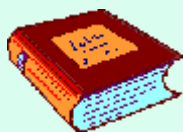


Pequeño diccionario de números naturales



Edición 2026

Colección Hojamat.es

© Antonio Roldán Martínez

<https://www.hojamat.es>

PRESENTACIÓN

Esta publicación Integra los cuatro pequeños diccionarios publicados en hojamat.es. Esta página está actualmente en periodo de simplificación y eliminación de material que ya no se visita. Por eso es conveniente descargarla de enlaces y unificar los materiales más interesantes.

Se han añadido algunos términos que se echaban de menos e insertado algunas imágenes y gráficos.

Seguirá siendo un glosario de tipo elemental o medio, que era el pretendido desde su primera edición.

El Contenido se ha dividido en cuatro apartados, y dentro de ellos, algunos rangos del alfabeto. No se ha visto estético separar enlaces a distintas letras.

Se puede efectuar una búsqueda con CTRL-F en Windows o Comando F en Mac.

CONTENIDO

Presentación	2
Contenido	3
Aritmética	4
De A a H	4
De I a O.....	37
De P a Z.....	53
Divisibilidad.....	75
De A a H	75
De I a O.....	105
De P a Z.....	113
Combinatoria	136
A a M	136
N a Z.....	145
Aritmética Modular.....	155

ARITMÉTICA

DE A A H

Absoluto

Valor absoluto

El valor absoluto de un número real se define como él mismo si es positivo o cero, o su opuesto si es negativo. Se representa con el símbolo $|n|$

Si $n \geq 0$, $|n| = n$ Si $n < 0$, $|n| = -n$

Abeliano

Sinónimo de [conmutativo](#).

Adición

Es la operación de [sumar](#) dos números.

Afortunado

Aunque se usa también en otros sentidos, se llama número afortunado al que sobrevive a una criba. Por ejemplo, los números primos son afortunados para la criba de Eratóstenes.

Algoritmo

Es una serie finita de reglas o cálculos en un orden determinado para obtener un resultado a partir de unos datos

Algoritmo de la numeración

Conjunto de reglas y convenios que permiten, dada una **BASE DE NUMERACIÓN**, representar cualquier número mediante un conjunto de símbolos llamados cifras.

Algoritmo 196

Consiste en ir sumando cada número natural expresado en el sistema decimal con el formado con las mismas cifras invertidas. Esta operación se repite hasta desembocar en un capicúa. Por ejemplo: $337+733=1070$; $1070+0701 = 1771$, que es capicúa. Existen números, como el 196, para los que aún no se sabe si la iteración termina en un capicúa o no. Son los llamados números de Lychrel: 196, 295, 394, 493, 592

Anagramático

Dos números naturales son anagramáticos si las cifras de uno son anagramas de las del otro, es decir, ambos tienen las mismas cifras (contando repetidas) pero en distinto orden. Por ejemplo, 151047 y 104571.

Anillo

Estructura algebraica formada por un conjunto dotado de dos operaciones (las llamaremos suma y producto) tales que se cumple:

El conjunto para la suma constituye un grupo aditivo

El producto convierte al conjunto en semigrupo multiplicativo

El producto es distributivo respecto a la suma.

Aritmética/o

Aritmética

Es la ciencia que estudia las operaciones básicas con números racionales. Como tal ciencia se considera fundada por Pitágoras.

Triángulo aritmético

Nombre dado también al triángulo de Pascal o Tartaglia.

Sucesión o progresión aritmética

Es aquella en la que cada término es igual al anterior sumado con un número constante llamado **diferencia**.

Su fórmula de recurrencia es: $a_1 = a$; $a_n = a_{n-1} + d$, donde **a** (valor inicial) y **d** (diferencia) son constantes.

Media aritmética

Ver [Media](#)

Armónico

Un número armónico H_n es un número racional formado mediante la suma de los inversos de los números naturales hasta n , es decir

$$H_n = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{n}$$

La sucesión de los números armónicos tiene límite infinito, por ser divergente la serie armónica a la que pertenecen los sumandos. Es fácil ver que los denominadores de los números armónicos son, salvo simplificaciones, los primeros factoriales.

Otra acepción

Media armónica

Ver [Media](#)

Arquimediano

Un grupo aditivo totalmente ordenado es *arquimediano* cuando dados dos elementos del grupo $x > 0$ e $y > 0$, existe siempre un número natural n tal que el producto

de x por n (en el sentido de suma repetida) es mayor que y ($x \cdot n > y$) Se suele expresar coloquialmente como que todos los elementos de ese grupo son alcanzables.

Los números enteros Z son arquimedianos.

Asociativa

Propiedad asociativa

Una operación definida sobre un conjunto se llama *asociativa* cuando se cumple, para toda terna de elementos **a**, **b** y **c** del conjunto que

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Automórfico

Número automórfico

Un número se define como automórfico cuando su cuadrado tiene como últimas cifras las mismas que ese número. Los primeros números automórficos son 5, 6, 25, 76, 376, 625... En efecto: $5^2=25$, $6^2=36$, $25^2=625$, $76^2=5776$, $376^2=141376$,...

Para cada número de cifras existen al menos dos números automórficos, uno terminado en 5 y otro en 6.

Número trimórfico

Es similar al anterior, pero la propiedad la cumple con el cubo: $4^3 = 64$, $24^3 = 13824$, $249^3 = 15438249$.

Todos los números automórficos son también trimórficos.

Autonúmero

Su definición es algo extraña, porque son aquellos números enteros positivos que no pueden ser expresados como la suma de otro entero con la suma de sus cifras. Por ejemplo, 20, no puede generarse con números más pequeños a los que les sumamos sus cifras. Con los de una cifra se ve que es imposible, y con los de dos: $11+1+1=13$, $12+1+2=15$, $13+1+3=17$, $14+1+4=19$, $15+1+5=21$, y el resto tampoco daría como resultado 20.

Son estos:

1, 3, 5, 7, 9, 20, 31, 42, 53, 64, 75, 86, 97, 108, 110, 121, 132, 143, 154, 165, 176, 187, 198, ...

B

Bachet de Meziriac

Conjetura de Bachet de Meziriac

Todo número natural puede expresarse como suma de a lo más cuatro cuadrados.

(Fue demostrado más tarde por Lagrange)

Teorema de Bachet de Meziriac

El sistema $x^2 = y^2 + z^2$; $y \cdot z = 2t^2$ no tiene solución.

Es decir: "No hay triángulo rectángulo pitagórico con área expresada por un número cuadrado"

Base

Base de un sistema de numeración

Es el número de unidades de orden inferior necesarias para obtener una unidad de orden inmediato superior. Coincide con el número de símbolos necesarios para escribir cualquier número en ese sistema de numeración.

Base de una potencia

Ver [Potencia](#)

Belga

Estos números han sido introducidos por Eric Angelini. Hay varios tipos, por lo que comenzaremos con los 0-Belgas. Estos números tienen la propiedad de que si a partir del número 0 vamos sumando reiteradamente las cifras (por orden) del número dado, se forma una sucesión que contiene a ese número. Por ejemplo, el 18 es 0-belga, porque a partir del 0 vamos a ir sumando sucesivamente 1, 8, 1, 8,... hasta llegar o sobrepasar el 18: 0, 1, 9, 10, 18, resultando que el mismo 18 es término de la sucesión.

Bell

Números de Bell

Los números de Bell son los términos de la sucesión 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597, ...

Representan las formas de colocar n bolas etiquetadas en n cajas indistinguibles. Por ejemplo, los símbolos a, b y c se pueden situar en tres cajas (eventualmente vacías) de 5 formas: (abc) , $(a)(bc)$, $(b)(ac)$, $(c)(ab)$ y $(a)(b)(c)$.

También representan las formas de expresar como producto de factores un número compuesto que equivale al producto de n factores primos distintos. Es

el caso del número $30 = 2 \cdot 3 \cdot 5$ y que también se puede descomponer en producto de 5 formas distintas: $30 = 6 \cdot 5 = 3 \cdot 10 = 15 \cdot 2 = 2 \cdot 3 \cdot 5$

Benford

Ley de Benford

La ley de Benford, también conocida como la ley del primer dígito, asegura que, en los números que existen en la vida real, la primera cifra es 1 con mucha más frecuencia que el resto de los números.

Biyectivo/a

Correspondencia biyectiva

Una correspondencia entre conjuntos se llama biyectiva cuando todos los elementos de uno tienen imagen en el otro y una sola.

Buen orden

Diremos que un conjunto está bien ordenado cuando todo subconjunto no vacío del mismo posee un elemento mínimo.

