (why?). So, give a complete characterization of the endpoints of ℓ mod all a_i.
27. Prove $f(1) = 0$
28. If $\mathcal{S}_\ell$ is the sum of powers, then what is $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$?
29. Remove the ceiling by introducing a new variable.
30. Consider elements of the form $ax_i + 1$ where $x_i \in \mathcal{S}_p$.
31. You should get $y^{p-1} + y \le p(y+1)$.
32. The process never ends unless $a = b$. What solutions do you get in this case?
33. There is a prime divisor p of $2^a - 1$ which is $\equiv 3 \pmod 4$.
34. Take the smallest prime divisor p of n and consider $d_{k-1}d_k$.
35. If $b \equiv z^2$, then show that $(2-z)(2+z) = 4-b$ is a QR. What can you say about $2-z, 2+z$?
36. You should get x_i is periodic with period $c^2 - c$. Does this cause any issues?
37. Use a variant of Euclid's construction (for the infinitude of primes).
38. It does have solutions! Work it out algebraically instead of number theoretic ways (like mod)
39. Prove it for $n = 2^k$, then $2^k + 2^{k-1}$. What do you do in general?
40. Pick p to be a quadratic residue modulo all prime divisors of n except one, so it becomes a NQR. How do you do this?
41. Use $m - n \mid f(m) - f(n)$ repeatedly.
42. The answer is $k = 2$.
43. Consider $(x+a)(x+b)(x+c)$ and $(x-d)(x-e)(x-f)$.
44. If a is a power of 2, then $f(n) = ag(n)$ has a unique solution due to a parity argument.
45. Consider the intervals $(2^k, 2^{k+1}]$.
46. Using $\gcd(x, n+1) = 1$, you should be able to show $\gcd(m, y-1) = 1$.
47. What is the simplest lower bound on the row,column sums?
48. For $\deg P \ge 2$, the intuition is that P grows very fast and skips a lot of numbers. Based on this idea, try to construct a sequence $\{a_i\}$ that doesn't satisfy the problem's property.
49. Your best bet is induction.
50. Let g be a primitive root. What are the others?
51. You would like $\deg Q = \deg P = d$. For how many points do you need to define Q? What values do you choose?
52. Use $a^3 + b^3 + c^3 - 3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ca)$.

53. Use LTE to show $r \leq 2$.

54. Show that any divisor of $2^{3^i}+1$ is either 1 or 3 modulo 8. How do we ensure that $2^{2\cdot 3^i}-2^{3^i}+1$ gives a new prime of the form $8k+3$?

55. The numerator is the sum of $\frac{n!}{i}$. Pair up consecutive odd, even terms.

56. Let y be a primitive root. What w should you choose to set $a \equiv y^w$?

57. The number of pairs (a,b) with a,b coprime and $a+b=n$ is $\varphi(n)/2$. This is also atmost the number of possible values of $a = 2^k 5^\ell$. What bound does this give you?

58. Why do you only need to prove the result for $n = p^\alpha$?

59. Convert lcm into gcd .

60. If $y^{p-1}+x \mid x^{p-1}+y \equiv (-y)^{p(p-1)}+y$. What does LTE give?

61. Take $z=1$. So now you want infinitely many pairs $(x,y) \in \mathbb{N}^2$ such that $\frac{y+1}{x}+\frac{x+1}{y} \in \mathbb{Z}$. How do you do this?

62. Use the fact that $1^i+2^i+\cdots+(p-1)^i \equiv 0 \pmod p$ for a prime p and $0 \leq i < p-1$ to show the formula you had before is 0 modulo a_1.

63. There is no AP that satisfies $a\ldots(a+(n-1)d) = (a+d)\ldots(a+nd)$. So make a slight adjustment to the sequence $\{a_i\}$.

64. Both the polynomials have a root $\alpha \in (0,1)$.

65. Prove that any prime factor p of 2^n-1 must be $\pm 1 \pmod{12}$.

66. Show that $p-2 \notin A, p-4 \notin A$ are impossible.

67. Show $p \mid 2(p-3)!+1$. Assume $n \leq -4$ now.

68. Show that $\gcd(2^{2\cdot 3^i}-2^{3^i}+1, 2^{3^i}+1)$ is atmost 3.

69. Express u^2, v^2 in terms of d, a, b and then eliminate a.

70. Can 5 divide any of them?

71. If the elements are $a+\frac{n}{a}, b+\frac{n}{b}, c+\frac{n}{c}$, then using the fact that they are consecutive find c in terms of $x=a-b, y=b-c$.

72. The idea is to force two equal a_i, a_j to be equal. Show that we only need to show this over a finite set of primes.

73. What about the case $k=3$?

74. Take $m = p^{2\nu_p(a_n)+\nu_p(n)+1}$ to get a complete characterization of good sequences.

75. Try to prove that $\varphi(N) = \varphi(p_1\ldots,p_k)$ has at least k solutions in n with each prime factor of N being one of p_i.

76. The answer to the second part is yes. Construct is inductively.

77. This shows $\left\{\frac{x}{y}\right\} = \frac{1}{2}$ for every $x > y$ in S.

78. Multiply the two relations you got to obtain a divisibility relation involving $ac+bd, ab+cd, ad+bc$.

79. Write $a = x/z$ and $b = y/z$ so that $z^n \mid x^n - y^n$.

80. Suppose it is montonic for $n \geq N$. Then why is $d((n+1)^2+1) > d(n^2)+2$?

81. We have $x^n = (y-1)m$. What is $m \pmod{y-1}$?

82. For any c, consider $\theta(p - p(c))$.

83. What is the maximum possible value of $\gcd(x, k)$ for any x?

84. What is $d \pmod 4$?

85. If d is the gcd, then write $a_i^n = dk_i - P$. The definition of P gives a polynomial identity in P^n. What relation in d, P does it give?

86. Show that $n = 2^k m^2$ for some nonnegative integer k and odd natural m.

87. You would like terms of the form $N! + m = m\left(1 + \frac{N!}{m}\right)$. What's the obvious scenario in which this isn't a perfect power?

88. You must have $\nu_2(2q-2) = \nu_2(\text{ord}_p(5)) \leq \nu_2(p-1)$.

89. Let $f(n)$ be the number of operations it takes to reach 2. If $n = 2^k p_1^{\alpha_1} ... p_t^{\alpha_t}$, show that $f(n) = k - 1 + \alpha_1 f(p_1) + ... + \alpha_t f(p_t)$. What do you get for n odd?

90. You should get $b + d + a - c \mid (a+b)(a+d)$ and a similar result for $b + d - a + c$.

91. $13(2x + 3y) = 26x + 39y$. Why is this useful?

92. If $\nu_2(n_k) = 0$, then when is S odd?

93. Use Fermat's Little Theorem to reduce the relation $503 \mid y^3 + z^3$. What do you get?

94. Suppose the fractions are $(x+1)/N, (x+2)/N, \ldots$. How do you ensure the denominators are distinct?

95. If $k^2 \leq 4n + 1 < (k+1)^2$, between which squares would $4n+2, 4n+3$ lie?

96. $\text{ord}_{(2p+1)}(2) \in \{1, 2, p, 2p\}$.

97. Simplify the congruence to a congruence involving $3, -4, -12$.

98. Take a prime divisor $p > 2$ of $x + y$. What can you say about $\nu_p(x+y)$ when n is odd?

99. Divide by 2^3 and give a factor of 2 to each term. You should get $a^k + b^k = \pm 2$. What does this give?

100. Multiply a term by 4

101. Show that if $p < k$, then $p = 2$. Also, when is p not less than k?

102. What happens if n is odd?

103. What can you say about $p + m - 1$?

104. Show that $L = \text{lcm}(n+1, \ldots, 2n+1)$ divides $m - n$.

105. Find an n such that $5^n \equiv 5^{20} \pmod{10^{20}}$. Why does this work?

106. $2n + 1$ is always odd. What does this mean?

107. Apply the same method of grouping.

108. Use Bézout's theorem on m, n.

109. Suppose $n = \ell$ works. Construct an $n > \ell$ that works too.

110. What can you say about a common divisor of $M + i, M + j$?

111. If $A = \{a_1, \ldots, a_k\}$, bound $a_2 - a_1, a_k - a_{k-1}$ by our previous observations.

112. Take $(a, b) = (x, -x)$ and similar values to directly find $P(x)$.

113. If $d \mid n$, then how many times does d occur in $f(n)$?

114. To show non-powers of 2 don't have a unique solution, why does it suffice to show this just for odd integers?

115. Use the Pigeonhole Principle to finish.

116. For the next two part, the prime factors of which numbers are the easiest to control?

117. Get $10^n S = n_k!$. So $n_k \mid 10$. Then if $2, 5 \mid n_k$, then $\gcd(S, 10) = 1$. What does this mean?

118. What is $\text{ord}_k(3)$?

119. Use induction to show the result for any k, not just 2015.

120. Write $Q(x) = x^d R(x)$ so that $x \nmid R(x)$. We would like to show R is a constant.

121. Count how many terms in the product are divisible by p, how many by p^2 and so on.

122. Let $k = \lfloor \sqrt{n} \rfloor$. How do you remove the square root?

123. You should get $P(x) - x \mid P^2(x) - P(x) \mid \cdots \mid P^k(x) - P^{k-1}(x) \mid P^{k+1}(x) - P^k(x) = P(x) - x$.

124. When $x = 2$, show $|y - z| = 1$ and hence show $y + z = 503$.

125. The solution is $\theta(p) = p(c)$ for a constant c.

126. Now use mod 11 to find the possible values of a.

127. What is another formula for $\zeta(n)$?

128. $x^2y \cdot y^2z \cdot z^2x = (xyz)^3$.

129. Generate a new quadruple (a^*, b, c, d).

130. $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$.

131. Multiply to get the key equation: $\frac{a^n - b^n}{a-b} \cdot \frac{b^n - c^n}{b-c} \cdot \frac{c^n - a^n}{c-a} = -p^3$.

132. You want to show the existence of x_0 for which the polynomial $P(x_0) = x_0^2 + x_0 + 1$ is divisible by at least $n + 1$ primes.

133. If $a = 2^k 5^\ell$, then $a < n$. So how many such numbers are possible?

134. The key observation is that one of the two divides the other.

135. $5^8 \equiv 5^4 \pmod{10^4}$, so the last digits become 0625.

136. Define the sequence of integers $b_k = (a_1 + \cdots + a_k)/k$. The given question is equivalent to showing what about the sequence $\langle b_k \rangle$?

137. Find an algebraic way to convert $2x + 3y$ to $9x + 5y$ by adding/subtracting/multiplying things.

138. Combine all the conditions using CRT. (There's a catch in using CRT. Try to find and fix it)

139. Suppose $2 \in A$ and write $A = \{2, x_1, \ldots, x_i, 4 - x_1, \ldots, 4 - x_i\}$ and $B = \{y_1, \ldots, y_j, 4 - y_i, \ldots, 4 - y_j\}$. Show that you can map each pair $(x_i, 4 - x_i), (y_i, 4 - y_i)$ to an element of B. What more can you say about this map?

140. If $\mathcal{S}$ is the set of p^{2^i}, then which elements from $\mathcal{S}$ multiply to give $f(2^k)$?

141. Take $p > 2$ and show $p + 1$ divides $n^p + 1$. What is the order of $n \bmod p + 1$?

142. Show that $481 \mid x, y$.

143. If $n = 2^k$, then which primes of the form $4k + 3$ can divide $2^n - 1$?

144. Use Pigeonhole to show all $\deg P = 1$ work.

145. Guess a quadratic polynomial that works.

146. Take x, y so that $u = \nu_p(A^x - B) < \nu_p(A^y - B) = v$.

147. Using the induction hypothesis, $N = np_{k+1}$ give k solutions where n satisfies the case k, How do you get 1 more?

148. Pick a q from this set of prime divisors. Take a clever choice for c to get a contradiction.

149. Is $n = p$ possible? What about p^2? What about p^k?

150. If $x_1 \neq 2$, then show that $x_2, x_3 \equiv 3 \pmod 4$ and hence -2 is a quadratic nonresidue mod x_3.

151. Give a construction to show S_k is infinite if k has an odd prime factor.

152. The key trick here is to consider b_i to be a translated sequence of a_i, i.e. set $b_1 = a_2, b_2 = a_3, \ldots$. Now we need to handle the endpoints carefully so that the product is the same.

153. In the $1+1/2+\cdots+1/n$ problem, we considered ν_2. In the $1+1/3+\ldots$ problem we considered ν_3. However, in our problem, if for some i $p_i \in \{2, 3\}$, then ν_2, ν_3 are useless. Which ν_p should we consider here?

154. Instead of directly showing $a = b$, try to show $a \equiv b \pmod p$ for any prime p.

155. Show that $d = 2 \cdot 3^7$ or $d = 2 \cdot 3^3 p$ for a prime p.

156. Can you ensure infinitely many solutions to $a + kb = n^t$ for some t, k?

157. Assume $\theta(x) = 0$. Why does it suffice to show $\theta(p) = 0$ for all polynomials $p \in \mathbb{Z}[X]$ with $p(0) = 0$?

158. You get $p \mid f(0)$. Why does this cause issues?

159. Take $a_1 = m, a_2 = mb_1, a_3 = mb_2, \ldots$ for some m.

160. Say the first one is x^2 and the second is y^2. Find a, b in terms of x^2, y^2.

161. This time take ν_3.

162. Show that you only have to show the result for primes.

163. Assume $5 \neq p \neq q \neq 5$. Use $p \mid 5^p + 5^q$.

164. Show that $P \in \mathbb{Q}[X]$.

165. Show that n is odd

166. Choose $t \in \mathbb{Q}$ wisely and set $x = \pi$. Use the fact that π is transcendental (i.e. it is not the root of any polynomial with rational coefficients).

167. It's easier to work with $k = c - 2 = \frac{a^2+b^2+a+b}{ab}$.

168. Show that $ab + cd > ac + bd > ad + bc$.

169. Suppose $x + y = 2^\ell$. When can we use LTE?

170. Try to count the number of times a segment of ℓ can appear.

171. For any x in A or B, in which set is $x(4 - x)$?

172. Suppose $p \mid P(n)$. In terms of n, what other $P(\bullet)$ does p divide?

173. In general, write $k = 2^s x - 1$ for $x < k$ odd. Find an equation showing k is expressible assuming x is.

174. You should get $\varphi(k) \geq k - 1$.

175. To use $p - 1 = 2q$ with q an odd prime, show that $\operatorname{ord}_p(x) \in \{q, 2q\}$ for $x \in \{3, -4, -12\}$.

176. $\operatorname{ord}_p(5) \neq q - 1$ but divides $2q - 2$. When is this possible?

177. Let $\gcd(a, b) = d$, $a = dk, b = d\ell$.

178. What is a ν_p way of writing what we want to prove?

179. Find sum of elements and sum of squares of elements.

180. Write $p - 1 \equiv -1, p - 2 \equiv -2$, and so on.

181. Recall Example 9.4.5.

182. To show the new root is less than x, use estimates such as $4ac > 4a^2 = b(c^2 - a^2) - f$.

183. Show that we must have $2^n - 1 = 3\ell$ for some m all of whose prime factors are $\equiv 1 \pmod 4$. Does the required m exist now?

184. Add one more condition on the primes to ensure $(x+i), N$ have only the prime p_i in common.

185. $\nu_p(x + y) = \min\{\nu_p(x), \nu_p(y)\}$ when $\nu_p(x) \neq \nu_p(y)$.

186. If you have added till a_i, take a_{i+2} to be the integer of smallest magnitude not yet in the sequence (can you think why we do this?). Then choose a_{i+1} wisely.

187. For the second part, you can try to show $\lfloor 5x \rfloor + \lfloor 5y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor + \lfloor 3x + y \rfloor + \lfloor 3y + x \rfloor$. Why does this follow from the identity you proved before?

188. See Example 9.3.1

189. Can n be even?

190. Use $f(n) \mid f(n + kf(n))$.

191. If $p \mid n$, then $\gcd(p, cd + 1) = 1$ for all $0 \le c \le k - 1$. If $p < k$, what does this mean?

192. Let $m - n = L\gamma$. Let y be the largest power of 2 in γ. What is the power of 2 in $\frac{L\gamma}{n+i}$ for each i?

193. Use a primitive root g.

194. Fix $i < j$. How many values of k satisfy $a_i + ki \equiv a_k + kj \pmod{p}$?

195. If n is even, use the expression for $n/2$. If n is odd, use the expression for $(n + 1)/2$.

196. You get $d \mid 2P^n$.

197. Now suppose $\gcd(10, s) > 1$. Find a way to fix the number you found before such that the factors of $2, 5$ in s don't cause any issue.

