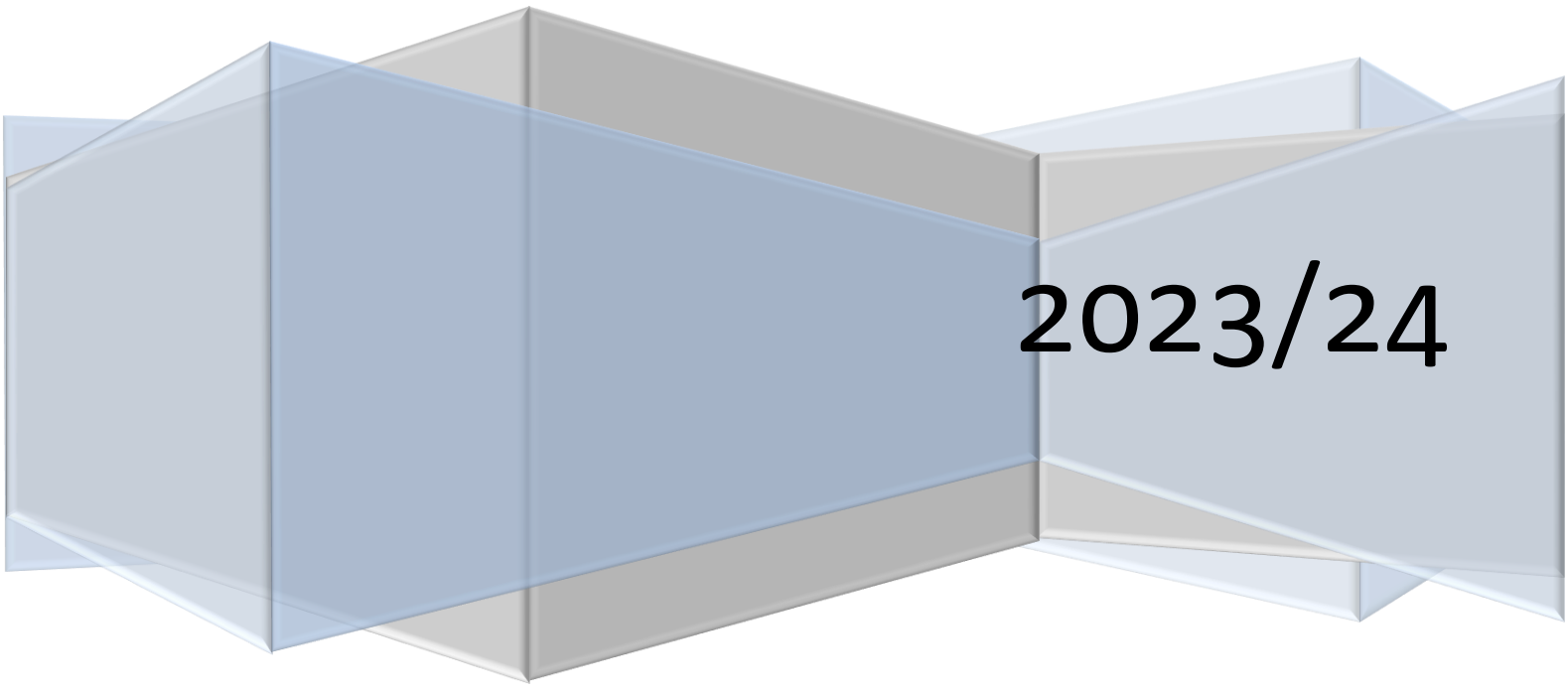
TEORÍA DE OLIMPIADAS MATEMÁTICAS

Nivel Bachillerato (actualizado: 17 Nov -2023)

Editado por Francisco José Valladares Herrera (redacción original de José Miguel Manzano)



INDICE:

TEMA 1: TEORÍA DE NÚMEROS.

Lección 0. Números enteros e inducción matemática

Nuestro principal objeto de estudio son los números naturales, que son los números más sencillos (los que se usan para contar) y que denotaremos por

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, \ldots\}$$

Así, $\mathbb{N}$ es un conjunto en el que se puede sumar y multiplicar, es decir, si sumamos o multiplicamos dos números naturales obtenemos otro número natural. El problema surge cuando queremos restar números naturales: por ejemplo $5 - 3$ es el número natural 2 pero $3 - 5$ no puede ser ningún número natural. Se crea de esta forma la necesidad de ampliar nuestro conjunto de números a los enteros $\mathbb{Z}$, ampliación que consiste en añadir los opuestos de los naturales junto con el cero. Esto lo escribimos como

$$\mathbb{Z} = \{\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}.$$

Aquí no termina la cosa pues, si bien ahora podemos sumar, restar y multiplicar números enteros y el resultado sigue siendo un número entero, no podemos dividir dos números enteros cualesquiera; por ejemplo $21 : 7 = 3$ ó $(-48) : 8 = 6$ son números enteros pero $1 : 2$ no puede ser ningún número entero. Este impedimento vuelve a arreglarse considerando los números racionales o fraccionarios $\mathbb{Q}$, que son los números de la forma $\frac{a}{b}$, donde a y b son números enteros, que se llaman numerador y denominador de la fracción $\frac{a}{b}$ respectivamente. No obstante, no es posible que el denominador sea cero (no se puede dividir por cero), lo que nos lleva a excluirlo como denominador. Con mayor rigor matemático, esto se resume en la siguiente definición

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$$

(se lee: $\mathbb{Q}$ es el conjunto de los números de la forma $\frac{a}{b}$, donde a y b son números enteros y b es distinto de cero). Observemos que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$, es decir, los números naturales están contenidos en los números enteros que, a su vez, están contenidos en los números racionales. Es posible completar este esquema con conjuntos más grandes de números, como los números reales $\mathbb{R}$ ó los números complejos $\mathbb{C}$, pero el objetivo de esta sección se centra en $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$; concretamente en $\mathbb{N}$, de donde pueden obtenerse los demás mediante las cuatro operaciones básicas.

Principio de inducción

La propiedad fundamental que define al conjunto $\mathbb{N}$ es la propiedad de inducción. Esta nos dice que si A es un conjunto de números naturales que cumple que

a. A contiene al uno.

b. Si A contiene a un número n, entonces también contiene a $n + 1$.

Entonces A contiene a todos los números naturales.

Es fácil darse cuenta de por qué este principio es cierto. Supongamos que un conjunto de números naturales A cumple las condiciones (a) y (b) anteriores y cojamos un número natural: el 5, por ejemplo. Para responder a la pregunta de si 5 pertenece a A, razonamos como sigue: según (a) tenemos que $1 \in A$, de que $1 \in A$ deducimos que $2 \in A$ usando ahora (b), volviendo a usar (b) (y como $2 \in A$) tenemos que $3 \in A$; usando (b) dos veces más tenemos que $4 \in A$ y $5 \in A$. Es obvio que este proceso se podría haber hecho con cualquier número natural en lugar de 5, aunque hubiera sido más tedioso escribir todos los pasos.

La principal utilidad del principio de inducción es que nos permite demostrar una gran cantidad de propiedades concernientes a números naturales. Concretamente, si $P(n)$ es una afirmación para cada número natural n y probamos que $P(1)$ es cierta y que si $P(k)$ es cierta también lo es $P(k+1)$, habremos probado que $P(n)$ es cierta para cualquier número natural n. Esto es consecuencia de tomar en el principio de inducción ??? el conjunto A como el conjunto de los números naturales k para los que $P(k)$ es cierta. Veamos cómo se aplica todo esto con un ejemplo.

Ejercicio resuelto

Demostrar que, para cualquier número natural n, se cumple que

$$1+2+\ldots+n=\frac{1}{2}n(n+1).$$

Solución. En este caso, la afirmación $P(n)$ es $1+2+\ldots+n=\frac{1}{2}n(n+1)$; por ejemplo,

$$P(1) \longrightarrow 1=\tfrac{1}{2}\cdot 1\cdot(1+1) \qquad P(2) \longrightarrow 1+2=\tfrac{1}{2}\cdot 2\cdot(2+1)$$
$$P(3) \longrightarrow 1+2+3=\tfrac{1}{2}\cdot 3\cdot(3+1) \qquad P(4) \longrightarrow 1+2+3+4=\tfrac{1}{2}\cdot 4\cdot(4+1)$$

es decir, la fórmula que queremos probar para un valor concreto. $P(1)$ es cierta ya que ambos miembros de la igualdad toman el valor 1. Supongamos que k es un número natural para el que $P(k)$ es cierta, es decir, tal que se cumple que $1+2+\ldots+k=\frac{1}{2}k(k+1)$ y veamos que $P(k+1)$ es cierta, es decir, tendremos que probar que $1+2+\ldots+(k+1)=\frac{1}{2}(k+1)(k+2)$. Observemos que

$$\begin{aligned}1+2+\ldots+(k+1) &= (1+2+\ldots+k)+(k+1)\\ &= \frac{1}{2}k(k+1)+(k+1)=\frac{1}{2}(k+1)(k+2),\end{aligned}$$

lo que nos da la demostración buscada. Obviamente, hemos tenido que usar que $P(k)$ es cierta para probar que también lo es $P(k+1)$ y es por esto que suele llamarse hipótesis de inducción a la suposición de que $P(k)$ es cierta (si no usáramos la hipótesis de inducción, no estaríamos demostrando el enunciado por el principio de inducción).

Conviene aquí resaltar que no es usual ni necesario especificar con tanto detalle las demostraciones en que se usa el método de inducción ni tampoco es necesario usar la variable genérica n y cambiarla a otra variable k cuando se pasa al caso concreto. La solución del problema anterior podría escribirse mucho más resumida pero igualmente válida de la siguiente manera.

Solución. La igualdad es cierta para $n = 1$ pues ambos miembros son iguales a 1. Supuesto que es cierta para $n \in \mathbb{N}$, para $n+1$ tendremos que

$$\begin{aligned} 1 + 2 + \ldots + (n+1) &= (1 + 2 + \ldots + n) + (n+1) \\ &= \frac{1}{2}n(n+1) + (n+1) = \frac{1}{2}(n+1)(n+2), \end{aligned}$$

lo que prueba por inducción la igualdad del enunciado.

Ejercicio propuesto

Comprobar que, para cualquier número natural n, se cumple que

a. $1^2 + 2^2 + \ldots + n^2 = \frac{1}{6}n(n+1)(2n+1)$

b. $1^3 + 2^3 + \ldots + n^3 = \frac{1}{4}n^2(n+1)^2$

c. $1 + x + x^2 + \ldots + x^n = \frac{x^{n+1}-1}{x-1}$ para cualquier número real $x \neq 1$.

Otro caso en el que vamos a usar el principio de inducción y que conviene destacar ahora es el cálculo de la suma de los términos de una progresión aritmética y de una progresión geométrica.

a. Una *progresión aritmética* es una sucesión de números en la que la diferencia entre dos términos consecutivos es constante (por ejemplo, la sucesión $1, 5, 9, 13, 17, \ldots$, donde la diferencia es 4). Las progresiones aritméticas vienen determinadas por el término inicial y la diferencia: si el término inicial es a_1 y la diferencia es d, los siguientes términos serán $a_2 = a_1 + d$, $a_3 = a_2 + d = a_1 + 2d$, $a_4 = a_3 + d = a_1 + 3d$, etc,... y, en general, $a_n = a_1 + (n-1)d$. La suma de los términos de esta sucesión está dada por

$$\begin{aligned} a_1 + (a_1 + d) + \ldots + (a_1 + (n-1)d) &= na_1 + d(1 + 2 + \ldots + (n-1)) \\ &= na_1 + \frac{1}{2}dn(n-1), \end{aligned}$$

donde se ha usado la fórmula del ejercicio resuelto para $1 + 2 + \ldots + n$.

b. Una *progresión geométrica* es una sucesión de números en la que cada término se obtiene multiplicando el anterior por una constante, que se llama *razón* de la progresión (por ejemplo, la sucesión $1, 2, 4, 8, 16, \ldots$, donde la razón es 2). Las progresiones geométricas vienen determinadas por el término inicial y la razón: si el término inicial es a_1 y la razón es r, los siguientes términos serán $a_2 = ra_1$, $a_3 = ra_2 = r^2a_1$, $a_4 = ra_3 = r^3a_1$, etc,... y, en general, $a_n = r^{n-1}a_1$. La suma de los términos de esta sucesión está dada por

$$a_1 + ra_1 + r^2a_1 + \ldots + r^{n-1}a_1 = a_1(1 + r + r^2 + \ldots + r^{n-1}) = a_1\frac{r^n - 1}{r-1} = \frac{a_{n+1} - a_1}{r-1},$$

donde se ha usado la fórmula del apartado c del ejercicio propuesto anteriormente.

Lección 1. Divisibilidad

Definición de divisibilidad, divisor y múltiplo

Dados $a, b \in \mathbb{Z}$, diremos que a divide a b (ó que a es un divisor de b ó que b es un múltiplo de a) cuando exista $q \in \mathbb{Z}$ de forma que $b = aq$. Lo denotaremos por $a|b$.

A continuación recogemos algunas propiedades elementales de la divisibilidad de números, cuya comprobación es inmediata y se deja como ejercicio. Dados $a, b, c \in \mathbb{Z}$, demostrar que

- Si $a|b$, entonces $|a| \leq |b|$.
- Si $a|b$ y $b|c$, entonces $a|c$.
- Si $a|b$ y $a|c$, entonces $a|(b+c)$.
- Si $a|b$, entonces $a|bx$ para cualquier $x \in \mathbb{Z}$.

Algunos casos concretos de divisibilidad conviene tenerlos en cuenta pues dan lugar a algunas confusiones.

- Todos los números enteros dividen a cero, mientras que cero sólo se divide a sí mismo. Esto se deduce directamente de la definición.
- 1 y -1 dividen a cualquier número pero los únicos números que dividen a 1 y -1 son ellos mismos. Es fácil probarlo a partir de las propiedades anteriores.

Con la propia definición no es fácil saber si un número divide o no a otro ya que tendríamos que ir multiplicándolo sucesivamente por números para ver si nos da el segundo número. Necesitamos un proceso que nos muestre si es divisible o no.

División euclídea

Dados $a, b \in \mathbb{Z}$, existen $q, r \in \mathbb{Z}$ tales que $0 \leq r < b$ y

$$a = q \cdot b + r$$

Los números q y r son únicos cumpliendo estas relaciones. Al número q se le llama cociente y a r resto de la división euclídea de a entre b.

Demostración. Hagamos la demostración cuando $a, b > 0$ (los otros casos los dejamos como ejercicio). Consideremos $R = \{a - tb \geq 0 : t \in \mathbb{Z}\}$. Claramente $a = a - 0b \in R$ luego R no es vacío y tiene un elemento mínimo, que llamaremos $r = \min R$. Como $r \in R$, existirá $q \in \mathbb{Z}$ tal que $r = a - qb$, es decir, $a = qb + r$. Bastará ver que $r < b$, pero si $r \geq b$, entonces $0 \leq r - b = a - (q+1)b \in R$ contradiciendo que r es el elemento mínimo de r. Para probar que r y q son únicos, supongamos que pudiéramos escribir $a = qb + r$ y $a = q'b + r'$ con $0 \leq r, r' < b$ y demostremos que tiene que ocurrir que $r = r'$ y $q = q'$. Restando las expresiones anteriores obtenemos $0 = (q - q')b + (r - r')$, de donde $r - r'|b$, pero $|r - r'| < b$, de donde necesariamente $r - r' = 0$ y tenemos que $0 = (q - q')b$ luego $q - q' = 0$ ya que $b \neq 0$.

A partir de la proposición es fácil comprobar que a es divisible entre b si, y sólo si, el resto de la división de a entre b es cero. Además, la división euclídea se puede calcular mediante el algoritmo que todo el mundo aprende en el colegio. Por ejemplo, para dividir 4528 entre 7, tenemos que

$$\begin{array}{rrrrrrrr} 4 & 5 & 8 & 2 & & 7 & & \\ & 3 & 8 & & & 6 & 5 & 4 \\ & & 3 & 2 & & & & \\ & & & \underline{4} & & & & \end{array} \quad \Longrightarrow \quad 4582 = 654 \cdot 7 + 4$$

luego el cociente de la división euclídea es 654 y el resto es 4.

Visto esto, ¿qué ocurre con la división de números negativos? Observemos que, si dividimos 8 entre 5, tenemos cociente 1 y resto 3, es decir, $8 = 1 \cdot 5 + 3$. Si intentamos dividir -8 entre 5, podemos estar tentados de escribir $(-8) = (-1) \cdot 5 + (-3)$ y decir que el cociente es -1 y el resto -3 pero ¡el resto tiene que estar entre 0 y 4! Para corregir esto, intuitivamente quitamos una unidad al cociente y arreglamos el resto, es decir, $(-8) = (-2) \cdot 5 + 2$ luego el cociente es -2 y el resto 2.

La noción de divisibilidad nos conduce directamente a preguntarnos cuáles son los divisores de un número. Hasta la próxima sección no vamos a poder responder de forma precisa a esta pregunta; necesitaremos antes una herramienta que nos explique cómo son los divisores comunes a dos números. Observemos que 1 siempre es un divisor común a cualquier par de números y todo divisor es menor en valor absoluto que cualquiera de los dos números, lo que nos dice que siempre habrá un mayor divisor común.

Definición de máximo común divisor y mínimo común múltiplo

Dados $a, b \in \mathbb{N}$, se llama máximo común divisor de a y b al mayor número natural d que cumpla que $d|a$ y $d|b$ y lo denotaremos por $\mathrm{mcd}(a, b)$. Se llama mínimo común múltiplo de a y b al menor número natural m que cumpla que $a|m$ y $b|m$, y lo denotaremos por $\mathrm{mcm}(a, b)$.

Identidad de Bézout

Dados $a, b \in \mathbb{Z}$ y $d = \mathrm{mcd}(a, b)$, existen $u, v \in \mathbb{Z}$ tales que

$$d = au + bv.$$

Demostración. Lo demostraremos sólo para el caso $a, b > 0$ pues los demás casos se deducen fácilmente a partir de este. Consideremos $D = \{as + bt : s, t \in \mathbb{Z}\}$ y $D^+ = \{x \in D : x > 0\}$. Entonces D^+ es no vacío (ya que $a = a \cdot 1 + b \cdot 0 \in D^+$) y podemos considerar $h = \min D^+ > 0$, que podremos escribir como $h = au + bv$ para ciertos $u, v \in \mathbb{Z}$. Veamos que $h = d$ y habremos terminado la demostración. Por un lado, tenemos que $d|a$ y $d|b$ por ser un divisor común luego $d|h = au + bv$ luego $d \leq h$ y será suficiente probar que $h|a$ y $h|b$. Si a no fuera divisible por h, haciendo la división euclídea de a entre h, existirán $q, r \in \mathbb{N}$ tales que $0 < r < h$ y $a = qh + r$ luego $0 < r = a - qh = (1 - qu)a - qbv$ lo que nos llevaría a que $r \in D^+$ y $r < h$, contradiciendo que h es el mínimo. Esta contradicción nos dice que a tiene que ser divisible por h y, de la misma forma, se razona que b también tiene que serlo, luego h es un divisor común de a y b.

Para concluir las generalidades sobre el máximo común divisor, damos un método bastante rápido para calcularlo. Este método se basa en la siguiente propiedad útil en la práctica, cuya demostración se deja como ejercicio.

Ejercicio propuesto

Si tenemos dos números $a, b \in \mathbb{N}$ y hacemos su división, obtenemos $q, r \in \mathbb{N}$ tales que $a = bq + r$ y $0 \leq r < b$. Demostrar que $\text{mcd}(a, b) = \text{mcd}(b, r)$.

Algoritmo de Euclides

Sean $a, b \in \mathbb{Z}$ con $a, b > 0$ y definimos la sucesión $\{r_n\}$ como $r_1 = a$, $r_2 = b$ y tal que, para $n \geq 3$, r_n es el resto de dividir r_{n-2} entre r_{n-1}. Entonces, existe un primer término nulo r_N y se cumple que $\text{mcd}(a, b) = r_{N-1}$.

Demostración. Mientras r_{n-2} sea distinto de cero, la condición de que r_n sea el resto de dividir r_{n-1} entre r_{n-2} nos asegura que $r_n < r_{n-1}$. Como los restos son todos números naturales, necesariamente habrá un primer término r_N nulo (no puede haber una sucesión descendente infinita de números naturales por el principio del mínimo). Además, el ejercicio anterior aplicado a este caso nos asegura que

$$\begin{aligned}\text{mcd}(a, b) &= \text{mcd}(r - 1, r_2) = \text{mcd}(r_2, r_3) = \ldots = \text{mcd}(r_{N-2}, r_{N-1}) \\ &= \text{mcd}(qr_{N-1}, r - N - 1) = r_{N-1}\end{aligned}$$

ya que, al ser $r_N = 0$, la división euclídea nos dice que $r_{N-2} = qr_{N-1} + 0$ para algún $q \in \mathbb{N}$.

Por ejemplo, si queremos hallar $\text{mcd}(96, 348)$, procedemos de la siguiente manera:

- Dividimos 348 entre 96 y obtenemos $324 = 3 \cdot 96 + 60$: el resto es 60.
- Dividimos 96 entre 60 y obtenemos $96 = 1 \cdot 60 + 36$: el resto es 36.
- Dividimos 60 entre 36 y obtenemos $60 = 1 \cdot 36 + 24$: el resto es 24.
- Dividimos 36 entre 24 y obtenemos $36 = 1 \cdot 24 + 12$: el resto es 12.
- Dividimos 24 entre 12 y obtenemos $24 = 2 \cdot 12 + 0$: el resto es 0. Como este último resto es el primer resto cero, llegamos a que $\text{mcd}(348, 96) = 12$, el último resto no nulo.

Para calcular el mínimo común múltiplo de dos números no hay un método tan directo. Sin embargo, la siguiente fórmula, válida para cualesquiera $a, b \in \mathbb{Z}$, nos permite calcularlo a partir del máximo común divisor:

$$\text{mcd}(a, b) \cdot \text{mcm}(a, b) = a \cdot b.$$

Veremos una forma sencilla de demostrarlo cuando hablemos de factorizaciones, aunque quien se atreva que la demuestre ahora.