C

Cadena

Sinónimo de subconjunto [totalmente ordenado](#). Por ejemplo, los múltiplos de 5 para la relación \leq , o las potencias de 7 para la relación de ser múltiplo"

Capicúa

Sinónimo de [palindrómico](#).

Cardinal

Cardinal de un conjunto

Un número natural n es el *cardinal* de un conjunto cuando se puede establecer una correspondencia biyectiva entre los elementos del conjunto y los números $\{1, 2, 3, \dots, n\}$. Es evidente que si entre dos conjuntos es posible construir una correspondencia biyectiva, tendrán el mismo cardinal. Es una relación que clasifica a los conjuntos en clases de equivalencia.

Cartesiano

Producto cartesiano

El producto cartesiano de dos conjuntos A y B es otro conjunto formado por todos los pares posibles formados por un elemento de A y otro de B en ese orden.

X	A	B	C	D
1	A1	B1	C1	D1
2	A2	B2	C2	D2
3	A3	B3	C3	D3

Casi-cuadrado

Números casi-cuadrados

Son aquellos números naturales que se pueden expresar como $n^2 - 1$, siendo n otro número natural. Por ejemplo, son casi-cuadrados el 8, el 24, el 48, etc.

Catalan

Números de Catalan

Llamaremos *números de Catalan* a los términos de la sucesión 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796,...

Ecuación de Catalan

Es la ecuación diofántica $x^m - y^n = 1$ con todos x,y,m y n naturales mayores que 1

Conjetura de Catalan

Sólo existe una solución para la ecuación anterior: $3^2 - 2^3 = 1$

Cerrado/a

Conjunto cerrado para una operación

Un conjunto es cerrado para una operación (o también, la operación es cerrada en el conjunto) cuando dados dos elementos del conjunto, el resultado de aplicar la operación entre ellos da siempre como resultado otro elemento del conjunto.

Cíclico/a

Número cíclico

Un número natural de **n** cifras se llama ***cíclico*** cuando al multiplicarlo por cualquier otro número natural entre **1** y **n** se obtiene un resultado formado por las mismas cifras que él, pero desplazadas cíclicamente.

Por ejemplo, el número **142857** al multiplicarlo por **2** se convierte en **285714** y al multiplicarlo por **3** en **428571**. Intenta todos los productos por los números 1, 2, 3, 4, 5 y 6

Cifra

Cifras en un sistema de numeración

Son los distintos símbolos usados en ese sistema, así 1,2,3...9,0 en el sistema decimal o M,C,D,... en el romano.

Cociente

Cociente en una división

Ver [División](#)

Cociente en una fracción continua

Ver [Fracción continua](#)

Collatz

Conjetura de Collatz

Se toma un número entero positivo N cualquiera, por ejemplo el 13, y se le aplica la siguiente operación, a la que llamaremos función COLL(N):

- Si el número es par, se divide entre 2.
- Si el número es impar, se multiplica por 3 y se suma 1.

En el caso del 13, como es impar, se le aplicará la segunda, y quedará $\text{COLL}(13)=13*3+1=40$.

La idea de la conjetura es que sigamos aplicando esta operación a todos los resultados que obtengamos, En nuestro caso sería $\text{COLL}(40)=20$ (por ser par),

$\text{COLL}(20)=10$, $\text{COLL}(10)=5$, $\text{COLL}(5)=3*5+1=16$,
 $\text{COLL}(16)=8$, $\text{COLL}(8)=4$, $\text{COLL}(4)=2$, $\text{COLL}(2)=1$, y a
partir del 1 se entra en el ciclo $\{4, 2, 1\}$

La conjetura afirma que este final en el 1 y el ciclo
posterior **ocurre para cualquier otro entero positivo.**
Sea cual sea el comienzo, se llegará al número 1.
Todas las sucesiones construidas así terminarán en el
ciclo 4, 2, 1.

Conjetura

Una conjetura es una afirmación que parece ser cierta
en muchos casos, pero que no se ha podido demostrar.

Conmutativa

Propiedad conmutativa

Una operación definida en un conjunto tiene la
propiedad *conmutativa* cuando para todo par de
elementos a y b del conjunto se cumple

$$\mathbf{a*b = b*a}$$

Grupo, anillo o cuerpo conmutativo

Son aquellos en los que es válida la propiedad
conmutativa. También se llaman *abelianos*

Contar

Operación de contar

Es la operación de construir una correspondencia biyectiva entre los elementos de un conjunto dado y el conjunto adecuado de los n primeros números naturales. Al valor de n le llamaremos *cardinal* del conjunto.

Contraarmónica

La *media contraarmónica* de un conjunto de números positivos se define como la media aritmética de los cuadrados de los números dividida por la media aritmética de los números. En el caso de dos, a y b , sería $(a^2+b^2)/(a+b)$

Convergente

Convergente de una fracción continua

Es sinónimo de [fracción reducida](#).

Coordinable

Conjuntos coordinables

Dos conjuntos son coordinables cuando se puede establecer una correspondencia [biyectiva](#) entre los elementos de uno y otro.

Correspondencia

Una correspondencia entre dos conjuntos es cualquier subconjunto de su [producto cartesiano](#). En la práctica consiste en asignar una pareja o varias a todos o algunos elementos del conjunto.

Cósico

Número cósico

Un número natural **a** se llama *cósico* cuando es potencia exacta de otro número natural. Como casos particulares están los números [cuadrados](#), [cúbicos](#), etc.

Cuadrado

Números cuadrados

Un número natural **a** se llama *cuadrado* cuando existe otro número natural **n** tal que $a=n^2$.

Cuadrados mágicos

Un cuadrado mágico es una matriz cuadrada de números en la que las sumas por filas, columnas y diagonales son todas iguales.

Cúbico

Número cúbico

Un número natural **a** se llama *cúbico* si es la tercera potencia (cubo) de otro número natural.

Cuerpo

Cuerpo como estructura algebraica

Un cuerpo es un anillo con elemento neutro para el producto (llamado unidad) en el que todos los elementos salvo el cero (elemento neutro para la suma) poseen un inverso.

Cumulantes

Algoritmo de los cumulantes

Es el algoritmo (también se llaman cumulantes los distintos resultados del mismo) que encuentra las reducidas de una fracción continua.

D

Decimal

Sistema de numeración decimal

Es aquel sistema de numeración posicional en el que cada tipo de unidad (unidades, decenas, centenas, millares, etc.) es diez veces mayor que su inmediata precedente. Sus cifras son 0,1,2,3,4,5,6,7,8 y 9.

Definición por recursividad

Una sucesión de números naturales puede ser definida por recursividad. Esta definición se compone de dos declaraciones:

- a) Se definen directamente los valores de los primeros términos de la sucesión: $a_1=m$, $a_2=n$, $a_3=p$,...
- b) El resto de términos se define en función de los anteriores $a_n = f(a_{n-1}, a_{n-2}, a_{n-3}...)$

Ejemplo de recursividad es la definición de factorial: $1! = 1$, $n! = (n-1)! * n$ o la de la sucesión de Fibonacci: $a_1=1$, $a_2=1$, $a_n = a_{n-1} + a_{n-2}$

Densidad

Dada una sucesión A cualquiera, deberemos conocer una función de conteo $a(n)$, definida como el número de elementos de A que son menores o iguales a n. Entonces definiremos la densidad **d** natural de A (si

existe) como el cociente $a(n)/n$ cuando n tiende a infinito.

Descomposición

Descomposición de un conjunto en sumas

Ver [Partición](#)

Desigualdad

Desigualdad de números naturales

Un número natural **a** es *menor* que otro número **b** cuando cualquier conjunto del que es cardinal **a** es [coordinable](#) con una parte estricta de otro conjunto cuyo cardinal es **b**. Si se permite que esa parte pueda ser todo el conjunto, diremos que **a** es *menor o igual* que **b**.

Las relaciones inversas serán *mayor* y *mayor o igual*.

Dos números son *desiguales* si uno de ellos es menor que el otro.

Devlali

Números de Devlali, autonúmeros o números colombianos.

Son aquellos números enteros positivos que no pueden ser expresados como la suma de otro entero con la suma de sus cifras (Kaprekar llamó a esta operación digitadición).

Diferencia

La diferencia entre dos números **a** (*minuendo*) y **b** (*sustraendo*), con **a** mayor o igual que **b**, es otro número natural **c** (*diferencia*) que sumado con **b** da una suma igual a **a**.

Dígito

Número natural de una sola cifra

Diofántico/a

Ecuación diofántica

Una ecuación diofántica es aquella definida en el conjunto de los enteros, tanto para sus coeficiente como para los valores que puedan tomar las incógnitas.