198. Try Hermite's identity. See the next hints for a second solution

199. Show $(y + 1)^n > m > y^n$ if $n > 1$.

200. Firstly assume $\gcd(s, 10) = 1$. What is the simplest number with sum of digits s?

201. Show that all t_i are integers now! What about s_i?

202. Apply Fermat's Little Theorem to find a periodicity result for f.

203. Find the answer for $3^a, 3^a \cdot 5^b, 3^a \cdot 5^b \cdot 7^c$. Guess a pattern

204. Define A to be the set of a such that $a^{p-1} \not\equiv 1 \pmod{p^2}$. Can both $a, p - a$ not be in A?

205. Use $f(n) \mid f(n + kf(n))$.

206. Almost every approach leads to a solution here. For a short one, try to complete the square

207. This time, show $p^2 \mid i^p + (p - i)^p$.

208. If $x \neq 0$, you get a bijection from $T \mapsto T$ and hence two equal sets.

209. Write m in terms of p in the divisibility relation you obtain.

210. Eliminate $n = 2$

211. Suppose $p \mid a_1$. Show that $p \mid a_{p+1}$.

212. Guess the answer

213. Take cases on p; it's size determines if $d_8 = 27$ or p or 54.

214. Pick p to be the smallest prime factor of n.

215. The discriminant must be a square.

216. Show that $b \mid 22n$ and prove that the only prime divisor of b is 11 with maximum power 1, i.e. $b = 11$.

217. Show $\lfloor 2x \rfloor - 2 \lfloor x \rfloor \le 1$ so $\nu_p\left(\binom{2n}{n}\right) \le k$, where k is such that $p^k \le 2n < p^{k+1}$. Why is $\nu_p(\text{lcm}) \ge k$?

218. Show that at least one number in each pair in $\{(2, 3), (4, 5), \ldots, (p - 3, p - 2)\}$ is in A.

219. Get an alternate expression for $g-1$ (you might motivate this from the quadratic $x^2 = x+1$).

220. In the case c odd, you should show every odd composite number is possible.

221. We basically want $2^n \mod n$ to be odd (why?). Go with your gut feeling about the answer (i.e. true or false)

222. Grouping the coefficients (and ignoring them), you get sums of powers. Does this ring a bell?

223. Show that the given implies $k^2 + k\ell + \ell^2 \mid d$. Can you get the bound now?

224. Characterize all n for which $d(n) = 2^k$?

225. Use Problem 3.4.6

226. Bound $\operatorname{lcm}(a, b, c)$ to show it must equal bc.

227. Pick primes p_i such that $p_i \mid x + i$ using the Chinese Remainder Theorem.

228. Show that 2 is a quadratic nonresidue.

229. Consider modulo a suitable number. Guess it by experimenting

230. You can't have $b - a = 1$. What about $b - a = 2$?

231. Show that $i^p + (p-i)^p + \left(\frac{p+1}{2}\right)^p - \left(\frac{p-1}{2}\right)^p$ is divisible by p. Group terms accordingly now.

232. Add elements of the equal sets to conclude $x = 1$.

233. Consider the set $0 \notin \mathcal{S}_p$ formed by the elements of $\mathcal{S}$ mod p for some prime p.

234. Lastly you just need to show that the set of primes dividing elements of $P(1), P(2), \ldots$ is infinite. Does this ring a bell?

235. Show that composite n don't work.

236. Write $n = 2^x 3^y 5^z p_1^{\alpha_1} \ldots$ and define c to be the part inside $\lceil \bullet \rceil$ in the formula for $d_1(n)$. Take cases for c even, odd.

237. If $k \geq 4$, then $a_1 a_k = a_2 a_{k-1} = \ldots$ and a similar result for divisors of m. What do you get?

238. This is very similar to to Problem 6.7.11.

239. Define the set B to be elements b for which $b, 4-b$ are both quadratic residues.

240. If f is discontinuous, we try to make the intervals where f is increasing or decreasing. Let g be a "jump" function which helps to change intervals.

241. Make a table (or graph) with each row corresponding to a value of k. Join two elements by a line in a row if they are congruent for that k. How many lines are there in the table?

242. The formula would be the sum of a polynomial $p(x)$ as x varies over all possible values of ℓ (which you found before). What is the degree of p?

243. Choose $\deg Q = 4$ and something of the form $(kx^2 + \ell)^2$, so that $Q(a) \equiv Q(b)$ gives $a \equiv -b$ or $ka^2 + \ell \equiv -kb^2 - \ell$.

244. Write $a^b - 1 = (a^d)^{b/d} - 1$ and use LTE now.

245. z, z^2 have the same set of prime divisors.

246. Show $p \mid f(j^2/4) = 0$ for some j and infinitely many primes p.

247. Use loose but careful estimates.

248. Define $f(n) = n^2 + n + 1$. What's the relation of this with our sequence?

249. Since $s_i t_i \in \mathbb{Z}$, hence the denominator of s_i divides t_i. So what should r be?

250. Which famous inequality gives $1 + p + \cdots + p^\alpha \geq (\alpha + 1)p^{\alpha/2}$?

251. Noting that $x > y$, just use Vieta Jumping

252. Try $n = p^2$ for some prime p now.

253. $p - 2k$ is bounded but there are infinite possibilities for p, k. What does this show?

254. Set $c = b + k$. Which k is a good choice?

255. We want $a \equiv x_1 \pmod{p_i}$ for k primes such that $p_i \mid P(x_i)$.

256. A segment is characterized by its endpoints. What congruence relations must the endpoints satisfy for the segment to have length?

257. What is S in terms of a primitive root g?

258. Finally, show the set of primes diving T is finite.

259. Suppose it's a $a \times b$ table with $a \geq b$. What happens if $b = 1$?

260. You let $p_1, \ldots, p_k$ to be the first k prime numbers, so that any prime factor of $p_i - 1$ is also from this set. Further, every prime factor of x should be one of p_i.

261. Write $a = pk$ back in the equation. What happens?

262. $P(x_0) \equiv 0 \pmod{p_1 p_1} \iff P(x_0) \equiv 0 \pmod{p_1}, P(x_0) \equiv 0 \pmod{p_2}$.

263. Use the result derived to show that if T is the set of quadratic residues except $\{0, 1\}$. then $t \in T \implies (t-1)x + 1 \in T$, where x is any x_i.

264. What is the relation between b_i, b_{i+1}?

265. What is the most obvious sequence with a set of fixed prime factors?

266. Explicitly find the orders of $3, -4, -12$. What does order $= 2q$ mean?

267. Find an ℓ such that $A^\ell - B$ is divisible by p^{v+1}.

268. Now that we know f is multiplicative, what do we do?

269. Now you just need the sum of quadratic residues mod p (why?)

270. Can m be a perfect power?

271. Show that if $p^M \mid T$ and $p^m \mid Q(n)$, then M is bounded.

272. For any $t \in \mathbb{Q}$, what's the leading term and coefficient of $P(x) + P(t - x)$?

273. Can you bound $f(2p)$?

274. Show $n_k = n_{k-1} + 1$

275. Show that $4k+1$ is expressible. To show $4k+3$ is expressible, you $8k+3$ is expressible. For $8k+7$, again make two cases.

276. For the second part, think $11(4a+5b-3c)$.

277. How many times can k appear in the three gcds? What about a smaller divisor of k?

278. Show that if k is odd, then $2^k + \cdots + 1$ has at least one prime divisor $p \equiv 3 \pmod 4$

279. Write $d = \gcd(xy+1, xy+x+2) = \gcd(x+1, y-1)$ so that $xy+1 = du^2, xy+x+2 = dv^2$.

280. Suppose 5^k is the smallest of all, and attained for $a_1^{2018} + a_2$. What does this assumption give?

281. If $a > b$, you should get $p \mid a$ but not b.

282. Use induction

283. You can assume $0 \le x, y \le \frac{p-1}{2}$. How many solutions does $x^2 + y^2 \equiv 1$ have?

284. In the remaining expression, what is $\frac{i^p+(p-i)^p}{p^2} \pmod p$?

285. Show $p \mid P(2^q)$ for all primes p. What does this mean?

286. Show $d(n^2+1) \le n$ for even n to conclude.

287. This can be seen as a quadratic in a. One solution is $(2,2,2,2)$.

288. Phrase it in terms of modular things.

289. Use induction to finish.

290. Take p to be the smallest prime factor of n.

291. Pick $n = 2p$ such that $2p > \ell$. In which cases does $2p$ not work? How do you handle these cases?

292. How would you define the polynomial $Q(n)$? What could be it's degree?

293. Show that $f(2^{2a-2}) = a2^{2a-2}$.

294. Suppose we add a restriction: f is continuous. What happens?

295. Pick a prime p. What's the simplest upper bound on $\nu_p\left(\binom{2n}{n}\right)$?

296. Vieta Jumping! But simplify the numerator first

297. When is $\frac{a}{b}, \frac{b}{a}$ is terminating for a pair of coprime integers a, b?

298. Suppose $p \mid a+b$. When can LTE work?

299. For $f(a+1), f(a+2), \ldots$ set up similar systems.

300. What's the best way to deal with the case $p = 3$?

301. $\gcd(a_i + j, a_j + i) = \gcd(a_i + i + a_j + j, a_j + i)$. Can you force $p \nmid (a_i + i) + (a_j + j)$ for all i, j by taking a suitable sequence?

302. By Heron's formula, $A = x\sqrt{3(x^2-1)}$. You want $\frac{x^2-1}{3}$ to be a square. Does this remind you of something?

303. Use LTE to show $5^k \mid a^{2018^{2018}} + 1$ is not possible.

304. Introduce $k = |m - n|$.

305. Instead of the sum of d, look at the sum of n/d.

306. Show $\gcd(2n + 4, 14n + 3) = 1$.

307. Can $||f(i)||$ be strictly decreasing?

308. Use $f(a + d) \equiv f(a) \pmod{d}$.

309. You get $\alpha^m + \alpha^{m+1} = \alpha(1 + \alpha) = \alpha^n$. What bound on n does this give you?

310. The identity should have a difference of squares.

311. Show $k \leq 2$ and deal with these cases.

312. Suppose n has two prime factors and write $n = p^\alpha m$, with p the smallest prime factor of n.

313. Consider a change of variables to $A, B \in \mathbb{Q}^+$ so that the problem becomes about the terms $A^n - B$ which are ALL divisible by p.

314. Let $p < q$ be the two smallest primes factors of n. Where could p, q be? What about $\frac{n}{p}, \frac{n}{q}$?

315. Let k be such that $2^k \leq n < 2^{k+1}$. Keep pairing up consecutive terms to get ν_2 of the numerator is $\nu_2(n!/2^k)$.

316. Set $n \equiv 0 \pmod{p - 1}$ and another congruence. Then use CRT to combine them.

317. To do this, first construct a k such that $\nu_p(A^k - 1) = v$. Then consider $A^{kr+y} - B$, and select r decisively.

318. Consider ν_2.

319. Prove $f(x) = c(x - 1)^r$. How do you bound r

320. If $p \mid q - 1$, try to find a suitable a such that $x^{-1} + 1 \equiv a \pmod{p}$ gives the result.

321. Write $f(x) = x + c$. Use Wilson's theorem to eliminate some values of c.

322. Show that $x, 2^{2^x} + 1$ are coprime.

323. You get the bound for large enough primes p. How do you "ignore" the small primes?

324. Use some estimates on $\varphi(n)$ to show this can't hold for infinitely many n.

325. Introduce the fractional part!

326. $a_1 + a_2 + \cdots + a_k \equiv a_2 + \cdots + a_k$, and the left side is k times a square while the right is $k - 1$ times a square. Is this possible for all k?

327. You want $a^b \equiv (-1)^a a^a \pmod{a+b}$. So set a to be odd. You then want $a^{b-a} \equiv 1 \pmod{a+b}$.

328. How many powers of 2 can you find in $n + 1, n + 2, \ldots, 2n + 1$?

329. Multiply 5 to the left and you get 5^n.

330. Pick $k = 1$.

331. If $q \mid (x + 1)^p - x^p$, what is $\text{ord}_q(x^{-1} + 1)$?

332. For $n = 3$, assume $a + b + c = 1$. Then normalize by writing $a = x/(x + y + z), \ldots$

333. To make use of the condition, expand $(wx_i + 1)^n \pmod p$ over all x_i.

334. It's a cyclic expression, so assume an ordering on $\nu_p(a), \nu_p(b), \nu_p(c)$.

335. What happens now if $p \mid n$?

336. Show that all the new terms are pairwise coprime.

337. First show that $\nu_p(a_n) - \nu_p(a_1) \le \mathbb{H}_{n-1}\nu_p(C)$, where $\mathbb{H}_n = 1 + 1/2 + \cdots + 1/n$.

338. We don't have a good formula for $\mathcal{S}_\ell$ if $\ell \ge 4$. How do we prove the formulas for $\mathcal{S}_2, \mathcal{S}_3$? Maybe try and use those methods

339. Use induction

340. What is the value of each summand?

341. Can $\deg f$ be greater than 1?

342. Instead of proving your expression is ≥ 0, prove that it is > -1. This gives you more freedom on estimates.

343. Assume $a \ge b \ge c$ and show $a \mid bc$.

344. Show in the original equation that each $0 < n - m < q$ gives a valid (n, m) pair.

345. Suppose you have a set of prime factors $S = \{p_1, \ldots, p_k\}$. To keep $\varphi(x) = \varphi(n)$ for a fixed n and many x, you want each prime factor of $\varphi(x)$ to be from S. How do you ensure this?

346. The cubic factorizes!

347. If $p = 2$ divides z, use LTE to show $\nu_2(n)$ is bounded.

348. Can you find a m such that $\nu_p(m) > \nu_p(n)$ and $\nu_p(a_m) > \nu_p(a_n)$.

349. You have $a^{k\varphi(b)+1} \equiv a \pmod b$. Are a, b coprime?

350. Group terms in the most natural way possible.

351. Write n in binary and do this.

352. If k is a prime, then why do you need to show 3 is a quadratic nonresidue?

353. To attach a new prime dividing $2^\ell - n$, we would want $\gcd(p, x) = 1$.

354. Observe that $g(g - 2) \equiv -(g - 1) \pmod p$.

355. Ensure all the 3 conditions of LTE

356. Let $s = \max_j \nu_p(a_j)$, and say $s = \nu_p(a_w)$. What can be the ν_p of the rest of the terms?

357. This is similar to Wolstenholme's theorem. Try Gaussian pairing.

358. Evaluate the small cases by hand. For the larger ones, consider mod 8.

359. Look at tuples of the form $(\nu_{p_1}(a_n), \ldots, \nu_{p_k}(a_n))$, so that we have to force two tuples to be equal (why?). Count the number of such tuples and use the bound on $\nu_p(a_n)$ from before.

360. In $p \mid P(n + pk)$, pick a k such that $p - 1 \mid n + k$. What do you get?

361. If $k = 2^\ell$, then what can you say about $\text{ord}_p(a \cdot b^{-1})$ where p is a prime?

362. If $n = 3^x p_1^{\alpha_1} \dots$, then you should get $d_1(n) = \prod_{p_i \equiv 1}(\alpha_i + 1) \left\lceil \frac{1}{2} \prod_{p_j \equiv 2}(\alpha_j + 1) \right\rceil$, where the indices are mod 3.

363. Show that $x \in \{1, 2\}$ using the fact that $x \mid 2012 = 2^2 \cdot 503$.

364. Show that $x_1, \dots, x_k$ must be prime.

365. To show a z exists, try an approach like in Example 2.12.1.

366. Fix n and induct on m.

367. Pick r to be the gcd of all t_i.

368. If $2^k - 1 \mid 2^n - 1$ with k odd, then it has a prime factor $p \equiv 3 \pmod 4$. What next?

369. Write $x + y = 3k, x - y = b$.

370. Create a polynomial to find expressions of the form $a + b + c, ab + bc + ca$.

371. Show that $p \mid a_{k+1}$ for our choice of k.

372. Consider $(2n)! + k$.

373. What's the best way to deal with the case $p \mid x$?

374. Try Vieta Jumping

375. What are the possible lengths of any segment? It would obviously be an integer, but can you explicitly say which values it can take?

376. Write $(n + 1)^\ell - 1$ as the telescoping sum of $(i + 1)^\ell - i^\ell$ as i goes from i to n. (this is how formulas for $\mathcal{S}_2, \mathcal{S}_3$ are derived)

377. Write $p + m - 1 = p^\alpha$ and use $p^\alpha + m - 1 \mid n$.

378. You should get $3^{n-1} + 5^{n-1} \mid 2 \cdot 3^{n-1}$. Why are we done?

379. Work mod some special number.

380. mod 10.

381. The right side is not multiplicative (why?). So what do we do?

382. Show that $f = \varphi * \text{id}$.

383. Consider $n = pq$ for two distinct odd primes p, q.

384. Show that that if $R(m^c), R(m)$ have the same prime divisors, then so do $R(m^{c-1})$ and $R(m)$.

385. Why must we have $p = 2$?

386. Derive a formula for $d_1(n)$.

387. Pick any prime $p \in \{2, \dots, 100\}$. Then what does $\frac{(n+1)^p - 1}{n}$ give by the telescoping method?

388. You get $2^{k+1}m^2 + 1 = (2^k + \dots + 1)\sigma(m)$. What happens if k is odd?

389. Guess the answer

390. What does $(i, j) = (2m, 2n)$ give?

391. Get a quadratic in x.

392. What can you add/subtract from $n^2 + km^2$ to get $k + 1$?

393. Use the result from Problem 8.4.2.

394. Characterize all n such $\mathcal{F}(n)$ has two consecutive elements

395. Product of $4x - a^2$ works.

396. Just do some bounding now.

397. Consider a number with all digits 1. Write $n = 10^{x_1} + \cdots + 10^{x_s}$. What can you choose the x_i to be such that this becomes divisible by s?