Ejercicio propuesto

Mediante el algoritmo de Euclides, calcular $\text{mcd}(a, b)$ en los siguientes casos:

a. $a = 48$, $b = 72$
b. $a = 2463$, $b = 1246$
c. $a = 32768$, $b = 16554$
d. $a = 14511644$, $b = 8292368$

Lección 2. Números primos y factorizaciones

Nuestro principal objetivo es determinar de alguna forma sencilla los divisores de un número. Sabemos que todo número $n \in \mathbb{Z}$ tiene por lo menos cuatro divisores enteros: ± 1 y $\pm n$. Si éstos fueran los únicos (como por ejemplo para $n = 2$), el número sería lo más sencillo posible en lo que se refiere a divisibilidad A estos números se les llama números primos, nombre que proviene de *número primero* y es que los números primos son los ladrillos fundamentales de los números enteros. Esto quedará claro una vez que veamos el Teorema fundamental de la aritmética.

Definición de número primo

Un número $p \in \mathbb{N}$ se dice primo cuando tenga exactamente dos divisores positivos, es decir, 1 y p. En caso contrario, diremos que p es compuesto.

Es importante darse cuenta que el número 1 no es un número primo porque tiene sólo un divisor positivo: el propio 1. En general, se puede hablar también de primos negativos: $-p$ es primo si, y sólo si, p es primo. En la siguiente tabla podemos los cien primeros números primos positivos:

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541

Si observas la tabla, pronto descubrirás que no hay ninguna regla sencilla que te permita pasar de un primo al siguiente y es que realmente no se conoce ninguna forma sencilla de generar los números primos. ¿Qué hay que hacer entonces para ver si un número es primo? Pues no queda otra opción que comenzar a dividirlo por otros números más pequeños a ver si la división es o no exacta. Tendríamos que probar con todos los números menores que el número, pero esto se puede acortar un poco y lo vamos a ver con un ejemplo. Imaginemos que tenemos el número 7919 y queremos ver si es primo: lo dividimos porn 2, por 3, por 4, y así sucesivamente (en cuanto veamos el Teorema fundamental de la aritmética veremos que sólo hace falta probar con los primos). Vemos que no nos sale exacta la división por ningún número, pero cuando llegamos a dividir por 88 obtenemos cociente 89 y resto 87 y, cuando dividimos por 89, obtenemos cociente 88 y resto 87. No nos ha salido ninguna división exacta pero el cociente empieza a ser menor que el divisor: evidentemente ya no nos saldrá ninguna porque si $7919 = a \cdot b$ y $a > 89$, entonces $b < 89$ y nos tendría que haber salido el factor b antes. Por tanto, 7919 es primo (es el primo número 1000). Todo esto se resume en la siguiente regla.

Regla para calcular números primos

Si un número $n \in \mathbb{N}$ es compuesto, entonces tiene un divisor d tal que $1 < d \leq \sqrt{n}$.

Los números primos son los más sencillos en todo lo que a productos y divisibilidades se refiera. Vamos a probar que todo número entero se puede expresar de forma única como producto de primos, pero antes necesitaremos una propiedad importante.

Lema

Si $p \in \mathbb{N}$ es un número primo y $a, b \in \mathbb{Z}$ cumplen que $p|ab$, entonces $p|a$ ó $p|b$.

Demostración. Supongamos que $a, b \in \mathbb{N}$ cumplen que $p|ab$ y p no divide a b y probemos que $p|a$. En efecto, en tal caso $\text{mcd}(p, b)$ es un divisor de p que no puede ser p (ya que en tal caso $p|b$) luego $\text{mcd}(p, b) = 1$ y, por la identidad de Bézout, existen $u, v \in \mathbb{Z}$ tales que $1 = pu + bv$ luego $a = apu + abv$. Como $p|abv$ y $p|apu$, tenemos que $p|a$.

Teorema fundamental de la aritmética

Todo número natural mayor que uno se puede expresar de forma única como producto de primos (salvo reordenación de éstos).

Demostración.

Para probar la existencia procedamos por inducción. Es obvio que 2 es un número primo luego cumple el enunciado. Supuesto que todo número menor que $n > 2$ pueda expresarse de tal manera, consideremos n. Si n es primo habremos acabado pero si no es primo es porque existen $a, b \in \mathbb{N}$ tales que $n = ab$ y $1 < a, b < n$, en cuyo caso aplicamos la hipótesis de inducción a a y a b obteniendo números primos $p_1, \ldots, p_r$ y $q_1, \ldots, q_s$ tales que $a = p_1 \cdots p_r$ y $b = q_q \cdots q_s$, de donde $n = p_1 \cdots p_r q_1 \cdots q_s$ y hemos expresado n como producto de primos.

Para la unicidad, supongamos que tenemos expresado $n = p_1 \cdots p_r = q_1 \cdots q_s$ de dos formas como producto de primos. Entonces $p_1|n = q_1 \cdots q_s$ de donde por el lema previo existe $i_1 \in \{1, \ldots, s\}$ tal que $p_1|q_{i_1}$ luego como $p_1 \neq 1$ tenemos que $p_1 = q_{i_1}$ y podemos cancelarlo en la expresión de n obteniendo $p_2 \cdots p_r = q_1 \cdots q_{i_1-1} q_{i_1+1} q_s$. Ahora repetimos el proceso con p_2, p_3, etc. Es claro así que debe ocurrir que $r = s$ y existe una permutación $i_1, \ldots, i_r$ de los números $1, \ldots, r$ tal que $p_k = q_{i_k}$ para cualquier k.

Si agrupamos todos los factores primos iguales de un número $n > 1$, podemos escribirlo de forma única como

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

donde los p_i son primos distintos y los exponentes e_i números naturales. A una expresión de esta forma la llamaremos descomposición de n en factores primos y sabemos que siempre existe.

Vamos a demostrar ahora uno de los resultados más conocidos de Euclides que nos asegura que hay tantos primos como queramos.

Proposición (Euclides)

Existen infinitos números primos.

Demostración. Razonando por contradicción, supongamos que hay un número finito de primos, pongamos $p_1, \ldots, p_n$ y consideremos el número natural $N = p_1 p_2 \cdots p_n + 1$. Ahora bien, N no puede ser primo pues es mayor que cualquier p_k, de donde deducimos que es producto de primos, pero ninguno de los anteriores divide a N (en tal caso dividirían a $N - p_1 \cdots p_n = 1$) y hemos llegado a una contradicción.

Vamos a aplicar la misma técnica a otro caso parecido.

Ejercicio resuelto

Existen infinitos primos de la forma $4k+3$.

Solución. Siguiendo el razonamiento de Euclides, supongamos que hay un número finito $p_1, \ldots, p_n$ y consideremos el número $N = p_1 \cdots p_n + 2$ si n es par ó $N = p_1 \cdots p_n + 4$ si n es impar. En cualquier caso, como el producto de dos números de la forma $4k+3$ es de la forma $4k+1$ y el producto de un número de la forma $4k+1$ con otro de la forma $4k+3$ vuelve a ser de la forma $4k+3$ (demostrarlo), N siempre es de la forma $4k+3$ y, como el producto de dos números de la forma $4k+1$ vuelve a ser de esta forma, de entre los factores primos de N tiene que haber alguno de la forma $4k+3$, es decir, algún p_k, pero entonces llegamos a una contradicción porque tal p_k tendría que dividir o bien a 2 o bien a 4, dependiendo de si n es par o impar, y todos los p_k son impares.

Números primos entre sí

Hasta ahora hemos hablado de números primos y de cómo estos ayudan a comprender la estructura de todos los números. No obstante, a veces es útil hablar de números que son primos con otros números, lo que significa que los números en cuestión no tienen divisores comunes distintos de ± 1 o bien que su máximo común divisor es 1.

Definición de números primos entre sí

Dos números $a, b \in \mathbb{Z}$ son primos entre sí (o primos relativos) cuando $\text{mcd}(a,b) = 1$, es decir, cuando no tengan divisores primos comunes.

Como la misma definición dice, si $a, b \in \mathbb{Z}$ son primos entre sí, entonces no tienen factores primos comunes luego si descomponemos $a = p_1^{e_1} \cdots p_r^{e_r}$ y $b = q_1^{f_1} \cdots q_s^{f_s}$, donde $p_1, \ldots, p_s, q_1, \ldots, q_s$ son números primos y los exponentes son naturales, entonces ninguno de los factores primos p_i puede ser igual a uno de los factores q_j, es decir, las descomposiciones son disjuntas.

Si ahora a y b no son primos entre sí, entonces $d = \text{mcd}(a,b) > 1$, pero siempre podemos considerar $a' = \frac{a}{d}$ y $b' = \frac{b}{d}$. Estos nuevos números a' y b' sí son primos entre sí como puedes comprobar pues hemos eliminado todos los factores comunes. Esto no es nada nuevo pues es lo que se hace normalmente al simplificar una fracción: si tenemos el número racional $\frac{a}{b}$ (siempre que $b \neq 0$), entonces podemos multiplicar el numerador y el denominador simultáneamente por el número (distinto de cero) que queramos luego, si los multiplicamos por $\frac{1}{d}$, llegamos a la nueva fracción $\frac{a'}{b'}$, donde $\text{mcd}(a', b') = 1$. Esta fracción no puede simplificarse más y la llamamos fracción *irreducible*. Observa que las siguientes afirmaciones son equivalentes:

- a y b son primos entre sí.
- $\text{mcd}(a,b) = 1$
- No hay ningún primo p que divida a a y a b.
- La fracción $\frac{a}{b}$ es irreducible.

Ejercicio resuelto

Determina los valores de n para los que la siguiente fracción es irreducible:

$$\frac{2n+3}{3n+1}.$$

Solución. Queremos hallar los valores de n para los que $\mathrm{mcd}(2n+3, 3n+1) = 1$. El truco está en transformar este máximo común divisor usando que $\mathrm{mcd}(a,b) = \mathrm{mcd}(a, b-qa)$, es decir, a uno de los dos miembros podemos restarle un múltiplo del otro sin que varíe el máximo común divisor. Haciendo esto, podemos escribir

$$\mathrm{mcd}(2n+3, 3n+1) = \mathrm{mcd}(2n+3, n-2) = \mathrm{mcd}(7, n-2)$$

luego el máximo común divisor buscado es 1 ó 7 ya que estos son los divisores positivos de 7. A la vista de lo anterior, será 7 cuando $n-2$ sea múltiplo de 7, es decir, cuando n sea de la forma $7k+2$. Deducimos que la fracción es irreducible si, y sólo si, n no es de la forma $7k+2$.

Algunas aplicaciones de la factorización

Vamos a usar la descomposición de un número en factores primos para calcular el número de divisores de un número y la suma de éstos.

Supongamos que n es un número natural y lo descomponemos en factores primos como $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, donde sabemos que $p_1, \ldots, p_r$ son números primos distintos y $e_1, \ldots, e_r$ son números naturales. Entonces, si d es un divisor de n, se cumplirá que $n = d \cdot d'$ para cierto $d' \in \mathbb{N}$ (que también es divisor de n). Factorizando d y d' y multiplicando sus factorizaciones, llegamos a que d y d' tienen que tener los mismos factores primos que n, es decir, $d = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$ y $d' = p_1^{f_1'} p_2^{f_2'} \cdots p_r^{f_r'}$, donde cada f_k puede ser cero y $f_k + f_k' = e_k$. Por tanto, los divisores de n son los números de la forma

$$p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}, \text{ donde } 0 \le f_k \le e_k.$$

De aquí podemos sacar algunas conclusiones.

a. Si tenemos factorizado $n = p_1^{e_1} \cdots p_r^{e_r}$, cada divisor de n se corresponde con elegir $f_1, \ldots, f_r$ tales que $0 \le f_k \le e_k$ para $1 \le k \le r$. Por lo tanto, f_1 puede tomar los valores $0, 1, \ldots, e_1$ (un total de $e_1 + 1$ posibilidades), f_2 puede tomar los valores $0, 1, \ldots, e_2$ (un total de $e_2 + 1$ posibilidades) y así con todos los f_k. En consecuencia, el número total de divisores de n (que es el número total de posibilidades) es

$$\text{Número de divisores de } n \ \to \ (e_1+1)(e_2+1)\cdots(e_r+1).$$

b. Otra forma más ingeniosa de ver los divisores de n es que cada divisor de n es uno de los monomios que surgen al desarrollar el siguiente producto:

$$(1 + p_1 + p_1^2 + \cdots + p_1^{e_1})(1 + p_2 + p_2^2 + \cdots + p_2^{e_2}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{r_2})$$

(recordemos que el *producto de paréntesis* se puede hacer como la suma de los productos de elegir en cada uno de los paréntesis uno de los sumandos). Esta forma de ver los sumandos tiene la ventaja de que el valor de la expresión anterior es realmente la suma de todos los divisores de n y que cada paréntesis es la suma de los términos de una progresión geométrica. Por tanto, usando la fórmula de la suma de los términos de una progresión geométrica, podemos expresar la suma de los divisores de n como

$$\text{Suma de divisores de } n \ \to \ \frac{p_1^{e_1}-1}{p_1-1} \cdot \frac{p_2^{e_2}-1}{p_2-1} \cdots \frac{p_r^{e_r}-1}{p_r-1}.$$

Veamos cómo aplicar esto al caso de $n = 2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$. Como los exponentes son 3, 2, 1 y 1, el número de divisores de 2520 es $(3+1)\cdot(2+1)\cdot(1+1)\cdot(1+1) = 48$ y la suma de éstos es $(1+2+4+8)(1+3+9)(1+5)(1+7) = 15 \cdot 13 \cdot 6 \cdot 8 = 9360$.

También tenemos la siguiente regla conocida para hallar el máximo común divisor y el mínimo común múltiplo a partir de la factorización.

Cálculo del máximo común divisor y del mínimo común múltiplo

Supongamos que $a = p_1^{e_1} \cdots p_r^{e_r}$ y $b = p_1^{f_1} \cdots p_r^{f_r}$ son dos números naturales descompuestos como producto de números primos y exponentes mayores o iguales que cero. Entonces,

$$\mathrm{mcd}(a,b) = p_1^{\min(e_1,f_1)} \cdot p_2^{\min(e_2,f_2)} \cdots p_r^{\min(e_r,f_r)},$$

$$\mathrm{mcm}(a,b) = p_1^{\max(e_1,f_1)} \cdot p_2^{\max(e_2,f_2)} \cdots p_r^{\max(e_r,f_r)}.$$

donde $\min(e_i, f_i)$ es el más pequeño de los números e_i y f_i y $\max(e_i, f_i)$ el más grande.

La demostración la dejamos al lector pero antes observemos que el máximo común divisor coincide con la regla *comunes elevados al menor exponente* y el mínimo común múltiplo con *comunes y no comunes elevados al mayor exponente*.

Para terminar, simplemente comentar que el método de la factorización es un buen método teórico en general pero en la práctica es muy deficiente porque es muy difícil factorizar un número medianamente grande (es el mismo problema que tenemos para saber si un número es primo o no). Para convencernos, dejamos el siguiente ejercicio: calcular el máximo común divisor de 62773913 y 77075627 primero intentando factorizar y después mediante el algoritmo de Euclides... ¡Suerte!.

Lección 3. Los números y sus dígitos

Hay muchos problemas en los que se relacionan los números y las cifras que lo representan en el sistema decimal. Es importante empezar recordando que un número y sus cifras son dos cosas distintas. El número 1878 tiene tres cifras: el 1, el 8, el 7 y el 8, que son cuatro números que tienen sentido por sí mismos y pueden estar sujetos a otras operaciones en las que no interviene el número 1878. Por ejemplo, la suma de las cifras es $1+8+7+8=24$ y, para hallarla, no hemos usado el 1878 en ningún cálculo. Sabemos también que el sistema decimal es posicional y a cada cifra le corresponde un orden (unidades, decenas, centenas,...), de forma que el 1878 se recupera a partir de sus cifras como

$$1878 = 1\cdot 1000 + 8\cdot 100 + 7\cdot 10 + 8.$$

Con esta expresión se puede escribir matemáticamente la relación entre un número y sus cifras, lo que permite abordar la mayoría de los problemas de este tipo. Más explícitamente, un número natural N de k cifras se puede expresar como

$$N = 10^{k-1}a_{k-1} + 10^{k-2}a_{k-2} + \ldots + 100a_2 + 10a_1 + a_0$$

y cada dígito $a_{k-1}, a_{k-2}, \ldots, a_2, a_1, a_0$ es un número entre 0 y 9. Usualmente se suele tomar $a_{k-1}\neq 0$, en cuyo caso decimos que k es el número de cifras de N.

Ejercicio resuelto

Con tres dígitos distintos se forman seis números distintos de tres cifras. Si se suman los seis números resulta 4218. Si se ordenan los seis números, la suma de los tres mayores menos la suma de los tres menores resulta 792. Halla los tres dígitos.

Solución

Pongamos que los dígitos son a, b y c y cumplen que $a>b>c$. Por tanto, los seis números ordenados de mayor a menor son

$$\begin{aligned} 100a+10b+c > 100a+10c+b > 100b+10a+c \\ > 100b+10c+a > 100c+10a+b > 100c+10b+a. \end{aligned}$$

La suma de los seis números es

$$4218 = 100(2a+2b+2c)+10(2a+2b+2c)+(2a+2b+2c) = 222(a+b+c),$$

de donde deducimos que $a+b+c=19$. La suma de los tres mayores menos la suma de los tres menores es

$$792 = 100(2a-2c)+(2c-2a) = 198(a-c),$$

luego llegamos a que $a-c=4$. Distinguimos casos:

- Si $a = 9$, entonces $c = 5$ y, para que $a + b + c = 19$, tendríamos que $b = 5$, pero los dígitos tienen que ser distintos.
- Si $a = 8$, entonces $c = 4$ y, usando que $a + b + c = 19$, obtenemos que $b = 7$. Esta es una solución válida.
- Si $a \leq 7$, entonces $b \leq 6$ y $c \leq 3$, lo que nos da $a + b + c \leq 16$ y no puede ser que $a + b + c = 19$.

Deducimos que los dígitos son 8, 7 y 4.

A la hora de hacer operaciones elementales con números (sumas, restas, multiplicaciones y divisiones), usamos los dígitos en los distintos algoritmos. Podemos usar estos algoritmos para obtener información sobre los dígitos.

Ejercicio resuelto

Hallar el último dígito antes de la cola de ceros del número

$$19! + 20! + 21! + \ldots + 96! + 97!$$

(Olimpiada Matemática Argentina 1997, fase regional, problema 3)

Solución

El término $19!$ termina con tres ceros ya que es múltiplo de 1000 (es múltiplo de $4 \cdot 5 \cdot 10 \cdot 15 = 3000$). Como 5, 10 y 15 son los únicos factores múltiplos de 5, el número $19!$ no puede ser múltiplo de $10000 = 2^4 5^4$, luego no termina en más de tres ceros. Ahora bien, la siguiente cifra en $19!$ tras estos tres ceros es el producto de las cifras de las unidades del resto de los factores:

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 6 \cdot 7 \cdot 9 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 3 \cdot 16 \cdot 17 \cdot 18 \cdot 19,$$

Multiplicando las cifras de las unidades de los números anteriores, llegamos a que esta es 2, es decir, las últimas cuatro cifras de $19!$ son 2000. Finalmente, observamos que todos los números $20!$, $21!$,..., $97!$ tienen más ceros finales que $19!$ ya que tienen, al menos, un factor 20 adicional. Por tanto, las cuatro últimas cifras del número del enunciado son las mismas que las de $19!$, es decir, la solución al problema es 2.

Trabajando en otras bases

En todo lo anterior, el número 10 se llama *base* y juega un papel fundamental ya que los números se expresan como combinaciones de potencias de 10. El sistema posicional se ha consolidado porque con él podemos hacer algorítmicamente la mayoría de las operaciones y porque además permite representar números tan grandes como queramos. (Por ejemplo, ¿serías capaz de dividir MMMCDLXXXIII entre IX en números romanos sin pasar por los decimales? Investiga cómo lo hacían los romanos, si te interesa el tema.) Sin embargo, usar

la base 10 es simplemente un convenio que se heredó de las tradiciones india y arábe. Observa que también se usan otras bases como la base 2 (binario), la base 8 (octal) y la base 16 (hexadecimal) en informática.

El concepto de base es muy simple si has entendido la base 10: un número $N \geq 1$ tiene dígitos $a_{k-1}, a_{k-2}, \ldots, a_2, a_1, a_0$ en base $b \geq 2$ cuando se puede escribir como

$$N = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \ldots + a_2b^2 + a_1b + a_0.$$

siendo los dígitos números entre 0 y $b-1$. Lo indicaremos utilizando un subíndice entre paréntesis. Esto quiere decir que, en base 2, todos los números se escriben con dígitos 0 y 1, en base 3 con dígitos 0, 1 y 2, y así sucesivamente. Por ejemplo, el número $201221_{(3)}$ es un número escrito en base 3, que no es más que el número

$$201221_{(3)} = 2 \cdot 3^5 + 0 \cdot 3^4 + 1 \cdot 3^3 + 2 \cdot 3^2 + 2 \cdot 3^1 + 1 \cdot 3^0 = 538.$$

Es importante darse cuenta de que $201221_{(3)}$ y 538 son el mismo número natural que simplemente está en dos formas diferentes. El resultado clave para entender las bases de numeración es el siguiente:

Ejercicio propuesto

Responde razonadamente a las siguientes preguntas:

a. ¿Cómo se escribe el número $10202_{(3)}$ en base 5?

b. Si $73_{(b)}$ es exactamente el doble de $37_{(b)}$, ¿cuál es el valor de la base b?

c. ¿Cuál es la menor base $b > 10$ para la que $36_{(b)}$ es un cuadrado perfecto? ¿Y la menor base b para la que $37_{(b)}$ no es un número primo?

d. Si número natural se escribe como $xyy_{(7)}$ y como $yxx_{(6)}$, ¿cuál es el valor de los dígitos x e y?

e. Un número de tres cifras en base 104, *seescribecomo*xyz_{(7)}*ycomo*zyx_{(9)}$. ¿Cuál es el número?

Teorema fundamental de la numeración

Todo entero $N \geq 1$ se expresa de forma única como

$$N = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \ldots + a_2b^2 + a_1b + a_0,$$

siendo $a_{k-1}, a_{k-2}, \ldots, a_2, a_1, a_0$ enteros entre 0 y $b-1$.

La demostración anterior nos da de hecho una forma de pasar un número en base 10 a una base cualquiera b sin más que hacer divisiones euclídeas. Vamos a verlo con el número 538 (que hemos visto hace un momento que se expresa como $201221_{(3)}$).

- Dividimos 538 entre 3: cociente 179, resto 1.
- Dividimos 179 entre 3: cociente 59, resto 2.
- Dividimos 59 entre 3: cociente 19, resto 2.
- Dividimos 19 entre 3: cociente 6, resto 1.
- Dividimos 6 entre 3: cociente 2, resto 0.
- Dividimos 2 entre 3: cociente 0, resto 2.