Sistema diofántico

Es aquel que está formado por ecuaciones diofánticas.

Aproximación diofántica

Es aquella que busca aproximar un número real mediante números racionales. Un ejemplo típico es el de la aproximación a radicales cuadráticos mediante frcciones continuas.

Distributiva

Propiedad distributiva

Una operación $*$ es distributiva respecto a otra operación $+$ cuando se cumple, para toda terna de elementos a, b y c que

$$a*(b+c) = a*b+a*c$$

Dividendo

Ver [División](#)

División

División entera

Dados dos números naturales a (*dividendo*) y b (*divisor*), llamaremos división entera entre ellos a la operación de encontrar otros dos números naturales q (*cociente por defecto*) y r (*resto por defecto*), tales que se cumpla:

$$a = b.q + r \text{ con } r < b$$

Se demuestra que ambos números q y r siempre existen para a y b dados.

También se pueden definir el cociente por exceso y su resto correspondiente:

$$a = b.(q+1) - r' \text{ con } r' < b$$

Se cumple que $q + q' = d$

Además, si se multiplican por un mismo número natural **m** tanto el dividendo como el divisor, el cociente no varía, pero el resto queda multiplicado también por **m** (en ambas modalidades *por defecto* y *por exceso*)

División exacta

Dados dos números naturales **a** (dividendo) y **b** (divisor), llamaremos división exacta entre ellos a la operación de encontrar otro número **q** (cociente) tal que se cumpla **a=b.q**

Si esta operación es posible, diremos que **b** es divisor de **a**, o bien que **a** es múltiplo de **b**.

Divisor

Divisor en una división

Ver [División](#)

Número divisor de otro

Ver [División](#)

E

Ecuación

Ecuación diofántica

Una ecuación diofántica es aquella definida en el conjunto de los enteros, tanto para sus coeficiente como para los valores que puedan tomar las incógnitas.

Ecuación diofántica lineal

La ecuación diofántica de tipo lineal más sencilla es la del tipo **$Ax+By=C$**

Para que tenga solución ha de ser C múltiplo de $D=MCD(A,B)$. Se resuelve considerando el teorema que afirma que existen dos enteros m y n tales que $mA+nB=D$. Los valores de m y n se calculan mediante el algoritmo de Euclides y el algoritmo de las reducidas.

[Ecuación de Pell](#)

[Ecuación pitagórica](#)

Equilibrado

Número equilibrado

Un número es equilibrado en un sistema dado de numeración si (distintas definiciones):

(a) Todos sus dígitos aparecen con la misma frecuencia. Es popular el caso del sistema binario, en el que se exige que aparezcan el mismo número de 1 que de 0.

(b) Aparecen todos los dígitos posibles una vez.

(c) Posee el mismo número de dígitos pares que impares, o bien los pares figuran un número impar de veces y los impares un número par.

(d) Números de tres cifras en las una de ellas es promedio de las otras.

(e) Los primeros n dígitos tienen la misma suma que los n siguientes (en números de $2n$ cifras)

Primo equilibrado

Primo equilibrado es aquel que es promedio de su primo anterior y el siguiente.

Equipotente

Dos conjuntos se llaman equipotentes si es posible establecer entre ellos una correspondencia biyectiva. Los dos conjuntos tendrán el mismo [cardinal](#).

Especular

Números especulares

Dos números naturales se llaman especulares para la multiplicación cuando sus imágenes especulares dan el mismo producto que ellos. Por ejemplo:

$$23 \cdot 64 = 46 \cdot 32$$

Exponente

Ver [Potencia](#)

F

Factor

Factor en un producto

Se llaman factores en un [producto](#) a los dos o más números que se multiplican.

Factorial

Factorial de un número

Llamaremos factorial de un número natural n al producto

$$n! = n(n-1)(n-2)(n-3)\dots 3 \cdot 2 \cdot 1$$

También se llama **factorial de n de grado k y diferencia d** al producto

$a(a-d)(a-2d)\dots$ (hasta k factores)

Si la diferencia es $d=1$, el factorial se representa por

$a^{(n)} = a(a-1)(a-2)(a-3)\dots(a-k+1)$

Es fácil demostrar que $a^{(n)}$ es divisible entre $n!$

Feliz

Número feliz

Se define el siguiente algoritmo: Dado un número entero positivo expresado en el sistema de numeración decimal, se suman los cuadrados de sus dígitos, con lo que obtenemos otro número entero positivo. Volvemos a reiterar la operación de sumar los cuadrados de sus dígitos, y continuamos hasta llegar a 1 o a un ciclo que no lo contiene. Los números que llegan al final igual a 1 son los llamados **felices**, y al resto les llamaremos **infelices**.

El 203 es feliz, porque $2^2+3^2=13$; $1^2+3^2=10$; $1^2+0^2=1$

Son felices, por ejemplo, 1, 7, 10, 13, 19, 23, 28, 31, 32, 44, 49, 68, 70, 79, 82, 86, 91, 94, 97 y 100

4 no es feliz, porque entra en un bucle: 4, 16, 37, 58, 89, 145, 42, 20, 4...

Fermat

Conjetura de Fermat (o gran teorema)

La ecuación diofántica $x^n + y^n = z^n$ no tiene solución para $n > 2$

Euler la demostró para $n=3$ y $n=4$, Dirichlet para $n=7$ y Legendre para $n=14$.

En 1995 la demostró Wiles para todo n .

Ecuación de Fermat

La ecuación $y^2 - a \cdot x^2 = 1$

Si a no es un número cuadrado admite infinitas soluciones.

Fibonacci

Sucesión de Fibonacci

Se llama sucesión de Fibonacci a la siguiente: 1, 1, 2, 3, 5, 8, ...que cumple que cada elemento es suma de los dos anteriores, definiendo además a_1 como 1 y a_2 como 1

Multiplicación de Fibonacci

La representación de [Zeckendorf](#) da lugar a un producto muy curioso, que consiste, dados dos números representados como suma de elementos de Fibonacci, formar un sumatorio doble en el que cada sumando sea

un número de Fibonacci cuyo índice sea la suma de los índices de cada uno de los factores.

Figurado

Números figurados

Se llaman así aquellos números que representan conjuntos cuyos elementos se pueden situar en forma de figura geométrica regular. Pueden ser [triangulares](#), [cuadrados](#), pentagonales, [oblongos](#), etc.

Finito

Conjunto finito

Un conjunto es finito cuando es [coordinable](#) con un conjunto $\{1,2,3,\dots,n\}$ de números naturales para un cierto n , que sería su [cardinal](#). También se caracteriza porque no es coordinable con ninguno de sus subconjuntos propios.

Fracción continua

Llamamos fracción continua a la expresada de esta forma:

$$a + \frac{1}{b + \frac{1}{c + \frac{1}{d \dots}}}$$

donde a es entero y b, c...son enteros positivos llamados cocientes. Toda fracción ordinaria se puede expresar de esta forma, y todo número irracional admite aproximaciones mediante desarrollos de este tipo

Friedman

Número de Friedman

Es un tipo de número narcisista. Es aquel que en un base de numeración dada puede ser generado por todas sus cifras y los operadores +, -, *, / y ^ (potenciación). Se permiten paréntesis para salvaguardar la jerarquía de operaciones y la alteración del orden de las cifras. También se permite concatenar dos cifras.

Los primeros números de Friedman son: 25, 121, 125, 126, 127, 128, 153, 216, 289, 343, 347, 625, 688, 736, 1022, 1024, 1206, 1255, 1260, ..., pues $25=5^2$, $121=11^2$, $125=5^{(1+2)}$, $126=21*6$,...

G

Gauss

Teoremas famosos de Gauss

- a) Un número natural es suma de 3 cuadrados si y sólo si no es de la forma $4^a(8b-1)$
- b) Todo número natural es suma de a lo más tres cuadrados.
- c) Todo número natural es suma de a lo más tres triangulares.

Geométrico/a

Sucesión o progresión geométrica

Es aquella sucesión en la que cada término es igual al anterior multiplicado por un número constante llamado *razón*. El primer término se define aparte.

Media geométrica

Ver [Media](#)

Gnomon

La palabra *gnomon* tiene varios significados en Geometría y Trigonometría. Aquí nos interesa como *número figurado*. Un número es de tipo *gnomon* cuando

se pueden dibujar sus unidades como escuadras de lados iguales.

Golomb

Regla de Golomb

Se le da el nombre de Regla de Golomb a un conjunto de marcas señaladas en una regla imaginaria, tal que todas las diferencias entre marcas sean distintas.