398. Guess the answer.

399. What's the ν_p condition for a rational number to be an integer?

400. How does this relate to polynomials?

401. If $p \mid (b + c)$, then $p \mid bc$. What does this give?

402. Use induction.

403. $m + 1 \mid m^m + 1$ if m is odd. Which odd number should you choose?

404. Rearrange the equation and make the key substitution: $x = a + c, y = c - a$, where $c^2 = a^2 + \lceil 4a^2/b \rceil$.

405. Consider a prime p dividing $f(k^2)$ with $0 < k < p/2$. Then $p - 2k \leq A$. What does this mean?

406. Compute small powers and observe how consecutive zeroes occur.

407. How do you deal with $1/i \pmod p$?

408. Let $\operatorname{lcm}(n_1, \ldots, n_k) = x$. What do you get?

409. What formula did we find in Example 3.5.9?

410. Why do you need to show $F = G * \mathbb{1}$?

411. If $ab = 7 \cdot 2^k$, then $a = 7 \cdot 2^t, b = 2^{k-t}$ or $a = 2^t, b = 7 \cdot 2^{k-t}$. Why does this help here?

412. Gaussian pairing.

413. How do we handle the condition that P, Q are coprime?

414. Show that both the sides are multiplicative

415. Try the same method as the $n \mid 2^n - 1$ problem.

416. If $x = 2^k - n$, then find a class of ℓ for which $x \mid 2^\ell - n$.

417. The answer is yes.

418. Why can you assume $\gcd(a_1, \ldots, a_n) = 1$?

419. How do you prove $p \mid 1 + 2 + \cdots + p$?

420. Prove $f(n) \mid n^{f(n)}$.

421. Take $m = 2n - 1$.

422. Use $n - i \mid Q(n) - Q(i) = Q(n) - q_i$ for $0 \le i \le d$.

423. Take $Q(x) = (2x^2 - 1)^2$ and carefully count the number of repeated residues.

424. Pick a prime factor p common to d, P. What does it give you?

425. For a given prime p, smartly pick a n such that $p \mid a^n + n$ and $p \mid b^n - a^n \implies p \mid b - a$.

426. How does this give $p^3 \mid f(p)$?

427. Show that there is a row with all elements atmost n/b.

428. If $S = \{a_1, \ldots, a_n\}$, then $\max a_i \ge n - 1 + \min a_j$.

429. Make the same substitution as in Problem 4.9.19, i.e. $u = (X + Y)/2, v = (X - Y)/2$.

430. Use induction.

431. The left side should become the sum of $a\left(\left\lfloor \frac{(a+1)^2}{p} \right\rfloor - \left\lfloor \frac{a^2}{p} \right\rfloor\right)$.

432. Take $(n, 2n), (2n, 3n), (3n, n)$ to get $n \mid 2a_n^2$.

433. Show that $\nu_p(a_j) < s$ for all $j \ne w$.

434. When can you use LTE?

435. Look at 3^α for some α.

436. Now $p \mid 2(p-3)! - 2(p-n)!$ holds for all large primes and a fixed $n \le -4$. Why is this not possible?

437. This basically means $cd + 1$ is coprime to n for all $0 \le c \le k - 1$. What is d in terms of n, k?

438. Use $f(n^2) = f(n)f(n-1)$ to show it can't be strictly increasing either.

439. You want $1 - t > \frac{x \mod y}{y} > t$. A hint to do this is to consider $f(x) = \frac{\frac{x-1}{2}}{x}$, which gets closer to $\frac{1}{2}$ as x increases.

440. What's the solution of the Pell's equation $x^2 - 3y^2 = 1$.

441. In this case show that $\left\lfloor \frac{n_k}{2^j} \right\rfloor = \left\lfloor \frac{n_k}{5^j} \right\rfloor$ for all j. Why is this not possible?

442. What do you do when you have 2 equal sets?

443. If $p > 2$ divides z, find an inequality using LTE which can't hold for infinitely many n

444. Consider the restriction: n is a prime. What happens here?

445. You should get $b^2 = (k-2)^2(4k+1)$ so $4k + 1$ is an odd square. Use this to get a complete family of solutions.

446. For a fixed constant a, how many j satisfy $a = \lfloor \sqrt{jp} \rfloor$?

447. Use an argument similar to $n \mid 2^n - 1 \implies n = 1$ to show $p \mid f(p+1)$ for all large primes

448. If p is a prime, what is $f(p)$?

449. You have a sequence β such that $n = \prod_p \prod_{i=0}^{\beta(p)-1} p^{2^i}$. What constraint do the β satisfy?

450. We would like to construct a prime p such that n is a quadratic nonresidue mod p. If $n = p_i$, then we can easily do this using quadratic reciprocity and Dirichlet's theorem. What about the general case?

451. Show that $2^{Q(n)} - 1 \mid 3^T - 1$ where $T = \gcd(P(n + zQ(n))$. We just need to show T is bounded by a constant now (why?)

452. Pick a prime divisor p of n. What do you know about $\text{ord}_p(2)$? Is there a special p you should pick?

453. Show $n \leq 4$ using "vieta Flipping". Do all $n \in \{1, 2, 3, 4\}$ work?

454. Define $||x||$ to be the largest prime factor of x. If the problem statement is not true, then show that $||f(i)||$ must be monotone eventually.

455. Find the answer for $2^a, 2^a \cdot 3^b, 2^a \cdot 3^b \cdot 5^c$.

456. Show that $\nu_p(a_n) \leq A \log n$ for some fixed constant A.

457. If m satisfies the property, then show that so does mq for any prime q.

458. If a_{2m} is odd, show a_{2t+1} is odd for all t.

459. Make $n + c$ a prime p.

460. Use some smart bounding to show $Q(n) = q_n$ for all n.

461. Use Theorem 3.3.1.

462. Divide $(M + i)$ by $\gcd(M + i, (n - 1)!)$. What happens?

463. Prove the result for $n = p^k$. What about the general case?

464. Show $m < 2n$ and finish.

465. Let $p_{k+1} - 1 = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Then consider $N = p_1^{\alpha_1+1} \dots p_k^{\alpha_k+1}$.

466. You should get -15 is a quadratic residue mod 481. Is this possible?

467. $p - 1 \in A$. So $p - 2 \notin A$. So $p - 3 \in A$. So $p - 4 \notin A$. Is this possible?

468. use $b + d + a - c$ divides $ac + bd$ to get a more useful result.

469. Add elements one by one.

470. Let q be a prime divisor of x. Then $\text{ord}_q(p - 1) \mid 2x, q - 1$. Is there a special choice for q?

471. Take $x_1 x_2 \dots x_n - 1 \mod 2^{y+1}$.

472. Try to alter the terms so that you remove almost all factors less than $n - 1$.

473. If $\nu_5(n_k) = 0$, then S is odd. So?

474. This gives $q \mid p(p - 2)$ if q is the smallest prime factor of x.

475. You want $x^2 + y^2 \equiv 1 \pmod p$ with $1 < x^2 + y^2 < (p - 2)p + 1$.

476. What can you deduce about $\text{ord}_p(5), \text{ord}_q(5)$?

477. For $k \leq 2$, what can be the prime factorization of n?

478. What is $a_i \pmod 5$ over all i?

479. You should get $c = (\bullet)/(y - x)$. What's the simplest way of making this an integer?

480. Why is this sufficient to imply that only finitely many such primes exist?

481. Factorize $f(t) = (a + b)^t - a^t - b^t$ for $t = 3, 5, 7$.

482. Show that $(a^2 + ab + b^2)^2 \mid f(p)$ for certain primes p.

483. Take $f(x) = x, -x$ alternatively in these intervals, and let $g(x) = 2f(x)$.

484. Write $(6, 2, 2, 2)$ as $(2, 6, 2, 2)$. Then you have a new quadratic, new root!

485. We want to force as many terms to be equal as possible. $x \equiv -y \implies x^2 \equiv y^2$ hence $Q(x) = x^2$ removes half the pairs, but we need to remove more and so need $Q(a) = Q(b)$ to give more constraints. What degree should we choose?

486. We want $k = \prod \frac{2\alpha_i+1}{\alpha_i+1}$. Here, show all α_i are even and guess the answer.

487. Suppose you have a set of k terms from the sequence that are all pairwise relatively prime. Can you construct a new term?

488. Let p be the smallest prime not in the list.

Solutions to Selected Problems

Solution 1.4.2

Firstly, since p, q are odd, hence $p+q$ is even, so $2 \mid p+q$. Thus, $(p+q)/2$ is an integer. To show $p+q$ has at least three prime factors, we must show $(p+q)/2$ is not a prime. But

$$p < \frac{p+q}{2} < q.$$

By hypothesis, p, q are consecutive primes. Hence $(p+q)/2$, an integer between them, cannot be a prime! $\square$

Comment: Looking at examples for the first few primes, it might be tempting to show something like one of 3 or 5 always divides $p+q$. However, that approach fails. If thought logically, showing something like $3 \mid p+q$ almost always happens would be saying that their is a nice pattern that consecutive primes follow. However, we know how random they are, so our intuition should be enough to tell us that this approach cannot fail.

Solution 1.12.8 (Russia 2001 Grade 11 Day 2/2)

Let $d = \gcd(a, b)$ and write $a = dk, b = d\ell$, with $\gcd(k, \ell) = 1$. Then

$$d^2(k^2 + k\ell + \ell^2) \mid d^3 k\ell(k+\ell) \Leftrightarrow k^2 + k\ell + \ell^2 \mid dk\ell(k+\ell).$$

However, $\gcd(k, k^2 + k\ell + \ell^2) = \gcd(\ell, k^2 + k\ell + \ell^2) = 1$, and even $\gcd(k+\ell, k^2 + k\ell + \ell^2) = \gcd(k+\ell, k\ell) = 1$. Thus, $k^2 + k\ell + \ell^2 \mid d$. Hence $d \geq k^2 + k\ell + \ell^2$.

Thus,

$$\begin{aligned} |a-b|^3 &= d^2 \cdot d \cdot |k-\ell|^3 \\ &\geq d^2 \cdot (k^2 + k\ell + \ell^2) \cdot 1^3 \\ &= a^2 + ab + b^2 > ab. \end{aligned}$$

Hence, $|a-b| > \sqrt[3]{ab}$, which is the desired bound. $\square$

Solution 1.12.15 (INMO 2019/3)

Let $k = |m - n|$. We have to then prove

$$\gcd(m, k) + \gcd(m + 1, k) + \gcd(m + 2, k) \leq 2k + 1.$$

Clearly $k = 1$ works, and $k = 2$ works if m is even. Suppose $k > 2$ now.

Observe that k can appear at most once in the above three gcds. So,

$$\gcd(m, k) + \gcd(m + 1, k) + \gcd(m + 2, k) \leq k + \frac{k}{2} + \frac{k}{2} < 2k + 1.$$

Hence, the only equality cases are when m, n are consecutive, or differ by 2 and both are even.

Solution 1.12.16 (USAMO 2007/1)

Define $b_k = \frac{a_1+a_2+\cdots+a_k}{k}$. We know $b_k \in \mathbb{N}$ for all k by the hypothesis. They key observation is

$$b_{i+1} = \frac{a_1 + a_2 + \cdots + a_{i+1}}{i + 1} < \frac{a_1 + a_2 + \cdots + a_i + i}{i} = b_i + 1.$$

as $0 \leq a_{i+1} \leq i$. So, $b_{i+1} \leq b_i$ for all i, and hence $\{b_i\}$ is a non-increasing sequence. However, it is always positive and hence lower bounded, so it will eventually become constant. This is the key idea.

So, eventually $a_1 + a_2 + \cdots + a_n$ forms an arithmetic progression for large enough $n \geq i$, and hence the differences $a_{i+1}, a_{i+2}, \ldots$ are all equal. This is what we wanted to prove. □

Solution 1.12.17 (USAMO 2007/5)

The proof goes by induction on n, the base case $n = 1$ being clear. Now we have the following identity that can be proven by direct expansion:

$$\frac{x^7 + 1}{x + 1} = (x + 1)^6 - 7x(x^2 + x + 1)^2$$

So put $x = 7^{7^n}$ and note that the right side is a difference of squares, hence not a prime. Thus, $7^{7^{n+1}}$ has at least 2 primes factors more than $7^{7^n} + 1$, and this completed the induction.

Comment 9.6.1: This was inspired by the following identity:

$$(a + b)^7 - a^7 - b^7 = 7ab(a + b)(a^2 + ab + b^2)^2.$$

Some similar useful identities are

$$(a + b)^3 - a^3 - b^3 = 3ab$$
$$(a + b)^5 - a^5 - b^5 = 5ab(a + b)(a^2 + ab + b^2).$$

Solution 1.12.18 (ELMO 2017/1)

As the power of each term in both RHS and LHS is n, we can assume $\gcd(a_1, a_2, \ldots, a_n) = 1$ so we need to show

$$\gcd(a_1^n + P, a_2^n + P, \ldots, a_n^n + P) \leq 2.$$

Let $d = \gcd(a_1^n + P, a_2^n + P, \ldots, a_n^n + P)$, assume $d \neq 1, 2$ otherwise we are done. Consider a p, a prime factor of d. This means $p \mid a_i^n + P$ for all i. If for some i, $p \mid a_i$, then $p \mid P$, so $p \mid a_1^n, a_2^n, \ldots a_n^n$ or $p \mid a_1, a_2, \ldots, a_n$ which is false as $\gcd(a_1, \ldots, a_n) = 1$. This means $\gcd(d, P) = 1$. Finally we have, $d \mid a_i^n + P$, so let $a_i^n = dk_i - P$ for some integer k_i. Multiplying this over all i, we get

$$P^n = a_1^n a_2^n \ldots a_n^n = (dk_1 - P)(dk_2 - P) \ldots (dk_n - P).$$

If we multiply out each term on RHS, except $(-1)^n P^n = -P^n$ (as n is odd), all terms are divisible by d and on LHS P^n remains. Therefore $d \mid 2P^n$ but $\gcd(d, P) = 1$, so $d \mid 2$ and we are done. □

Solution 1.12.19 (IMO 2001/6)

The key claim is the following:

Claim. *We have $ac + bd \mid (ab + cd)(ad + bc)$.*

There are many ways to prove this. But before that, let's see how this finishes the problem. Now, $a > b > c > d$ implies $ab + cd > ac + bd > ad + bc$ (by the rearrangement inequality, or simply by expanding $(a - d)(b - c) > 0$ and $(a - b)(c - d) > 0$). So, if $ab + cd$ is a prime, then $ab + cd$ would be coprime to $ac + bd$. Hence $ac + bd \mid ad + bc$ which implies $ac + bd \leq ad + bc$, contradicting what we found earlier. Hence we are done. □

Now let's see how to prove the claim. The proof we give is just clever algebraic manipulations:

Proof. Firstly,

$$b + d + a - c \mid (ac + bd) + a(b + d + a - c) = (a + b)(a + d).$$

Similarly,

$$b + d - a + c \mid (ac + bd) + c(b + d - a + c) = (c + b)(c + d).$$

So,

$$\begin{aligned}&(b + d + a - c)(b + d - a + c) \mid (a + b)(a + d)(c + b)(c + d)\\ \Leftrightarrow\ &ac + bd \mid ((ac + bd) + (ad + bc))\,((ac + bd) + (ab + dc))\end{aligned}$$

This gives $ac + bd \mid (ab + cd)(ad + bc)$, which is what was desired. □

Comment: Expand and simplify the given condition to

$$a^2 - ac + c^2 = b^2 + bd + d^2.$$

So, by the cosine law, there exists a quadrilateral $ABCD$ with $AB = a, BC = c, CD = b, DA = d$ such that $\angle ABC = 60^\circ$ and $\angle CDA = 120^\circ$. Since $60^\circ + 120^\circ = 180^\circ$, hence $ABCD$ is cyclic. Now, using Ptolemy's theorem, there exists an expression for AC^2 just in terms of a, b, c, d. If you remember it, great! otherwise we can derive it now. Write $\alpha = 60^\circ$. Then

$$a^2 + c^2 - 2ac\cos\alpha = b^2 + d^2 + 2bd\cos\alpha \implies 2\cos\alpha = \frac{a^2 + c^2 - b^2 - d^2}{ac + bd}.$$

Hence,

$$AC^2 = a^2 + c^2 - 2ac \cdot \frac{a^2 + c^2 - b^2 - d^2}{ac + bd} = \frac{(ab + cd)(ad + bc)}{ac + bd}.$$

So $ac + bd \mid (ab + cd)(ad + bc)$, and this is a new proof of the claim!