Como el cociente es 0, hemos terminado. Ordenando, los restos obtenidos en sentido opuesto, tenemos el número $201221_{(3)}$.

En realidad, no es usual ver problemas de olimpiada en los que directamente se habla de expresiones en bases distintas (ya que se basa en conocimientos específicos que los participantes pueden no conocer), pero existen problemas en los que cambiar de base puede suponer una ayuda fundamental o en los que conocer la idea de cambio de base nos puede dar una idea feliz.

Ejercicio resuelto

Supongamos que $p(x)$ es un polinomio desconocido cuyos coeficientes son números naturales. Tenemos un programa de ordenador en el que podemos escribir un número n y nos devuelve el resultado $p(n)$. ¿Cuántos números tenemos que suministrarle al programa para poder determinar cualquier polinomio con la información que nos devuelve?

Solución

Con dos valores es suficiente para determinar el polinomio en general. Supongamos que tenemos un polinomio dado por $p(x) = a_0 + a_1x + \ldots + a_nx^n$ y queremos determinar $a_0, a_1, \ldots, a_n$ (y el propio n).

El primer número que le pasamos al programa es el 1, que nos devuelve la suma $S = P(1)$ de todos los coeficientes. En particular, todos los coeficientes son menores o iguales que S. Supongamos que $10^k > S$, es decir, tomamos una potencia de 10 mayor que S. Al evaluar $P(10^k)$ obtenemos

$$P(10^k) = a_0 + 10^k a_1 + 10^{2k} a_2 + \ldots + 10^{nk} a_n.$$

Este número contiene una copia de cada coeficiente separados en grupos de k dígitos. Por ejemplo, si $p(x) = 12 + 3x + 88x^2 + x^4$, evaluamos $p(1) = 104$ y seguidamente evaluamos $p(1000) = 1000088003012$, donde claramente se ven los coeficientes.

Lección 4. Congruencias

Si has seguido las lecciones anteriores de Teoría de Números, habrás observado que el quid de la divisibilidad se halla en la división euclídea ya que un número entero a es divisible entre otro número entero b si el resto de la división euclídea es exactamente cero. Es por ello interesante saber calcular el resto de la división y, de alguna forma ver como se comporta éste respecto a ciertas operaciones. Por ejemplo, sabemos que el resto de dividir 1003 entre 9 es igual a 4, luego si restamos 4 al número 1003, resulta 999, que tiene resto cero al dividirlo entre 9. Como veremos más adelante, el resto de la diferencia estará muy relacionado con la diferencia de los restos.

Para empezar, vamos a observar la siguiente tabla donde escribimos los restos de 16 enteros consecutivos al dividirlos entre 2, 3 y 5, respectivamente:

	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9
resto entre 2	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
resto entre 3	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
resto entre 5	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4

Si nos fijamos, en cada fila los restos se van repitiendo periódicamente y el resto oscila entre 0 y una unidad menos que el divisor. Recuerda cómo hay que dividir un número negativo para preservar esta regla del resto (por ejemplo, para dividir -6 entre 5, el cociente es -2 y el resto 4 porque el resto nunca puede ser negativo).

Entonces, generalizando este resultado, los posibles restos de dividir entre m son $0, 1, 2, \ldots, m-1$ y son cíclicos pues cuando sumamos una unidad a un número de resto $m-1$ vuelve a aparecer el resto 0, es decir, los restos se repiten de m en m. Es por ello que dos números tienen el mismo resto al dividirlos entre m si su diferencia es un múltiplo de m. En tal caso diremos que son congruentes módulo m.

Definición de congruencia

Dados $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}$, diremos que a y b son congruentes módulo m cuando tengan el mismo resto al dividirlos entre m, es decir, cuando $b-a$ sea un múltiplo de m. Para resumir esta información, simplemente escribiremos $a \equiv b \pmod{m}$.

Es importante que te pares un momento a pensar bien la definición y, una vez lo hayas hecho, intentes demostrar que las siguientes congruencias son ciertas:

- $17 \equiv 3 \pmod{7}$
- $1545 \equiv 5 \pmod{10}$
- $12345678 \equiv 0 \pmod{9}$
- $-145 \equiv -4 \equiv 43 \pmod{47}$

Operaciones con congruencias

Nuestra intención ahora es desarrollar reglas con las que podamos hacer cálculos con congruencias mucho más rápidos que hacer la división para hallar el resto. Vamos a ellas directamente.

Suma y producto de congruencias

Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces

$$a + c \equiv b + d \pmod{m}, \qquad a \cdot c \equiv b \cdot d \pmod{m}.$$

Antes de pasar a la demostración, veamos un ejemplo. Supongamos que queremos hallar el resto de dividir $1234 \cdot 6789$ entre 7. Como el resto de dividir 1234 es 2 y el resto de dividir 6789 es 6, tenemos que $1234 \cdot 6789 \equiv 2 \cdot 6 = 12 \equiv 5 \pmod{7}$. Si queremos hallar el resto de dividir $1 + 2 + \ldots + 9999$ entre 9, observemos que los restos de los números naturales se van repitiendo en ciclos de 9 luego tendremos que

$$1 + 2 + \ldots + 9999 \equiv 1111 \cdot (1 + 2 + \ldots + 8 + 0) = 1111 \cdot 36 \equiv 4 \cdot 0 \equiv 0 \pmod{9},$$

lo que demuestra que $1 + \ldots + 9999$ es múltiplo de 9, aunque esto es también fácil de ver usando la suma de los términos de una progresión aritmética.

Demostración. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces existen enteros $q, h \in \mathbb{Z}$ tales que $a - b = qm$ y $c - d = hm$, luego $(a + c) - (b + d) = (a - b) + (c - d) = (q + h)m$ es un múltiplo de m, luego $a + c \equiv b + d \pmod{m}$.

Para ver lo que pasa con la multiplicación, hacemos el siguiente truco: $ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d) = qmc + bhm$, que también es múltiplo de m luego $ac \equiv bd \pmod{m}$.

Es interesante fijarse que si tomamos $a = c$ y $b = d$, la regla del producto nos dice que $a^2 \equiv b^2 \pmod{m}$. Esto se puede repetir indefinidamente, dando lugar a la siguiente regla para la potencia.

Potencia de congruencias

Si $a \equiv b \pmod{m}$ y $n \in \mathbb{N}$, entonces $a^n \equiv b^n \pmod{m}$.

En otras palabras, estamos diciendo que podemos sustituir la base por otra congruente con ella, pero en general el exponente no puede sustituirse. Veamos algunos ejercicios resueltos donde se ve la potencia de cálculo que ofrecen las congruencias y cómo dar una solución al problema de los exponentes.

Ejercicio resuelto

¿Para qué valores de n el número $n^4 - 2n^2 + n + 4$ es múltiplo de 9?

Solución. Lo que nos dicen las reglas de la suma y producto de congruencias es que el resto de dividir $n^4+7n^3-2n^2+n+4$ entre 9 sólo depende del resto de dividir n entre 9. Por ello, en estos casos lo más fácil es hacer una tabla con los posibles restos de n:

n	n^2	n^3	n^4	$n^4+7n^3-2n^2+n+4$	
0	0	0	0	4	No
1	1	1	1	2	No
2	4	8	7	7	No
3	0	0	0	7	No
4	7	1	4	5	No
5	7	8	4	1	No
6	0	0	0	1	No
7	4	1	7	8	No
8	1	8	1	4	No

Deducimos que n^4-2n^2+n+4 no es múltiplo de 9 para ningún valor de n.

Ejercicio resuelto

Demostrar que $2222^{5555}+5555^{2222}$ es múltiplo de 7.

Solución. Comencemos con el primer sumando. Como $2222\equiv 3 \pmod 7$, tenemos que $2222^{5555}\equiv 3^{5555} \pmod 7$. Ahora bien, ¿cómo simplificamos el exponente? Observemos que, trabajando módulo 7, tenemos que $3^1\equiv 3$, $3^2\equiv 2$, $3^3\equiv 6$, $3^4\equiv 4$, $3^5\equiv 5$ y $3^6\equiv 1$. Hemos llegado a una potencia que es congruente con 1. Ahora si dividimos 5555 entre 6 obtenemos que $5555=925\cdot 6+5$, luego $3^{5555}=(3^6)^{925}\cdot 3^5\equiv 1^{925}\cdot 5\equiv 5 \pmod 7$. Llegamos así a que $2222^{5555}\equiv 5 \pmod 7$.

Se deja como ejercicio comprobar que $5555^{2222}\equiv 2 \pmod 7$ lo que termina de probar el enunciado.

Ejercicio propuesto

a. Probar que si a no es múltiplo de 3, entonces $a^2\equiv 1 \pmod 3$.

b. Probar que si a no es múltiplo de 5, entonces $a^2\equiv 1 \pmod 5$ ó $a^2\equiv 4 \pmod 5$.

c. Probar que si 2^n-1 es múltiplo de 9, entonces n es múltiplo de 6.

d. ¿Para qué valores de a el número a^3-4a^2+2a-1 es múltiplo de 7?

Hemos visto cómo simplificar un exponente siempre que encontremos una potencia que sea congruente con 1. El problema es cómo encontrarla porque en el ejercicio resuelto hemos ido probando caso por caso y hemos tenido suerte porque el módulo era pequeño. El siguiente teorema ofrece una respuesta al problema de encontrar la potencia en el caso muy particular de que el módulo sea primo, que generalizaremos en el Teorema de Euler más adelante.

Teorema pequeño de Fermat I

Sea p un número primo y a un número natural cualquiera. Entonces,

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

Si pudiéramos simplificar a en cada uno de los miembros de la congruencia del teorema, tendríamos una potencia del número congruente con 1, pero la simplificación no es siempre posible; por ejemplo, $2 \cdot 3 \equiv 2 \cdot 0 \pmod 6$ pero $3 \not\equiv 0 \pmod 6$. En el siguiente apartado, veremos qué números se pueden simplificar y cuáles no y veremos una demostración alternativa del Teorema pequeño de Fermat.

Inversos modulares

Si $a \cdot c \equiv b \cdot c \pmod m$, nos preguntamos cuándo podemos eliminar c y deducir que $a \equiv b \pmod m$. Como acabamos de ver esto no es cierto en general, pero será cierto siempre que exista un número entero d tal que $c \cdot d \equiv 1 \pmod m$ ya que bastará multiplicar la congruencia inicial por este número para obtener la simplificación deseada. A un número d que cumpla esta condición se le llama inverso de c módulo m.

Existencia de inversos

Un número entero a tiene inverso módulo m si, y sólo si, $\text{mcd}(a, m) = 1$.

Demostración. Si a tiene inverso módulo m, entonces existe $b \in \mathbb{Z}$ tal que $ab - 1 = km$ para cierto $k \in \mathbb{Z}$ luego si a y m tuvieran algún factor común, también sería factor común de 1, lo que nos dice que $\text{mcd}(a, m) = 1$. Recíprocamente, si $\text{mcd}(a, m) = 1$, la identidad de Bézout nos asegura que existen $u, v \in \mathbb{Z}$ tales que $1 = au + mv$. Tomando congruencias módulo m, es inmediato que u es un inverso de a módulo m.

Esto nos permite dar una segunda versión del Teorema pequeño de Fermat para cuanado $\text{mcd}(a, p) = 1$, es decir, cuando a no es múltiplo de p porque en tal caso la caracterización anterior nos permite simplificar a. No obstante, vamos a dar una demostración alternativa.

Teorema pequeño de Fermat II

Sea p un número primo y a un número natural que no sea múltiplo de p. Entonces,

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

Reducción y ampliación de módulo

Hemos visto cómo manejar bastante bien las congruencias en lo que se refiere a los números involucrados, pero ¿qué ocurre si queremos hacer operaciones con los módulos? La respuesta no es tan fácil como en el otro caso pero algo se puede hacer.

Comencemos respondiendo a una pregunta: ¿Qué nos da más información, decir que $a \equiv 7 \pmod{15}$ o decir que $a \equiv 7 \pmod{30}$? Si lo piensas un momento, los números positivos congruentes con 7 módulo 15 son $7, 22, 37, 52, 67$,... mientras que los congruentes con 7 módulo 30 son $7, 37, 67, 97$,... Por tanto, hay *menos* números que verifiquen la segunda afirmación en el sentido de que todos lo que verifican la segunda, también verifican la primera. Es por ello que la afirmación $a \equiv 7 \pmod{30}$ da más información que la misma con módulo 15. Veamos esto con más rigor en el siguiente resultado.

Reducción de módulo

Si $a \equiv b \pmod{m}$ y d es un divisor de m, entonces $a \equiv b \pmod{d}$.

Demostración. Si $a \equiv b \pmod{m}$, entonces $a - b$ es múltiplo de m luego también es múltiplo de d si d es un divisor de m.

Este truco es muy cómodo pues siempre podemos sustituir el módulo por un divisor suyo (pero siempre perderemos información). El proceso contrario (sustituirlo por un múltiplo) no es válido en general pues, siguiendo con los ejemplos anteriores, $22 \equiv 7 \pmod{15}$ pero $22 \not\equiv 7 \pmod{30}$.

Veamos otro ejemplo. Supongamos que $a \equiv 1 \pmod{3}$ y queremos estudiar qué ocurre con a módulo 12. Que $a \equiv 1 \pmod{3}$ quiere decir que existe $k \in \mathbb{Z}$ tal que $a = 3k + 1$ y ahora k será de la forma $4h + j$, donde j es uno de los números $\{0, 1, 2, 3\}$, luego $a = 3k + 1 = 12h + 3j + 1$. Tomando módulo 12 llegamos a que $a \equiv 3j + 1 \pmod{12}$ y, sustituyendo por j por los valores $0, 1, 2, 3$, tenemos que $a \equiv 1 \pmod{12}$ ó $a \equiv 4 \pmod{12}$ ó $a \equiv 7 \pmod{12}$ ó $a \equiv 10 \pmod{12}$. Estas son las cuatro posibilidades de a módulo 12. El ejemplo es suficiente para entenderlo pero vamos a intentar expresarlo de forma rigurosa (la demostración la dejamos al lector).

Ampliación de módulo

Si $a \equiv b \pmod{m}$ y $k \in \mathbb{N}$, entonces existe $j \in \{0, 1, \ldots, k-1\}$ tal que $a \equiv b + j \cdot m \pmod{k \cdot m}$.

Para fijar ideas, veamos un ejemplo donde puede aplicarse. Cuando estudiemos más adelante ecuaciones con congruencias y el Teorema Chino del Resto, veremos una generalización de todas estas ideas.

Ejercicio resuelto

Sea $p \geq 7$ un número primo. Hallar los posibles restos de dividir p^2 entre 30.

Solución. Observemos que $7^2 = 49$ tiene resto 19 al dividirlo entre 30 y $11^2 = 121$ tiene resto 1 al dividirlo entre 30. Vamos a demostrar que 1 y 19 son las únicas posibilidades.

Utilizando las ideas anteriores y viendo que $30 = 2 \cdot 3 \cdot 5$, intentemos calcular el resto de dividir p^2 entre 2, 3 y 5. Como p^2 es impar, se tiene que $p^2 \equiv 1 \pmod{2}$ y, como no es múltiplo de 3, se tiene que $p^2 \equiv 1 \pmod{3}$. La primera congruencia nos lleva a que, módulo 6, p^2 es congruente con 1, 3 ó 5 y la segunda a que lo es con 1 ó con 4 luego la única posibilidad es que $p^2 \equiv 1 \pmod{6}$ de donde, módulo 30, p^2 puede ser congruente con 1, 7, 13, 19 ó 25. Finalmente, como p^2 no es múltiplo de 5, deducimos que $p^2 \equiv 1$ ó $p^2 \equiv 4 \pmod{5}$ y, de las posibilidades anteriores, sólo quedan 1 y 19, como queríamos probar.

Algunas aplicaciones

En primer lugar, vamos a utilizar las congruencias para obtener criterios de divisibilidad. Todo el mundo sabe que un número es múltiplo de 2 cuando su última cifra es par, o es múltiplo de 5 cuando su última cifra es 0 ó 5. Aquí vamos a ver criterios para decidir rápidamente si un número es múltiplo de 9 y de 11 y dejaremos algunos ejercicios propuestos para otros números.

En cualquier caso, si tomamos un número natural N y lo expresamos en base 10 (en el sistema decimal), podremos escribirlo como

$$N = a_0 + 10 \cdot a_1 + 100 \cdot a_2 + \cdots + 10^n \cdot a_n.$$

En otras palabras, a_0 es la cifra de las unidades, a_1 la de las decenas, a_2 la de las centenas y así sucesivamente.

- **Criterio del 9.** Observemos que $10^k = 9\ldots9+1$ luego $10^k \equiv 1 \pmod 9$. Esto quiere decir que, tomando congruencias módulo 9 en la expresión en base 10 de N, obtenemos que

  $$N \equiv a_0 + a_1 + a_2 + \cdots + a_n \pmod 9,$$

  es decir, todo número es congruente con la suma de sus cifras módulo 9. Será por tanto múltiplo de 9 cuando la suma de sus cifras lo sea.
- **Criterio del 11.** Observemos que $10 \equiv -1 \pmod{11}$, todas las demás potencias de 10 repetirán cíclicamente los restos -1 y 1 módulo 11 y podemos escribir

  $$N \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n \pmod{11},$$

  es decir, el número N es congruente con la suma alternada de sus cifras. Será múltiplo de 11 cuando esta suma alternada lo sea.

Ejercicio propuesto

a. Probar que un número es congruente con la suma de sus cifras módulo 3.

b. Probar que un número es congruente con el número formado por sus dos últimos dígitos módulo 4.

c. Probar que un número es congruente con el número formado por sus tres últimos dígitos módulo 8.

d. Dar un criterio de divisibilidad módulo 7.

Para dar otra aplicación vamos a intentar usar las congruencias para calcular las últimas cifras de un número. Está claro que la última cifra de un número es su resto módulo 10, las dos últimas su resto módulo 100 y, en general, las k últimas cifras su resto módulo 10^k. Veamos un ejemplo en el que se usa esta técnica.

Ejercicio resuelto

Hallar las dos últimas cifras del número $3^{1000000}$.

Solución. Queremos hallar $3^{1000000}$ módulo 100. Si empezamos a probar para encontrar un exponente k tal que $3^k \equiv 1 \pmod{100}$, después de un tiempo llegamos a que $k = 20$ cumple $3^{20} \equiv 1 \pmod{100}$. Como 1000000 es múltiplo de 20, deducimos que $3^{1000000} \equiv (3^{20})^{50000} \equiv 1 \pmod{100}$, es decir, las dos últimas cifras de $3^{1000000}$ son 01.

Lección 5. El teorema de Euler-Fermat

La función φ de Euler

Para cada número natural n, consideremos todos los números entre 1 y n y nos quedamos con los que sean primos relativos con n. Por ejemplo,

n	números primos relativos con n entre 1 y n
8	$1, 3, 5, 7$
15	$1, 2, 4, 7, 8, 11, 13, 14$
44	$1, 3, 5, 7, 9, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 35, 37, 39, 41, 43$
48	$1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47$
100	$1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49,$ $51, 53, 57, 59, 61, 63, 67, 69, 71, 73, 77, 79, 81, 83, 87, 89, 91, 93, 97, 99$

Definición de la función φ de Euler

Para cada número natural n, se define $\varphi(n)$ como la cantidad de números entre 1 y n primos relativos con n.

Por lo tanto, a la vista de la tabla anterior, podemos escribir

$$\varphi(8) = 4, \quad \varphi(15) = 8, \quad \varphi(44) = 20, \quad \varphi(48) = 16, \quad \varphi(100) = 40.$$

A continuación, mostramos una forma de calcular estos números sin necesidad de contarlos uno por uno.

Cálculo de la función φ de Euler

Si descomponemos en factores primos $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, entonces se cumple que

$$\varphi(n) = p_1^{e_1-1} p_2^{e_2-1} \cdots p_r^{e_r-1} (p_1 - 1)(p_2 - 1) \cdots (p_r - 1).$$

Volviendo a los ejemplos anteriores, tenemos que

$$\begin{aligned} \varphi(8) &= \varphi(2^3) = 2^2(2-1) = 4, \\ \varphi(15) &= \varphi(3 \cdot 5) = 3^0 \cdot 5^0 \cdot (3-1)(5-1) = 8, \\ \varphi(44) &= \varphi(2^2 \cdot 11) = 2^1 \cdot 11^0 \cdot (2-1)(11-1) = 20, \\ \varphi(100) &= \varphi(2^2 \cdot 5^2) = 2^1 \cdot 5^1 \cdot (2-1)(5-1) = 40. \end{aligned}$$

Esto debería bastar para convencernos de que la fórmula simplifica considerablemente los cálculos. Es fácil ver que esta también se puede escribir como

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

Ejercicio propuesto

Responde razonadamente a las siguientes preguntas:

a. ¿Para qué valores de n se tiene que $\varphi(n)$ es impar?

b. ¿Qué valores de n cumplen que $\varphi(n) = n - 1$?

c. ¿Qué valores de n verifican que $\varphi(n) = 2$? ¿Y $\varphi(n) = 4$? ¿Y $\varphi(n) = 6$?

d. ¿Qué valores de n cumplen que $\varphi(n)$ es un divisor de n?

El teorema de Euler-Fermat

Teorema de Euler-Fermat

Si $\text{mcd}(a, m) = 1$, entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Este resultado ya es lo más general posible, puesto que si $\text{mcd}(a, m) \neq 1$, entonces no puede existir un exponente n tal que $a^n \equiv 1 \pmod{m}$. Es interesante también darse cuenta de que si $a^n \equiv 1 \pmod{m}$, entonces el inverso de a módulo m existe y es igual a a^{n-1}. Veremos a continuación algunos problemas donde se usa este resultado.

Ejercicio resuelto

Demostrar que todo número que no es multiplo de 2 ni de 5 tiene un múltiplo cuya expresión decimal sólo tiene nueves.

Solución

Si un número a no es múltiplo de 2 ni de 5, entonces $\text{mcd}(a, 10) = 1$, luego se tiene que $10^{\varphi(a)} \equiv 1 \pmod{a}$. Esto quiere decir que $10^{\varphi(a)} - 1$, que se escribe sólo con nueves, es múltiplo de a.

Ejercicio propuesto

Demostrar que todo número que no es multiplo de 2 ni de 5 tiene un múltiplo cuya expresión decimal es de la forma $10101\ldots01$.