Sucesión de Golomb

Tiene una definición muy curiosa, y es que $a(n)$ representa el número de veces que aparece n en la sucesión, si además definimos $a(1)=1$ e implícitamente aceptamos que cada valor de n ocupa el mínimo número de orden posible. Sus primeros elementos son:

1, 2, 2, 3, 3, 4, 4, 4, 5, 5, 5, 6, 6, 6, 6, 7, 7, 7, 7, 8, 8, 8, 8, 9, 9, 9, 9, 9, 10, 10, 10, 10, 10, 11, 11, 11, 11, 11, 12, 12, 12, 12, 12, ...

Grupo

Un conjunto dotado de una operación tiene estructura de *grupo* cuando para esa operación constituye un [semigrupo](#) y además existe un elemento [neutro](#) y cada elemento del conjunto posee un [inverso](#). Si además

posee la propiedad conmutativa diremos que el grupo es abeliano.

H

Hamming

Distancia de Hamming

Hamming definió su distancia para palabra binarias como el número total de bit en los que ambas se diferencian, comparando, como es de esperar cada uno con el que ocupa el mismo lugar en la otra palabra. Así, la distancia de Hamming entre 11001011 y 11100011 es de 2, porque son diferentes entre sí los dígitos resaltados en negrita.

Harshad

Un **número de Harshad** o **número de Niven** es un número entero divisible entre la suma de sus dígitos en una base dada.

Es claro que los números de una cifra son todos de Niven. Así que es más interesante estudiar los de varias cifras. También se comprende que los números de Niven de más de una cifra no pueden ser primos.

Heterómero

Número heterómero

Sinónimo de Oblongo

Hexagonal

Número poligonal de seis lados. Su fórmula es
 $H(n)=n(2n-1)$

DE I A O

I

Idempotente

Una operación definida en un conjunto tiene la propiedad *idempotente* cuando para todo elemento a del conjunto se cumple

$$a * a = a$$

Por ejemplo, son idempotentes el MCD, el MCM o el orden \leq

Igualdad

Números iguales

Dos números son iguales cuando representan como [cardinales](#) al mismo conjunto o a conjuntos [coordinables](#).

Impar

Número impar

Un número se llama *impar* si no es divisible entre 2. Se le puede representar por la fórmula $2n+1$

Inducción completa

Método de demostración de propiedades referentes a números naturales consistente en:

- a. Demostrar la propiedad para $n=1$.
- b. Demostrar que si la propiedad es cierta para n , también lo es siempre para $n+1$.

Con esto quedará demostrado que es cierto para todo n natural.

Por ejemplo. Demuestra así que la suma de los n primeros números impares es igual a n^2 .

Infinito

Conjunto de tipo infinito

Un conjunto es de tipo infinito cuando es coordinable con algún subconjunto propio. Por ejemplo, el conjunto de los números naturales $1,2,3,4\dots$ es infinito, porque es coordinable con $2,4,6,8\dots$

Inverso

Elemento inverso en un grupo

Un elemento b de un grupo es inverso de otro a y se representa por a^{-1} , cuando la operación entre ambos da como resultado el elemento neutro:

$$a*b = e, \text{ o bien } a*a^{-1} = e$$

Si el grupo es aditivo, el inverso se suele llamar *opuesto* $(-a)$, y en ese caso se cumple $a + (-a) = 0$

J

Jacobsthal

Sucesión de Jacobsthal

Es una sucesión recurrente de segundo orden, definida por

$$X_0=0, \quad X_1=1, \quad X_n=X_{n-1}+2X_{n-2}$$

Sus primeros términos son: 0, 1, 1, 3, 5, 11, 21, 43, 85, 171, 341, 683, 1365, 2731, 5461, 10923, 21845, 43691, ...

Jerarquía de operaciones

La jerarquía de una operación es el orden de prioridad que posee en un cálculo complejo cuando no hay paréntesis presentes. Consiste en el siguiente orden:

1. Potencias y raíces
2. Multiplicaciones y divisiones
3. Sumas y restas

K

Kaprekar

En 1949 este matemático indio estudió la rutina u operación que lleva su nombre. A partir de cualquier número de cuatro cifras N no todas iguales formó dos números distintos: N' formado por las mismas cifras en orden decreciente y N'' formado mediante una ordenación creciente. A la diferencia $K(N) = N' - N''$ la llamaremos **Función de Kaprekar** de N . Así $K(2543) = 5432 - 2345 = 3087$. Esta función puede iterarse, y formar $K(K(N))$, $K(K(K(N)))$, etc. En el ejemplo $K(K(2543)) = K(3087) = 7803 - 3087 = 4716$. Estas definiciones se extienden a número cualquiera de cifras, aunque Kaprekar sólo estudió el caso de cuatro.

Si se itera la función de Kaprekar puede llegarse **al número cero, a una constante o a un ciclo**. Este resultado depende del número de cifras y del valor de N . En el caso de terminar en una constante, esto se produce porque $K(N)=N$. Esto ocurre con el número 495 en el caso de tres cifras y con 6174 en el caso de cuatro (en sistema de numeración decimal), a los que se les llama constantes de Kaprekar para ese número de cifras.

Para dos cifras no existen constantes, pero se producen ciclos, como 9 , 81, 63, 27, 45, 9. Para cinco cifras no

existen números invariantes respecto a la función K , pero sí se producen ciclos. Con seis existen dos: 549945 y 631764.

L

Ley

Ley

La palabra **ley** puede significar en general toda fórmula, algoritmo o regla que determina la estructura o formación de un objeto matemático.

Ley de composición interna

Dado un conjunto S , llamaremos Ley de Composición Interna a toda aplicación del conjunto $S \times S$ en S , es decir, una aplicación que hace corresponder a cualquier par de elementos del conjunto S en otro elemento del mismo conjunto.

Las operaciones de sumar y multiplicar suelen estar definidas de forma que constituyan leyes de composición interna. No así la resta y la división.

Ley formal

Se utiliza como sinónimo de propiedad de una operación.

Lösch

Números de Lösch

Estos números son aquellos que se pueden representar como $N=x^2+xy+y^2$, con x e y números enteros. Como X e Y pueden tener distinto signo, una definición alternativa es la de pueden escribirse como $N=x^2-xy+y^2$.

Aparecen como las normas de los números enteros de Eisenstein, pero no seguiremos por ahí porque es un tema de números complejos. Estos números son cerrados para la operación de multiplicar, por lo que si m y n pertenecen a este tipo, también lo serán mn , m^k y n^k .

Lucas

Sucesión de Lucas

Se llama sucesión de Lucas a la siguiente: 1, 3, 4, 7, 11, 18, ...que cumple que cada elemento es suma de los dos anteriores, definiendo además a_1 como 1 y a_2 como 3. Es muy a la de [fibonacci](#), con la que comparte propiedades.

Lychrel

Números de Lychrel

Se llaman números de Lychrel a aquellos para los que no se sabe si el Algoritmo 196 tiene parada o no

M

Mayor

Ver [Desigualdad](#)

McNugget

Un número entero positivo “McNugget”, es aquel que es expresable como combinación lineal, con coeficientes enteros no negativos, de los números 6, 9 y 20. Se llama así porque 6, 9 y 20 eran los contenidos de las cajas de McDonald's® Chicken McNuggets™.

Media

Aritmética

La media aritmética de un conjunto de números es el cociente de dividir su suma entre el número de elementos.

$$\bar{a} = \frac{a_1 + a_2 + a_3 + \dots + a_k}{k}$$

Geométrica

La media aritmética de un conjunto de números es la raíz de índice el número de elementos del producto de los mismos.

$$g = \sqrt[k]{a_1 \cdot a_2 \cdot a_3 \cdot \dots \cdot a_k}$$

Armónica

La media armónica de un conjunto es el número inverso de la media aritmética de los inversos de los elementos de ese conjunto.

$$h = \frac{k}{\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \dots + \frac{1}{a_k}}$$

Contraarmónica Ver [contraarmónica](#)

Menor

Ver [Desigualdad](#)

Mian-Chowla

Sucesión de Mian-Chowla

Esta sucesión se define por recurrencia de dos formas equivalentes:

(a) $a(1) = 1$, $a(n)$ es el menor número mayor que $a(n-1)$ tal que todas las sumas $a(i)+a(j)$ con $i, j \leq n$ son distintas.

(b) $a(1) = 1$, $a(n)$ es el menor número mayor que $a(n-1)$ tal que todas las diferencias $a(i)-a(j)$ con $i, j \leq n$ $i > j$ son distintas.