In fact, we can remove the geometry from the above problem completely by working $1 = 2 \cdot \frac{1}{2}$ instead of $2\cos\alpha$[a] So,

$$a^2 + c^2 - ac = b^2 + d^2 + bd \implies a^2 + c^2 - b^2 - d^2 = ac + bd.$$

So,

$$(ac+bd)(a^2+c^2-ac) = (ac+bd)(a^2+c^2) - ac(a^2+c^2-b^2-d^2) = (ab+cd)(ad+bc).$$

This can be thought of as a "third proof" of the claim. It would generally be written as a "clever algebraic manipulation", however a geometric interpretation makes it very easy to discover.

[a] Constants are harder to note since they are just sitting there. Variables, on the other hand, are much easier to work with since you can see them in action. This is one of the weird moments when a general version is easier to deal with than the normal one.

Solution 2.14.11 (Sierpiński)

Let $n = 2^\alpha 5^\beta \gamma$, where γ is coprime to 10. Consider the number

$$n = 10^{\alpha+\beta}(10^{s\varphi(\gamma)} + \cdots + 10^{\varphi(\gamma)}).$$

Clearly, the sum of digits of n is s. Further, $2^\alpha 5^\beta \mid n$ and by Euler's Theorem,

$$10^{s\varphi(\gamma)} + \cdots + 10^{\varphi(\gamma)} \equiv \underbrace{1 + 1 + \cdots + 1}_{s} = s \equiv 0 \pmod{\gamma}.$$

Hence, $s \mid n$ and our construction works.

Solution 2.14.13 (USAMO 2018/4)

The key observation is the following:

Claim. *For any $i < j$, there is exactly one value of k for which $a_i + ki \equiv a_j + kj \pmod p$.*

Proof. Just observe that the two being congruent is the same as $k \equiv (a_i - a_j) \cdot (j-i)^{-1} \pmod p$, which is a unique number only depending on i, j. □

Now, make a table whose kth row is elements of the form $a_i + ki$. For each row, join two elements by a line if they are congruent modulo p. [5] Now, a pair (a_i, a_j) for some i, j is connected only in one row in the entire table by the claim. Hence, the total number of lines in the table is the number of pairs, which is $\binom{p}{2}$.

Further, there are p rows. Hence one rows contains at most $\frac{1}{p}\binom{p}{2} = \frac{1}{2}(p-1)$ lines. Hence, at most $(p-1)/2$ pairs are congruent, meaning that we have at least $\frac{1}{2}(p+1)$ remainders, as desired. □

Solution 2.14.15 (Iran 2017 Round 3/1)

The idea is to use Bézout's theorem. We find integers a, b such that $am + bn = 1$. So

$$x \equiv x^{am+bn} = x^{am}x^{bn} \equiv \left(y^a x^b\right)^n \pmod p.$$

Similarly,

$$y \equiv y^{am+bn} = y^{am}y^{bn} \equiv \left(y^a x^b\right)^m \pmod p.$$

Hence $z = y^a x^b$ works.

To prove uniqueness, assume on the contrary that z_1, z_2 exist that satisfy the given conditions. So $z_1^n \equiv z_1^n \equiv a \pmod p$ and $z_1^m \equiv z_2^m \equiv b \pmod p$. So, if $z = z_1 \cdot z_2^{-1}$, then $z^m \equiv 1 \equiv z^n \pmod p$. However, by Example 2.12.1, we find $z \equiv z^{\gcd(m,n)} \equiv 1 \pmod p$, giving $z_1 \equiv z_2$, a contradiction. □

Solution 2.14.16 (IMO Shortlist 2015 N3)

Observe that $x_k - 1 = \frac{m-n}{n+k}$. Hence, $m-n$ is divisible by all $n+1, n+2, \ldots, 2n+1$, hence divisible by their LCM. Write $\operatorname{lcm}(n+1, n+2, \ldots, 2n+1) = L$ and $m - n = L\gamma$. Now, assume the result is not true. So there exists $k \in \mathbb{N}$ such that

$$\left(\frac{L\gamma}{n+1}+1\right)\left(\frac{L\gamma}{n+2}+1\right)\ldots\left(\frac{L\gamma}{2n+1}+1\right) - 1 = 2^k.$$

Now the key observation is that there is exactly one power of 2 in $n+1, n+2, \ldots, 2n+1$ since $2n+1 = 2(n+1)-1$. Suppose this is 2^w. Clearly, the highest power of 2 in L's prime factorization is also w.

[5] Alternatively, make a graph $\mathcal{G}_k$ whose vertices are a_ℓ and two elements a_i, a_j are joined if $a_i + ki \equiv a_j + kj \pmod p$.

So now $\frac{L\gamma}{n+i}$ is odd if and only if $n+i=2^w$. Also, if the power of 2 in γ is y, then $2^y < \frac{L\gamma}{n+i} < 2^k$ and so $k \geq y+1$. So, $\frac{L\gamma}{n+i} \equiv 0 \pmod{2^{y+1}}$ unless $n+i=2^w$, in which case this remainder is 2^z. Hence

$$\begin{aligned} 0 &\equiv \left(\frac{L\gamma}{n+1}+1\right)\left(\frac{L\gamma}{n+2}+1\right)\ldots\left(\frac{L\gamma}{2n+1}+1\right)-1 \\ &\equiv 1\cdot 1\ldots 1\cdot(2^y+1)-1 \\ &\equiv 2^y \pmod{2^{y+1}} \end{aligned}$$

which is a contradiction. □

Solution 2.14.17 (ELMO 2019/5)

They key claim is the following:

Claim. *Let p be a prime. Let $\mathcal{S}_p$ denote the the set $\mathcal{S}$ whose elements are reduced modulo p. Then if $0 \notin \mathcal{S}_p$, then $|\mathcal{S}_p| = 1$.*

Proof. Assume $\mathcal{S}_p = \{x_1, \ldots, x_n\}$ and $0 \notin \mathcal{S}_p$, so that $n < p$. Pick any $a \in \mathcal{S}_p$, and observe that all elements of $\{ax_1+1, \ldots, ax_n+1\}$ are distinct modulo p. However, all these are in $\mathcal{S}$, and this set has n elements too. Hence, we must have

$$\mathcal{S}_p = \{ax_1+1, ax_2+1, \ldots, ax_n+1\}.$$

Summing up the elements yields

$$x_1+\cdots+x_n \equiv a(x_1+\cdots+x_n)+n \Leftrightarrow (a-1)(x_1+\cdots+x_n) \equiv -n \pmod{p}.$$

Since $n<p$, hence $p \nmid n$ meaning that $x_1+\cdots+x_n \not\equiv 0 \pmod{p}$. Now the above holds for *all* $a \in \mathcal{S}_p$, which is impossible since $a \equiv -n\cdot(x_1+\cdots+x_n)^{-1} \pmod{p}$ is unique. Hence, we must have $n=1$, as desired. □

So if p divides no element of $\mathcal{S}$, then all elements in $\mathcal{S}$ are congruent to s, where s is some element of $\mathcal{S}$. However, $s^2+1 \in \mathcal{S}$ implies $s^2+1 \equiv s \pmod{p}$, i.e. $p \mid s^2-s+1$.

Since s can be fixed (choose any one element of $\mathcal{S}$), hence s^2-s+1 is finite implying it has a finite number of prime factors. Hence, the number of primes p not dividing any element of $\mathcal{S}$ is finite too, and we are done.

Solution 3.7.12 (IMO Shortlist 2016 C2)

The answer is $n=1$. Suppose there are a rows and b columns. If $b=1$, then clearly we must have $n=1$ so say $a \geq b > 1$ now. The key idea is that the common row, column sums are $> n$ because n would be an element in some cell.

There are at most $b-1$ divisors of n that are greater than $\frac{n}{b}$, since divisors come in pairs $(k, n/k)$. However, $a > b-1$ and so there would be a row in which all divisors are at most $\frac{n}{b}$. But then the sum here becomes at most $b\cdot\frac{n}{b}=n$, contradicting our previous observation.

Comment 9.6.2 (Outline of a more Number Theoretic Approach): The above was, in heart, a combinatorial solution. However, we can use number-theoretic estimates too.

Solution 3.7.13 (St. Petersburg Mathematical Olympiad 1998)

Assume that it is monotonic for all $n \geq N$. Then

$$d((n+1)^2+1) \geq d(n^2+1)+2$$

because $d(x)$ is even if x is not a square. (We would normally have a $+1$, but here a simple observation helped us to change it to a $+2$. However, as we will see, the entire solution that follows hinges on this factor of 2.)

So we get for any $m \geq N$,

$$d(m^2+1) \geq d(N^2+1)+2(m-N).$$

For large enough m, we find $2(m-N) > m$. Hence $d(m^2+1) > m$ for all large enough m. We now show this isn't true for even m.

Half of the factors of m^2+1 are less than $\left\lfloor \sqrt{m^2+1} \right\rfloor = m$ (because divisors come in pairs $(k, n/k)$). Further if m is even, then no even number can be a divisor of m^2+1. So there are at most $2(m/2) = m$ divisors, which means $d(m^2+1) \leq m$ for all even m. This, however, contradicts what we had earlier. $\square$

Solution 3.7.16 (IMO Shortlist 2011 N1)

If $n = \prod_p p^{\alpha(p)}$, then $d(n) = 2^k$ if and only if we have a sequence β such that for each prime p, $\alpha(p) = 2^{\beta(p)} - 1 = 2^0 + 2^1 + \cdots + 2^{\beta(p)-1}$, and $\sum_p \beta(p) = k$. Hence, any such number n satisfies $d(n) = 2^k$ if and only if

$$n = \prod_p \prod_{i=0}^{\beta(p)-1} p^{2^i}, \quad k = \sum_p \beta(p).$$

Let $\mathcal{S}$ be the set of integers of the form p^{2^i} as p varies over primes. Then $d(n) = 2^k$ when n is the product of the elements of a finite subset $\mathcal{T} \subset \mathcal{S}$. Here, $\mathcal{T}$ has k terms and if any $t \in \mathcal{T}$, then every divisor $s \in \mathcal{S}$ of t is also in $\mathcal{T}$.

Note that the set $\mathcal{T}_k$ consisting of the smallest k elements from $\mathcal{S}$ satisfies the condition above. Further, given k, the smallest n with $d(n) = 2^k$ is the product of the elements of $\mathcal{T}_k$. This n is in fact $f(2^k)$. Also, we clearly have $\mathcal{T}_k \subset \mathcal{T}_{k+1}$, which proves the desired result.

Solution 3.7.17 (ELMO 2017/4)

Consider $a < n$ such that $\gcd(a, b) = 1$, or equivalently $\gcd(a, n) = 1$. Then one of a, b has no prime factors apart from $2, 5$, wlog say a.

Thus, for all large n and any pair $(a, b) \in \mathbb{N}^2$ with $a+b = n$ such that we have $\gcd(a, n) = \gcd(b, n) = 1$, we have $a = 2^k 5^l$ or $b = 2^k 5^l$ for some $k, l \in \mathbb{N}$. The number of such pairs for a fixed n is $\varphi(n)/2$. Also, since $a = 2^k 5^l < n$, the number of such pairs would be at most $(\log_2(n) + 1)(\log_5(n) + 1)$. Hence, we get for large n,

$$(\log_2(n) + 1)\,(\log_5(n) + 1) \geq \frac{\varphi(n)}{2}.$$

Since $n > 2$, hence the left side is at most

$$(2\log_2 n)(4\log_5 n) = \frac{8}{\log 2 \log 5} \cdot (\log n)^2 = c(\log n)^2$$

for a constant c (basically $\mathcal{O}((\log n)^2)$). However, we know $\varphi(n) \geq n - \sqrt{n}$. Now linear growth is faster than logarithmic growth, hence $c(\log n)^2 < n - \sqrt{n}$ for large enough n, and we have our contradiction. $\square$

Solution 3.7.19 (IMO Shortlist 2016 N2)

We claim the answer is 2 and all composite numbers. We prove that these work and are the only possibilities. Let p_i denote primes that are $1 \pmod 3$ and q_j the ones that are $\equiv 2 \pmod 3$. We first find a formula for $d_1(n)$.

Claim. *Let $n = 3^x p_1^{\alpha_1} \dots p_s^{\alpha_s} q_1^{\beta_1} \dots q_r^{\beta_r}$. Then*

$$d_1(n) = \prod_{i=1}^{s} (\alpha_i + 1) \left\lceil \frac{1}{2} \prod_{j=1}^{r} (\beta_j + 1) \right\rceil.$$

Proof. Since we want divisors that are $\equiv 1 \pmod 3$, hence we don't want any factor from 3. Further, we can arbitrarily choose prime factos from $\{p_i\}$, however we must have an even number of factors from $\{q_j\}$.

If $\prod(\beta_j + 1)$ is even, then at least one terms, say $(\beta_1 + 1)$, is even. Then except for q_1, we can arbitrarily choose primes from $\{q_i\}$. Then the parity of β_1 is uniquely determined by them, so there are $\frac{1}{2}(\beta_1 + 1)$ choices.

If all $\beta_j + 1$ are odd, then the idea is the same, but slightly more technical. There are $\left\lceil \frac{\beta_i+1}{2} \right\rceil$ choices for an even $\beta_i + 1$, and $\left\lfloor \frac{\beta_i+1}{2} \right\rfloor$ for an odd $\beta_i + 1$. So we can induct now, the inductive step being:

$$\left\lceil \prod_{j=1}^{r-1} (\beta_j + 1) \right\rceil \cdot \left\lceil \frac{\beta_r + 1}{2} \right\rceil + \left\lfloor \prod_{j=1}^{r-1} (\beta_j + 1) \right\rfloor \cdot \left\lfloor \frac{\beta_r + 1}{2} \right\rfloor = \left\lceil \frac{1}{2} \prod_{j=1}^{r} (\beta_j + 1) \right\rceil.$$

So the claim has been proven. $\square$

Now let $n = 3^x 2^y 5^z p_1^{\alpha_1} \dots p_s^{\alpha_k} q_1^{\beta_1} \dots q_r^{\beta_r}$. Then let $c = (y+2)(z+2)\prod(\beta_j+1)$. Then

$$\frac{d(10n)}{d_1(10n)} = \frac{(x+1)c}{\lceil c/2 \rceil}.$$

So if c is even, then the above becomes $2(x+1)$. Here, x can be any non-negative integer. Hence, all even numbers can be expressed in this way.

If c is odd, then y, z are odd too, and each β_j is even. hence the above ratio becomes

$$\frac{d(10n)}{d_1(10n)} = \frac{2(x+1)c}{c+1}.$$

This is an integer, so $c+1 \mid 2(x+1)$ as $\gcd(c, c+1) = 1$. Write $2(x+1) = k(c+1)$. So the above equals

$$kc = k(y+2)(z+2)\prod_{j=1}^{r}(\beta_j+1).$$

As y, z are odd, hence $y+2, z+2 \geq 3$. In particular, this shows the number is composite.

We now show every odd composite number ab with $a, b \geq 3$ is indeed possible (the smallest odd composite number is $3 \times 3 = 9$). Take $n = 3^{\frac{ab-1}{2}} 2^{a-2} 5^{b-2}$. Then $c = ab$ and so

$$\frac{d(10n)}{d_1(10n)} = \frac{2\left(\frac{ab-1}{2}+1\right)ab}{ab+1} = ab.$$

Hence, we are done.

Solution 3.7.20 (China Mathematical Olympiad 2017/5)

We claim that no n is possible. Let $A = \{a_1, \dots, a_k\}$. The solution can be broken into a bunch of steps:

Claim. *n cannot be a prime power.*

Proof. If $n = p^k$, then its divisors are $1, p, p^2, \dots, p^k$. However, there is no subset with ≥ 3 elements which forms arithmetic progression. □

Let $p < q$ be the smallest prime factors of n.

Claim. $n \in G$.

Proof. If $n \in A$, then any other element in A is at most $\frac{n}{2}$. But then the common difference becomes $\geq n - \frac{n}{2} = \frac{n}{2}$, and so A cannot have more than 2 elements. □

Claim. *At most 1 of $1, p, q$ are in G.*

Proof. Clearly p, q cannot both be in G since $\frac{q}{p} \notin \mathbb{Z}$. Further, if $\{1, p\}$ or $\{1, q\}$ are in G, then $n \in G$ implies n must be a prime power, which is impossible. □

This claim implies $a_2 - a_1 \geq p - 1$.

Claim. *At most one of* $\frac{n}{p}, \frac{n}{q}$ *is in* G.