Ejercicio resuelto

Dados números naturales a y n, demostrar que a^{4n+1} tiene la misma última cifra que a.

Solución

Las última cifra es el resto de dividir el número entre 10. En este sentido, el teorema de Euler-Fermat nos dice que $a^4 = a^{\varphi(10)} \equiv 1 \pmod{10}$ si $\text{mcd}(a, 10) = 1$

TEMA 2. DESIGUALDADES

Lección 0. Igualdades, desigualdades y cuadrados

Las desigualdades son una herramienta fundamental para trabajar con números reales. Podemos pensar que una fórmula con una igualdad es algo mucho mejor que una fórmula con una desigualdad y, obviamente, esto es cierto. Sin embargo, muchas veces no podemos tener una igualdad y la razón puede ser porque la igualdad no sea cierta, o bien porque sea suficiente conocer una desigualdad, o incluso porque demostrar la igualdad es más difícil que demostrar una desigualdad y podemos apañarnos sin ella.

Los símbolos fundamentales que vamos a manejar son los siguientes:

$=$ igual
$<$ menor que
$>$ mayor que
$\leq$ menor o igual que
$\geq$ mayor o igual que

No necesitan explicación pero una interpretación interesante es que, cuando representamos dos números en la recta real, uno es menor que otro si está a la izquierda de éste. Veamos algunas propiedades muy sencillas, válidas para cualesquiera números $a, b, c \in \mathbb{R}$:

- Si $a \leq b$ y $b \leq a$, entonces $a = b$
- Si $a \leq b$ y $b \leq c$, entonces $a \leq c$.
- Si no se cumple que $a \leq b$, entonces $a > b$.

Dejamos como ejercicio pensar qué ocurre si cambiamos los signos en las propiedades anteriores por otros distintos.

Desigualdades y operaciones

Recordemos ahora cómo se comportan las desigualdades frente a la suma y el producto de números reales, así como respecto de los opuestos e inversos. Son propiedades que se usan continuamente cuando se trabaja con desigualdades por lo que conviene enumerarlas.

- Dados $a, b, c, d \in \mathbb{R}$ tales que $a \leq b$ y $c \leq d$, entonces se cumple que $a + c \leq b + d$ y la igualdad se alcanza si, y sólo si, $a = b$ y $c = d$.
- Sean $a, b \in \mathbb{R}$ y $\lambda \in \mathbb{R}$ tales que $a \leq b$.
  - Si $\lambda \geq 0$, entonces $\lambda a \leq \lambda b$.
  - Si $\lambda \leq 0$, entonces $\lambda a \geq \lambda b$.

  En cualquiera de los dos casos, la igualdad se alcanza si, y sólo si, $a = b$ ó $\lambda = 0$.
- Sean $a, b \in \mathbb{R}$ distintos de cero.
  - Si $a \geq b > 0$, entonces $0 < \frac{1}{a} \leq \frac{1}{b}$.
  - Si $a \leq b < 0$, entonces $\frac{1}{b} \leq \frac{1}{a} < 0$.
  - Si $a < 0 < b$, entonces $\frac{1}{a} < 0 < \frac{1}{b}$.

  En cualquiera de los dos casos, la igualdad se alcanza si, y sólo si, $a = b$.

Por decirlo de otra forma: las sumas y los opuestos respetan las desigualdades mientras los productos y los inversos únicamente cuando los signos sean los adecuados. Algunos ejemplos que ilustran esta situación son los siguientes:

$$2<3 \Rightarrow \frac{1}{3}<\frac{1}{2}, \quad -5<-1 \Rightarrow 1<5 \Rightarrow \frac{1}{5}<1, \quad 0 \leq x<y \Rightarrow 0 \leq 2x<2y$$

Un caso especial de desigualdad es cuando el número cero está involucrado. Como todos sabemos, un número real a que cumple que $a<0$ se dice que es negativo y, si cumple que $a>0$, que es positivo. Pero el cero, ¿es positivo o negativo? Aquí diremos que el cero no es negativo ni positivo (ojo, esto es un convenio, un nombre). También se usarán las expresiones a *es no negativo* cuando queremos expresar que $a \geq 0$ y a *es no positivo* cuando $a \leq 0$. Algunas propiedades son las siguientes:

- La suma de dos números positivo es positiva. La suma de dos números negativos es negativa. La suma de un número positivo y otro negativo puede ser positiva, negativa o cero.
- El producto de dos números positivos es positivo. El producto de dos números negativos es también positivo. El producto de un número positivo y otro negativo es negativo.
- El opuesto de un número intercambia positivos y negativos. El inverso de un número conserva positivos y negativos.

Desigualdades y cuadrados

Una consencuencia mucho más interesante y cuya utilidad puede despreciarse en un principio es que un número al cuadrado nunca es negativo.

Desigualdad de los cuadrados

Sean $a_1, a_2, \ldots, a_n$ números reales. Entonces,

$$a_1^2+a_2^2+\ldots+a_n^2 \geq 0$$

y la igualdad se alcanza si, y sólo si, $a_1=a_2=\ldots=a_n=0$.

Veamos algunos casos resueltos donde se muestra la utilidad de este método.

Ejercicio resuelto

Demostrar que $x^2-6x+10 \geq 1$ para cualquier $x \in \mathbb{R}$.

Solución. Completando cudrados, podemos expresar $x^2-6x+10=(x-3)^2+1$. Como $(x-3)^2 \geq 0$, se tiene que $x^2-6x+10=(x-3)^2+1 \geq 1$, que es lo que queríamos demostrar.

Ejercicio resuelto

Demostrar que $\frac{1}{2}(x+y) \geq \sqrt{xy}$ para cualesquiera $x, y \geq 0$.

Solución. Por un lado, tenemos que $(\sqrt{x}-\sqrt{y})^2 \geq 0$ luego, desarrollando el cuadrado, nos queda $x+y-2\sqrt{xy} \geq 0$. Pasando la raíz al miembro de la derecha y dividiendo por 2, tenemos la desigualdad buscada.

Ejercicio resuelto

Demostrar que $x^2+y^2+z^2 \geq xy+yz+xz$ para cualesquiera $x, y, z \in \mathbb{R}$.

Solución. Partiendo de la desigualdad $(x-y)^2+(x-z)^2+(y-z)^2 \geq 0$ y desarrollando los cuadrados, tenemos que

$$x^2-2xy+y^2+x^2-2xz+z^2+y^2-2yz+z^2 \geq 0.$$

Agrupando términos y simplificando, llegamos a la desigualdad buscada.

Ejercicio resuelto

Demostrar que la suma de un número real positivo con su inverso siempre es mayor o igual que dos, es decir, $x+\frac{1}{x} \geq 2$ para cualquier $x>0$.

Solución. Haciendo operaciones, la desigualdad $x+\frac{1}{x} \geq 2$ es equivalente a $x^2+1 \geq 2x$ (observemos que, al ser $x>0$, podemos pasarlo multiplicando al miembro de la derecha sin cambiar el signo de la desigualdad) y esta es equivalente a $(x-1)^2 \geq 0$, que sabemos que es cierta.

En muchas ocasiones, es útil saber cuándo la desigualdad con la que estamos trabajando o queremos demostrar es realmente una igualdad. Por ejemplo, siempre se cumple que $(x-1)^2 \geq 0$ pero el único valor de x para el que $(x-1)^2=0$ es $x=1$ y, para cualquier otro $x \neq 1$, se tiene que $(x-1)^2>0$.

Como ya hemos dicho antes, la suma de los cuadrados de una serie de números es mayor o igual que cero. Ahora añadimos que dicha suma es igual a cero si, y sólo si, todos los números son cero. Esto permite analizar en los problemas anteriores cuándo se tiene una igualdad: en el primero cuando $x=3$ ya que la única desigualdad que hemos usado es que $(x-3)^2 \geq 0$; en el segundo, la igualdad se tiene cuando $\sqrt{x}-\sqrt{y}=0$, es decir, cuando $x=y$. En la tercera, la igualdad se tiene cuando $x-y=0$, $y-z=0$ y $x-z=0$, es decir, cuando $x=y=z$. Finalmente, en el último ejemplo la igualdad se tiene cuando $x=1$ ya que hemos usado que $(x-1)^2 \geq 0$.

Ejercicio resuelto

Demostrar que $x^4+2x^2y^2-x^2+2x+y^4-2y^2+2 \geq 0$ para cualesquiera $x, y \in \mathbb{R}$ y determinar para qué valores de x e y se alcanza la igualdad.

Solución. Si nos fijamos en los términos en los que aparece la variable y, no es difícil ver que podemos completar cuadrados para escribir la expresión del miembro de la izquierda de la desigualdad del enunciado como $(y^2+x^2-1)^2+(x+1)^2$ (darse cuenta de esto requiere cierto entrenamiento pero la pista la da el hecho de que los términos en los que aparece y tienen grado 2 y 4). Ahora es obvia la desigualdad el enunciado pues es suma de dos expresiones al cuadrado. Si ahora se da la igualdad para ciertos $x, y \in \mathbb{R}$, estos tienen que cumplir que $x^2+y^2-1=0$ y $x+1=0$, luego los únicos posibles valores de $x, y \in \mathbb{R}$ para los que se da la igualdad son $(x,y)=(-1,0)$. Si sustituimos estos valores en la desigualdad inicial, comprobamos que ciertamente estos son los únicos números que la cumplen.

Finalmente, observemos que si tenemos que usar varias desigualdades consecutivas para probar otra, la igualdad en esta última se tendrá cuando tengamos igualdad en todas las que hemos usado. Por ejemplo, si tenemos que $a \leq b \leq c \leq d$, cuando se cumpla $a=d$, tendremos que $a=b=c=d$. Veamos un ejemplo muy detallado de esta situación.

Ejercicio resuelto

Dados $a, b, c \in \mathbb{R}$ positivos, demostrar que

$$\frac{a+b}{c}+\frac{a+c}{b}+\frac{b+c}{a} \geq 6$$

y analizar en qué casos se obtiene una igualdad.

Solución. El truco está en darse cuenta de que el miembro de la izquierda se puede escribir como

$$\left(\frac{a}{b}+\frac{b}{a}\right)+\left(\frac{b}{c}+\frac{c}{b}\right)+\left(\frac{c}{a}+\frac{a}{c}\right).$$

En esta expresión, cada paréntesis es igual a la suma de un número más su inverso luego, por un ejercicio resuelto anteriormente, es mayor o igual que 2. La suma de los tres es mayor o igual que 6, como se quiere demostrar. Ahora bien, si se da la igualdad, cada uno de los paréntesis tiene que ser igual a 2 y, por tanto, $\frac{a}{b}=\frac{b}{c}=\frac{c}{a}=1$, de donde deducimos que $a=b=c$. En otras palabras, la igualdad se tiene cuando los tres números son iguales.

Lección 1. La desigualdad de Cauchy-Schwarz

En esta sección vamos a estudiar una desigualdad muy útil a la hora de probar otras desigualdades. Si tenemos números reales $x_1, x_2, y_1, y_2 \in \mathbb{R}$, observemos que

$$\begin{aligned}(x_1y_2 - x_2y_1)^2 \geq 0 &\Leftrightarrow x_1^2y_2^2 - 2x_1x_2y_1y_2 + x_2^2y_1^2 \geq 0\\ &\Leftrightarrow x_1^2y_2^2 + x_2^2y_1^2 \geq 2x_1x_2y_1y_2\\ &\Leftrightarrow x_1^2y_1^2 + x_1^2y_2^2 + x_2^2y_1^2 + x_2^2y_2^2 \geq x_1^2y_1^2 + 2x_1x_2y_1y_2 + x_2^2y_2^2\\ &\Leftrightarrow (x_1^2 + x_2^2)(y_1^2 + y_2^2) \geq (x_1y_1 + x_2y_2)^2\end{aligned}$$

Por tanto, en esta desigualdad, la igualdad se alcanza cuando $x_1y_2 - x_2y_1 = 0$. Si analizamos más detenidamente esta última condición, deducimos lo siguiente:

- si $x_1 = x_2 = 0$, entonces claramente la igualdad $x_1y_2 - x_2y_1 = 0$ se cumple;
- si $x_1 \neq 0$ y tomamos $\lambda = \frac{y_1}{x_1}$, entonces $y_1 = \lambda x_1$ e $y_2 = \frac{y_1}{x_1}x_2 = \lambda x_2$
- si $x_2 \neq 0$ y tomamos $\lambda = \frac{y_2}{x_2}$, entonces $y_1 = \frac{y_2}{x_2}x_1 = \lambda x_1$ e $y_2 = \lambda x_2$.

En resumen, si $x_1 \neq 0$ ó $x_2 \neq 0$, la condición $x_1y_2 - x_2y_1 = 0$ equivale a que existe $\lambda \in \mathbb{R}$ tal que $x_1 = \lambda y_1$ y $x_2 = \lambda y_2$. A la vista de esto, vamos a enunciar una desigualdad más general.

Desigualdad de Cauchy-Schwarz

Dados $x_1, x_2, \ldots, x_n \in \mathbb{R}$ e $y_1, y_2, \ldots, y_n \in \mathbb{R}$, se cumple que

$$(x_1y_1 + x_2y_2 + \ldots + x_ny_n)^2 \leq (x_1^2 + x_2^2 + \ldots + x_n^2)(y_1^2 + y_2^2 + \ldots + y_n^2)$$

Si algún x_k es no nulo, la igualdad se alcanza si, y sólo si, existe $\lambda \in \mathbb{R}$ tal que $y_k = \lambda x_k$ para cualquier subíndice k.

Se deja como ejercicio para los que se atrevan algunas ideas para la demostración general. Por otro lado, al final indicaremos una forma alternativa de enfocar esta desigualdad con vectores.

Ejercicio propuesto

Demostrar la desigualdad de Cauchy-Schwartz para $n = 3$ usando la desigualdad

$$(x_1y_2 - x_2y_1)^2 + (x_1y_3 - x_3y_1)^2 + (x_2y_3 - x_3y_2)^2 \geq 0.$$

¿Cómo podría generalizarse esta idea para cualquier número natural n?

Veamos ahora algunos ejemplos donde puede aplicarse esta desigualdad. Observemos que para aplicarla, siemplemente es necesario sustituir los números $x_1, \ldots, x_n$ e $y_1, \ldots, y_n$ por otras expresiones y no hay restricción alguna ya que éstos pueden ser cualesquiera números reales.

Ejercicio resuelto

Demostrar que, para cualesquiera para cualesquiera $x_1, x_2, \ldots, x_n \in \mathbb{R}$,

$$(x_1 + x_2 + \ldots + x_n)^2 \leq n(x_1^2 + x_2^2 + \ldots + x_n^2).$$

Solución. Bastará aplicar la desigualdad de Cauchy-Schwartz a los números $x_1, \ldots, x_n$ del enunciado y a los números $y_1 = y_2 = \ldots = y_n = 1$.

Ejercicio resuelto

Demostrar que, para cualquier número natural $n \geq 2$, se cumple que

$$1 + 2\sqrt{2} + 3\sqrt{3} + \ldots + n\sqrt{n} < \frac{n(n+1)}{6}\sqrt{6n+3}.$$

Solución. Apliquemos la desigualdad de Cauchy-Schwartz a los números $x_1 = 1, x_2 = 2, \ldots, x_n = n$ e $y_1 = 1, y_2 = \sqrt{2}, \ldots, y_n = \sqrt{n}$, lo que nos asegura que

$$(1 + 2\sqrt{2} + 3\sqrt{3} + \ldots + n\sqrt{n})^2 \leq (1 + 2^2 + \ldots + n^2)(1 + 2 + \ldots + n)$$

Si ahora usamos que

$$1 + 2 + \ldots + n = \tfrac{1}{2}n(n+1), \quad 1 + 2^2 + \ldots + n^2 = \tfrac{1}{6}n(n+1)(2n+1),$$

tenemos la desigualdad buscada sin más que operar, aunque falta ver que no puede darse la igualdad para lo que usaremos que $n \geq 2$. Observemos que si esta se alcanzase, entonces existiría λ tal que $1 = \lambda \cdot 1$ y $2 = \lambda\sqrt{2}$, pero de la primera igualdad deducimos que $\lambda = 1$ y de la segunda que $\lambda = \sqrt{2}$, lo cual es una contradicción.

Una versión vectorial de la desigualdad de Cauchy-Schwarz

Si los números $x_1, \ldots, x_n$ y los números $y_1, \ldots, y_n$ los escribimos como vectores de $\mathbb{R}^n$, es decir,

$$x = (x_1, x_2, \ldots, x_n),$$
$$y = (y_1, y_2, \ldots, y_n).$$

entonces el miembro de la izquierda de la desigualdad de Cauchy-Schwarz no es otra cosa que el cuadrado del producto escalar $x \cdot y$ de estos dos vectores (recordemos que el producto escalar de dos vectores es la suma de los productos de las componentes correspondientes) y el miembro de la derecha tiene dos factores: uno de ellos el módulo del vector x al cuadrado y el otro el módulo del vector y al cuadrado. Si denotamos por $|x|$ e $|y|$ a estos módulos, podemos escribir la desigualdad como

$$(x \cdot y)^2 \leq |x|^2 \cdot |y|^2.$$

El módulo de un vector siempre es mayor o igual que cero (es cero sólo cuando el vector tiene todas sus componentes cero) pero el producto escalar no tiene porqué luego, si quitáramos los cuadrados de esas expresiones seguiría siendo cierta la desigualdad, pero habríamos perdido información. Una forma de arreglar esto es escribir

$$|x \cdot y| \leq |x| \cdot |y|$$

(observa que el miembro de la izquierda no es un módulo sino un valor absoluto). Dicho de otra forma, el producto escalar de dos vectores no supera nunca el producto de sus módulos.

La igualdad se alcanza cuando los dos vectores son proporcionales o linealmente dependientes.

Lección 2. Las desigualdades de las medias

En esta sección, vamos a introducir una familia más grande de desigualdades que pueden aplicarse en multitud de ocasiones para resolver problemas. Conocer estas desigualdades suele ser útil para tratar con desigualdades en las que aparecen potencias o raíces como veremos a continuación.

¿Qué es una media?

Seguramente sabrás cómo se calcula la media aritmética de una cierta cantidad de datos (se suman todos y se divide por el número de datos). Este concepto se usa para obtener *un solo valor* que *represente* los datos que nos han dado. Por ejemplo, si en tres exámenes que has hecho has sacado puntuaciones de 7, 5 y 6 es como si hubieras sacado un 6 en los tres pues puedes pasar un punto del 7 al 5. Aquí vamos a ver otras formas de calcular medias y a interpretar un poco qué significan. Sin embargo, sea cual sea la media que hagamos, tendrá que cumplir algunas propiedades razonables: por ejemplo, si alguien saca mejores notas en los exámenes que otro, también tendrá que tener mejor media, ¿no? Más explícitamente, la media M de ciertos números $x_1, x_2, \ldots, x_n$ tendrá que cumplir las siguientes condiciones:

- M estará comprendida entre el valor mínimo y el máximo de los x_i.
- Si M' es la media de otros números $y_1, \ldots, y_n$ y se cumple que $x_i \leq y_i$ para todo i, entonces $M \leq M'$.
- Si todos los números x_i son iguales entonces la media M también es igual a este número.

El primer ejemplo de media es la media aritmética: si tenemos n números reales $x_1, x_2, \ldots, x_n \in \mathbb{R}$, su media aritmética no es otra cosa que

$$M_1 = \frac{x_1 + x_2 + \ldots + x_n}{n}.$$

Otra forma de hacer una media es lo que se conoce como media cuadrática:

$$M_2 = \sqrt{\frac{x_1^2 + x_2^2 + \ldots + x_n^2}{n}}.$$

Puedes comprobar que cumple las condiciones para ser una media que hemos puesto arriba pero, ¿por qué esta fórmula? Fíjate que es la raíz cuadrada de la media aritmética de los cuadrados de los números. Si sólo hacemos la media de los cuadrados, obtendremos un número que será un valor intermedio a los cuadrados luego para que sea del orden de los números originales, tomamos la raíz cuadrada.Esto nos permite definir más medias como

$$M_a = \sqrt[a]{\frac{x_1^a + x_2^a + \ldots + x_n^a}{n}}$$

y siempre obtendremos medias. Para $a = 3$ y $a = 4$, se llaman medias cúbica y cuártica, pero puede calcularse para cualquier número natural a (la raíz siempre se puede hacer puesto que el radicando es positivo para a par), pero también se puede calcular para cualquier número $a \neq 0$ siempre que los números $x_1, \ldots, x_n$ sean positivos. Para $a = -1$ obtenemos la media armónica

$$M_{-1} = \frac{n}{\frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n}}.$$

La filosofía es elevar a una potencia, hacer la media aritmética y después tomar la raíz del mismo índice, es decir, *hacer y deshacer* la operación potencia. Finalmente, definimos la media geométrica de los números (positivos) $x_1, \ldots, x_n$ como

$$M_0 = \sqrt[n]{x_1 \cdot x_2 \cdots x_n}.$$

Es como la media aritmética pero sustituyendo sumas por productos y cociente por raíz. Ahora tenemos definida una media M_a para cualquier número real a. Antes de seguir, deberías pensar por qué todas estas funciones son medias, aunque tienes que recordar de aquí en adelante que siempre vamos a suponer que los números a los que calculamos la media son positivos.

Visto eso, veamos qué interpretación tienen las medias y para eso supongamos que en 5 exámenes has obtenido las puntuaciones 2, 5, 6, 8 y 9. Entonces, redondeando con dos decimales, puedes calcular las siguientes medias de estas notas:

$$\begin{aligned} M_{-5} &= 2.75 \\ M_{-1} &= 4.53 \\ M_0 &= 5.33 \\ M_1 &= 6 \\ M_2 &= 6.48 \\ M_5 &= 7.28 \end{aligned}$$

¿Qué ocurre? La media aritmética es 6 pero según vamos bajando el orden de la media que usamos el resultado también baja y, si subimos, entonces sube. Aunque no vamos a entrar en más detalle, lo que pasa a grosso modo es lo siguiente:

- Para $a > 1$, la media M_a le da más peso a las notas altas. Por ejemplo, esta media valora más a un alumno que haya sacado un 8 y un 10 que a uno que ha sacado dos veces 9. Un profesor puede usarla para valorar que sacar un 10 es más difícil que sacar un 9. La media cuadrática se ha usado muchas veces en competiciones matemáticas para desempatar a participantes que han obtenido la misma puntuación (media aritmética).
- Para $a < 1$, la media M_a le da más peso a las notas bajas. Por ejemplo, en la situación en que un alumno ha sacado un 8 y un 10 mientras que otro ha sacado dos veces 9, le da ventaja al de los dos 9 porque el 8 perjudica al primer alumno. Este tipo de medias puede usarse para valorar la constancia.
- Cuando a se hace muy pequeño, es decir, se acerca a $-\infty$, el valor de M_a se acerca al número más pequeño. De la misma forma, cuando a se acerca a $+\infty$, la media se acerca al número más grande.