Minuendo

Primer dato de una operación de [restar](#). Así en $a-b$ llamamos **minuendo** a **a** y sustraendo a **b**.

Moessner

Algoritmo (simple curiosidad) para extraer potencias de la serie natural tachando de forma periódica. Este algoritmo lo propuso Alfred Moessner y fue demostrada su validez para cualquier valor natural por Oskar Perron en 1951 usando la inducción matemática.

Monotonía

Propiedad monótona

Una operación $*$ es monótona cuando $a > b$ implica que $a * c > b * c$ para todo número c del conjunto en el que se opera.

Así, son monótonas la adición y la multiplicación por un número positivo.

Multiplicación

Multiplicación como operación

Operación de hallar el [producto](#)

Multiplicación "rusa"

Es una forma de multiplicar que viene de la antigüedad y se popularizó en Rusia. Requiere velocidad de cálculo mental para duplicar reiteradamente uno de los factores mientras se divide entre dos el otro (de forma entera, sin decimales). Finalmente se suman las duplicaciones que correspondan a las mitades *impares*. Así:

Multiplicar 23 por 120

Dividir

entre	Duplicar	Sumar los correspondientes a
dos el	el 120	impares
23		

	120	120
--	-----	-----

11	240	240
----	-----	-----

5	480	480
---	-----	-----

2	960	
---	-----	--

1	1920	1920
---	------	------

Suma de la
tercera columna $2760 = 23 \cdot 120$

El fundamento de este método es la representación del primer número en base binaria: $23 = 2^4 + 2^3 + 2^2 + 1$, es decir, como $11101_{(2)}$. Las cifras 1 indican qué potencia se ha de sumar.

Múltiplo

Número múltiplo de otro

Ver [División](#)

N

Narayana

Sucesión de las vacas de Narayana

Sucesión similar a la de Fibonacci, con este planteamiento:

Una vaca tiene anualmente una cría. Cada una de ellas, cuando ya es novilla a los cuatro años, también tiene una cría anual ¿Cuántas vacas habrá a los N años?

Sus primeros términos son 1, 1, 1, 2, 3, 4, 6, 9, 13, 19, 28, 41, 60, ...

Narcisista

Número narcisista

Un número es narcisista en el sistema de numeración decimal cuando equivale a la suma de las potencias de sus cifras elevadas todas al mismo índice. El más pequeño que se conoce es el 153, que equivale a $1^3+5^3+3^3$ y le sigue el $370 = 3^3+7^3+0^3$

Un narcisista impresionante es $4^{10} + 6^{10} + 7^{10} + 9^{10} + 3^{10} + 0^{10} + 7^{10} + 7^{10} + 7^{10} + 4^{10} = 4679307774$

Un tipo de números similar es el de [Friedman](#).

Natural

Número natural

Son los números 1,2,3,4....(a veces se incluye el 0 para algunas cuestiones), los más sencillos que existen y los primeros en ser inventados por la Humanidad. Su definición rigurosa se construye a partir de los Axiomas de Peano. Se representan por N.

El conjunto N es semigrupo para la adición y la multiplicación.

Neutro

Elemento neutro

En elemento O se llama **neutro** para una operación $*$ cuando $a*O=O*a=a$ para todo a del conjunto en el que se opera. En la suma de enteros el neutro es el 0 y en la multiplicación, el 1.

Numeración

Sistema de numeración

Es un conjunto de símbolos finitos y reglas que permiten representar todos los números naturales.

Sistema de numeración decimal

Es el constituido por las cifras 0,1,2,3...9 unidas mediante un sistema de representación posicional, es decir, en el que cada cifra tiene un valor distinto según su posición.

Número

Ver Número

[Automórfico](#), [Cardinal](#), [Cuadrado](#), [Figurado](#),
[Heterómero](#), [Impar](#), [Narcisista](#), [Par](#), [Piramidal](#),
[Plástico](#), [Poligonal](#), [Triangular](#), [Trimórfico](#)

Ver Números

[Proporcionales](#)

O

Oblongo

Número del tipo $n(n+1)$, siendo n un número natural.

Operación

Es toda ley que hace corresponder a cada par de elementos de un conjunto, otro elemento único de ese conjunto. Son operaciones la adición, sustracción, multiplicación, etc.

Opuesto

Ver [inverso](#)

Orden

Definición de relación de orden

Una [relación](#) \leq definida en un conjunto A se llama **de orden** cuando cumple las tres propiedades

Reflexiva: Para todo elemento a de A se cumple que $a \leq a$

Antisimétrica: Si dos elementos de A , a y b , cumplen simultáneamente que $a \leq b$ y $b \leq a$, entonces $a=b$, es decir, son idénticos

Transitiva: Si tres elementos a , b y c de A cumplen que $a \leq b$ y que $b \leq c$, entonces, $a \leq c$

Si un conjunto está dotado de una relación de orden, le llamaremos ordenado. Así, los números naturales están ordenados mediante la relación "menor o igual" y otras muchas.

Orden total

Los números naturales, para la relación \leq presentan un **orden total**, porque para cada par de números a y b siempre se verifica $a \leq b$ o bien $b \leq a$ (son comparables).

Orden parcial

Los números naturales, para la relación de *ser múltiplo* presentan un **orden parcial**, dado que existen pares de números no comparables, como 4 y 7 que ninguno de ellos es múltiplo del otro. **Buen orden**

El orden natural de los números posee buena ordenación, es decir, en cada conjunto finito de números naturales podemos elegir siempre el mínimo.

Cotas y máximos

Diremos que un elemento a es **cota superior** de un conjunto ordenado A , cuando se verifica $x \leq a \ \forall x \in A$ (para todo x de A). Por ejemplo, número 2 es una cota superior de los números negativos.

Si, por el contrario, se verifica $a \leq x \forall x \in A$ diremos que a es **cota inferior** del conjunto A . De forma similar al ejemplo anterior, el cero es cota inferior de los positivos.

Llamaremos **extremo superior o supremo** a una cota superior tal que no exista ninguna otra cota superior que sea inferior a ella. Si además pertenece al conjunto, la llamaremos **máximo** del conjunto. Así, El número 24 es el máximo de sus propios divisores 1,2,3,4,6...24, y el número 0 es extremo superior de los negativos, pero no es su máximo.

Igualmente podemos definir **extremo inferior o ínfimo**, y mínimo. El extremo inferior es la mayor cota inferior del conjunto. El cero es extremo inferior de los números reales positivos. El mínimo es un extremo inferior de A que pertenece al mismo A . El 1 es el mínimo divisor de cualquier otro número natural.

Un elemento es **maximal** en un conjunto ordenado si no existe en el conjunto otro elemento mayor que él. En un mismo conjunto pueden existir varios elementos maximales. Por ejemplo, en el conjunto 2, 3, 5, 6, 12, 15 de divisores de 60, ordenados por la relación divisor - múltiplo, los números 12 y 15 son maximales (pero no máximos). De forma simétrica se definen los **minimales**. En el ejemplo anterior lo serían 2,3 y 5.

DE P A Z

P

Padovan

Sucesión de Padovan

Es la sucesión definida por recurrencia:

$$P(0)=1, P(1)=1, P(2)=1, P(n)=P(n-2)+P(n-3)$$

Sus primeros términos son: 1, 1, 1, 2, 2, 3, 4, 5, 7, 9, 12,
...

Palindrómico

Número palindrómico (o capicúa) es aquel que es igual a su reverso. Los números de una sola cifra se consideran palindrómicos

Pandigital

Número pandigital

Número pandigital es aquel que contiene en su expresión decimal las diez cifras 0123456789. Se

puede extender la definición a otras bases. Es sinónimo de capicúa.

Par

Número par

Un número se llama *par* si es divisible entre 2. Se le puede representar por la fórmula $2n$, con **n** natural.

Paridad

Paridad de un número natural

Es el carácter par o impar de ese número.

Peano

Axiomas de Peano

El conjunto N de números naturales se puede definir axiomáticamente mediante cinco axiomas debidos a Peano:

Los números naturales son los elementos de un conjunto N en el que existe un elemento llamado 1 y una relación llamada *siguiente* ($sg(n)$) que cumple:

- El 1 pertenece a N .
- A cada elemento **m** de N le corresponde otro **sg(m)** llamado *siguiente de m*, que es único.
- El número 1 no es siguiente de otro elemento.