Proof. This is because $\frac{n/q}{n/p} \notin \mathbb{Z}$. □

This claim shows $a_k - a_{k-1} \geq \frac{n}{q(q+1)}$. However since $a_2 - a_1 = a_k - a_{k-1}$, hence we get $p - 1 \geq \frac{n}{q(q+1)}$, which shows

$$n \leq q(pq + p - q + 1) < q^3.$$

Since n has at least 6 divisors, hence $n \in \{p^2q, pq^2, pqr\}$ (keeping in mind that q is the second smallest divisor of q). A simple case work along with our claims from above suffice to show that neither is possible, and we are done. □

Solution 3.7.21 (China 2015 TST 3/6)

Firstly observe that $n = 6$ works. We will inductively find an increasing sequence of working integers. They claim is the following:

Claim. *If* p *is a prime, then* $f(p) = d(p!)/2$ *and*

$$f(2p) > \frac{d((2p-1)!)}{2}.$$

Proof. The former is clear. For the latter, let S denote the set of divisors of $\frac{(2p-1)!}{p}$, and let $|S| = k$. Then, any divisor of $(2p-1)!$ would be either in S or pS, so $d((2p-1)!) = 2k$. Further, any number in S, pS, p^2S would be a divisor of $(2p)!$. So $d((2p)!) \geq 3k$. Hence

$$f(2p) = d((2p)!) - d((2p-1)!) \geq k = \frac{d((2p-1)!}{2},$$

as claimed. □

Now suppose $n = \ell$ works. Let p be a prime such that $2p > \ell$. Then if $n = 2p$ works, we are done. Otherwise there is a number $x < 2p$ with $f(x) \geq f(2p)$. Here x cannot be a prime since then $f(x) = \frac{d(x!)}{2} < \frac{(2p-1)!}{2} < f(2p)$. Hence x is composite. But then pick the smallest such composite number less than $2p$ and it works. □

Comment 9.6.3: In fact, $n = 2p$ always works.

Solution 4.9.9

We claim that the solutions are $(a, b) = (k, 1), (l, 11)$, where k is any integer and l is any integer such that $11|l \pm 1$. These work, and now we will show that these are the only solutions.

Firstly assume $b > 1$, and say that $P(n-1), P(n), P(n+1) \in \mathbb{Z}$. Then

$$P(n+1) + P(n-1) - 2P(n) \in \mathbb{Z} \implies b | 20n^3 + 10n \tag{9.2}$$
$$P(n+1) - P(n-1) \in \mathbb{Z} \implies b | 10n^4 + 20n^2 + 2 \tag{9.3}$$

Hence, $b|2(10n^4+20n^2+2) - n(20n^3+10n) = 30n^2+4$ and $b|2n(30n^2+4) - 3(20n^3+10n) = -22n$. Thus, $b|22n$, which we will refer to as (3).

Claim. *If $p|b$, then $p = 11$. Further, $v_{11}(b) \leq 1$*

Proof. If $p = 2$, then $2|n^5 + a$ and $2|(n+1)^5 + a$ which implies $2|(n+1)^5 - n^5$, which is not possible.

Next assume $p > 2$. Then we must have $p \nmid 2n$, otherwise $(2) \implies p|2$, absurd. So $p \nmid 2n, p|22n \implies p = 11$ Now $11 \nmid 2n \implies 11 \nmid n$ and so $v_{11}(b) \leq v_{11}(22n) = 1$, and the claim has been proven □

Thus, $b = 11$ as $b > 1$ by our assumption. Now we have proven that $11 \nmid n$ and so $(1) \implies 11|2n^2 + 1$. Thus $n^2 \equiv 5 \Leftrightarrow n \in \{4, 7\} \pmod{11}$. Now since $(4-1)^5 \equiv 4^5 \equiv (4+1)^5 \equiv 1 \pmod{11}$ as well as $(7-1)^5 \equiv 7^5 \equiv (7+1)^5 \equiv -1 \pmod{11}$, hence the solutions are indeed the claimed ones. □

Solution 4.9.12

One solution is $(2, 2, 2, 2)$. Now consider the quadratic $x^2 - bcdx + b^2 + c^2 + d^2 = 0$ with $b = c = d = 2$. One root is 2, and the other is 6. So $(6, 2, 2, 2)$ is also a solution. Permute this to $(2, 6, 2, 2)$ now, and consider the same quadratic with $(b, c, d) = (6, 2, 2)$ this time, and keep proceeding.

For instance you get the following solutions in this way:

$$(2, 2, 2, 2) \to (6, 2, 2, 2) \to (22, 6, 2, 2) \to (262, 22, 6, 2) \to (34852, 262, 22, 6) \to \dots$$

In fact we can just keep swapping a, b keeping $c = d = 2$ constant throughout.

Solution 4.9.17 (IMO Shortlist 2008 N1)

If two of a, b, c are equal, then it is easy to see that all must be equal. So assume all are pairwise distinct. Now we get relations of the form $a^n - b^n = -p(b - c)$. Multiplying them gives our key identity

$$\frac{a^n - b^n}{a - b} \cdot \frac{b^n - c^n}{b - c} \cdot \frac{c^n - a^n}{c - a} = -p^3. \tag{9.4}$$

Now suppose that $p > 2$. We show that, in fact, being prime is too strong a condition, the following more general claim is also true:

Claim. *Equation 9.4 cannot hold for any odd integer p.*

Proof. We make two crucial observations: the first is that if n is odd, then $x^n - y^n, x - y$ have the sign, and hence the left side becomes positive. So n is even. The second observation is that

$$\frac{x^n - y^n}{x - y} = x^{n-1} + x^{n-2}y + \cdots + y^{n-1} \equiv x^{n-1} \equiv 0 \pmod 2$$

if $x \equiv y \pmod 2$. In our case, the pigeonhole principle gives shows that two elements in $\{a, b, c\}$ have the same parity, giving the desired contradiction since $-p^3$ is odd. Hence the claim has been proven. □

Now suppose $p = 2$. Then Equation 9.4 shows that a, b, c have the same parity, otherwise an odd number would divide -2^3. As before, we can show that n is even, say $n = 2k$. Write Equation 9.4 as

$$\frac{a^k + b^k}{2} \cdot \frac{a^k - b^k}{a - b} \cdot \frac{b^k + c^k}{2} \cdot \frac{b^k - c^k}{b - c} \cdot \frac{c^k + a^k}{2} \cdot \frac{c^k - a^k}{c - a} = -1.$$

Hence each term is ± 1. But then $a^k + b^k = \pm 1$. If k is even, then this means $|a| = 1 = |b|$. But then $a^k - b^k = 0$, contradicting the identity above.

If k is odd, then $a + b \mid a^k + b^k = \pm 2$. since a, b have the same parity, hence $a + b = \pm 2$. Similarly $b + c, c + a = \pm 2$. But then two of these have the sign, which is impossible since these are distinct integers. Hence we have exhausted all the possibilities.

Solution 4.9.18 (IMO Shortlist 2017 N6)

We claim the answer is $n = 3$. Firstly, $n = 1$ is clearly not possible. So suppose there exist infinitely many solutions for $n = 2$. Suppose $a + b = x$ and $\frac{1}{a} + \frac{1}{b} = y$ where $x, y \in \mathbb{Z}$. Write $a = p/q$ with p, q coprime. Then

$$y = \frac{1}{a} + \frac{1}{x - a} = \frac{x}{a(x - a)} = \frac{q^2 x}{p(xq - p)}.$$

So $p \mid x$. Write $x = pk$. Then

$$y = \frac{q^2 pk}{p(pqk - p)} = \frac{q^2 k}{p(qk - 1)}.$$

Now, clearly $\gcd(qk - 1, q^2 k) = 1$, hence we must have $qk - 1 = 1$, i.e. $qk = 2$. If $q = 1$, then a is an integer and $x = 2a$, meaning $b = a$. But then $ab \mid a + b$ and so $a = b = 1$ or 2. If $q = 2$ and $k = 1$, which means $x = p$ and $a = p/2$. But then $p \mid 4$ and so $a = b = \frac{1}{2}$. So we only have finitely many possibilities.

Now we show the result for $n = 3$. Here, we take

$$\left(\frac{1}{1 + x + y}, \frac{x}{1 + x + y}, \frac{y}{1 + x + y} \right)$$

where x, y are positive integers. Then we just want

$$\frac{x + 1}{y} + \frac{y + 1}{x} \in \mathbb{Z}$$

for infinitely many $(x, y) \in \mathbb{N}^2$. Let's see how we do this. Suppose the above is k for some k.

Suppose for some k we have a solution (x, y) with $x \leq y$. We thus get the equation $x^2 - (ky - 1)x + y^2 + y = 0$, and now employ vieta jumping. Let the other root be x_0. Then $xx_0 = y^2 + y > 0$ and $x_0 = ky - 1 - x \in \mathbb{Z}$. Hence, $x_0 \in \mathbb{N}$. So we jump

$$(x, y) \mapsto \left(\frac{y^2 + y}{x}, y\right).$$

Now, if can show $x_0 > y$, then we have found a larger pair, and we can keep on proceeding forever. But this is clear since

$$\frac{y^2 + y}{x} \geq \frac{y^2 + y}{y} = y + 1 > y.$$

So we went $(x, y) \mapsto (x_0, y)$ where $x \leq y < x_0$. Now we need to pick a suitable k such that we have a valid solution at the start. if $k = 4$, then $(x, y) = (1, 1)$ works and we get

$$(1, 1) \to (2, 1) \to (2, 6) \to (21, 6) \to (21, 77) \to \ldots.$$

Solution 4.9.19 (IMO Shortlist 2019 N8)

Assume on the contrary. Then there exists an $0 \leq f < b$ such that the equation becomes

$$a^2 + \frac{4a^2 + f}{b} = c^2$$

for some c. Clearly, $c > a (> 0)$. This rearranges to

$$(b + 4)a^2 - bc^2 = -f.$$

So the above becomes $b(a - c)(a + c) + 4a^2 = -f$. So if we write $x = a + c$ and $y = c - a$, then the above becomes

$$-xyb + 4\left(\frac{x + y}{2}\right)^2 = -f \iff x^2 - (b - 2)xy + y^2 + f = 0.$$

We now employ Vieta Jumping. Since $c > a$, hence $x, y \in \mathbb{N}$ and $x > y \geq 1$. From a solution (x, y), we jump:

$$(x, y) \mapsto (x_0, y) = \left(\frac{y^2 + f}{x}, y\right),$$

Now, $x_0 = (y^2 + f)/x > 0$ and is an integer since it equals $b - 2 - x$. So if we can show $x_0 < x$, then we have established a descent. Note that $x_0 < x \iff y^2 + f < x^2$. Now,

$$x^2 - y^2 = 4ac > 4a^2 = b(c^2 - a^2) - f > b > f$$

since $c^2 - a^2 = (c - a)(c + a) > 2$. Hence, we are done. □

Solution 4.9.20 (China TST 3 2018 Day 3/2)

We will show that there are no solutions. Firstly, $\gcd(xy+1, xy+x+2) = \gcd(xy+1, x+1) = \gcd(y-1, x+1)$. So let $x+1 = da$ and $y-1 = db$, where $\gcd(a,b) = 1$. Then we have

$$xy+1 = d \cdot u^2 \quad \text{and} \quad xy+x+2 = d \cdot v^2$$

for some relatively prime (u, v). Thus, $du^2 = d^2ab + d(a-b)$ and $dv^2 = d^2ab + d(2a-b)$. So,

$$(d \cdot b + 1)v^2 - (d \cdot b + 2)u^2 = b.$$

Since $v > u$, we can let $v = \frac{X+Y}{2}$ and $u = \frac{X-Y}{2}$ for some positive integers X and Y. Thus the equation becomes

$$X^2 - (4bd+6)XY + Y^2 + 4b = 0.$$

Vieta jumping works now: assume for contradiction there is a solution (X, Y) in positive integers. Assume $X \geq Y$ by symmetry. We jump

$$(X, Y) \mapsto \left(\frac{Y^2+4b}{X}, Y\right).$$

We give a different finish than what we normally do in Vieta Jumping. Suppose we must eventually reach a pair of pairs (X_1, Y) and (X_2, Y) with $X_1 > X_2 \geq Y$, so that the proces stops there. This means that we should have $X_1 + X_2 = (4bd+6)Y$ and $X_1X_2 = Y^2 + 4b$.

But since $X_1, X_2 > Y$, hence $X_1 + X_2 = (4bd+6) \cdot Y$, then

$$X_1 \cdot X_2 \geq Y \cdot (4bd+5)Y > Y^2 + 4b,$$

a contradiction. So the process goes on forever, which again is a contradiction.

Solution 5.9.14 (Iran 2016 Round 3 NT/1)

Clearly, we must have that $q \nmid x$ because otherwise $q|(x+1)^p - x^p$ would imply $q|1$, absurd.

Suppose $(x+1)^p \equiv x^p \pmod{q}$. Since $\gcd(q, x) = 1$, hence this gives

$$\left(x^{-1}+1\right)^p \equiv 1 \pmod{q}.$$

Let $a = x^{-1} + 1$. Then, $\mathrm{ord}_q(a)|p$ and since p is a prime, we have $\mathrm{ord}_q(a) \in \{1, p\}$. If $\mathrm{ord}_q(a) = 1$, then $a \equiv 1 \pmod{q}$, which implies $x + 1 \equiv x \pmod{q}$, absurd. Hence, $\mathrm{ord}_q(a) = p$. So we find $p \mid q-1$ and so $q \equiv 1 \pmod{p}$.

Conversely, if $p|q-1$, then set $q = pk+1$ for some integer k. We know that there always exists a primitive root modulo any prime. Let y be a primitive root modulo q, so that $y^{q-1} \equiv 1 \pmod{q}$. Let $a = y^k$ and note that

$$a^p = (y^k)^p = y^{pk} = y^{q-1} \equiv 1 \pmod{q}.$$

Also note that $\gcd(a-1, q) = \gcd(y^k - 1, q) = 1$ since y is a primitive root mod q and $k < q-1$. So there exists an integer x such that $x(a-1) \equiv 1 \pmod{q}$. This implies $x+1 \equiv xa \pmod{q}$. Raise both sides of the latter congruence equation to the power of p to obtain

$$(x+1)^p \equiv (xa)^p \equiv x^p \pmod{q}.$$

Thus, this value of x works, and this completes the proof.

Solution 5.9.17 (USA EGMO TST 2019/2)

Define

$$S_\ell := 1^\ell + 2^\ell + \cdots + n^\ell,$$

so that $n \mid S_\ell$ for all $\ell \in \{1, 2, \ldots, 99\}$. Let p be a prime in $\{2, 3, \ldots, 100\}$. Then

$$\begin{aligned}\frac{(n+1)^p - 1}{n} &= \frac{1}{n}\sum_{i=1}^{n} (i+1)^p - i^p \\ &= \frac{1}{n}\sum_{i=1}^{n} \binom{p}{1} i^{p-1} + \binom{p}{2} i^{p-2} + \cdots + \binom{p}{p-1} i + 1 \\ &= \left(\binom{p}{1}\frac{S_{p-1}}{n} + \binom{p}{2}\frac{S_{p-2}}{n} + \cdots + \binom{p}{p-1}\frac{S_1}{n}\right) + 1\end{aligned}$$

Since each binomial coefficient on the right is divisible by p, and each fraction is an integer by the hypothesis, hence modulo p, the above gives

$$\frac{(n+1)^p - 1}{n} \equiv 1 \pmod{p}.$$

However, if $p \mid n$, then the left side is

$$(n+1)^{p-1} + (n+1)^{p-2} + \cdots + (n+1) + 1 \equiv 1 + 1 + \cdots + 1 \equiv 0 \not\equiv 1 \pmod{p},$$

which is a contradiction. Thus, no prime in $\{2, 3, \ldots, 100\}$ divides n, so done.

Comment 9.6.4: The power sum formula works for $k = 1, 2, 3$, however we don't have any (simple) formula for $k \geq 4$. So, we fall to first principles, which in this case is the proof of the cases $k = 2, 3$ which solves the problem!

Solution 5.9.18 (IMO Shortlist 2014 N6)

The idea is to group up segments of the same length, i.e. for a possible length ℓ, find how many segments can have length ℓ. Clearly, $0 < \ell < a_1$ otherwise there would be a multiple of a_1 inside $\mathcal{L}$, hence $\ell \in \{1, \ldots, a_1 - 1\}$. Pick any one segment $\mathcal{L}$ of length ℓ. Now, $\mathcal{L}$ is characterized by its endpoints.

So we can find a subset $A \subset \{a_1, \ldots, a_n\}$ and a subset $B \subset \{a_1, \ldots, a_n\}$ such that the left endpoint of $\mathcal{L}$ is divisible by elements A and the right by elements of B. So we basically want x such that $x \equiv 0 \pmod{a}$ for all $a \in A$, $x \equiv -\ell \pmod{b}$ for all $b \in B$.

Another condition we need to ensure is that no multiple of any other terms lies inside $\mathcal{L}$. Clearly, no multiple of an element from A or B can be inside $\mathcal{L}$ because $\ell < a_1 < a_i$ for all i. Also, A, B are disjoint for the same reason. So let $C = (A \cup B)^c$, i.e. the elements in $\{a_1, \ldots, a_n\}$ not in A or B. So for any $c \in C$, we want no multiple of c inside $\mathcal{L}$, i.e.

no multiple between $x, x+\ell$. Hence, x can be $1, 2, \ldots, c-\ell-1 \pmod c$. So, we have the following conditions:

$$\begin{cases} x \equiv 0 \pmod a & \forall\ a \in A; \\ x \equiv -\ell \pmod b & \forall\ b \in B; \\ x \in \{1, 2, \ldots, c-\ell-1\} \pmod c & \forall\ c \in C = (A \cup B)^c. \end{cases}.$$

The key observation now is that any marked point in I is precisely defined by its value (mod a_i) for all i.[6] Hence the above constraints uniquely define a_i.