La ordenación de las medias

Resumiendo la información anterior, tenemos el siguiente enunciado.

Desigualdad de las medias

Tomemos $x_1, x_2, \ldots, x_n \in \mathbb{R}$ positivos y $a, b \in \mathbb{R}$ cualesquiera. Si $a < b$, entonces las medias M_a y M_b definidas anteriormente verifican que

$$M_a \leq M_b.$$

Además, la igualdad se obtiene si, y sólo si, $x_1 = x_2 = \ldots = x_n$.

La demostración general de este resultado la veremos cuando estudiemos la desigualdad de Jensen más adelante. Y también veremos otra demostración de la desigualdad entre las medias aritmética y geométrica cuando veamos la desigualdad de reordenación. Por ahora, dejamos como ejercicio probar alguna de estas desigualdades con lo que ya sabemos.

Ejercicio propuesto

a. Usando la desigualdad de Cauchy-Schwarz, demostrar la desigualdad entre las medias aritmética y cuadrática.

b. Usando la desigualdad de Cauchy-Schwarz, demostrar la desigualdad entre las medias aritmética y armónica.

c. Demostrar, para $n = 2$, que la media geométrica está entre las medias aritmética y armónica.

En lo que queda de esta sección, vamos a ver ejemplos de cómo utilizar estas desigualdades. En primer lugar, la media geométrica suele ser útil en desigualdades que involucren el producto de más de dos números.

Ejercicio resuelto

Demostrar que, para cualesquiera $a, b, c > 0$, se cumple que

$$(a^2b + b^2c + c^2a)(ab^2 + bc^2 + ca^2) \geq 9a^2b^2c^2.$$

Solución. La desigualdad entre las medias aritmética y geométrica nos dice que

$$\frac{a^2b + b^2c + c^2a}{3} \geq \sqrt[3]{a^3b^3c^3} \Rightarrow a^2b + b^2c + c^2a \geq 3abc,$$
$$\frac{ab^2 + bc^2 + ca^2}{3} \geq \sqrt[3]{a^3b^3c^3} \Rightarrow ab^2 + bc^2 + ca^2 \geq 3abc,$$

luego

$$(a^2b + b^2c + c^2a)(ab^2 + bc^2 + ca^2) \geq (3abc)(3abc) = 9a^2b^2c^2.$$

La igualdad se alcanza si, y sólo si, $a = b = c$ (¿por qué?).

Ejercicio resuelto

Demostrar que dados $x_1, \ldots, x_n > 0$, se cumple que

$$\frac{x_1}{x_2} + \frac{x_2}{x_3} + \frac{x_3}{x_4} + \ldots + \frac{x_{n-1}}{x_n} + \frac{x_n}{x_1} \geq n.$$

Solución. La desigualdad entre las medias aritmética y geométrica nos dice que

$$\frac{x_1}{x_2} + \frac{x_2}{x_3} + \ldots + \frac{x_n}{x_1} \geq n\sqrt[n]{\frac{x_1}{x_2} \cdot \frac{x_2}{x_3} \cdots \frac{x_n}{x_1}} = n.$$

La igualdad se da si, y sólo si, todos los x_i son iguales (¿por qué?).

La desigualdad entre las medias aritmética y armónica nos dice que si multiplicamos una suma de n números positivos por la suma de los inversos, entonces obtenemos al menos n^2 y es con eso con lo que tenemos que quedarnos:

$$(a_1 + a_2 + \ldots + a_n)\left(\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_n}\right) \geq n^2.$$

Ejercicio resuelto (Desigualdad de Nesbitt)

Dados tres números $a, b, c > 0$, demostrar que

$$\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} \geq \frac{3}{2},$$

y que la igualdad se alcanza si, y sólo si, $a = b = c$.

Solución. Si sumamos 1 a cada fracción y operamos, tenemos que

$$\begin{aligned}\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} &= \left(1 + \frac{a}{b+c}\right) + \left(1 + \frac{b}{a+c}\right) + \left(1 + \frac{c}{a+c}\right) - 3 \\ &= \frac{a+b+c}{b+c} + \frac{a+b+c}{a+c} + \frac{a+b+c}{a+b} - 3 \\ &= (a+b+c)\left(\frac{1}{b+c} + \frac{1}{a+c} + \frac{1}{a+b}\right) - 3\end{aligned}$$

Aplicando la desigualdad entre las medias aritmética y armónica a los números $a+b$, $b+c$ y $a+c$, obtenemos que

$$(a+b+c)\left(\frac{1}{b+c} + \frac{1}{a+c} + \frac{1}{a+b}\right) \geq \frac{9}{2}.$$

Combinando esto con lo que ya teníamos, obtenemos la desigualdad del enunciado. La igualdad se alcanza cuando los números $a+b$, $b+c$ y $a+c$ sean iguales, es decir, cuando $a = b = c$.

Lección 3. Manipulando desigualdades I: reordenación

Si has seguido las lecciones anteriores, tendrás ya algunas ideas para atacar desigualdades, aunque la mayoría de ellas consisten en aplicar desigualdades conocidas a ciertas cantidades y hacer operaciones. Ahora vamos a ver algunas técnicas más para transformar algunas desigualdades en otras que posiblemente sean más sencillas.

Reordenando términos

Imagina que has ganado un concurso y el premio consiste en 6 regalos. Sin embargo, hay tres tipos de regalos: unos valorados en 100€, otros valorados en 200€ y otros valorados en 500€, y, de los seis regalos, se te permite escoger tres de un valor, dos de otro valor y el último del tercer valor. ¿Cómo hacer para maximizar el valor del premio? Bueno, todo el mundo sabe que lo ideal es coger tres regalos de 500€, dos de 200€ y el último de 100€. Es decir, el máximo número posible de los regalos de más valor, después el máximo número posible de los del segundo mejor valor, y así sucesivamente. Esta es la idea que subyace en la desigualdad de reordenación.

Desigualdad de reordenación

Sean $a_1, a_2, \ldots, a_n$ y $b_1, b_2, \ldots, b_n$ números reales tales que

$$a_1 \leq a_2 \leq \cdots \leq a_n,$$
$$b_1 \leq b_2 \leq \cdots \leq b_n.$$

Consideremos todas las sumas de la forma

$$a_1 b_{i_1} + a_2 b_{i_2} + \ldots a_n b_{i_n},$$

donde $(i_1, i_2, \ldots, i_n)$ es una reordenación de los números $(1, 2, \ldots, n)$. Entonces, la suma máxima se alcanza para $(i_1, i_2, \ldots, i_n) = (1, 2, \ldots, n)$ y la suma mínima para $(i_1, i_2, \ldots, i_n) = (n, n-1, \ldots, 1)$.

En otras palabras, la desigualdad de reordenación nos dice que la suma es máxima cuando emparejamos el mayor con el mayor, el segundo mayor con el segundo mayor, y así sucesivamente. La suma es mínima cuando emparejamos el mayor con el menor, el segundo mayor con el segundo menor, etc. Antes de pasar a ver algunos ejemplos, vamos a hacer algunas observaciones importantes:

- En las desigualdades que hemos tratado hasta ahora, esta es la primera en que tenemos que comprobar que los números a los que se la aplicamos están en cierto orden, es decir, no podemos reordenar todo lo que queramos y como queramos.
- Hay un caso en el que la ordenación de las variables es de regalo: cuando la desigualdad es *simétrica*, es decir, al permutar las variables la expresión no cambia. Aunque trataremos más adelante con desigualdades simétricas, conviene saber ahora que si una expresión es simétrica en sus variables, podemos suponer que éstas tienen el orden que queramos. Por ejemplo, para analizar la expresión

$$\frac{\sqrt[3]{\ln(1+x^2)+\ln(1+y^2)}}{5-\cos(x)\cos(y)} + \frac{\sqrt[3]{\ln(1+y^2)+\ln(1+z^2)}}{5-\cos(y)\cos(z)} + \frac{\sqrt[3]{\ln(1+x^2)+\ln(1+z^2)}}{5-\cos(x)\cos(z)}$$

  podemos cambiar x por y, y por z ó x por z las veces que queramos que la expresión no cambiará. Por tanto, podemos hacer los cambios que queramos para suponer que $x \leq y \leq z$. Puede que esto nos sirva o no, pero es otra herramienta a nuestra disposición.

Ejercicio propuesto

Supongamos que x, y, z son tres números reales tales que $0 < x \leq y \leq z$. Demostrar las siguientes desigualdades:

a. $x^a \leq y^a \leq z^a$ para cualquier $a \geq 0$.

b. $z^a \leq y^a \leq x^a$ para cualquier $a \leq 0$.

c. $xy \leq yz \leq xz$.

d. $x + y \leq y + z \leq x + z$.

Vamos a ver ahora algunos ejemplos en los que aplicar estas ideas (hay que decir que no siempre es fácil usar la desigualdad de reordenación, pero cuando se usa resulta ser muy útil).

Ejercicio resuelto

Demostrar las siguientes desigualdades:

a. $xy + yz + xz \leq x^2 + y^2 + z^2$ para cualesquiera $x, y, z \in \mathbb{R}$.

b. $x^2y + y^2z + x^2z \leq x^3 + y^3 + z^3$ para cualesquiera $x, y, z > 0$.

c. $xyz^2 + yzx^2 + xzy^2 \leq x^4 + y^4 + z^4$ para cualesquiera $x, y, z \in \mathbb{R}$.

Solución. La primera desigualdad ya la habíamos demostrado usando que $(x-y)^2 + (y-z)^2 + (x-z)^2 \geq 0$, pero vamos a ver cómo hacerlo usando reordenación. Podemos suponer que $x \leq y \leq z$ sin perder generalidad, luego aplicando la desigualdad para $a_1 = b_1 = x$, $a_2 = b_2 = y$, $a_3 = b_3 = z$, tenemos que

$$xy + yz + xz = a_1b_2 + a_2b_3 + a_3b_1 \leq a_1b_1 + a_2b_2 + a_3b_3 = x^2 + y^2 + z^2.$$

Para la segunda desigualdad, ya no podemos suponer que las variables están en el orden que queramos porque no hay simetría, pero da igual porque los cuadrados están en el mismo orden que los números (es importante que sean positivos). Por tanto,

$$x^2y + y^2z + x^2z \leq x^2 \cdot x + y^3 \cdot y + z^2 \cdot z = x^3 + y^3 + z^3.$$

Para la tercera desigualdad, tampoco hay simetría, pero observa que podemos escribir el miembro de la izquierda como $(xz)(yz) + (xy)(xz) + (xy)(yz)$. Aplicando el primer apartado a los números xy, yz y xz, y después a los números x^2, y^2 y z^2, obtenemos que

$$xyz^2 + yzx^2 + xzy^2 \leq x^2y^2 + x^2z^2 + y^2z^2 \leq x^4 + y^4 + z^4.$$

Ejercicio resuelto

Demostrar que para cualesquiera $x, y, z > 0$, se cumple que

$$\frac{x(y+z-2x)}{y^2+z^2} + \frac{y(x+z-2y)}{x^2+z^2} + \frac{z(x+y-2z)}{x^2+y^2} \leq 0.$$

Solución. Como la expresión del enunciado es simétrica, podemos suponer que $0 < x \leq y \leq z$. Entonces, se cumple que

$$\frac{x}{y^2+z^2} \leq \frac{y}{x^2+z^2} \leq \frac{z}{x^2+y^2}.$$

Escribamos ahora la desigualdad del enunciado como $E_1 + E_2 \leq 2E_3$, donde

$$\begin{aligned} E_1 &= y \cdot \frac{x}{y^2+z^2} + z \cdot \frac{y}{x^2+z^2} + x \cdot \frac{z}{x^2+y^2}, \\ E_2 &= z \cdot \frac{x}{y^2+z^2} + x \cdot \frac{y}{x^2+z^2} + y \cdot \frac{z}{x^2+y^2}, \\ E_3 &= x \cdot \frac{x}{y^2+z^2} + y \cdot \frac{y}{x^2+z^2} + z \cdot \frac{z}{x^2+y^2} \end{aligned}$$

La desigualdad de reordenación nos dice ahora que $E_1 \leq E_3$ y $E_2 \leq E_3$, de donde obtenemos la desigualdad buscada.

Demostración de la desigualdad de reordenación

En realidad, la demostración de la desigualdad es muy sencilla. Para verlo, vamos a comenzar viendo lo que ocurre para $n = 2$, es decir, tendremos $a_1 \leq a_2$ y $b_1 \leq b_2$ y queremos probar que

$$a_1b_2 + a_2b_1 \leq a_1b_1 + a_2b_2$$

(observa que con $n = 2$ sólo hay dos ordenaciones posibles). Si pasamos todo al segundo miembro, la desigualdad es equivalente a

$$0 \leq a_1b_1 + a_2b_2 - a_1b_2 - a_2b_1 = (a_2 - a_1)(b_2 - b_1),$$

que obviamente es cierta porque $a_2 - a_1 \geq 0$ y $b_2 - b_1 \geq 0$.

¿Cómo puede ayudarnos esto al caso general? Bueno, si tenemos $n > 2$, entonces podemos ir cambiando los números de dos en dos. Sería bueno que te convencieras de esto, aunque aquí vamos a ver un ejemplo concreto: dados $a_1 \leq a_2 \leq a_3$ y $b_1 \leq b_2 \leq b_3$, probemos que

$$a_1b_3 + a_2b_1 + a_3b_2 \leq a_1b_1 + a_2b_2 + a_3b_3,$$

para lo que usamos el caso $n = 2$ con el primer y el segundo sumando y luego con el segundo y el tercero:

$$a_1b_3 + a_2b_1 + a_3b_2 \leq a_1b_1 + a_2b_3 + a_3b_2 \leq a_1b_1 + a_2b_2 + a_3b_3,$$

En otras palabras, nos llevamos primero el mayor con el mayor, luego el segundo mayor con el segundo mayor y así sucesivamente. Intenta entender por qué esto se puede hacer siempre.

Desigualdad entre las medias aritmética y geométrica

Aunque ya veremos otra demostración de este resultado, vamos a utilizar la desigualdad de reordenación para demostrar la desigualdad entre las medias aritmética y geométrica de un conjunto de números $x_1, x_2, \ldots, x_n > 0$, es decir, para demostrar que

$$\sqrt[n]{x_1x_2\cdots x_n} \leq \frac{x_1 + x_2 + \ldots + x_n}{n}.$$

Para eso, vamos a considerar los números auxiliares

$$y_1 = \frac{x_1}{\sqrt[n]{x_1 \cdots x_n}}, \quad y_2 = \frac{x_2}{\sqrt[n]{x_1 \cdots x_n}}, \cdots \quad y_n = \frac{x_n}{\sqrt[n]{x_1 \cdots x_n}},$$

que cumplen que $y_1 y_2 \cdots y_n = 1$. Entonces, vamos a escribir

$$y_1 = \frac{a_1}{1}, \quad y_2 = \frac{a_2}{a_1}, \quad y_3 = \frac{a_3}{a_2}, \cdots \quad y_{n-1} = \frac{a_{n-1}}{a_{n-2}}.$$

para ciertos números positivos $a_1, a_2, \ldots, a_{n-1}$ (esto puede hacerse siempre por ser $y_1, y_2, \ldots, y_{n-1}$ positivos). Ahora bien, como $y_1 y_2 \cdots y_n = 1$, tendremos que

$$y_n = \frac{1}{y_1 y_2 \cdots y_{n-1}} = \frac{1 \cdot a_1 \cdot a_2 \cdots a_{n-2}}{a_1 \cdot a_2 \cdots a_{n-1}} = \frac{1}{a_{n-1}}.$$

Aplicando la desigualdad de reordenación a $\{1, a_1, a_2, \ldots, a_{n-1}\}$ y a sus inversos (que están ordenados en orden opuesto), tenemos que

$$y_1 + y_2 + \ldots + y_n = \frac{1}{a_1} + \frac{a_1}{a_2} + \ldots + \frac{a_{n-2}}{a_{n-1}} + \frac{1}{a_{n-1}} \geq \frac{1}{1} + \frac{a_1}{a_1} + \ldots + \frac{a_{n-1}}{a_{n-1}} = n.$$

Finalmente, tenemos que

$$n \leq y_1 + y_2 + \ldots + y_n = \frac{x_1 + x_2 + \ldots + x_n}{\sqrt[n]{x_1 x_2 \cdots x_n}},$$

de donde deducimos la desigualdad buscada.

Lección 4. Manipulando desigualdades II: cambios de variable

Una técnica que en general es muy fructífera en matemáticas es el cambio de variables. Muchas veces reescribir un problema en otros términos hace que veamos la situación desde una nueva óptica que puede clarificar el razonamiento y darnos alguna pista para seguir. Aquí aplicaremos esta idea para resolver desigualdades.

Ejercicio resuelto (Desigualdad de Nesbitt)

Dados tres números $a, b, c > 0$, demostrar que

$$\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} \geq \frac{3}{2},$$

y que la igualdad se alcanza si, y sólo si, $a = b = c$.

Solución. Consideremos los tres números positivos $x = b + c$, $y = a + c$, $z = a + b$. Podemos despejar a, b y c en términos de x, y y z resolviendo el sistema como

$$a = \frac{1}{2}(-x + y + z), \quad b = \frac{1}{2}(x - y + z), \quad c = \frac{1}{2}(x + y - z).$$

Sustituyendo estos valores llegamos a que

$$\begin{aligned}\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} &= \frac{-x+y+z}{2x} + \frac{x-y+z}{2y} + \frac{x+y-z}{2z} \\ &= \frac{1}{2}\left[\left(\frac{x}{y} + \frac{y}{x}\right) + \left(\frac{y}{z} + \frac{z}{y}\right) + \left(\frac{z}{x} + \frac{x}{z}\right)\right] - \frac{3}{2}\end{aligned}$$

Como la suma de un número positivo más su inverso es siempre mayor o igual que 2, llegamos a que la expresión del enunciado es mayor o igual que $\frac{3}{2}$ como queríamos probar.

Lo que hemos hecho en el ejercicio anterior es invocar unas nuevas variables x, y, z para expresar la desigualdad en términos de las mismas y hemos visto que se simplifica bastante (hemos usado una técnica que suele funcionar algunas veces: sustituir según el valor de los denominadores). En realidad, hay dos formas distintas de enfocar el cambio de variables:

- La primera forma es, como hemos hecho en el ejercicio resuelto, definir nuevas variables. Es importante ver que las expresión original pueda escribirse sólo en términos de las nuevas variables y saber dónde se mueven estas últimas.
- Otra forma es, directamente, sustituir las variables originales por expresiones que dependen de nuevas variables. En este caso, es importante saber que cuando las nuevas variables toman todos los valores posibles, las nuevas también lo hacen, es decir, se barre todo el dominio de las variables originales.

Ahora vamos a centrarnos en casos concretos.

Cambios lineales

Supongamos que tenemos una expresión que depende de tres variables a, b, c. Entonces, podemos hacer un cambio lineal, es decir, definir nuevas variables a, b, c como combinación lineal de estas:

$$\begin{aligned} x &= h_{11}a + h_{12}b + h_{13}c, \\ y &= h_{21}a + h_{22}b + h_{23}c, \\ z &= h_{31}a + h_{32}b + h_{33}c, \end{aligned}$$

donde $h_{11}, h_{12}, \ldots$ son números reales. Entonces, estas constantes definen a a, b, c linealmente a partir de x, y, z. Es importante que el sistema sea invertible, es decir, que se puedan despejar a, b, c en términos de x, y, z, tal y como hicimos en el ejemplo resuelto. Algunos casos que suelen ser útiles son los siguientes, para dos y tres variables:

$$\begin{aligned} x &= a + b \\ y &= a - b \end{aligned} \qquad\qquad \begin{aligned} x &= b + c \\ y &= a + c \\ z &= a + b \end{aligned}$$

Lo importante es darse cuenta de que estos cambios son invertibles (prueba a despejar las antiguas variables en función de las nuevas), luego si a, b, c se mueven en $\mathbb{R}$ también x, y, z se mueven en $\mathbb{R}$. Eso no quiere decir que si a, b, c son positivos, también lo sean x, y, z o viceversa.

Ejercicio propuesto

Sean a, b, c números reales positivos. Demostrar que

$$\frac{a+b+3c}{3a+3b+2c} + \frac{a+3b+c}{3a+2b+3c} + \frac{3a+b+c}{2a+3b+3c} \geq \frac{15}{8}.$$

Indicación: cambia los denominadores por nuevas variables x, y, z.

Cambios para salvar restricciones

En muchas ocasiones, las desigualdades con las que tratamos tienen alguna restricción; por ejemplo, se nos dice que las variables tienen una suma o un producto concreto:

- Si $x_1, x_2, \ldots, x_n$ son positivos y $x_1 x_2 \cdots x_n = 1$, entonces podemos hacer el cambio

$$x_1 = \frac{a_1}{a_2}, \quad x_2 = \frac{a_2}{a_3}, \quad \ldots, \quad x_{n-1} = \frac{a_{n-1}}{a_n}, \quad x_n = \frac{a_n}{a_1}.$$

  Parece que este cambio complica las cosas pero ahora $a_1, a_2, \ldots, a_n$ son números positivos cualesquiera y la restricción ha desaparecido.

- Si $x_1, x_2, \ldots, x_n$ son números reales tales que $x_1 + x_2 + \ldots + x_n = 0$, entonces podemos hacer el cambio

$$x_1 = a_1 - a_2, \quad x_2 = a_2 - a_3, \quad \ldots, \quad x_{n-1} = a_{n-1} - a_n, \quad x_n = a_n - a_1,$$

  donde ahora $a_1, \ldots, a_n$ son números reales cualesquiera.