- Si dos siguientes $\text{sg}(\mathbf{m}) = \text{sg}(\mathbf{p})$ son iguales, sus antecedentes $\mathbf{m}=\mathbf{p}$ también son iguales.
- Si un subconjunto C de N cumple las condiciones:
 - A) 1 pertenece a N
 - B) Si \mathbf{m} pertenece a C, entonces $\text{sg}(\mathbf{m})$ también pertenece a C
 entonces $C=N$

Pell

Ecuación de Pell

Es aquella del tipo $\mathbf{ax}^2+1 = \mathbf{y}^2$, con \mathbf{a} entero positivo.

Si \mathbf{a} es cuadrado perfecto, no existen soluciones a esta ecuación, pero si no lo es, obtendremos infinitas soluciones.

Esta ecuación no la estudió Pell (fue un error de Euler, que le dio ese nombre), pero sí Fermat y Wallis.

Es útil en muchos problemas, como el de hallar números triangulares y cuadrados a la vez.

Números de Pell

Se llaman números de Pell o números lambda a los términos e la sucesión: 0, 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, 5741, 13860, 33461, 80782, 195025, 470832, 1136689, ..., que se obtienen mediante la fórmula de recurrencia $\mathbf{a}_1 = 0, \mathbf{a}_2=1, \mathbf{a}_n=2*\mathbf{a}_{n-1} + \mathbf{a}_{n-2}$.

Estos números coinciden con los coeficientes de la aproximación a la raíz cuadrada de 2 mediante [fracciones continuas](#). Dicha aproximación da lugar a una sucesión de fracciones

1	3	7	17	41	99	239	577	1393
1	2	5	12	29	70	169	408	985

en la que los denominadores coinciden con los números de Pell y a los numeradores se les conoce como números de Pell-Lucas. Sus cocientes se aproximan a la raíz de 2.

Pentagonal

Número [poligonal](#) de cinco lados. Su fórmula es $P(n)=n(3n-1)/2$

Perrin

Sucesión de Perrin

Es la sucesión definida por recurrencia:

$$P(0)=3, P(1)=0, P(2)=2, P(n)=P(n-2)+P(n-3)$$

Sus primeros términos son: 3, 0, 2, 3, 2, 5, 5, 7, 10, 12, 17, 22, ...

Persistencia (aditiva o multiplicativa)

Neil Sloane introdujo este término en su artículo [The persistence of a number, J. Recreational Math., 6 (1973), 97-98] En él define esta persistencia multiplicativa (existe otra muy popular, aditiva) de la forma siguiente:

Se multiplican (o se suman si es aditiva) las cifras del número y se reitera esta operación con los números obtenidos. Estos productos formarán una sucesión decreciente, y se cuentan las iteraciones necesarias hasta llegar a un producto de una sola cifra. Al número de esos pasos se le denomina índice de persistencia.

Piramidal

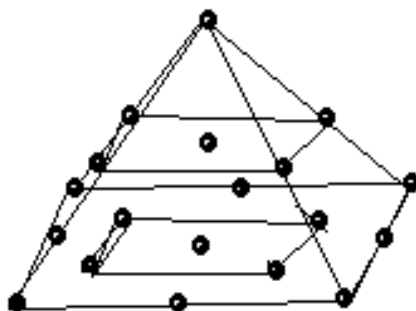
Número Piramidal

Es aquel tal que las unidades del conjunto que representa se pueden situar en forma de pirámide. Son sumas de poligonales consecutivos.

Por ejemplo, los piramidales triangulares serán 1, 4, 10, 20, 35, etc. y su fórmula general $(n(n+1)(n+2))/6$

Piramidal centrado

Es un número piramidal en el que los sumandos son poligonales centrados.



Pitagórica

Ecuación pitagórica

Es aquella que tiene la forma $a^2 + b^2 = c^2$

Sus soluciones primitivas, en las que **a**, **b** y **c** son primos entre sí, vienen dadas por las expresiones

$$a=m*n, b=(n^2 - m^2)/2, c=(n^2 + m^2)/2$$

En las que **n** y **m** son números impares primos entre sí, con $n > m$

Plástico

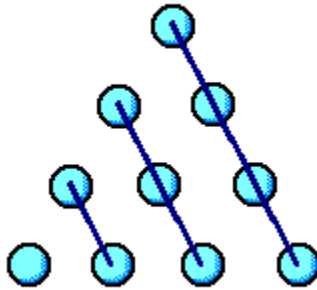
Se da el nombre de *número plástico* al número 1,3247179572..., raíz de la ecuación $x^3 = x + 1$

Aparece como límite del cociente $A(n)/A(n-1)$ en las sucesiones de Perrin y Padovan.

Poligonal

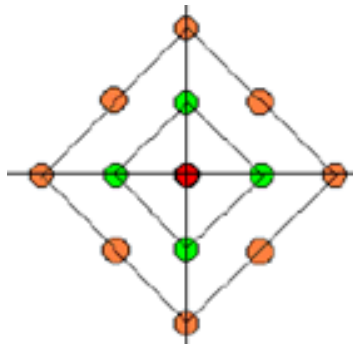
Número Poligonal

Es un número figurado tal que las unidades del conjunto que representa se pueden situar ordenadamente en forma de polígono. Pueden ser [triangulares](#), [cuadrados](#), pentagonales, etc.



Poligonal centrado

Es un poligonal en el que las sumas parciales que lo forman son a su vez poligonales con un centro.



En la figura se representa un cuadrado centrado de orden 3.

Poligorial

Los números poligoriales se definen de forma similar a los factoriales, pero en lugar de multiplicar números naturales consecutivos, lo hacen con los números poligonales.

Un número poligorial de orden k equivale al producto de los primeros números poligonales de orden k . Por ejemplo, 180 es poligorial de orden 3, porque es el producto de los cuatro primeros números triangulares: $180=1*3*6*10$.

Potencia

Potencia de un número natural con exponente natural

Llamaremos potencia de *exponente* k de un número natural n llamado *base*, y la representaremos por n^k , al producto $n.n.n\dots n$ de k factores iguales a n .

Potenciación

Operación de calcular la [potencia](#) de un número

Producto

Producto de dos números

El producto de dos números naturales **a** y **b** es otro número **c** obtenido como **b** sumas reiteradas de **a**. Coincide con la suma reiterada **a** veces del número **b**.

Proporción

Una proporción es una igualdad de dos fracciones o razones: $a/b = c/d$. Los números que forman una proporción se llaman *proporcionales*.

Proporcional

Cuatro números son proporcionales cuando forman una proporción entre ellos

R

Radicación

Es la operación de calcular la raíz de un número.

Raíz

Raíz enésima entera

Dado un número natural **a**, llamaremos raíz enésima entera del mismo a otro número natural **s** que cumpla:
 $s^n \leq a < (s+1)^n$

Llamaremos **resto** de esta operación de **radicación** al número **r** que cumple: $a = s^n + r$

Si **r** es igual a 0, diremos que la raíz es **exacta**.

Razón

Sinónimo de fracción, cociente o comparación.

Ramanujan

Número de Ramanujan

Es el 1729 como el menor número que se expresa de dos formas distintas como suma de dos cubos:
 $1729 = 1^3 + 12^3 = 10^3 + 9^3$

Recamán

Sucesión de Recamán

Es una original sucesión que Bernardo Recamán Santos envió a N. J. A. Sloane en 1991 para su colección, y que desde entonces ha originado múltiples desarrollos.

Su definición es la siguiente (versión con $a(1)=1$):

$$a(1) = 1$$

$a(n) = a(n-1) - n$, si este valor es positivo y no figura ya en la sucesión

$a(n) = a(n-1) + n$, en caso contrario.

Sus primeros términos son: 1, 3, 6, 2, 7, 13, 20, 12, 21, 11, 22, 10, 23, 9, 24, 8, 25, 43, 62, 42, 63, 41, 18, 42, 17, 43, 16, 44, 15, 45, 14, 46, 79, 113, 78, 114, 77, 39, 78, 38, 79, 37, 80, 36, 81, 35, 82, 34, 83, 33, 84, 32, 85, 31, 86, 30, 87, 29, 88, 28, 89, 27, 90, 26, 91, 157,... (existe otra versión que comienza en 0, idéntica a esta en todo lo demás <http://oeis.org/A005132>)

Rectangular

Es un número cuyas unidades se pueden ordenar en forma de rectángulo de lados mayores que uno.

Recurrencia

Sucesiones recurrentes

Una sucesión es recurrente cuando, a partir de cierto índice, todos los elementos se definen en función de los anteriores.

Recurrencia lineal de primer orden

Es aquella definida por una relación del tipo $x_n = a_1 x_{n-1} + a_2$

Recurrencia lineal de segundo orden

Es aquella definida por una relación del tipo $x_n = a_1 x_{n-1} + a_2 x_{n-2} + a_3$

Reducida

Fracción reducida

Se llama *fracción reducida* de una fracción continua a la resultante de eliminar de la misma su últimos cocientes. También recibe este nombre a toda fracción resultante del algoritmo de los cumulantes aplicados los restos del algoritmo de Euclides.