The final observation is that A, B can be any disjoint subsets of $\{a_1, \ldots, a_n\}$. Hence, the number of segments with length ℓ becomes

$$\sum_{A \cap B = \phi} \prod_{c \in (A \cup B)^c} (c - \ell - 1).$$

Hence, our desired sum becomes

$$\sum_{\ell=1}^{a_1 - 1} \sum_{A \cap B = \phi} \ell^2 \prod_{c \in (A \cup B)^c} (c - \ell - 1).$$

This feels weird, but here's how the magic happens: Note that the sum over A, B is the same for all ℓ, and the product after it is a polynomial in ℓ, say $p(x)$. So the above becomes the sum of $p(\ell)$ from $\ell = 1$ to $a_1 = 1$. Since $|A|, |B| \geq 1$, hence $\deg p \leq 2 + (n-2) = n \leq a_1 - 2$. Now since

$$1^i + 2^i + \cdots + (p-1)^i \equiv 0 \pmod p$$

for all $0 \leq i \leq p-2$ (Example 5.5.1), hence the above sum is 0 mod a_1 (as a_i is a prime), and we are done!

Comment 9.6.5: The idea we saw at the end will be repetitive in the chapter on quadratic residues. To write it out explicitly, for instance with $f(x) = x^3 + 2x + 1$ and $p = 5$, we have

$$\begin{aligned} \sum_{x=1}^{p-1} f(x) &= \sum_{x=1}^{4} x^3 + 2x + 1 \\ &= \sum_{x=1}^{4} x^3 + 2\left(\sum_{x=1}^{4} x\right) + 1\left(\sum_{x=1}^{4} 1\right) \\ &\equiv 0 + 0 + 0 = 0 \pmod 5 \end{aligned}$$

Basically, we pair up terms according to their powers, and irrespective of their coefficients, they add to 0.

[6] This is quite intuitive, however to formalize it we use the "Chinese Remainder Theorem", which we discuss in the chapter on Constructions.

Solution 6.7.17 (Iran 2017 Round 3 NT/1)

Let p be the smallest prime not in the list $p_1, p_2, \ldots, p_k$. Out of all ν_p, let s be the maximum achieved for a_w. The key claim is the following:

Claim. *For all $i \neq w$, we have $\nu_p(a_i) < s$.*

Proof. Suppose $\nu_p(a_i) = s$, and write $a_i = cp^s$. Now both a_i, a_w cannot be equal to p^s, so assume without loss of generality that $a_i \neq p^s$, i.e. $c > 1$. Then c can't have any prime factor from $p_1, \ldots, p_k$ and further $p \nmid c$. By minimality of p, this means $c > p$. Hence, $p^{s+1} < a_i < n$. But then one of $\{a_j\}$ must equal p^{s+1}, contradicting the maximality of s. □

The claim finishes the problem since ν_p of the sum equals $\min \nu_p(a_w^{-1}) = -s < 0$.

Comment 9.6.6: This is a generalization of the two classic problems asking to show

$$\mathbb{H}_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n} \notin \mathbb{Z}, \quad 1 + \frac{1}{3} + \cdots + \frac{1}{2n-1} \notin \mathbb{Z}.$$

In the first one, the set $\{p_i\} = \phi$, and in the second case $\{p_i\} = \{2\}$. The proofs are also identical, for instance in the first we consider ν_2 and 2 is the smallest prime factor not in $\{p_i\}$. Further, we show $\nu_2(\mathbb{H}_n) = -k$ where k is such that $2^k \leq n < 2^{k+1}$, which was possible since $\nu_p(i^{-1}) \neq -k$ for any other i. This is precisely what we did here.

Solution 6.7.18 (China TST 2 2019/4)

Pick an odd prime p. Let $p^k \leq m < p^{k+1}$. Then we have to prove

$$\nu_p(m!) - \left\lfloor \frac{m}{2p} \right\rfloor - \left\lfloor \frac{m}{4p} \right\rfloor - \cdots \geq k.$$

Let $2^t p \leq m < 2^{t+1}p$. Then

$$\begin{aligned} \left\lfloor \frac{m}{2p} \right\rfloor + \left\lfloor \frac{m}{4p} \right\rfloor + \ldots &\leq \left\lfloor \frac{m}{2p} \right\rfloor + \left(\frac{m}{4p} + \frac{m}{8p} + \ldots \right) - \left(\frac{m}{2^{t+1}p} + \frac{m}{2^{t+2}p} + \ldots \right) \\ &= \left\lfloor \frac{m}{2p} \right\rfloor + \frac{m}{2p} - \frac{m}{2^t p}. \end{aligned}$$

Since the Legendre's formula of $\nu_p(m!)$ has only k non-zero terms, hence we can split that $\nu_p(m!) - k$ to the sum of $(\lfloor n/p^s \rfloor - 1)$ where $s = 1$ to k. Hence,

$$\begin{aligned} \nu_p(m!) - k - \left\lfloor \frac{m}{2p} \right\rfloor - \left\lfloor \frac{m}{4p} \right\rfloor - \ldots &= \left(\left\lfloor \frac{m}{p} \right\rfloor - 1 \right) + \cdots + \left(\left\lfloor \frac{m}{p^k} \right\rfloor - 1 \right) - \left(\left\lfloor \frac{m}{2p} \right\rfloor + \left\lfloor \frac{m}{4p} \right\rfloor + \ldots \right) \\ &> \left(\left(\frac{m}{p} - 1 \right) - 1 - \left\lfloor \frac{m}{2p} \right\rfloor - \frac{m}{2p} + \frac{m}{2^t p} \right) + \left(\left\lfloor \frac{m}{p^2} \right\rfloor - 1 \right) + \ldots \left(\left\lfloor \frac{m}{p^k} \right\rfloor - 1 \right) \\ &\geq \left(\left\{ \frac{m}{2p} \right\} - 1 \right) + \left(\frac{m}{2^t p} - 1 \right) \geq -1. \end{aligned}$$

Hence, the LHS is ≥ 0 (as it's in integer) and hence we are done. □

Solution 6.7.20 (Tuymaada Olympiad)

Write this as

$$10^n((n_1+1)\dots(n_k-1)n_k+\dots+(n_{k-1}+1)\dots(n_k-1)n_k+1)=n_k!.$$

Let the quantity in the bracket be S, so that $10^nS=n_k!$. So $n_k \mid 10$ so write $n_k=2^a5^b$. Now we analyze the possible values of a,b:

- Suppose $a,b>0$. Then $10 \mid n_k$ and so $\gcd(S,10)=1$. But $10^nS=n_k!$, and so we must have $\nu_2(n_k!)=\nu_5(n_k!)$. However, clearly

$$\nu_2(n_k!)=\sum\left\lfloor\frac{n_k}{2^j}\right\rfloor\geq\sum\left\lfloor\frac{n_k}{5^j}\right\rfloor=\nu_5(n_k!)$$

  since $\lfloor n_k/2^j\rfloor\geq\lfloor n_k/5^j\rfloor$. Hence equality holds so that $\lfloor n_k/2^j\rfloor=\lfloor n_k/5^j\rfloor$ for all j. This, however, means $n_k\leq 3$, and these cases can be manually ruled off.

- Suppose $b=0$. Then $2 \mid n_k$ so S is odd. Hence, $\nu_5(n_k!)\geq\nu_2(10^n)=\nu_2(n_k!)$ (because S might contribute some factors of 5). As before, this is impossible.

- Suppose $a=0$. Then $5 \mid n_k$ so $\gcd(5,S)=1$. Now, the key observation in this case is that S is odd if $n_k>n_{k-1}+1$. However, as before S odd causes issues. So $n_k=n_{k-1}+1$. But then $4 \mid n_k-1$ (since n_k is a power of 5), hence $S\equiv 2 \pmod 4$, i.e. $\nu_2(S)=1$. Hence, $\nu_2(n_k!)=1+\nu_2(10^n)=n+1=\nu_5(n_k!)+1$. As before, this means $\lfloor n_k/2\rfloor=1+\lfloor n_k/5\rfloor$ and so $n_k\leq 6$. Since n_k is a power of 5, hence $n_k=5, n_{k-1}=4$, which can be checked to not work.

Solution 6.7.23 (USA TSTST 2014/6)

Let s be the order of $a\cdot b^{-1}$. Then the terms in the sequence divisible by p are precisely those of the form $ca^k-db^k, ca^{k+s}-db^{k+s}, ca^{k+2s}-db^{k+2s},\dots$. So define

$$A=\frac{a^s}{b^s},\quad B=\frac{db^k}{ca^k}.$$

Then we have reduced the problem to:

Claim. *Let $A,B\in\mathbb{Q}^+$ and p be a prime such that $A\equiv B\equiv 1 \pmod p$. Consider the sequence $\{A^n-B\}$ as n goes over non-negative integers. Then we need to show that if $\{\nu_p(A^t-B)\}_{t=0}^{\infty}$ is not constant, then it is unbounded.*

Assume on the contrary x,y such that $u=\nu_p(A^x-B)<\nu_p(A^y-B)=v$. It is enough to construct a ℓ such that $\nu_p(A^\ell-B)>v$. Then

$$\nu_p(A^{y-x}-1)=\nu_p((A^y-B)-(A^x-B))=\nu(A^x-B)=u.$$

So using LTE, we can find a k such that $\nu_p(A^k-1)=v$, namely $k=(y-x)p^{v-u}$. Now write $A^k=p^v\alpha+1$ and $A^y=p^v\beta+B$ with $\gcd(p,\alpha)=\gcd(p,\beta)=1$. Then (using the binomial theorem)

$$\begin{aligned} A^{kr+y}-B &= (p^v\alpha+1)^r(p^v\beta+B)-B \\ &\equiv (rp^v\alpha+1)(p^v\beta+B)-B \\ &= p^v(r\alpha B+\beta) \pmod{p^{v+1}}. \end{aligned}$$

So if we choose r such that $r\equiv -\beta/(B\alpha)\equiv -\beta/\alpha \pmod p$, then the above becomes 0. Thus, $\nu_p(A^{kr+y}-B)\geq v+1$. This gives the desired contradiction. □

Solution 6.7.24 (ELMO 2017 N3)

The answer is no. Suppose not for a fixed C. Consider any prime p. Then the problem gives

$$k\nu_p(a_{k+1})\leq k\nu_p(C)+\nu_p(a_1)+\cdots+\nu_p(a_k). \tag{9.5}$$

Now we have the following key claim (guessed by small values)

Claim. *Let $\mathbb{H}_n$ denote the nth harmonic number defined by*

$$\mathbb{H}_n=\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{n}.$$

Then

$$\nu_p(a_n)-\nu_p(a_1)\leq \mathbb{H}_{n-1}\nu_p(C).$$

Proof. The proof is just strong induction on n. Firstly, put $k=1$ in Equation 9.5 to get

$$\nu_p(a_2)-\nu_p(a_1)\leq 1\nu_p(C),$$

which serves as the base case since $\mathbb{H}_1=1$. Now assume the result till some n. Then putting $k=n$ in Equation 9.5, we find

$$\begin{aligned} n\nu_p(a_{n+1}) &\leq n\nu_p(C)+\nu_p(a_1)+\nu_p(a_2)+\cdots+\nu_p(a_n) \\ &\leq n\nu_p(C)+\nu_p(a_1)+(\nu_p(a_1)+\mathbb{H}_1\nu_p(C))+\cdots+(\nu_p(a_1)+\mathbb{H}_{n-1}\nu_p(C)) \\ &= n\nu_p(a_1)+(n+\mathbb{H}_1+\cdots+\mathbb{H}_{n-1})\,. \end{aligned}$$

and hence

$$\begin{aligned} \nu_p(a_{n+1})-\nu_p(a_1) &\leq \frac{1}{n}\left(n+\left(\frac{1}{1}\right)+\cdots+\left(\frac{1}{1}+\cdots+\frac{1}{n-1}\right)\right) \\ &= \frac{1}{n}\left(\left(1+\underbrace{\frac{1}{2}+\frac{1}{2}}_{2}+\cdots+\underbrace{\frac{1}{n}+\cdots+\frac{1}{n}}_{n}\right)+\left(\frac{1}{1}\right)+\cdots+\left(\frac{1}{1}+\cdots+\frac{1}{n-1}\right)\right) \\ &= \frac{1}{n}\left(n\cdot\frac{1}{1}+n\cdot\frac{1}{2}+\cdots+n\cdot\frac{1}{n}\right)=\mathbb{H}_n. \end{aligned}$$

and the induction is complete. □

The key hypothesis we need now is that a_i are pairwise distinct. We want to try to force $\nu_p(a_i) = \nu_p(a_j)$ for all primes to get a contradiction. It is not too hard to observe from Equation 9.5 that that any prime divisor of a_k must divide Ca_1. So we only need to worry about a finite set of prime factors, say $\mathbb{P} = \{p_1, \ldots, p_k\}$.

We have the famous estimate for $\mathbb{H}_n$:

$$\mathbb{H}_n \leq 1 + \log(n+1) \implies \mathbb{H}_n \leq \log n + \log n^2 = 3 \log n.$$

(basically $\mathbb{H}_n = \mathcal{O}(\log n)$[7]). Now for any prime $p \in \mathbb{P}$ and any $n \geq 1$,

$$\nu_p(a_n) \leq \mathbb{H}_{n-1}\nu_p(C) + \nu_p(a_1) \leq A \log n$$

for some large enough A (since $\mathbb{P}$ is a finite set, hence $\nu_p(C), \nu_p(a_1)$ are always less than some fixed constants).

Hence if we look at k tuples of the form $(\nu_{p_1}(a_n), \ldots, \nu_{p_k}(a_n))$, then there are at most

$$\prod_{i=1}^{k} (1 + A \log n) \leq (B \log n)^k$$

for some large enough constant B (basically the product is $\mathcal{O}((\log n)^k)$.)

However, the number of tuples also has to be at least $n+1$ (because if two tuples are the same, then the numbers are the same).So

$$(n+1) \leq (B \log n)^k$$

for all n. However, clearly this fails for large enough n since linear growth exceed logarithmic growth.

Solution 7.7.9 (USAMO 1995/4)

Let the degree of P be d. Then $|q_n| < Cn^d$ for some $c \neq 0$ and all n.

Define the polynomial Q by $Q(i) = q_i$ for all $0 \leq i \leq d$. Then it suffices to show $Q(n) = q_n$ for all n.

Pick any n and $0 \leq i \leq d$. Then

$$n - i \mid q_n - q_i, \quad \text{and} \quad n - i \mid Q(n) - Q(i) = Q(n) - q_i$$

Thus, we get $n - i \mid Q(n) - q_n$ for all $0 \leq i \leq d$. If $Q(n) - q_n \neq 0$, then we get the bound

$$\operatorname{lcm}(n, n-1, \ldots, n-d) \leq Cn^d.$$

[7]Relevant Term for interested readers: "Big O Notation"

The heuristic is that this cannot be true for large enough n. To formalize it, we would need some more rigorous bounding. There are many ways to do this. One way is to observe that

$$\begin{aligned}\operatorname{lcm}(n, n-1, \ldots, n-d) &= \operatorname{lcm}(\operatorname{lcm}(n, n-1, \ldots, n-d+1), n-d) \\ &= \frac{\operatorname{lcm}(n, n-1, \ldots, n-d)(n-d)}{\gcd(\operatorname{lcm}(n, n-1, \ldots, n-d+1), n-d)} \\ &\geq \frac{\operatorname{lcm}(n, n-1, \ldots, n-d)(n-d)}{\gcd(n(n-1)\ldots(n-d+1), n-d)} \\ &\geq \frac{\operatorname{lcm}(n, n-1, \ldots, n-d)(n-d)}{d!}\end{aligned}$$

where the last line is because if $p \mid \gcd(n(n-1)\ldots(n-d+1), n-d)$, then $p \mid n+i, n+d$ implies $p \mid d-i$, which means $p \leq d-i < d$. Further, there are atmost

This is just a generalizat

Now, we can show that $n(n-1)\ldots(n-d) \mid \operatorname{lcm}(n, n-1, \ldots, n-d)T$, where $T = \sum_{i \neq j} \gcd(n-i, n-j) < d\binom{d+1}{2} = k$. So,

$$Cn^d \geq kn(n-1)\ldots(n-d).$$

However, this fails for large n since the right side is a degree $d+1$ polynomial. for some $\varepsilon > 0$. This fails for large n. So for all $n > N$, we have $Q(n) = q_n$. For some $d < n < N$, we get by $m - n \mid Q(n) - q_n$ for any $m > N$, which is absurd due to size reasons unless $Q(n) = q_n$, and so we are done.

Solution 7.7.10 (Iran 2016 Round 3 NT/2)

Suppose that P is non-constant, and without loss of generality the leading coefficient of P is positive. Hence, for large enough n, we have $P(n) > 2$. This means there is a prime $p \mid P(n)$, and so $p \mid P(n+pk)$ for all k. This also shows $p \mid f(n+pk)$.