Ejercicio resuelto

Dados tres números $a, b, c > 0$ tales que $abc = 1$, demostrar que

$$\frac{2}{(a+1)^2+b^2+1} + \frac{2}{(b+1)^2+c^2+1} + \frac{2}{(c+1)^2+a^2+1} \leq 1.$$

Solución. En primer lugar, vamos a aplicar la desigualdad entre las medias aritmética y geométrica para transformar los denominadores. Concretamente,

$$(a+1)^2+b^2+1 = a^2+2a+b^2+2 \geq 2ab+2a+2,$$

y lo mismo con los otros dos. Por tanto, si llamamos E al miembro de la izquierda en el enunciado, tenemos que

$$E \leq \frac{1}{ab+a+1} + \frac{1}{bc+c+1} + \frac{1}{ac+c+1}.$$

Ahora usamos el cambio que hemos propuesto antes, escribiendo

$$a = \frac{x}{y}, \quad b = \frac{y}{z}, \quad c = \frac{z}{x}.$$

Sustituyendo en lo anterior y operando, llegamos a que

$$\frac{1}{ab+a+1} + \frac{1}{bc+c+1} + \frac{1}{ac+c+1} = \frac{yz}{xy+yz+xz} + \frac{xz}{xy+yz+xz} + \frac{xy}{xy+yz+xz}$$

y esta última suma es igual a uno.

Desigualdades con los lados de un triángulo

Para terminar con esta lección, vamos a estudiar un caso que se presenta frecuentemente al tratar problemas de desigualdades. Muchos problemas comienzan diciendo *Si a, b y c son los lados de un triángulo, demostrar que...* La pregunta es: ¿Qué tienen los lados de un triángulo que no tengan otros números? En primer lugar, son siempre positivos (las longitudes son positivas) pero además tienen que cumplir la *desigualdad triangular*. Por ejemplos 3, 8 y 20 no son los lados de ningún triángulo porque no se puede formar un triángulo con esas longitudes. Estas desigualdades triangulares nos dicen que a, b, c son los lados de un triángulo si, y sólo si,

$$a \leq b+c, \quad b \leq a+c, \quad c \leq a+b.$$

En otras palabras, un lado no puede ser mayor que la suma de los otros dos. Ahora hay dos caminos principales para atacar estas desigualdades: primero, usar técnicas geométricas y relacionar la expresión que estamos manejando con elementos geométricos del triángulo (área, alturas, medianas, bisectrices, radios inscrito o circunscrito,...) y después usar un razonamiento geométrico; o bien, segundo, hacer el cambio $a = x+y$, $b = y+z$, $c = x+z$, siendo x, y, z números reales positivos cualesquiera, y trabajar con las técnicas de desigualdades. Más concretamente, tenemos el siguiente resultado.

Cambio de variables para los lados de un triángulo

Tres números reales a, b, c son los lados de un triángulo si, y sólo si,

$$a = x + y, \quad b = y + z, \quad c = x + z,$$

para ciertos reales positivos x, y, z.

Se deja como ejercicio ver que esto es cierto, es decir, los números $x + y, y + z, x + z$ siempre son los lados de un triángulo y los lados de un triángulo siempre se expresan de esta forma. Finalizamos con un ejemplo.

Ejercicio resuelto (desigualdad de Euler)

Demostrar que en cualquier triángulo, el radio de la circunferencia circunscrita es mayor o igual que el diámetro de la circunferencia inscrita.

Solución. Este es un teorema de geometría clásica que tiene multitud de demostraciones, casi todas más elegantes que la que vamos a presentar aquí, pero queremos ver cómo aplicar el cambio de variable. Si a, b y c son los lados del triángulo, entonces los radios de las circunferencias inscrita y circunscrita, que denotaremos por r y R, respectivamente, están dados en función de los lados por

$$r = \sqrt{\frac{(p-a)(p-b)(p-c)}{p}}, \quad R = \frac{abc}{4\sqrt{p(p-a)(p-b)(p-c)}},$$

donde $p = \frac{1}{2}(a + b + c)$ es el semiperímetro (si quieres ver de dónde proceden estas fórmulas, consulta la sección de geometría). Entonces, la desigualdad a probar es $2r \leq R$, que se puede escribir usando las fórmulas anteriores como

$$8(p-a)(p-b)(p-c) \leq abc.$$

Si hacemos el cambio $a = x + y$, $b = y + z$, $c = x + z$, para x, y, z positivos, entonces resulta $p - a = z$, $p - b = x$ y $p - c = y$. La desigualdad anterior se escribe ahora como

$$8xyz \leq (x + y)(y + z)(x + z)$$

para cualesquiera $x, y, z > 0$. Usando la desigualdad entre las medias aritmética y geométrica, tenemos que $2\sqrt{xy} \leq x + y$, $2\sqrt{yz} \leq y + z$, $2\sqrt{xz} \leq x + z$. Multiplicando estas tres desigualdades, obtenemos el resultado.

TEMA 3: GEOMETRÍA.

Lección 0. Distancias, ángulos y áreas

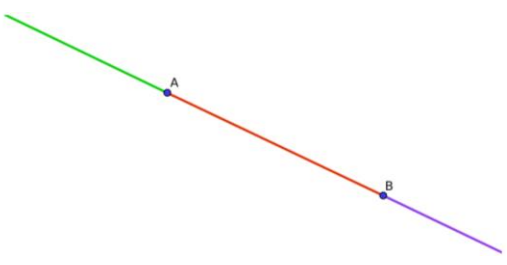
La geometría clásica, llamada así por tener sus orígenes en la Antigüedad, es una rama de las matemáticas que estudia distintos objetos del plano y el espacio mediante la comparación de longitudes y ángulos (ejemplos de tales objetos son los puntos, las rectas o los polígonos). Este tipo de geometría es uno de los temas centrales en el currículo de olimpiadas por basarse en el razonamiento geométrico puro, al estilo de los Elementos de Euclides. En esta lección introductoria presentaremos los ingredientes básicos que vamos a utilizar para estudiar la geometría del plano; más adelante, se tratarán algunas características de la geometría del espacio. Esta introducción no pretende ser rigurosa ni exhaustiva sino presentar definiciones y propiedades elementales que aparecerán más adelante (como recordatorio, ya que todos estamos familiarizados con ellas).

Puntos, rectas y segmentos

Los puntos son las unidades indivisibles de la geometría y todas las demás figuras se componen de ellos. Una recta es una colección unidimensional de puntos y un plano es una colección bidimensional de puntos. Definir rigurosamente una recta o un plano puede ser complejo, así que simplemente diremos que son figuras ilimitadas cuyos puntos son indistinguibles unos de otros: si nos colocaran en un punto de una recta o un plano sin referencia alguna, no sabríamos decir en qué punto estamos (piensa que otras figuras como una circunferencia o un triángulo no cumplen estas propiedades).

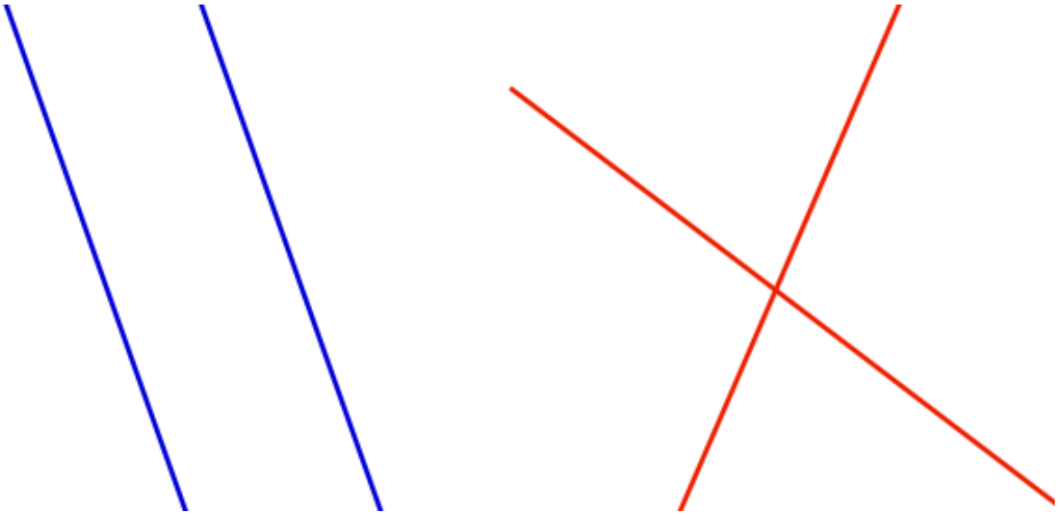
Si un punto pertenece a una recta, diremos que la recta *pasa* por el punto, en cuyo caso la separa en dos subconjuntos disjuntos llamados *semirrectas* con extremo en dicho punto. Por dos puntos distintos pasa una única recta, aunque esto no es cierto para tres o más puntos (en caso de que ocurra, tales puntos se dice que están *alineados* o que son *colineales*). Dos puntos en una recta la dividen en tres subconjuntos: dos semirrectas (ilimitadas) y un segmento (limitado), como se muestra en la figura más abajo. Estos dos puntos se llaman extremos del segmento. Normalmente supondremos que los segmentos y semirrectas contienen a sus extremos salvo que se diga lo contrario.

En la siguiente figura se muestra la recta que pasa por dos puntos distintos A y B, recta que suele representarse por $\overline{AB}$:



- El segmento con extremos A y B, se escribe simplemente como AB y se corresponde con la parte roja de la recta, incluyendo los puntos A y B.
- La semirrecta con extremo en A que pasa por B se escribe como $\overrightarrow{AB}$ y se corresponde con las partes roja y morada. Esta semirrecta es distinta de $\overrightarrow{BA}$, que se corresponde con las partes roja y verde.

Dos rectas distintas en el plano pueden cortarse o no en algún punto. Si no se cortan, se dice que son *paralelas* y, si se cortan, se dice que son *secantes*. Dos rectas secantes se cortan en un único punto (¿por qué?). En la siguiente figura se puede ver un par de rectas secantes (en rojo) y un par de rectas paralelas (en azul):

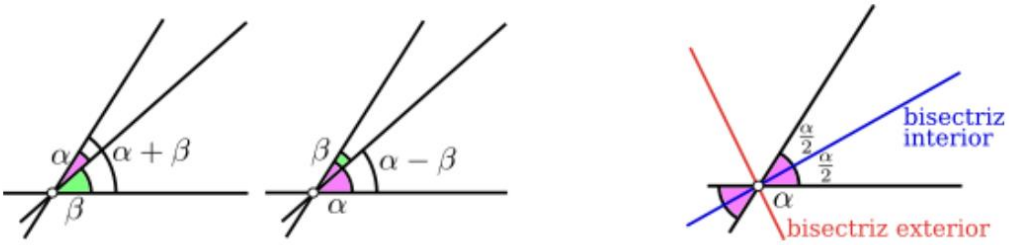


Ángulos

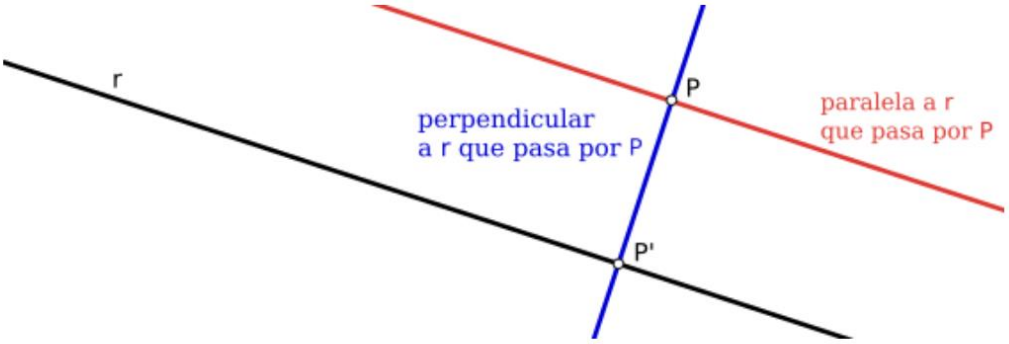
Dos semirrectas en el plano con vértice común en un punto O dividen al plano en dos regiones, llamadas *ángulos* con vértice en O. Cuando las dos semirrectas son la misma, una de estas dos regiones "desaparece" y a la otra se le llama ángulo completo y se le asigna el valor 360º. Este es un valor arbitrario que resulta de haber elegido los grados sexagesimales (º) como unidad. Más adelante también trabajaremos con otra unidad, el radián, de forma que el ángulo completo mide 2π radianes. A cada ángulo del plano se le puede asignar un valor entre 0º y 360º, de forma que cumple las siguientes propiedades:

- Si un ángulo está contenido en otro, entonces su valor es menor o igual que el de este último.
- Si un ángulo se descompone como unión de dos ángulos, entonces su valor es la suma de estos dos ángulos.

Dos rectas secantes determinan cuatro semirrectas con vértice en el punto de intersección y, por tanto, cuatro ángulos. De estos cuatro ángulos, los que sólo comparten el vértice se llaman *opuestos por el vértice* y son iguales. Los que comparten una semirrecta se llaman *suplementarios* y suman 180º. Si los cuatro ángulos formados por dos rectas son iguales, su valor es 90^o y las rectas se llaman *perpendiculares*. Los ángulos de 90^o se llaman *rectos*, los de más de 90^o *obtusos* y los de menos de 90^o *agudos*. Si una recta divide a un ángulo α en dos ángulos iguales, éstos tendrán un valor $\frac{\alpha}{2}$ y dicha recta se llama *bisectriz (interior)* del ángulo. Suele hablarse de bisectriz exterior para referirse a la bisectriz del ángulo suplementario, como puede verse en la figura. La bisectriz interior y exterior de un ángulo son perpendiculares (¿sabrías demostrarlo?).

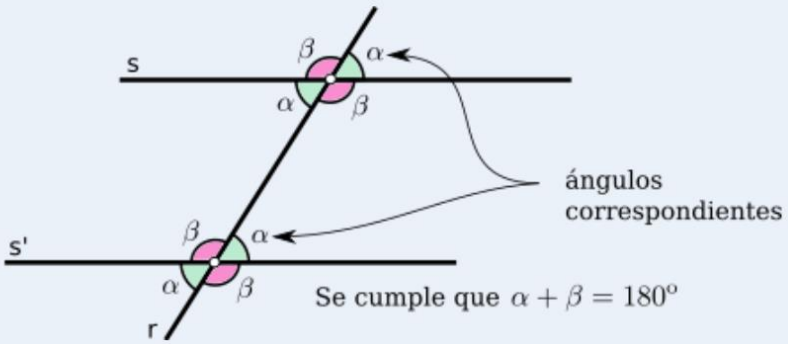


Dada una recta r, por todo punto P pasa una única recta perpendicular a r y una única recta paralela a r. Además, la perpendicular es secante con r en un punto P' que suele llamarse *pie de la perpendicular* por P a r. Lo representamos en la siguiente figura:



Rectas paralelas cortadas por una secante

Si r y s son dos rectas secantes y s' es otra recta paralela a s, entonces r y s' son secantes. Además, de entre los ocho ángulos formados por r, s y s', los *correspondientes* son iguales.

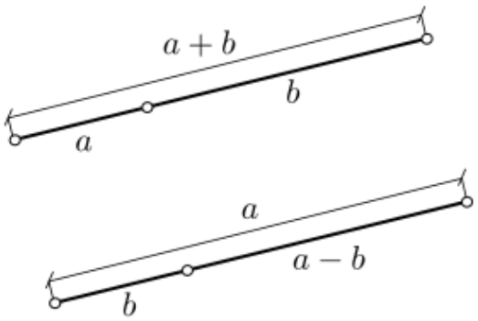


Longitudes

La longitud es un número mayor o igual que cero que se le asigna a cada segmento del plano y que representa la distancia entre los extremos del segmento. Si el segmento es AB, suele usarse la misma notación AB para hacer referencia a la dicha longitud. La longitud puede ser cero en el caso degenerado en que $A = B$ y el segmento se reduce a un único punto. Algunas propiedades de la longitud son las siguientes:

- Si un segmento de longitud a está contenido en otro de longitud b, entonces $a \leq b$.
- Dados dos puntos A y B, se tiene que $AB = BA$. Dado un punto P en el segmento AB, se cumple que $AB = AP + PB$.

De la misma forma que ocurría con los ángulos, esta última propiedad nos permite sumar y restar longitudes de forma geométrica:



Una propiedad más interesante es la siguiente desigualdad, que nos dice que para ir de un punto A a un punto B seguir el segmento AB es más corto que pasar por un tercer punto C que no está en el segmento AB.

Desigualdad triangular

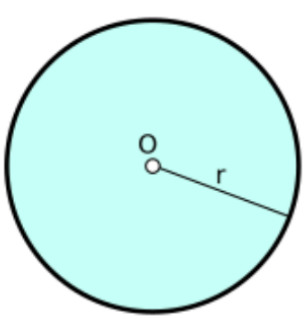
Dados tres puntos A, B y C, se cumple que

$$AB \leq AC + BC.$$

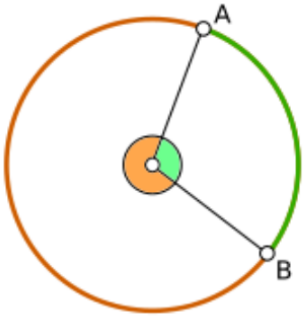
La igualdad se alcanza si, y sólo si, C pertenece al segmento AB.

Circunferencias

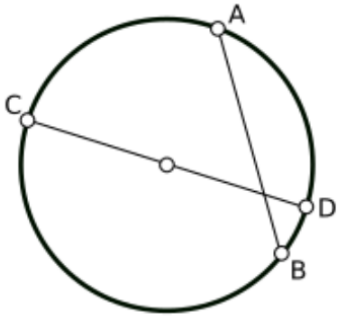
Dado un punto O y un número real $r > 0$, existen muchos puntos del plano a distancia r de O. Al conjunto de todos estos puntos se le llama *circunferencia* de centro O y radio r. Dos puntos A y B en una circunferencia la dividen en dos trozos curvilíneos llamados *arcos* de la circunferencia, mientras que el segmento que los une se llama *cuerda*. Una cuerda que pasa por el centro de la circunferencia se llama *diámetro*. El ángulo $\angle AOB$ se llama ángulo central correspondiente al arco AB. Esto nos permite identificar ángulos con vértice en el centro de la circunferencia y arcos de la misma. Además, a la región delimitada por el arco AB y los segmentos OA y OB se le llama *sector circular* de ángulo $\angle AOB$. Por otro lado, una circunferencia divide al plano en dos regiones, una limitada llamada *círculo* o *interior* y la otra no limitada llamada *exterior*.



Circunferencia de centro O y radio r

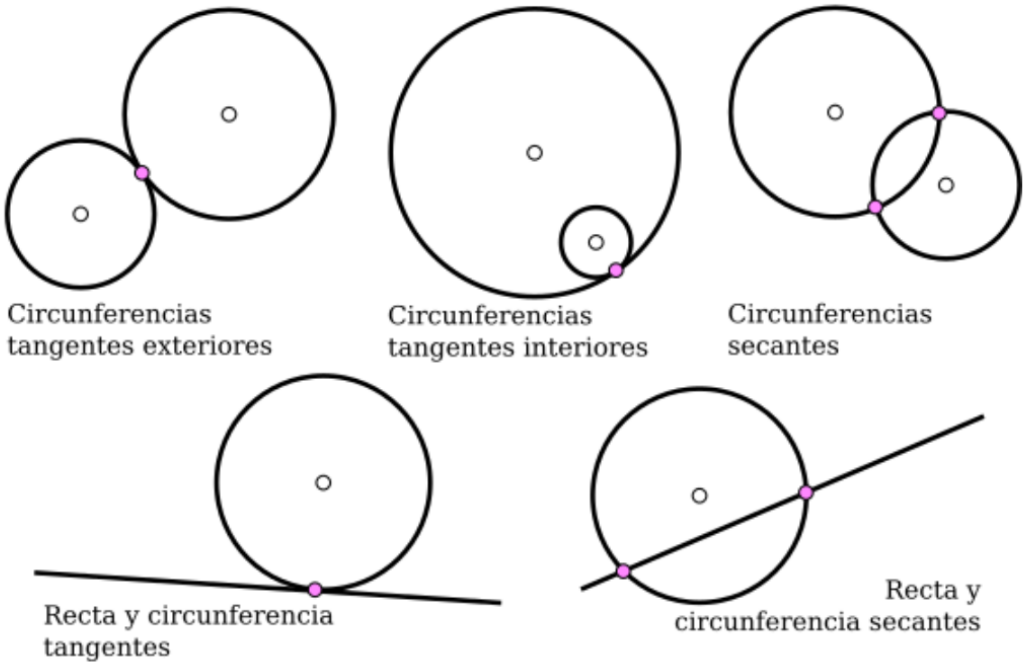


Arcos y ángulos centrales determinados por A y B



Cuerda AB y diámetro CD

Por tres puntos no alineados pasa una única circunferencia (esto se justificará cuando se hable de circunferencia circunscrita a un triángulo), por lo que dos circunferencias distintas se cortan en como mucho dos puntos. Si se cortan en dos puntos, se dicen *secantes* y si se cortan en un punto *tangentes*. Dos circunferencias tangentes pueden serlo *interiormente* si una está contenida en el interior de la otra, o *exteriormente* en caso contrario. De la misma forma, una circunferencia y una recta se cortan en un máximo de dos puntos. Si se cortan en dos puntos, se dicen *secantes* y si se cortan en un punto *tangentes*. En la siguiente figura mostramos estas posibilidades, indicando en color rosa los puntos de intersección y en blanco los centros de las circunferencias:



Circunferencias tangentes exteriores

Circunferencias tangentes interiores

Circunferencias secantes

Recta y circunferencia tangentes

Recta y circunferencia secantes

Si por cada tres puntos del plano no alineados pasa una única circunferencia, esto no es cierto en general para cuatro o más puntos. Se dice que ciertos puntos son *concíclicos* si por ellos pasa una circunferencia. Determinar si ciertos puntos están alineados o son concíclicos es un problema que puede llegar a ser muy complejo y que trataremos bastante a lo largo de estas lecciones.