Relación binaria

Una ***relación binaria*** en un conjunto A es un subconjunto R del producto cartesiano $A \times A$. Diremos que dos elementos x e y de A están **relacionados**, y escribiremos aRb cuando el par (a,b) pertenezca al subconjunto R

Repidígito

Un número es repidígito si en un sistema de numeración todas sus cifras son iguales, como 22222.

Repituno

Un número es repituno, repuno o repunit, si en un sistema de numeración todas sus cifras son iguales a la unidad: 111111.

Resta

Sinónimo de [sustracción](#)

Resto

Resto de una división

Ver [división](#)

Reverso

Sinónimo de número [simétrico](#) de otro.

Rhonda

Número de Rhonda

Los números de Rhonda son aquellos naturales que cumplen que el producto de sus cifras es igual a la base de numeración multiplicada por la suma de cifras de sus factores primos.

Un ejemplo es el número 5265 en base 10, que se descompone como $5265=3^4 \cdot 5 \cdot 13$, y se cumple que $5 \cdot 2 \cdot 6 \cdot 5=300=10 \cdot (3+3+3+3+5+13)=10 \cdot 30$

S

Saint-Exupery

Números de Saint-Exupery

Reciben este nombre aquellos números que coinciden con el producto de los tres lados de una terna pitagórica. El primero, como era de esperar, es 60, que es el producto de 3, 4 y 5, elementos de la terna más sencilla que conocemos. El segundo, 480, es el producto de sus dobles, $6 \cdot 8 \cdot 10$.

Semigrupo

Un conjunto dotado de una operación constituye un *semigrupo* cuando esa operación es [cerrada](#) y [asociativa](#) en ese conjunto. El semigrupo puede ser conmutativo si la operación tiene esa [propiedad](#) y también poseer un elemento [neutro](#).

Semifactorial

Llamaremos ***semifactorial*** de un número natural n al producto $n(n-2)(n-4)(n-6)\dots$ terminando el producto en 2 o 1, según la paridad de n y lo representaremos así: $n!!$

Sidon

Conjunto de Sidon

Un conjunto de números naturales se llama de Sidon cuando todas las sumas posibles entre sus elementos son distintas. Por ejemplo $\{3,5,8,9\}$ produce las sumas 8,11,12,13,14 y 17.

Simétrico

Número simétrico de otro en una base dada

Llamamos reverso o simétrico de un número natural a otro número que contiene las mismas cifras pero en orden opuesto.

Sistema

Sistema de numeración

Un sistema de numeración es un conjunto finito de símbolos y unas reglas de formación que permiten representar números válidos en dicho sistema.

Sólido

Se llama sólido a aquel número natural cuyas unidades se pueden disponer como un paralelepípedo rectángulo de lados mayores que uno. Equivale a decir que se puede expresar como producto de tres números naturales.

Sordo

Llamaremos *sordo* a todo número natural que no posea raíz exacta.

Sucesión

Sucesión de números naturales

Es toda función definida de \mathbb{N} (conjunto de los números naturales) en \mathbb{N} . A los elementos orígenes de la función les llamaremos **índices**, y a las imágenes **elementos** de la sucesión.

En la práctica es una secuencia ordenada de números naturales del tipo 2,4,7,11,12,.....representada por los símbolos

$a_1, a_2, a_3, a_4, \dots, a_n, \dots$ en la que a_n es el elemento y n el índice.

Suma

Suma de dos números naturales

La suma de dos números naturales **a** y **b** (llamados *sumandos*) es otro número **c** (llamado *suma*) que es el **cardinal** de un conjunto formado por la unión de otros dos conjuntos disjuntos cuyos cardinales son **a** y **b**. Es decir: se eligen dos conjuntos que representen a los

sumandos y que sean disjuntos. Su unión representará al número suma.

La operación de sumar, o hallara la suma se llama *adición*.

Sumando

Cada uno de los datos de una suma

Sustracción

Operación de restar a un número **a** otro **b**, es decir, encontrar otro número **c** tal que se cumpla: $a=b+c$

Sustraendo

Segundo dato de una operación de restar. Así en $a-b$ llamamos minuendo a **a** y **sustraendo** a **b**.

T

Teorema

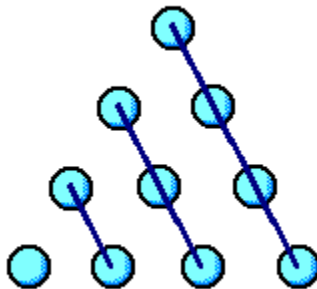
Ver Teoremas de [Bachet de Meziriac](#)

Terna pitagórica

Una terna de números enteros positivos se llama pitagórica si es solución de la ecuación $x^2 + y^2 = z^2$. Llamaremos ternas pitagóricas primitivas x_0 , y_0 y z_0 a aquellas que no tienen divisores comunes.

Tetractys

Nombre dado por los pitagóricos al número diez, considerado como número triangular..



Tetragonal

Número tetragonal

Se llaman tetragonales a los números piramidales de tres lados.

Son los números 1, 4, 10, 20, 35, etc. y su fórmula general es $(n(n+1)(n+2))/6$

Triangular

Número triangular

Un número triangular es aquel cuyas unidades se pueden situar en forma de triángulo

Los primeros números triangulares son: 1, 3, 6, 10, 15, 21, ...

Todos siguen la fórmula $n(n+1)/2$, con $n=0, 1, 2, 3, \dots$

Tribonacci

Sucesión de Tribonacci

Nombre coloquial con el que se conocen los elementos de la sucesión construida como la de Fibonacci, pero usando sumas de tres en tres, es decir:

$A(1)=1, A(2) = 1, A(3) = 2$, y como fórmula de recurrencia **$A(n) = A(n-3)+A(n-2)+A(n-1)$** para $n>3$

Los primeros términos son: 1, 1, 2, 4, 7, 13, 24, ...

U

Ulam

Sucesión de Ulam

Es la sucesión 1, 2, 3, 4, 6, 8, 11, 13, 16, 18, 26, 28, 36, 38, 47, ...definida por Stanislav Ulam

En ella $a_1=1$, $a_2=2$ y los siguientes términos son los menores números que pueden expresarse de forma única como suma de dos términos tomados entre sus anteriores. Así, $3=1+2$, $4=1+3$, $6=4+2$. El 5 no está porque $5=2+3=1+4$.

Espiral de Ulam

Es una disposición de los números en espiral en la que los números primos parecen seguir ciertas diagonales.

Números de Ulam

Se llaman *números de Ulam* a los que forman una sucesión construida de la siguiente forma:

Se declara $u(1)=1$ y $u(2)=2$ (esto se puede alterar) y después definiremos $u(n+1)$ como el primer número que se pueda expresar como **suma de dos números de Ulam anteriores distintos, de forma única.**

Unidad

Se le da el nombre de unidad al número 1, elemento neutro de la multiplicación.

W

Woodall

Un número de Woodall es un número natural de la forma $n \cdot 2^n - 1$. Los números de Woodall más pequeños son 1, 7, 23, 63, 159, 383, 895, ...

Y

Yellowstone

En sucesión se comienza con los valores $a(1)=1$, $a(2)=2$ y $a(3)=3$, y los siguientes $a(n)$ son los números naturales más pequeños que aún no hayan aparecido en la sucesión y que tengan algún factor común con $a(n-2)$ y ninguno con $a(n-1)$. Para entenderlo bien podemos ir generando términos según la definición. A 1, 2 y 3 le debe seguir el 4, que es el más pequeño que comparte factores primos con el 2 pero no con el 3. Tenemos ya 1, 2, 3 y 4.

El siguiente no puede ser 5, 6, 7 ni 8. Deberá ser el 9, que comparte el factor 3 con el 3 y ninguno con el 4. Así podemos seguir generando, hasta completar:

1, 2, 3, 4, 9, 8, 15, 14, 5, 6, 25, 12, 35, 16, 7, 10, 21, 20, 27, 22, 39, 11, 13, 33, 26, 45, 28, 51, 32, 17, 18, 85, 24, 55, 34, 65,...(<http://oeis.org/A098550>)

Z

Zeckendorf

Cada entero positivo puede expresarse de manera única como una suma de números distintos de Fibonacci no consecutivos. La secuencia de números de Fibonacci que se suman se denomina representación de Zeckendorf

DIVISIBILIDAD

DE A A H

Abundancia

Dado un número natural N , llamaremos abundancia de N al cociente entre $\sigma(N)$ entre N , es decir, entre la suma de sus divisores y él mismo. En los números perfectos la abundancia vale 2, en los deficientes menos de 2 y en los abundantes más de esa cantidad.