Now Fermat's Little Theorem gives us $f(m) \equiv f(n) \pmod{p}$ if $m \equiv n \pmod{p-1}$. Hence, $f(n+pk) \equiv f(n+k) \pmod{p}$. Thus, if we pick k such that $p-1 \mid n+k$, then $p \mid P(n+pk)$ implies $p \mid f(n+pk) \equiv f(n+k) \equiv f(0) \pmod{p}$. Hence, $p \mid f(0)$. But since f is non-zero by the hypothesis, hence this shows p is bounded, a contradiction to Schur's Theorem. $\square$

Solution 7.7.16 (IMO Shortlist 2011 N6)

Firstly, since $P(x), Q(X)$ are coprime over $\mathbb{Q}[X]$, hence by Bézout's lemma there exist polynomials $A, B \in \mathbb{Q}[X]$ such that $PA + QB = 1$. We can multiply both sides by a constant so that this becomes $Pa + Qb = N$ for a fixed $N \in \mathbb{Z}$ and $a, b \in \mathbb{Z}[X]$.

Now we use $f(n) \mid f(n + kf(n))$ for all $z \in \mathbb{Z}$. Thus, $Q(n) \mid Q(n + kQ(n))$ for all n and z. So,

$$2^{Q(n)} - 1 \mid 2^{Q(n+kQ(n))} - 1 \mid 3^{P(n+kQ(n))} - 1.$$

Considering this over all k, we find $2^{Q(n)} - 1$ divides $3^T - 1$ where

$$T = \langle \gcd(P(n + kQ(n))) \rangle_{z=-\infty}^{\infty} = \gcd(\dots, P(n), P(n + Q(n)), P(n + 2Q(n)), \dots).$$

We want to show that T is bounded by a constant, which would show $\deg Q = 0$.

Claim. *Suppose $p \mid T$. Then $\nu_p(T)$ is bounded.*

Proof. Let p^M be a prime power that divides T. If $p^M \mid Q(n)$, then $p^M \mid P(n)$ so $p^M \mid N$ hence M is bounded.

So say $p^M \nmid Q(n)$. If $p \nmid Q(n)$ then $P(x) + zQ(x)$ forms a complete residue class mod p, and hence $p^M \mid P(k)$ for all k. In particular, $p^M \mid P(1)$, so that M is bounded.

So let $\nu_p(Q(n)) = t$ and write $Q(n) = p^t \ell$. Then $p^M \mid P(n + z\ell p^t)$ for all z. However $\gcd(p, \ell) = 1$, so this gives $p^M \mid P(n + zp^t)$ by the complete residue class argument. So for a choice of z, $n + zp^t$ is between p^t and $2p^t$, say equals r (this is modulo p^M). But then $p^M \mid P(r)$, which shows $P^M < r^d < Cp^{td}$, so that $M < C't$ for fixed C'.

But since $p^t \mid P(n), Q(n)$, hence $p^t \mid N$ so t is bounded. So $M < C't$ also is bounded. □

Now we just want primes dividing T to be bounded. Let $p \mid T$, then pick $p > N$ so $p \nmid Q(n)$, and $p \mid P(n)$. Now $p \mid P(k)$ for all k. Thus, $p \mid P(1)$, so in all, $p \le \max(P(1), N)$, hence there are only finitely many primes diving T. We are thus done.

Solution 7.7.17 (2020 Korean MO winter camp Test 1 P3)

We claim the answer is $Q(x) = Ax^d$, which clearly works. Now let $Q(x) = x^d R(x)$ so that $R(0) \neq 0$. We aim to show R is constant. Assume that R is not constant and take any $m > R(0)$. Thus $m \nmid R(m^c)$ for any c.

Claim. *$R(m^c)$ and $R(m)$ have the same prime divisors for any c.*

Proof. Firstly, the second condition shows $R(m), R(m^2), R(m^{2^2}), \dots$ all have the same number of prime divisors.

Now suppose $R(m^c)$ and $R(m)$ have the same prime divisors. Since $R(m \cdot m^{c-1})$ and $R(m)R(m^{c-1})$ have the same prime divisors, hence every prime divisor of $R(m^c)$ is a prime divisor of $R(m)$. But $R(m^{c-2} \cdot c)$ and $R(m^{c-2})R(c)$ have the same prime divisors, and since $R(m^{c-2}) > 1$, hence $R(m^{c-1})$ has at least as many prime divisors as $R(c)$. So, $R(m^{c-1})$ and $R(m)$ have the same divisors.

So from every $R(m^{m^k})$ we can induct down to prove the claim. □

Let $q \mid R(m)$. We also have $m \nmid R(m)$. Suppose $\gcd(q, m) = 1$. So by Fermat's Little Theorem, $q \mid R(m^{q-1}) \equiv R(1)$, and hence $q \mid R(1)$. So q is bounded (note that $R(1) \ge 1$ by the hypothesis and so $R(1) \neq 0$). Otherwise $q \mid m$. But then $q \mid R(m) \equiv R(0)$, which is not zero since we assumed $x \nmid R(x)$.

Either way, q is bounded for any choice of m. However, by Schur's theorem this is a contradiction unless R is constant, and hence we are done.

Solution 8.7.13 (AMM)

Clearly $n = 1$ is a solution. We will show that there is no other solution. Clearly, n is odd since $3 \nmid 2^n - 1$.

Pick a prime divisor p of $2^n - 1$. Then $3^{n+1} \equiv 3 \pmod{p}$ implies 3 is a quadratic residue mod p. Hence, the quadratic reciprocity law gives

$$1 = \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} \left(\frac{p}{3}\right),$$

and so $p \equiv \pm 1 \pmod{12}$. This is true for all prime factors of $2^n - 1$, and hence $2^n - 1 \equiv \pm 1 \pmod{12}$, which gives $2^n \equiv 2$ or $0 \pmod{12}$. The latter is impossible, and the former is only possible if $n = 1$. Hence we are done.

Solution 8.7.14 (Taiwan 1997)

First say that k is a prime. Clearly we just have to show that k is a quadratic nonresidue. Since $n > 0$, hence $k \equiv 1 \pmod{4}$. Further, $k = 4^{2^{n-1}} + 1 \equiv 2 \pmod{3}$. Hence

$$\left(\frac{3}{k}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{k}{3}\right) = -1.$$

Now for the other direction, since $3^{\frac{k-1}{2}} \equiv -1 \pmod{k}$, hence $3^{k-1} \equiv 1 \pmod{k}$. In particular, $\operatorname{ord}_k(3) \mid k - 1 = 2^{2^n}$ but $\operatorname{ord}_k(3) \nmid \frac{k-1}{2} = 2^{2^{n-1}}$. Hence the order is $k - 1 = 2^{2^n}$.

But then the order divides $\varphi(k)$, and hence $k - 1 \leq \varphi(k)$. However, this means all elements in $\{1, 2, \ldots, k-1\}$ are coprime to k, showing that k is a prime.

Solution 8.7.15 (ELMO 2011/5)

The conditions $p = 2q + 1$ gives the following key claim:

Claim. *Any residue $x \in \{3, -4, 12\}$ is a primitive root if and only if it is not a quadratic residue.*

Proof. Generally, being a primitive root implies not a quadratic residue. In this case, however, the converse holds too. Since $\operatorname{ord}_p(x) \mid p - 1 = 2q$, hence $\operatorname{ord}_p(x) \in \{1, 2, q, 2q\}$. For our values of x, we can check that $1, 2$ are not possible as $p > 13$. So, the order being a quadratic residue is equivalent to the order being q, which implies it is not a primitive root, and this proves the claim. □

The next claim is more explicit:

Claim. $-4, -12$ *are primitive roots modulo p, while 3 isn't, i.e.* $\operatorname{ord}_p(-4), \operatorname{ord}_p(-12) = 2q$ *while* $\operatorname{ord}_p(3) = q$.

Proof. Since $(p-1)/2 = q$ is odd, hence -1 is not a quadratic residue. So

$$\left(\frac{-4}{p}\right) = \left(\frac{2^2}{p}\right)\left(\frac{-1}{p}\right) = -1.$$

So -4 is a primitive root. Now, 3 isn't a primitive root if it is a quadratic residue. Now $q > 3$, and hence $p = 2q+1 \in \{2\cdot 1+1, 2\cdot 2+1\} \equiv \{0,2\} \pmod 3$. Since $p > 3$, we get $p \equiv 2 \pmod 3$. So, by quadratic reciprocity,

$$\left(\frac{3}{p}\right) = (-1)^q \left(\frac{p}{3}\right) = (-1)\cdot(-1) = 1.$$

Hence, 3 is a quadratic residue. Finally,

$$\left(\frac{-12}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = -1$$

meaning that -12 is a primitive root. Hence we are done. □

Now, rewrite the given condition:

$$\begin{aligned} 3^m + (-12)^m \equiv 3^n + (-12)^n \pmod p &\Leftrightarrow 1 + (-4)^m \equiv 3^{n-m} + (-4)^n \cdot 3^{n-m} \pmod p \\ &\Leftrightarrow 1 - 3^{n-m} \equiv (-4)^m\left((-12)^{n-m} - 1\right) \pmod p. \end{aligned}$$

Now $3^{n-m} \equiv 1 \pmod p$ happens if $q = \mathrm{ord}_p(3) \mid n-m$. If this is not true, then the above is

$$(-4)^m \equiv \left((-12)^{n-m} - 1\right)\cdot\left(1 - 3^{n-m}\right)^{-1} \pmod p.$$

Now, the right depends completely on $n-m$. Also, since $\mathrm{ord}_p(3) = q$, hence each value of $n-m$ between 1 and $q-1$ (we are not considering $q \nmid n-m$) gives a different value for the right side. Now since (-4) is a primitive root, hence there would exist some m such that $(-4)^m$ is congruent to the right side.

Hence, for every $n-m$, there exists a m. Now each $(m, n-m)$ pair uniquely gives a (m,n) pair. Hence, the fact that there are $q-1$ values of $n-m$ means $q-1$ solutions in this case.

So, we just need to deal with the case when $q \mid n-m$. In fact, if $q \nmid n-m$, then our equation gives $0 \equiv (-4)^m((-1)-1) \pmod p$ since $\mathrm{ord}_p(-12) = 2q$. However, this is impossible. Hence no solutions in this case. So the $q-1$ solutions we analyzed above are the only ones.

Solution 8.7.16 (Iran TST 2020/6)

The answer is all sets in which $x_i \in \{0,1\}$ for all i. Clearly it works, so now we will prove that this is the only possibility.

The key idea in this approach is to expand $(tx_i+1)^n$ and sum over all x_i to use the given condition. The fact that $n = \frac{p-1}{2}$ is made use of by Euler's Criterion. Let s be the common sum in the problem statement. Then

$$\begin{aligned}\sum_i \left(\frac{wx_i+1}{p}\right) &\equiv \sum_i (wx_i+1)^n \\ &= \sum_i (wx_i)^n + \binom{n}{1}(wx_i)^{n-1} + \cdots + \binom{n}{n-1}(wx_i) + 1 \\ &\equiv s\left(w^n + \binom{n}{1}w^{n-1} + \cdots + \binom{n}{n-1}w + 1\right) + n - s \\ &= s\left[\left(\frac{w+1}{p}\right) - 1\right] + n \pmod p.\end{aligned}$$

So, picking $w+1$ to be a quadratic residue, we can prove the following key result:

Claim. *Whenever t is a quadratic residue with $t \neq 0, 1$, then $(t-1)x_i + 1$ is a non-zero quadratic residue for all i.*

It turns out this claim is sufficient to solve the problem. Consider T to be the set of quadratic residues not equal to 0 or 1. Fix some $x = x_i$. Suppose $x \neq 0$. Then we can see that the map

$$T \mapsto T : t \mapsto (t-1)x + 1$$

is a bijection by the claim. So we have two equal sets. We now add and compare the elements from both the sets. Since

$$\sum_{t \in T} t \equiv -1 \pmod p$$

for all $p > 3$, hence

$$x(-1-(n-1)) + (n-1) \equiv -1 \pmod p,$$

which gives $x \equiv 1 \pmod p$, as desired. □

Solution 8.7.17 (USA TST 2014/2)

Firstly note that each term of the sequence is also a square. Now let $p \mid a_1$. Then $p \mid (a_1 + \cdots + a_p)$ and $p \mid (a_2 + \cdots + a_{p+1})$. Hence $a_1 \equiv a_{p+1} \pmod p$. In a similar way we can prove the following more general claim:

Claim. *If $p \mid a_j$, then $p \mid a_{j\pm p}$.*

Now let $k > 1$ be the least quadratic non-residue modulo p. Let $\mathcal{Z}^2$ denote the set of perfect squares. Then

$$k\mathcal{Z}^2 \ni a_1 + \cdots + a_k \equiv a_2 + \cdots + a_k \in (k-1)\mathcal{Z}^2 \pmod p.$$

However, unless $p \mid a_2 + \cdots + a_k$, this is impossible since it shows $\left(\frac{k}{p}\right) = \left(\frac{k-1}{p}\right)$, contradicting minimality of k. Thus $p \mid a_1 + \cdots + a_k$. But then

$$\mathcal{Z}^2 \ni a_{k+1} \equiv a_2 + \cdots + a_{k+1} \in k\mathcal{Z}^2 \pmod p,$$

which is impossible again unless $p \mid a_{k+1}$. In general,

Claim. *If $p \mid a_j$, then $p \mid a_{j\pm k}$.*

Since $\gcd(k,p) = 1$, hence the above claims give $p \mid a_i$ (for instance use Bézout Lemma to find u, v such that $ku + pv = d$ for any integer d. Then $0 \equiv a_1 \equiv a_{1+ku} \equiv a_{1+ku+pv} = a_{1+d} \pmod{p}$ for any integer d). Then we can divide all the terms of the sequence by p and obtain a "smaller sequence", and keep repeating this process to show that the set of prime factors is the same for all terms.

Solution 8.7.18 (USOMO 2020/3)

We claim the answer is always 2 irrespective of p. Define the set $B = \{b : b, 4-b \in \text{QR}\}\backslash\{0,4\}$. We work in $\mathbb{F}_p$, so that each equality below is actually a congruence mod p. Define $X = (A \cup B)\backslash\{2\}$. We start by establishing the following key claim:

Claim. *For any b, $b \in B \Leftrightarrow b = x(4-x)$ for some $x \in A$ or B.*

Proof. Clearly for $x \in A$ or B, $x(4-x)$ is a QR. Now suppose $b \in B$. Then

$$4 - b = y^2 \iff b = 4 - y^2 = (2-y)(2+y).$$

So take $x = y + 2$. Then $x(4-x)$ is a QR and so $x \in A$ or B, and $b = x(4-x)$ so this works. □

The claim gives us a natural mapping from $f : X \mapsto B$ given by $x \mapsto x(4-x)$, which is in B. The key observation now is that $f(\alpha) = f(\beta) \iff \alpha = \beta$ or $\alpha + \beta = 4$. Hence, for $x \neq 2$, each pair $(x, 4-x) \in X^2$ maps to a unique element of B, and this covers all the elements of B. Hence,

$$2\prod_{b\in B} b = \left(\prod_{x\in X} x\right) = \left(\prod_{a\in A} a\right)\left(\prod_{b\in B} b\right) \implies \prod_{a\in A} a = 2.$$

Solution 9.6.10 (APMO 2009/4)

Pick a set $\mathcal{P}$ of n primes $p_1, \ldots, p_n$ such that $p_1 > p_2 > \cdots > p_n > n$. Then, using the Chinese Remainder Theorem, pick an x such that

$$x \equiv -i \pmod{p_i}$$

for all i. Pick $N = p_1 p_2 \cdots p_n$. We then claim that the following fractions (on being reduced) work:

$$\frac{x+1}{N}, \ldots, \frac{x+n}{N}$$

Clearly $\gcd(x+i, x+j) = \gcd(x+i, j-i) \leq |j-i| < n < p_i, p_j$. So for each i, the only prime from $\mathcal{P}$ dividing $x_i + i$ is p_i. Thus

$$\frac{x+i}{N} = \frac{(x+i)/p_i}{N/p_i}$$

is the reduced form of each fraction. The reduced denominators of all the fractions are clearly distinct. Also, no reduced numerator would equal a reduced denominator since the only $p \in \mathcal{P}$ dividing $x+i$ is p_i.

Finally we see that that if for some $j > i$, we have $\frac{x+i}{p_i} = \frac{x+j}{p_j}$, then $\frac{x+i}{x+j} = \frac{p_i}{p_j} > 1 \implies i > j$, absurd. Hence, the numerators are also pairwise distinct.