Para terminar con hechos generales de la circunferencia, hemos de decir que su longitud es igual a $2\pi r$, siendo r su radio. Esto nos permite calcular la longitud ℓ de un arco entre dos puntos A y B ya que ésta debe ser proporcional al correspondiente ángulo central $\alpha = \angle AOB$. Como un ángulo central de 360 corresponde a la circunferencia completa de longitud $2\pi r$, tenemos que

$$\frac{360}{2\pi r} = \frac{\alpha}{\ell} \iff \ell = \frac{\pi r \alpha}{180}.$$

Polígonos

Una línea *poligonal* es una curva formada por una sucesión de segmentos de forma que el extremo final de cada segmento es el extremo inicial del siguiente. Si el extremo final del último segmento es el extremo inicial del primero, entonces se dice que la poligonal es *cerrada*. Si además cada segmento sólo tiene intersección con el siguiente y el anterior en los mencionados extremos, entonces la poligonal bordea una región del plano llamada *polígono*. Cada segmento de la poligonal es un *lado* del polígono y cada extremo de un lado es un *vértice*. Un polígono tiene, por tanto, el mismo número de vértices que de lados. Además, en cada vértice de un polígono se tocan exactamente dos lados (que se dicen *adyacentes* a dicho vértice), que forman dos ángulos: un ángulo interior (hacia el interior del polígono) y un ángulo exterior. Los vértices de un polígono son $A_1, A_2, \ldots, A_n$ (escritos en orden consecutivo), determinan completamente al polígono, por lo que es usual escribir simplemente $A_1A_2 \ldots A_n$ para hacer referencia al polígono. Los lados de este polígono se expresan escribiendo los pares de vértices consecutivos que son sus extremos, es decir, A_1A_2, A_2A_3, etc.

Un polígono es un triángulo si tiene tres lados, un cuadrilátero si tiene cuatro lados, un pentágono si tiene cinco lados, etc. En general, si queremos expresar que tiene un número n de lados, suele decirse que es un n-ágono. Veamos algunos nombres importantes que reciben algunos polígonos destacados:

- Un triángulo se dice...
  - *equilátero* si tiene los tres ángulos iguales,
  - *isósceles* si tiene dos ángulos iguales,
  - *escaleno* si tiene los tres ángulos distintos,
  - *acutángulo* si tiene los tres ángulos agudos,
  - *rectángulo* si tiene un ángulo recto,
  - *obtusángulo* si tiene un ángulo obtuso.
- Un cuadrilátero se dice...
  - un *paralelogramo* si sus dos pares de ángulos opuestos son iguales,
  - un *rectángulo* si todos sus ángulos son iguales,
  - un *cuadrado* si es un rectángulo y tiene los cuatro lados iguales,

  - un *trapecio* si dos de sus lados son paralelos,
  - un *rombo* si tiene los cuatro lados iguales,
- Un polígono se dice *regular* si tiene todos sus lados iguales y todos sus ángulos interiores iguales.
- Un polígono se dice *convexo* si todos sus ángulos interiores son menores o iguales que un ángulo llano (180º). Esto es lo mismo que decir que, dados dos puntos del polígono, el segmento que los une está contenido en el polígono.

Estas definiciones no son excluyentes. Por ejemplo, todo triángulo equilátero es isósceles; todos los cuadrados son rectángulos; todos los rectángulos y rombos son paralelogramos; todos los paralelogramos son trapecios. En la siguiente lección, veremos que hay otras definiciones o formas de comprobar estas definiciones. Por ejemplo, un paralelogramo también es todo cuadrilátero que tiene sus lados opuestos iguales (en el caso del rectángulo, a estas dos longitudes se les llama *base* y *altura*). Por otro lado, los adjetivos acutángulo, rectángulo y obtusángulo sí que son excluyentes, como consecuencia del siguiente resultado.

Ángulos de un triángulo

Los ángulos de cualquier triángulo suman 180°.

Ejercicio propuesto

Justificar las siguientes afirmaciones:

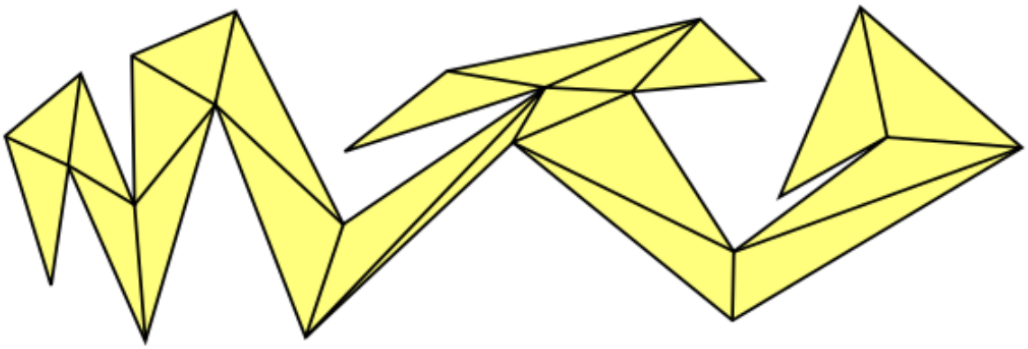
a. Un triángulo no puede tener dos ángulos rectos.

b. Todo triángulo es acutángulo, rectángulo u obtusángulo.

c. Los ángulos de un triángulo rectángulo e isósceles son 90°, 45° y 45°.

d. Los ángulos de un triángulo equilátero son iguales a 60°.

Todo polígono de se puede descomponer en triángulos de forma que dos cualesquiera de esos triángulos se toquen sólo a lo largo de un vértice o una arista y a este proceso se le llama *triangulación* del polígono. De hecho, un polígono de n-lados se puede triangular con $n-2$ triángulos. Por ejemplo, en la siguiente figura se muestra uno 24-ágono no convexo pintado de amarillo triangulado en 22 triángulos (obviamente, la forma de triangularlo no es única):



Ejercicio propuesto

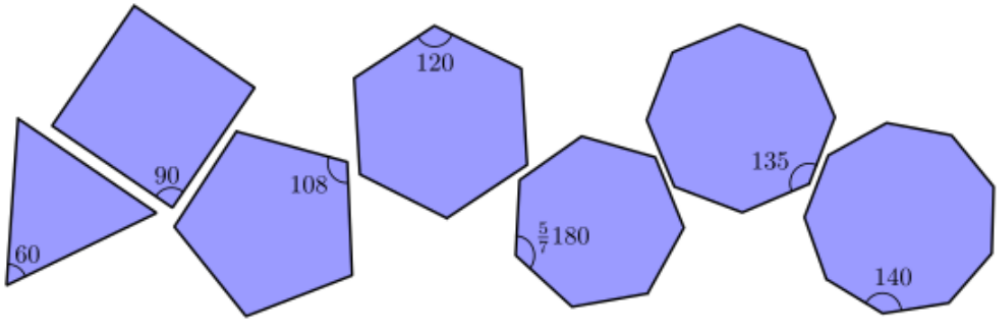
Demostrar que en un polígono de n lados, se cumplen las siguientes afirmaciones:

a. La suma de los ángulos internos es $180(n-2)$.

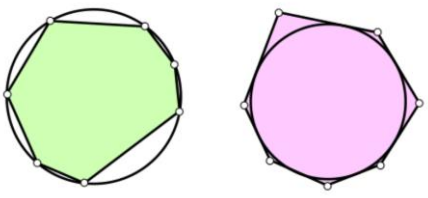
b. La suma de los ángulos externos es $180(n+2)$.

c. Si el polígono es regular, entonces cada ángulo interno es igual a $180 - \frac{360}{n}$ y cada ángulo externo es igual a $180 + \frac{360}{n}$.

En la siguiente figura pueden verse los ángulos interiores de los polígonos regulares, desde el triángulo hasta el eneágono:



Un polígono se dice *cíclico* o que tiene una *circunferencia circunscrita* si hay una circunferencia que pasa por todos sus vértices, es decir, si dichos vértices son concíclicos. Se dice que tiene una *circunferencia inscrita* si hay una circunferencia tangente a todos los lados del polígono. Más adelante, veremos que todo triángulo admite circunferencias inscrita y circunscrita, aunque esto no es siempre cierto para polígonos con más de tres lados. En la siguiente imagen se pueden ver heptágonos con circunferencia circunscrita e inscrita:



Los polígonos regulares tienen circunferencia circunscrita y también circunferencia inscrita. El centro de estas circunferencias coincide y se llama *centro* del polígono. Al radio de la circunferencia inscrita también se le llama *apotema* del polígono.

A la suma de las longitudes de todos los lados de un polígono se le llama *perímetro* del polígono. En un n-ágono regular, el perímetro es n veces la longitud del lado.

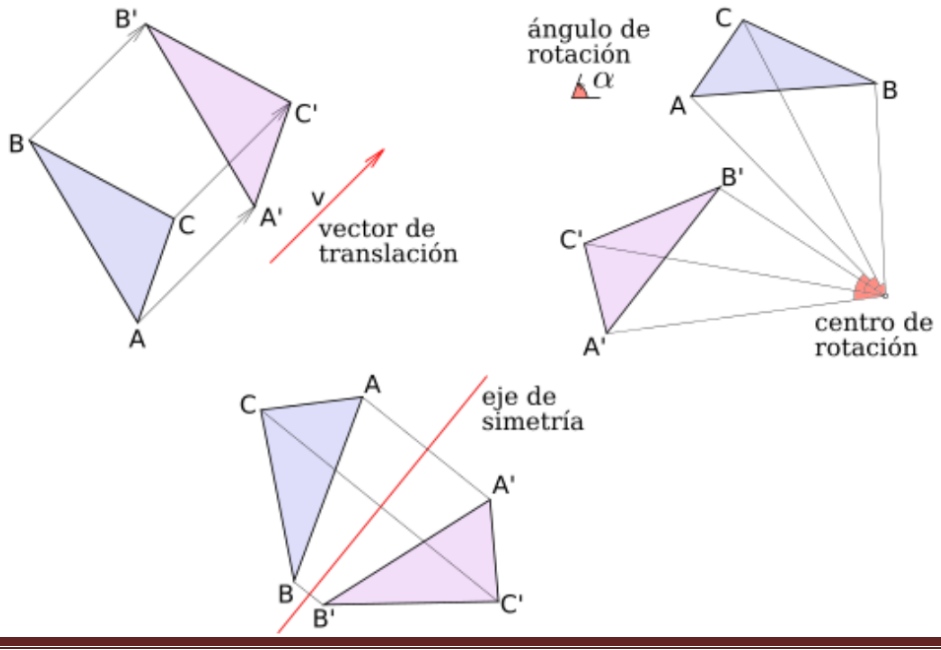
Movimientos del plano

Un *movimiento rígido* o *isometría* del plano es una transformación que conserva las distancias. Sobre este tema volveremos más adelante con mucha mayor profundidad, pero conviene saber que las siguientes aplicaciones son movimientos rígidos:

- **Traslación.** Consisten en moverse una longitud prefijada en una dirección y sentido prefijados, lo que puede resumirse en dar un *vector* de traslación.
- **Rotación.** Consisten en girar un cierto ángulo prefijado respecto de un punto prefijado llamado *centro* de rotación.
- **Simetría.** Consisten en reflejar respecto de una recta prefijada llamada *eje* de simetría como si se tratara de la imagen a través del espejo.

Los movimientos conservan todos los elementos geométricos: las distancias, los ángulos y, como comentaremos a continuación, las áreas. Además, llevan rectas en rectas y circunferencias en circunferencias del mismo radio.

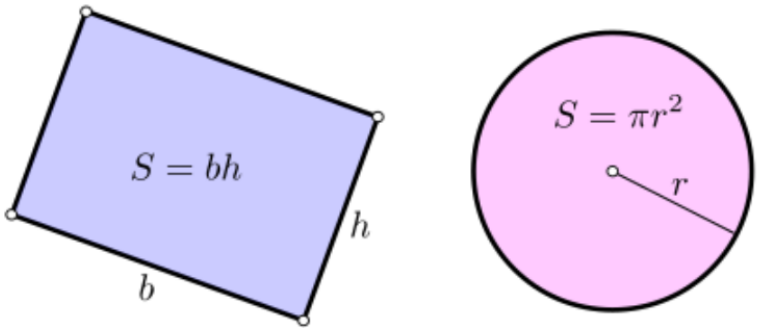
Si podemos pasar de una figura a otra aplicando uno o varios movimientos consecutivos, se dice que las figuras son *congruentes*. Intuitivamente, si el plano estuviera hecho de papel, dos figuras son congruentes cuando una puede recortarse y superponerse perfectamente sobre la otra. En la figura pueden verse ejemplos de triángulos $A'B'C'$ congruentes por los movimientos arriba mencionados con un triángulo ABC (es usual utilizar $'$ para denotar los puntos correspondientes, también llamados *homólogos*):



Áreas

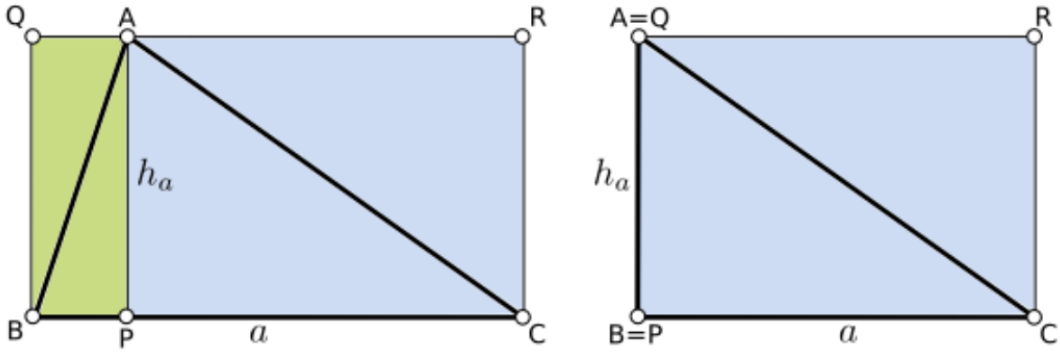
Para terminar con las generalidades, hablaremos del área de las regiones del plano. La definición matemática de área es muy sofisticada, pero aquí sólo hablaremos de regiones delimitadas por trozos de rectas y circunferencias y nos ceñiremos a la idea intuitiva del área, para lo que basta saber que se cumplen las siguientes propiedades:

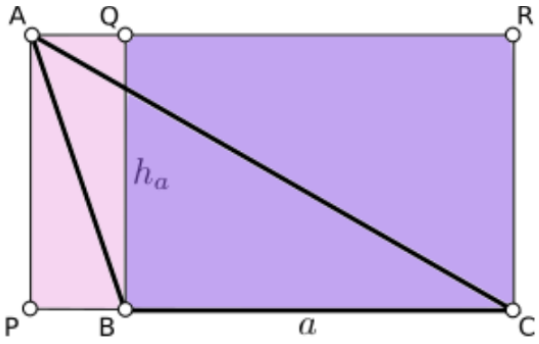
- El área de un rectángulo de base b y altura h es bh.
- El área de un círculo de radio r es πr^2.
- Si una región se descompone como unión de varias trozos que no se solapan, entonces su área es la suma de las áreas de estos trozos.
- Si dos regiones son congruentes, entonces tienen la misma área.



Veamos cómo aplicar estas ideas al cálculo del área de un triángulo ABC. Para ello, consideraremos el segmento AP perpendicular en su extremo P a la recta que contiene el lado $a = BC$. Este segmento se llama *altura* del triángulo respecto del vértice A y P se llama pie de la altura. También tomaremos la recta paralela a BC que pasa por A y los puntos Q y R que son pies de las perpendiculares a esta recta que pasan por B y C, respectivamente.

Este cálculo tiene una particularidad que aparece frecuentemente en los problemas y es que hay que distinguir casos ya que la demostración no es idéntica si el ángulo A es agudo, recto u obtuso. Estos tres casos se pueden ver en la figura siguiente:





- En el caso en que A es agudo, los dos triángulos verdes y los dos triángulos azules son congruentes, luego tienen la misma área. Por tanto, el área del triángulo ABC es la mitad del área del rectángulo $BQRC$, que es igual a ah_a (base por altura).
- En el caso en que A es recto, los triángulos verdes desaparecen y el argumento es similar al anterior.
- Finalmente, si A es obtuso, el área de ABC es el área de APC menos el área de APB. El área de APC es la mitad del área de $APRC$ y el área de APB es la mitad del área de $APBQ$ (triángulos rosas). Por tanto, el área de ABC es la mitad de la diferencia entre las áreas de $APRC$ y $APBQ$, es decir, la mitad del área de $BQRC$, que es igual a ah_a.

El área no depende de haber elegido el ángulo A y podría haberse hecho el mismo razonamiento usando B ó C y considerando las correspondientes alturas h_b y h_c.

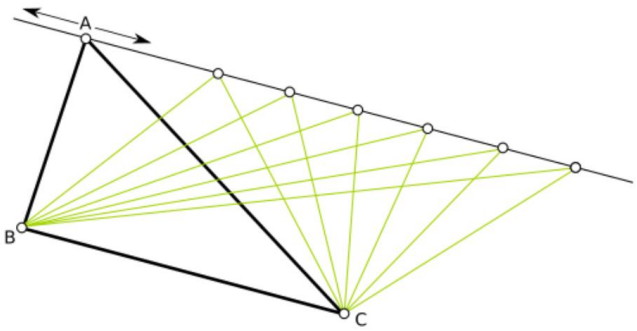
Área de un triángulo

El área de un triángulo ABC es igual a

$$S = \frac{ah_a}{2} = \frac{bh_b}{2} = \frac{ch_c}{2},$$

siendo a, b y c las longitudes de sus lados y h_a, h_b y h_c las longitudes de las alturas correspondientes.

Una consecuencia importante de esta fórmula para el área de un triángulo es que si trasladamos un vértice del triángulo paralelamente al lado opuesto, entonces los triángulos resultantes tienen el mismo área que el original:



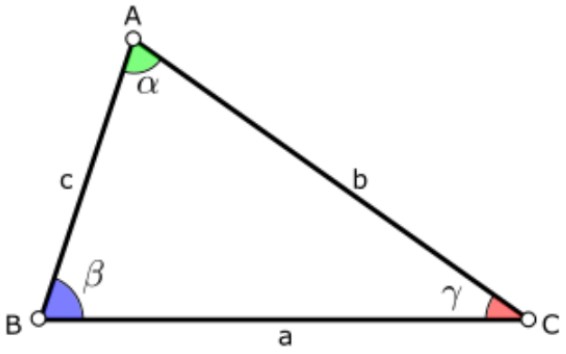
Los polígonos de más de tres lados pueden triangularse para calcular su área como la suma de las áreas de los triángulos que aparecen en la triangulación. En cuanto a un sector circular de radio r, el área es proporcional a su ángulo central; teniendo en cuenta que un ángulo de 360° corresponde a πr^2, un ángulo central α dará lugar a un área S dada por

$$\frac{360}{\pi r^2} = \frac{\alpha}{S} \Leftrightarrow S = \frac{\pi r^2 \alpha}{360}.$$

Lección 1. Congruencia y semejanza de triángulos

La herramienta geométrica más útil y que se aplica en mayor sin duda en la resolución de problemas de geometría de olimpiada es la semejanza de triángulos. Encontrar triángulos semejantes en un problema suele dar siempre información útil para su resolución. En esta lección, aprenderemos la diferencia entre triángulos iguales, triángulos congruentes y triángulos semejantes, cómo identificarlos y algunas propiedades relacionadas.

Por fijar notación para esta lección y algunas siguientes, cuando trabajamos con un triángulo ABC, las letras mayúsculas A, B y C denotan los vértices del triángulo, mientras que usaremos las minúsculas a, b y c para los lados opuestos a dichos vértices. También denotaremos por α, β y γ los ángulos interiores en estos vértices. Todo ello queda resumido en la siguiente figura:



Triángulos congruentes

Dos triángulos son *congruentes* cuando puede pasarse de uno a otro mediante sucesivos movimientos rígidos del plano (como son las simetrías, las traslaciones o las rotaciones). Informalmente, esto quiere decir que se puede recortar uno de ellos y pegarlo sobre el otro haciéndolo coincidir de forma exacta. Aunque suele decirse que dos triángulos congruentes son *triángulos iguales*, esta terminología no es del todo correcta ya que no son *el mismo triángulo* sino que difieren en un movimiento del plano.

Supongamos que los triángulos ABC y $A'B'C'$ son congruentes, donde el vértice A' corresponde con A, el vértice B' con B y el vértice C' con C. Entonces los lados y ángulos homólogos coinciden:

$$a = a', \quad b = b', \quad c = c', \qquad \alpha = \alpha', \quad \beta = \beta', \quad \gamma = \gamma',$$

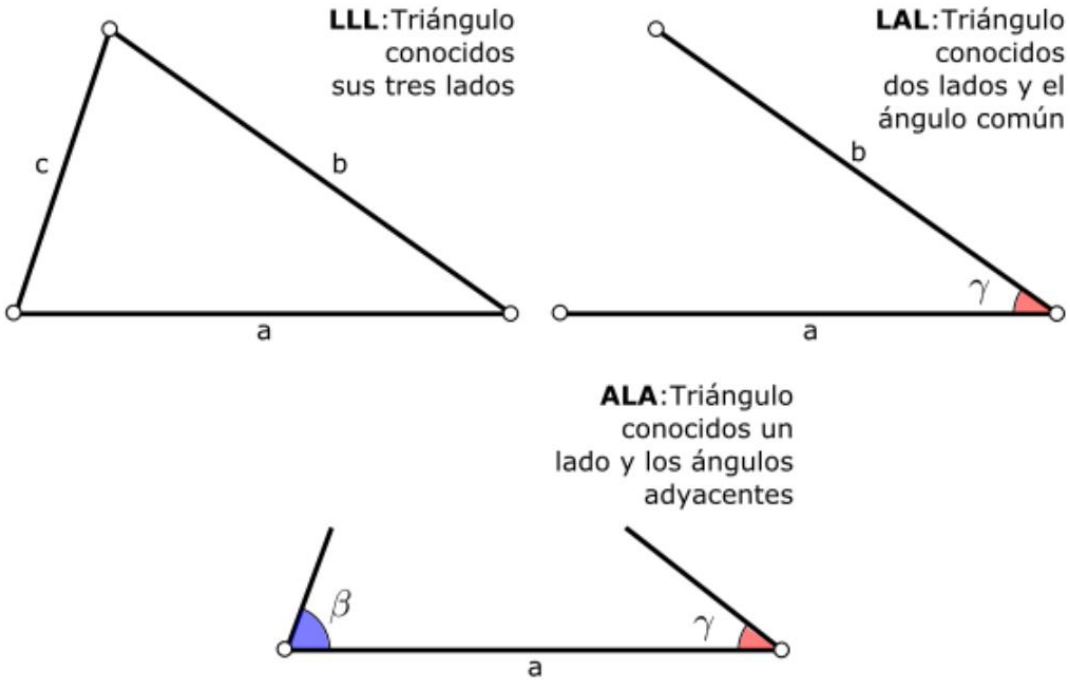
donde $'$ denota los elementos de $A'B'C'$. Esto es consecuencia de que los movimientos rígidos conservan distancias y ángulos. Recíprocamente, si dos triángulos tienen las mismas longitudes de lados y los mismos ángulos, entonces son congruentes. No obstante, no hay que conocer estos seis datos (tres lados y tres ángulos) para saber si son congruentes ya que son sufientes tres de ellos. Esta es la filosofía de los siguientes criterios.