Solution 9.6.13

Assume without loss of generality that the number n is square-free. Suppose $n = p_1 p_2 \dots p_k$. We will show that there exist arbitrarily large primes p such n is a quadratic nonresidue mod p. We do this very greedily. Now

$$\left(\frac{p_i}{p}\right) = (-1)^{\frac{p_i-1}{2}\cdot\frac{p-1}{2}} \left(\frac{p}{p_i}\right), \quad p_i \neq 2.$$

Hence, if we set $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod{p_i}$, then the right side above becomes $+1$ meaning that p_i is a quadratic residue mod p. On the same note, if we choose p to be a quadratic nonresidue mod p_i, then the right side becomes -1 and hence p_i is a quadratic nonresidue mod p. So set up the system: (also if $p_i = 2$, then p_i is a QR mod p if $p \equiv 1 \pmod 8$, so we set $p \equiv 1 \pmod 8$ below instead of just $p \equiv 1 \pmod 4$)

$$\begin{cases} p \equiv 1 \pmod 8 \\ p \equiv 1 \pmod{p_i}, \quad 1 \leq i \leq k, p_i \neq 2 \\ p \equiv a \pmod{p_k} \end{cases}$$

where a is a quadratic nonresidue mod p_k, then by Chinese Remainder Theorem the above gives us a congruence $p \equiv z \pmod N$. By Dirichlet's theorem, this has infinitely many prime solutions, and for any such p,

$$\left(\frac{n}{p}\right) = \left(\prod_{1\leq i\leq k-1} \underbrace{\left(\frac{p_i}{p}\right)}_{+1}\right) \underbrace{\left(\frac{p_k}{p}\right)}_{-1} = -1.$$

Hence, pick a very large prime p satisfying $p \equiv z \pmod N$ and we get a contradiction. $\square$

Solution 9.6.15 (IMO Shortlist 2005 N6)

The given condition gives $a^n + n \mid b^n - a^n$ for all n. We cleverly pick n now given by the system of congruence (this has a solution by the Chinese Remainder Theorem)

$$\begin{cases} n \equiv 0 \pmod{p-1} \\ n \equiv -a \pmod p \end{cases}$$

for any prime p. By Fermat's Little Theorem, such an n gives $a^n \equiv a, b^n \equiv b \pmod p$. Further, $a^n + n \equiv a + n \equiv 0 \pmod p$. Hence, $p \mid b^n - a^n$ implies $a \equiv b \pmod p$. Since this is true for all primes p, hence $a = b$.

Solution 9.6.16 (EGMO 2018/6)

Let $S = \{a_1, \cdots, a_n\}$ where $a_i < a_j$ when $i < j$. Since $a_i \in \mathbb{N}$, hence $a_n \geq a_1 + n - 1$, which implies that $\frac{a_1}{a_n}$ can get arbitrarily small for large n. So take $m = 0$, and choose a sufficiently large n such that

$$\left| \frac{a_1}{a_n} - 0 \right| < t$$

which is enough to solve the first part. □

The answer to the second part is yes. We construct this set recursively. They key observation is that for any $x, y \in S$, we must have

$$1 - t > \left\{ \frac{x}{y} \right\} > t \Leftrightarrow 1 - t > \frac{x \bmod y}{y} > t.$$

Note that $f(x) = \frac{\frac{x-1}{2}}{x}$ get closer to $\frac{1}{2}$ as x increases. So we act greedily and choose a prime p_1 such that $1 - t > \frac{1}{2} > f(p_1) > t$. So set p_1 to be the first element of S. Then, by Dirichlet, we can choose a prime p_2 such that $p_2 \equiv \frac{p_1 - 1}{2} \pmod{p_1}$ and $p_2 > 2p_1$. Next, choose a prime p_3 such that

$$\begin{cases} p_3 \equiv \frac{p_1 - 1}{2} & (\text{mod } p_1) \\ p_3 \equiv \frac{p_2 - 1}{2} & (\text{mod } p_2) \\ p_3 > 2p_2 \end{cases}$$

Such a prime exists by Dirichlet and The Chinese Remainder Theorem. Proceed and construct the primes p_i for all $i \geq 1$. Then we claim that the infinite set

$$S = \{p_1, p_2, p_3, \cdots\} \text{ works.}$$

The reason is simple. Firstly, see that for $j > i$, $0 < \frac{p_i}{p_j} < \frac{1}{2}$ and since $m \neq 0$, hence this works. Also, if $j > i$, then $\left\{ \frac{p_j}{p_i} \right\} = f(p_i)$, which by assumption lies in $\left(t, \frac{1}{2}\right)$. □

Solution 9.6.19 (China TST 1 2019/2)

The answer is yes. Take $m > 1$ such that $m^n \equiv 1 \pmod{n}$ (this can be done by choosing a m such that $m \equiv 1 \pmod{n}$). Let $d = \frac{m^n - 1}{n}$, and set

$$\begin{array}{lllll} a_1 = m, & a_2 = m(1+d), & a_3 = m(1+2d), & \ldots & a_n = m(1+(n-1)d) \\ & b_1 = (1+d), & b_2 = (1+2d), & \ldots & b_{n-1} = (1+(n-1)d), \quad b_n = (1+nd). \end{array}$$

Then

$$\prod_{i=0}^{n} a_i = \underbrace{m^n}_{=(1+nd)} \cdot \prod_{i=0}^{n-1} (1+id) = \prod_{i=0}^{n} (1+id) = \prod_{i=0}^{n} b_i.$$

Further, it is easy to check that the GCD of all terms is 1, and hence our construction works. Now we want to show there are infinitely many such sequences. However, this is true since we have infinitely many choices for m. □

Solution 9.6.20 (INMO 2019/4)

The key observation is that if z is any common divisor of $M+i, M+j$, then $z \mid i-j$ implying $z \leq |i-j| \leq n-1$. Now the following is the key claim:

Claim. *Define*

$$x_i = \frac{M+i}{\gcd(M+i,(n-1)!)}.$$

Then $x_1, \ldots, x_n$ are all pairwise coprime.

Proof. Suppose p is a prime dividing both x_i, x_j. Then $p \mid M+i, M+j$ and hence $p \leq n-1$. So even after dividing by the gcd if we have a leftover factor of p in x_i, x_j (with $i \neq j$), then

$$\nu_p(M+i), \nu_p(M+j) > \nu_p((n-1)!) = w.$$

Then $p^{w+1} \mid (M+i), (M+j)$ implies $p^{w+1} \leq n-1$. But this means p^{w+1} occurs in the product $(n-1)!$, which contradicts the fact that $\nu_p((n-1)!) = w < w+1$. □

Now, since $M > n^{n-1} > (n-1)!$ for all $n \geq 1$, all $x_i > 1$, implying they have a prime factor. So pick the set $\{p_i\}$ such that p_i is any prime factor of x_i. Clearly this works. □

> **Comment 9.6.7:** Note that this proof improves the bound from $M > n^{n-1}$ to $M > (n-1)!$. We present a second proof which is perhaps easier to come up with.

Proof. Assume on the contrary. As before, if a number z divides two terms $M+i, M+j$, then $z \leq n-1$. Now for numbers with at least n prime factors, we can pick a prime easily for them. So ignore them for now.

Suppose that $M+i$ has less than n prime factors. Then since $M+i > n^{n-1}$, there exists some prime factor p of $M+i$ such that $p^\alpha = p^{\nu_p(M+i)} > n$. Pick this prime p for $M+i$. If p is also chosen for another $M+j$, then we must have also $p^\beta = p^{\nu_p(M+j)} > n$. However, then $\gcd(p^\alpha, p^\beta) > n$, contradicting the fact that any common divisor of $M+i, M+j$ must be less than n. □

Solution 9.6.21 (USA TSTST 2015/5)

We show by induction on k that for any k, there exists an integer m such that $\varphi(n) = m$ has at least k solutions. The key idea is to take the **first** k **primes** $2 = p_1 < p_2 < \cdots < p_k$.

Claim. *Let $\mathcal{P}_k$ denote the product $p_1 \ldots p_k$. Then there exist at least k solutions to $\varphi(n) = \varphi(\mathcal{P}_k)$ such that all prime factors of n are from the set $\{p_1, \ldots, p_k\}$.*

Proof. For $k = 1$, the result is clearly true, so assume it till some k. Take any n such that $\varphi(n) = \varphi(\mathcal{P}_k)$. Then $\varphi(np_{k+1}) = \varphi(n)\varphi(p_{k+1}) = \varphi(\mathcal{P}_{k+1})$, since $p_{k+1} \nmid n$.

Hence, we have at least k solutions to $\varphi(N) = \varphi(\mathcal{P}_{k+1})$, and we just need 1 more. For this, observe that

$$\varphi(\mathcal{P}_{k+1}) = (p_{k+1}-1)\varphi(\mathcal{P}_k).$$

Now comes the main argument: Since $p_{k+1}-1 < p_{k+1}$, hence all its prime factors are from the set $\{p_1, \ldots, p_k\}$, since these are the first k prime numbers. So we claim that $N = \mathcal{P}_k(p_{k+1}-1)$ works.

Indeed, if $p_{k+1} - 1 = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, then

$$\varphi(\mathcal{P}_k(p_{k+1}-1)) = \varphi\left(\prod_i p_i^{\alpha_i+1}\right) = \left(\prod_i p_i^{\alpha_i}\right)\left(\prod_i (p_i-1)\right) = (p_{k+1}-1)\varphi(\mathcal{P}_k) = \varphi(\mathcal{P}_{k+1})$$

and we are done. □

Comment 9.6.8: If we want to explicitly see the numbers we get from the above induction, we get

$$\begin{aligned} n_1 &= (p_1-1)p_2 \ldots p_k \\ n_2 &= p_1(p_2-1)\ldots p_k \\ &\vdots \\ n_k &= p_1 p_2 \ldots (p_k-1). \end{aligned}$$

All these numbers satisfy

$$\varphi(n_i) = \varphi(\mathcal{P}_k) = (p_1-1)(p_2-1)\ldots(p_k-1).$$

Solution 9.6.22 (APMO 2020/4)

The answer is all linear polynomials. First, we show these work. Let $P(x) = mx + n$. Define $s_i = a_1 + \cdots + a_i$.

Consider $m+1$ numbers $x_1, \ldots, x_{m+1} > 1$ that are all congruent to $n \pmod m$. Then take the $m+1$ pairs $s_{x_1-1}, s_{x_2-1}, \ldots, s_{x_{m+1}-1},$. By the Pigeonhole Principle, two are the same mod m, say s_{x_i-1}, and s_{x_j-1}. Then $a_{x_i} + a_{x_i+1} + \cdots + a_{x_j-1} \equiv 0 \pmod m$, and hence

$$a_{x_i} + a_{x_i+1} + \cdots + a_{x_j} \equiv a_{x_j} \equiv n \pmod m$$

and so this works.

Now suppose $\deg P > 2$. Then we will construct a sequence $\{a_i\}$ such that for any $i < j$, there does not exist a k such that

$$a_i + a_{i+1} + \cdots + a_j = P(k).$$

We do this inductively, and suppose that you have added elements till a_i. Let m be the integer of smallest magnitude that hasn't occurred in the sequence yet. The key is to set $a_{i+2} = m$ (not a_{i+1}). Now, any sum of consecutive terms containing a_{i+2} will have a_{i+1}. Hence, all

possible sums would be in a fixed vicinity around a_{i+1}, i.e. between $I = (a_{i+1} - k, a_{i+1} + \ell)$ for some fixed k, ℓ (since $a_1, \ldots, a_i$ are fixed).

Now we just want to choose an a_{i+1} such that no $P(k)$ lies in I. Now, I has length $k + \ell$. However, since $\deg P \geq 2$, hence $P(x+1) - P(x)$ depends on x (unlike the case $\deg = 1$) and hence grows arbitrarily large. So, eventually there would exist an interval of length $k+\ell$ which is completely skipped by P, i.e. no value in the interval would be of the form $P(k)$ for an integer k. So we choose a_{i+1} so that I becomes this interval. □

Comment 9.6.9: The fact that each integer appears in the sequence is guaranteed by the fact that we are choosing the smallest magnitude integer not yet in the sequence. Since a_i can be arbitrary and we want each integer to appear exactly once (a weird condition), it's better to construct it inductively step by step rather than, say, find a nice formula for a_n.

Solution 9.6.23 (USA TSTST 2016/3)

Firstly, suppose n is a sufficiently large prime $p > 2$ (we define "sufficient" later). Pick

$$Q(x) = (2x^2 - 1)^2.$$

Now, consider the list $\mathcal{L}$ numbers $0, 1, \ldots, p-1$ and delete a number x if $Q(x) \equiv Q(x_0)$ for some $x_0 < x$ (i.e. the residue has appeared before). Since $Q(a) \equiv Q(-a)$, the second half is completely erased, meaning we only have the numbers $0, 1, \ldots, (p-1)/2$ in $\mathcal{L}$. We need to show more numbers are deleted here so that at most $0.499p$ numbers remain.

We do this by using that fact that $x^2 \equiv y^2$ is also possible when $x \equiv -y$. Hence, $Q(a) \equiv Q(b)$ also holds when

$$2a^2 - 1 \equiv 1 - 2b^2 \pmod{p} \iff a^2 + b^2 \equiv 1 \pmod{p}. \tag{9.6}$$

By Theorem 8.5.1, we know this has $p - (-1)^{\frac{p-1}{2}} \geq p - 1$ solutions. However, we only need to consider pairs (a, b) such that a, b aren't already erased, so we have to consider $0 \leq a < b \leq \frac{p-1}{2}$. So we need to remove some of the $p - 1$ solutions.

If $(a, b) \neq (0, \pm 1), (\pm 1, 0)$ is a solution to Equation 9.6, then so are $(\pm a, \pm b), (\pm b, \pm a)$. Further, at most one solution will have $a \equiv b$ which is counted four times (as $(\pm a, \pm a)$). Hence, the number of repeated residues in $\mathcal{L}$ becomes $\geq \frac{(p-1)-4-4}{8} = \frac{p-1}{8} - 1$. Hence, the number of numbers remaining in $\mathcal{L}$ is

$$\frac{p+1}{2} - \frac{p-1}{8} + 1 = \frac{3p}{8} + \frac{13}{8}.$$

For sufficiently large p, this quantity becomes at most $0.499p$, and so we are done in the case $n = p$ for "sufficiently large" primes p.

Now, if $\{2, p_1, \ldots, p_k\}$ are primes not sufficiently large, then take $N = 4p_1p_2 \ldots p_k$ and set

$$Q(x) = N(2x^2 - 1)^2.$$

This works for $n = 4, p_1, \ldots, p_k$. Now for a composite number n, take any prime factor p of n. Then since polynomials are periodic mod p, hence we find at most $0.499p$ residues mod p. This gives the result for n too.

About the Author

Aditya Khurmi is currently in grade 12th and is a maths enthusiast from India. He has been doing Mathematics Olympiads for the past 4 years, and is an Indian National Mathematical Olympiad (INMO) 2020 awardee

References and Further Reading

[1] Dorin Andrica and Titu Andreescu. *Number Theory: Structures, Examples, and Problems*.

[2] Evan Chen. *Napkin*. URL: https://web.evanchen.cc/napkin.html.

[3] Evan Chen. *Orders Modulo A Prime*. URL: https://web.evanchen.cc/handouts/ORPR/ORPR.pdf.

[4] Evan Chen. *OTIS Excerpts*. URL: https://web.evanchen.cc/excerpts.html.

[5] Evan Chen. *Summation*. URL: https://web.evanchen.cc/handouts/Summation/Summation.pdf.

[6] Evan Chen. *The Chinese Remainder Theorem*. URL: https://web.evanchen.cc/handouts/CRT/CRT.pdf.

[7] Ion Cucurezeanu Dorin Andrica and Titu Andreescu. *An Introduction to Diophantine Equations: A Problem-Based Approach*.

[8] Mathematical Excalibur. *Zsigmondy's Theorem*. URL: https://www.math.ust.hk/excalibur/v16_n4.pdf.

[9] Aditya Khurmi and Satyam Mishra. *AoPS Mock Olympiad "SORY"*. URL: https://artofproblemsolving.com/community/q2h1906972p13051397.

[10] Bart Michels. *Zsigmondy's Theorem*. URL: https://pommetatin.be/files/zsigmondy_en.pdf.

[11] Ayan Nath. *Analytic Number Theory*. URL: https://artofproblemsolving.com/community/c6h2251201.

[12] Waclaw Sierpinski. *250 Problems in Elementary Number Theory*.

[13] Justin Stevens. *Olympiad Number Theory Through Challenging Problems*. URL: https://s3.amazonaws.com/aops-cdn.artofproblemsolving.com/resources/articles/olympiad-number-theory.pdf.

[14] Gabriel Dospinescu Titu Andreescu. *Problems from the Book*.

[15] Zuming Feng Titu Andreescu Dorin Andrica. *104 Number Theory Problems: From The Training Of The Usa Imo Team*.

[16] *Unofficial IMOTC 2020 notes*. URL: https://artofproblemsolving.com/community/c260h2297326.

[17] Wikipedia. *Arithmetic Functions*. URL: https://en.wikipedia.org/wiki/Arithmetic_function.

[18] Qiaochu Yuan. *Square roots have no unexpected linear relationships*. URL: https://qchu.wordpress.com/2009/07/02/square-roots-have-no-unexpected-linear-relationships/.

[19] Yufei Zhao. *Integer Polynomials*. URL: https://yufeizhao.com/olympiad/intpoly.pdf.