Criterios de congruencia de triángulos

Criterio LLL: Dos triángulos son congruentes si, y sólo si, tienen tienen los tres lados iguales.

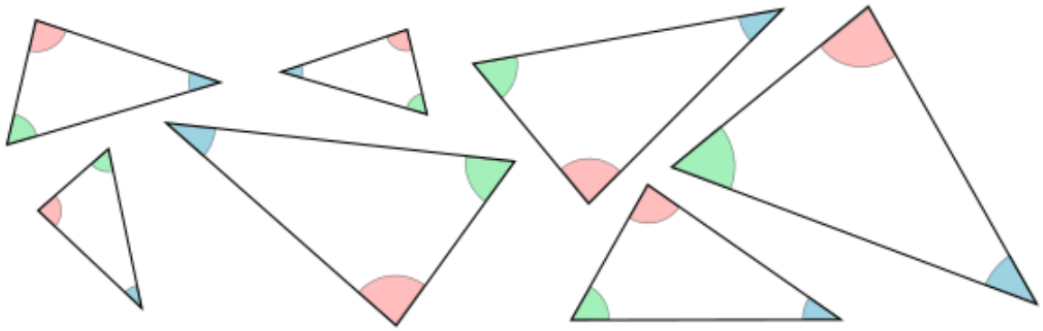
Criterio LAL: Dos triángulos son congruentes si, y sólo si, tienen tienen dos lados iguales y el ángulo común a estos igual.

Criterio ALA: Dos triángulos son congruentes si, y sólo si, tienen un lado igual y sus ángulos adyacentes iguales.



Triángulos semejantes

Dos triángulos son semejantes cuando puede pasarse de uno a otro usando movimientos rígidos del plano y también cambios de escala (homotecias). Esto último quiere decir que podemos multiplicar las longitudes de sus lados por una constante fija, por lo que los triángulos semejantes tienen lados proporcionales (a la constante de proporcionalidad se le llama *razón de semejanza*). Además, como tales transformaciones conservan los ángulos, no es difícil convencerse de que dos triángulos son semejantes cuando tienen los ángulos homólogos iguales. Por ejemplo, la siguiente figura muestra siete triángulos semejantes, con ángulos homólogos representados por el mismo color.



Criterios de semejanza de triángulos

Criterio LLL: Dos triángulos son semejantes si, y sólo si, tienen tienen los tres lados proporcionales.

Criterio LAL: Dos triángulos son semejantes si, y sólo si, tienen tienen dos lados proporcionales y el ángulo común a estos igual.

Criterio AAA: Dos triángulos son semejantes si, y sólo si, tienen sus tres ángulos iguales.

Un resultado fundamental para trabajar la semejanza es el teorema de Tales.

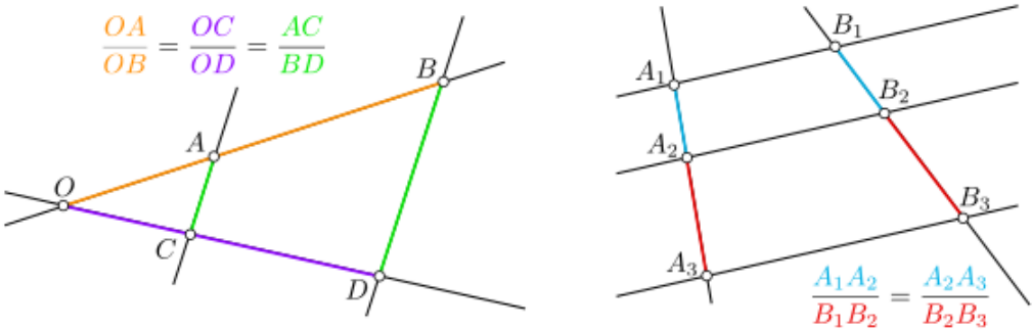
Teorema de Tales

Sea OAC un triángulo y sean B y D puntos sobre las semirrectas OA y OC, respectivamente. Entonces, AC es paralela a BD si, y sólo si,

$$\frac{OA}{OB} = \frac{OC}{OD}.$$

En tal caso, los triángulos OAC y OBD son semejantes.

Los triángulos OAC y OBD, que pueden verse en la siguiente figura, se dice que están en *posición de Tales*. Observemos que si las rectas AC y BD son paralelas, entonces los ángulos correspondientes que forman con la recta OB son iguales, es decir, $\angle OAC = \angle OBD$. De la misma forma, tenemos que $\angle OCA = \angle ODB$. Así, los triángulos OAB y OCD tienen sus tres ángulos iguales y son, por tanto, semejantes.

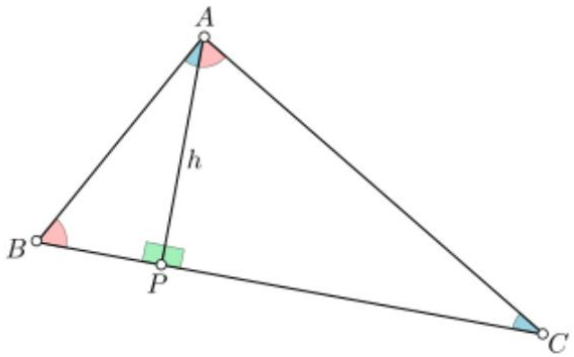


Una forma equivalente del teorema de Tales es que si tres o más paralelas cortan a dos rectas, entonces lo hacen en segmentos proporcionales, como puede verse en la figura de arriba a la derecha (su demostración se deja como ejercicio). En la resolución de problemas, siempre que aparezcan rectas paralelas, es buena idea comprobar si se puede aplicar Tales o si hay triángulos semejantes.

A partir de ahora, la congruencia y semejanza las usaremos como herramientas básicas para tratar multitud de problemas. Para facilitar la aplicación de los criterios y no confundir lados y ángulos homólogos, cuando digamos que ABC es semejante (o congruente) a DEF, implícitamente asumiremos que A se corresponde con D, B se corresponde con E y C se corresponde con F. Se recomienda seguir esta notación.

Triángulos rectángulos

Supongamos que ABC es un triángulo rectángulo con ángulo recto en el vértice A. Los lados AB y BC se llaman catetos del triángulo y el lado BC hipotenusa. Si llamamos P al pie de la perpendicular a BC que pasa por A, entonces el segmento AP se llama altura del triángulo y lo denotaremos por h. Dicha altura divide a ABC en los triángulos APB y APC, ambos rectángulos, como puede verse en la figura.



Los triángulos ABC y PBA son semejantes por el criterio AA ya que tienen dos ángulos iguales: uno recto $\angle BPA = \angle BAC = 90^\circ$ y otro coincidente $\angle ABP = \angle ABC$. Los ángulos iguales están representados por el mismo color en la figura. La semejanza nos da

$$\frac{AB}{BP} = \frac{BC}{AB} = \frac{AC}{AP} \iff \frac{c}{BP} = \frac{a}{c} = \frac{b}{h}.$$

De aquí obtenemos que $h = \frac{b \cdot BP}{c}$ y $BP = \frac{c^2}{a}$. También son semejantes ABC y PAC por la misma razón y obtenemos que

$$\frac{AB}{AP} = \frac{BC}{AC} = \frac{AC}{CP} \iff \frac{c}{h} = \frac{a}{b} = \frac{b}{CP},$$

de donde $h = \frac{c \cdot CP}{b}$ y $BP = \frac{b^2}{a}$. Multiplicando las dos expresiones que hemos obtenido para h, llegamos al conocido como teorema de la altura:

$$h^2 = \frac{b \cdot BP}{c} \cdot \frac{c \cdot CP}{b} = BP \cdot CP$$

Teorema de la altura

En un triángulo rectángulo, la altura sobre la hipotenusa divide a esta en dos segmentos cuyo producto es el cuadrado de dicha altura.

En cambio, si sumamos las expresiones para BP y CP, tenemos el teorema de Pitágoras:

$$a = BP + CP = \frac{b^2}{a} + \frac{c^2}{a} = \frac{b^2 + c^2}{a} \iff a^2 = b^2 + c^2.$$

Teorema de Pitágoras

En un triángulo rectángulo, el cuadrado de la hipotenusa es igual a la suma de los cuadrados de los catetos.

Ley del paralelogramo

En un paralelogramo $ABCD$ se cumple que

$$2(AB^2 + BC^2) = AC^2 + BD^2.$$

TEMA 4: ÁLGEBRA.

LECCIÓN 0: Ecuaciones funcionales

Una ecuación es, por definición, una igualdad entre expresiones algebraicas donde aparecen una o más variables, llamadas incógnitas. Resolver la ecuación es encontrar todos los posibles valores de las incógnitas para los que la igualdad es cierta (a tales valores se les llama soluciones). Por ejemplo, la ecuación $x + e^x = 1$ tiene una solución real, la ecuación $\cos(2x) = 0$ tiene infinitas soluciones reales y la ecuación $e^x + e^y = 0$ no tiene ninguna (¿sabrías demostrar por qué? ¿Sabrías hallarlas?).

Definición de ecuación funcional Una ecuación funcional es una ecuación en la que la incógnita no representa a un número sino a una función.

Por ejemplo, podemos preguntarnos qué funciones f cumplen la igualdad

$$f(x+1) = f(x) + 1$$

para todo valor de x. La incógnita en esta ecuación funcional no es x sino f. Una solución es elegir $f(x) = x$ para todo número natural $x \in \mathbb{N}$. Esto nos dice que

$$f(x+1) = x + 1, \qquad f(x) + 1 = x + 1,$$

luego esta elección de f cumple la igualdad propuesta. Si ahora pensamos que la variable x no es un número natural sino real, entonces otra solución es la función *parte entera* $f(x) = \lfloor x \rfloor$, ya que se cumple que $\lfloor x+1 \rfloor = \lfloor x \rfloor + 1$ para todo $x \in \mathbb{R}$. Es muy importante a la hora de resolver una ecuación funcional, entender el concepto de función y su dominio, así como entender qué significan las variables que aparecen en una ecuación funcional. Estos serán los objetivos de esta lección.

¿Qué es una función?

Solemos pensamos en las funciones como en fórmulas ya que muchas veces trabajamos con tales fórmulas en la práctica. Por ejemplo, podemos decir que la fórmula

$$\frac{\cos^3(x) - 2\sqrt{\ln(x^2+1)+2}}{\operatorname{tg}(x - e^x) + 8\pi(x^2-1)}$$

es una función en la variable real x y hacer cálculos con ella hallando límites, derivadas, integrales, etc. Sin embargo, muchas funciones importantes en matemáticas no están dadas por una fórmula, como por ejemplo la función de Euler $\varphi(n)$, que indica la cantidad de números naturales entre 1 y n que son primos relativos con n (es decir, no tiene factores comunes). Podemos calcular fácilmente su valor:

n	1	2	3	4	5	6	7	8	9	10	$\cdots$
$\varphi(n)$	1	1	2	2	4	2	6	5	6	4	$\cdots$

pero si buscamos una *fórmula* para $\varphi(n)$ usando funciones elementales (polinomios, potencias y raices, exponenciales, logaritmos, funciones trigonométricas directas o inversas,...), probablemente no la encontraremos. Aun así, φ es una función ya que para cada valor de n, el valor de $\varphi(n)$ está bien determinado. Dicho de otra forma, φ le asigna a cada elemento del conjunto $\mathbb{N}$ un único elemento del conjunto $\mathbb{N}$.

Definición de función Una función f es cualquier forma de asignar a cada elemento de un conjunto X un único elemento de un conjunto Y. En tal caso, se escribe $f: X \to Y$. Al conjunto X se le llama dominio de f y a Y se le llama codominio.

Por tanto, la función de Euler es una función $\varphi: \mathbb{N} \to \mathbb{N}$. Esto no quiere decir que todos los números del codominio tengan que estar asignados (por ejemplo, no existe ningún natural n tal que $\varphi(n) = 3$... ¿sabrías demostrar por qué?) ni que a dos números distintos del dominio se les tenga que asignar números distintos (por ejemplo, tenemos que $\varphi(5) = \varphi(10) = 4$). La única regla es que asignamos una único número a cada número del dominio. Vamos a reformular estas propiedades en términos más precisos.

Dada una función $f: X \to Y$:

- Al elemento $f(x) \in Y$ se le llama imagen del elemento $x \in X$. Al conjunto de todas las imágenes de todos los elementos se le llama imagen de f y suele denotarse por $f(X)$.
- No siempre ocurre que $f(X) = Y$. A las funciones que cumplen $f(X) = Y$ se les llama *sobreyectivas*.
- Dos elementos distintos pueden tener la misma imagen. A las funciones en que elementos distintos tienen imágenes distintas, se les llama *inyectivas*.

Ahora podemos decir que la función de Euler no es sobreyectiva ni inyectiva. Saber si una función es sobreyectiva o inyectiva suele dar información muy útil para resolver ecuaciones funcionales y lo analizaremos en una lección posterior.

Por otro lado, es muy importante identificar bien el dominio y el codominio de las funciones. Por ejemplo, tomemos la función $f: \mathbb{Q} \to \mathbb{R}$ dada por $f(x) = x^2 + 1$, cuyo dominio son los números racionales y codominio los reales. El valor las expresiones $f(\sqrt{2})$ y $f(\pi)$ no se puede hallar con la fórmula $x^2 + 1$ ni con otra y tampoco es que sea desconocido o indeterminado... ¡es que no está siquiera definido! Por tanto, jamás debemos evaluar una función en valores fuera de su dominio.

Para todo

Las ecuaciones funcionales suelen venir dadas por expresiones en las que cierta igualdad se cumple *para todo* valor de cierto conjunto. Entender esto es también fundamental para su resolución. Veamos dos ejemplos distintos, que explicaremos detalladamente.

En primer lugar, fíjate en el ejercicio resuelto de más abajo. El dominio y el codominio de las funciones que buscamos son todos los números reales. Ahora bien, la igualdad $f(x)+2f(-x)=(1+x)^2$ se cumple para cualquier valor de x, lo que nos permite sustituir x por un número real cualquiera. Por ejemplo, si sustituimos $x=0$, obtenemos la igualdad $f(0)+2f(0)=1$, que nos dice que $f(0)=\frac{1}{3}$. Dicho de otro modo, toda función f que cumpla la ecuación tendrá que cumplir que $f(0)=\frac{1}{3}$. No obstante, también podemos sustituir x por otras expresiones que representen números reales, como puede ser $-x$, $f(x)$, $\sqrt{1+x^2+y^2}$, siendo y otra variable real,... Lo importante es que al sustituir, lo hagamos en todos los sitios donde aparezca x.

Ejercicio resuelto

Ejercicio resuelto Encontrar todas las funciones $f:\mathbb{R}\to\mathbb{R}$ tales que

$$f(x)+2f(-x)=(1+x)^2 \quad \text{para todo } x\in\mathbb{R}.$$

Solución

Hagamos la sustitución $x\mapsto -x$. Esta nos dice que

$$f(-x)+2f(x)=(1+x)^2, \quad \text{para todo } x\in\mathbb{R}.$$

Esta es una nueva ecuación funcional que podemos usar junto con la original. De hecho, en ambas f aparece sólo en los términos $f(x)$ y $f(-x)$. Podemos entonces resolver el sistema lineal que forman ambas ecuaciones como si $f(x)$ y $f(-x)$ fueran las incógnitas:

$$\left.\begin{aligned} f(x)+2f(-x)&=(1+x)^2\\ 2f(x)+f(-x)&=(1-x)^2\end{aligned}\right\} \Leftrightarrow \begin{cases} f(x)=\frac{2(1-x)^2-(1+x)^2}{3}=\frac{x^2-6x+1}{3}\\ f(-x)=\frac{2(1+x)^2-(1-x)^2}{3}=\frac{x^2+6x+1}{3}\end{cases}$$

El valor de $f(-x)$ no nos interesa en realidad, pues hemos demostrado que la única solución posible a la ecuación original es $f(x)=\frac{x^2-6x+1}{3}$. Es necesario comprobar que se trata de una solución, para lo que verificamos la ecuación funcional del enunciado para esta elección de f:

$$f(x)+2f(-x)=\frac{x^2-6x+1}{3}+2\frac{x^2+6x+1}{3}=x^2+2x+1=(x+1)^2.$$

El paso final en la solución anterior es muy importante para resolver una ecuación funcional: cuando obtenemos las soluciones, **es necesario comprobar que se trata efectivamente de soluciones**. Esto es lo mismo que pasa en ecuaciones numéricas y, en el caso de las olimpiadas, suelen perderse puntos por no comprobar.

Ejercicio propuesto

Encuentra un cambio de variable adecuado para hallar todas las funciones f en cada uno de los siguientes casos:

a. $f:\mathbb{R}\to\mathbb{R}$ tales que $f(2-x)+2f(x)=x^3$ para todo $x\in\mathbb{R}$.

b. $f:\mathbb{R}\setminus\{0\}\to\mathbb{R}$ tales que $f(x)+2f(\frac{1}{x})=x^3$ para todo $x\neq 0$.

c. $f:\mathbb{R}\setminus\{-1\}\to\mathbb{R}\setminus\{-1\}$ tales que $f(x)+2f(\frac{1-x}{1+x})=x^3$ para todo $x\neq -1$.

Recordemos que $\mathbb{R}\setminus\{a\}$ es el conjunto de todos los números reales excepto a.

Lee ahora el segundo problema resuelto (que se encuentra más abajo), pero antes de intentarlo vamos a explorar el enunciado. En primer lugar, el dominio y el codominio son los números naturales $\mathbb{N}$, no los reales. Por tanto, en ningún momento pueden aparecer expresiones del tipo $f(\frac{1}{2})$ o $f(\sqrt{2})$ en nuestros razonamientos. Más aún, llegar a conclusiones como $f(\dots)=\frac{3}{2}$ es claramente una contradicción ya que no es un número natural. Vamos a fijarnos ahora en la expresión *para todo*: esta quiere decir que podemos sustituir n por cualquier número natural. En otras palabras, podemos sustituirlo por $1,2,3,4,\dots$, pero también por otra fórmula que involucre a n, a otras variables o incluso a la propia f y otras funciones, siempre que garanticemos que esa expresión sea un número natural. Por ejemplo, podemos hacer la sustitución $n\mapsto a^2+b^2$ siendo a y b números naturales, o la sustitución $n\mapsto f(n)$ ya que $f(n)$ es un número natural, pero no podemos sustituir $n\mapsto\sqrt{n^2+3n+7}$. Esto se debe a que $\sqrt{n^2+3n+7}$ no es un número natural para la mayoría de valores de $n\in\mathbb{N}$ (¿sabrías hallar para cuáles sí es un natural?).

Ejercicio resuelto

Demostrar que no existen funciones $f:\mathbb{N}\to\mathbb{N}$ tales que

$$f(f(n))=n+1$$

para cualquier número natural $n\in\mathbb{N}$. (OME 2000, problema 6)

Solución

La igualdad $f(f(n)) = n + 1$ nos dice que cuando encontramos f aplicada dos veces al mismo número, el resultado es el número más 1. Vamos a tomar f aplicada tres veces al mismo número n y calcular esto de dos formas distintas:

$$f(f(f(n))) = f(n) + 1$$
$$f(f(f(n))) = f(n + 1)$$

En la primera, hemos aplicado la ecuación funcional sustituyendo $n \mapsto f(n)$ y en la segunda hemos aplicado f a los dos miembros de la ecuación funcional. Por tanto, deducimos que $f(n + 1) = f(n) + 1$ para cualquier $n \in \mathbb{N}$. Esta es una nueva ecuación funcional que también debe cumplirse. Sustituyendo en esta última $n = 1, 2, 3, \ldots$ tenemos que

$$f(2) = f(1) + 1, \quad f(3) = f(2) + 1, \quad f(4) = f(3) + 1, \ldots$$

Como cada imagen se obtiene de la anterior sumando una unidad, llegamos a que los valores de f forman una progresión aritmética y se cumple que $f(n) = f(1) + n - 1$ para todo $n \in \mathbb{N}$. En resumen, hemos probado que si f es una solución de la ecuación original, entonces $f(n) = n + a - 1$ para todo $n \in \mathbb{N}$, siendo $a = f(1)$.

Para responder al enunciado bastará ver que estas funciones no cumplen la ecuación original y para ello sustituimos el valor de la función en la ecuación:

$$f(f(n)) = f(n + a - 1) = (n + a - 1) + a - 1 = n + 2a - 2.$$

Si esta última expresión debe ser igual a $n + 1$ para todo $n \in \mathbb{N}$, entonces necesariamente $2a - 2 = 1$, de donde despejamos $f(1) = a = \frac{3}{2}$. Esto contradice que la función debe tomar valores naturales.

Aquí volvemos a ver que es importante comprobar que los candidatos a soluciones son realmente soluciones (en este caso no lo eran).

Las ecuaciones funcionales son sistemas de ecuaciones

Encontrar una función $f : X \to Y$ es lo mismo que encontrar los valores de $f(x)$ para todos los elementos $x \in X$. Los dominios de funciones que suelen aparecer en las ecuaciones funcionales suelen ser infinitos ($\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$ o subconjuntos suyos), así que una ecuación funcional es como un sistema de ecuaciones con infinitas incógnitas. Por ejemplo, si tenemos la ecuación $f(n + 1) = f(n) + a$ sobre los naturales, entonces tenemos infnitas incógnitas

$$f(1), \quad f(2), \quad f(3), \quad f(4), \ldots$$

y también infinitas ecuaciones:

$$f(2) = f(1) + a, \quad f(3) = f(2) + a, \quad f(4) = f(3) + a, \ldots,$$

una para cada valor de n que podamos sustituir. Lo usual es que las infinitas ecuaciones sean suficientes para resolver las infinitas incógnitas.

Ejercicio propuesto

Hallar las funciones $f : \mathbb{N} \to \mathbb{N}$ que verifican cada una de las siguientes condiciones:

a. $f(n+1) = f(n) + a$ para todo $n \in \mathbb{N}$.

b. $f(n+2) = f(n) + a$ para todo $n \in \mathbb{N}$.

c. $f(n+1) = f(n) + n$ para todo $n \in \mathbb{N}$.

d. $f(n+1) = a\, f(n)$ para todo $n \in \mathbb{N}$.

e. $f(n+1) = (n+1) f(n)$ para todo $n \in \mathbb{N}$.

f. $n\, f(n+1) = (n+1) f(n)$ para todo $n \in \mathbb{N}$.