Abundante

Número abundante o excesivo

Un número es abundante si es menor que la suma de todos sus divisores propios, por ejemplo el 12.

Adenda

Recibe este nombre la función que está definida a partir de una suma extendida a todos los divisores de un número. Los elementos de esta suma se llaman adendum.

Aditiva

Función aditiva en Teoría de Números

Una función **g** definida sobre números naturales posee la propiedad **completamente aditiva** si se verifica que **$g(a \cdot b) = g(a) + g(b)$** para cualquier par de números naturales **a** y **b**.

Si únicamente se cumple para coprimos (primos entre sí), se dirá que es **aditiva** simplemente.

Un ejemplo de función completamente aditiva es el [logaritmo entero](#) o suma de factores primos con repetición. Si se sumaran los factores sin repetirlos, la función sólo sería aditiva.

Admirable

Son similares a los perfectos, pero en estos la coincidencia se da con la suma de todos los divisores propios (parte alícuota) y en los admirables a esa suma hay que restarle el doble de uno de los divisores, para que así cambie su signo en la suma. Por ejemplo, es admirable 650, porque

$$650 = 325 + 130 + 65 + 50 + 26 + 25 + 13 + 10 + 5 + 2 - 1$$

Algoritmo

Es una serie finita de reglas o cálculos en un orden determinado para obtener un resultado a partir de unos datos

Algoritmo de Euclides

Algoritmo que encuentra el MCD de dos números **a** y **b** mediante divisiones sucesivas.

Alícuota

Parte alícuota

Una parte alícuota de **n** es todo divisor propio del mismo, es decir, menor que **n**.

Sucesión alícuota

Una sucesión alícuota es aquella definida por recurrencia en la que cada término es la parte alícuota del anterior. Su final puede ser cero, un número constante, una sucesión periódica o bien ser desconocida hasta la fecha.

Altamente compuesto

Un número altamente compuesto es un entero positivo con más divisores que cualquier número entero positivo menor que él mismo.

Amigos

Números amigos

Dos números naturales son amigos si cada uno de ellos es igual a la suma de todos los divisores propios del otro.

Así, son amigos los pares 220 y 284

No hay fórmulas para encontrar todos los números amigos, aunque existen para construir algunos ([Ver Thabit idn Qurra](#))

Números casi amigos o comprometidos

Dos números m y n son comprometidos si la suma de los divisores no triviales de uno coincide con el valor del otro. Así, son de ese tipo, 48 y 75, ya que la suma de divisores (función SIGMA) de 48 es $48+24+16+12+8+6+4+3+2+1 = 124$, pero si no contamos el 1 y el propio 48 (divisores triviales) nos queda 75, que es el otro número. Recíprocamente, $SIGMA(75)=124$, y eliminando 75 y 1, nos queda 48.

Andrica

Conjetura de Andrica

“La diferencia entre las raíces cuadradas de dos números primos consecutivos es siempre menor que 1”

$$\sqrt{p_{n+1}} - \sqrt{p_n} < 1$$

Antidivisor

Un antidivisor K de N se define como el *no divisor* que se “acerca” a N dejando intervalos iguales entre N y dos múltiplos consecutivos de K . Por ejemplo, 10 es un antidivisor de 55, porque no es divisor de él, pero 55 equidista de dos de sus múltiplos: $50 < 55 < 60$, con $55 - 50 = 60 - 55$. Una ligera reflexión nos indica que si K es impar, no es posible la equidistancia, y se permite una diferencia de 1.

Antiarmónico

Número antiarmónico

Es aquel número entero en el que $\sigma(N)$ divide a $\sigma_2(N)$: la suma de sus divisores divide a la suma de los cuadrados de los mismos.

Antisigma

Función antisigma

Al igual que se ha definido la función $\text{SIGMA}(N)$ como la suma de todos los divisores de N (incluido él mismo), podemos definir la $\text{ANTISIGMA}(N)$, que es la suma de los números menores que N y que no lo dividen.

Aquiles

Número de Aquiles

Es aquel número natural poderoso (todos los exponentes de sus factores primos son mayores que 1) que no se puede expresar como potencia perfecta del tipo m^n con m y n naturales. Por ejemplo $108=3^3 \cdot 2^2$

Aritmético

Un número natural se llama aritmético si es entera la media aritmética de sus divisores. Por ejemplo, 14 es aritmético, porque $(1+2+7+14)/4=6$, media aritmética entera.

Aspirante

Número aspirante

Es aquel que al iniciar sobre él una sucesión alícuota el final es un número constante. Todos los números perfectos son aspirantes y también algunos no perfectos, como el 25, que produce la secuencia 25, 6, 6, 6, 6

B

Bertrand

Conjetura de Bertrand

Sea $P(x)$ el número de enteros primos inferiores o iguales a x .

Se cumplirá que $P(2x)-P(x)>0$ para todo $x>1$ (o sea, existe un primo entre n y $2n$) (Demostrado por Tchebychev en 1851 y por Erdős de forma más simple)

Bézout

Teorema de Bézout

Dos números naturales son primos entre sí si y sólo si existen dos enteros m y n tales que $m.a+n.b=1$

Bigomega

Función bigomega

La función bigomega $W(N)$ cuenta los factores primos distintos de N teniendo en cuenta las multiplicidades. Equivale a la suma de los exponentes de los factores primos.

Bogotá

Números bogotá

Estos números fueron llamados así por Tomás Uribe y Juan Pablo Fernández, por su similitud con los números colombianos o autonúmeros. Es un homenaje a Bernardo Recamán, matemático colombiano

Su definición es simple: se trata de números N que equivalen a uno de sus divisores multiplicado por el producto de sus cifras (su raíz digital). Un ejemplo es el número 520, que se puede expresar como $52 \cdot 5 \cdot 2$, o bien $8991 = 333 \cdot (3 \cdot 3 \cdot 3)$.

Brasileño

Números primos brasileños

Son números primos que se pueden formar con la suma de las primeras potencias de un número, es decir, cuándo una suma del tipo $1+n+n^2+n^3+n^4+n^5+\dots$ será un número primo. No se considera el caso en el que un primo p sea igual a $1+n$, ya que esto lo cumplen todos los primos.

Brillante

Números brillantes

Son aquellos que son semiprimos y sus dos factores tienen el mismo número de cifras en el sistema decimal.

Por ejemplo, $989=23*43$

Brocard

Conjetura de Brocard

Para $n>1$, si representamos como $p(n)$ al enésimo número primo, se verificará que entre $p(n)^2$ y $p(n+1)^2$ existirán al menos cuatro números primos.

Brun

Constante de Brun

La constante de Brun se define como la suma de la serie formada por la suma de los inversos de los números primos gemelos, que el mismo Brun demostró que es convergente.

$$B= 1/3 + 1/5 + 1/5 + 1/7 + 1/11 + 1/13 + \dots$$

Su valor aproximado es $B=1,902160$

C

Carmichael

Pseudoprimos de Carmichael

Hay algunos pseudoprimos que cumplen la condición $a^{m-1} \equiv 1 \pmod{m}$, para todos los números primos con él. A estos números se les llama de números de Carmichael o pseudoprimos absolutos.

Casiprimo

Un número se llama casiprimo de orden K o k -casiprimo cuando su descomposición factorial contiene K factores primos iguales o distintos. Así, los números [primos](#) son 1-casiprimos, los [semiprimos](#) 2-casiprimos, y así podríamos considerar los 3-casiprimos o 4-casiprimos. El conjunto de todos los números k casiprimos para un k dado se representa con el símbolo P_k . Así, $P_3 = \{8, 12, 18, 20, \dots\}$

Chen

Teorema de Chen

Todo número par suficientemente grande es suma de un primo y del producto de dos primos.

Compuesto

Número compuesto

Es el número que no es primo, es decir, que tiene divisores distintos de sí mismo y la unidad.

Congruencia

Relación de congruencia

Diremos que a y b son congruentes módulo n , siendo los tres números naturales, si la diferencia $b-a$ (o bien $a-b$) es un múltiplo de n . Representaremos la relación de congruencia como **$a \equiv b \pmod{n}$** .

La relación de congruencia es reflexiva, simétrica y transitiva, y por tanto da lugar a clases de equivalencia, llamadas también *residuales*.

Congruencias famosas

Congruencia de Fermat:

$A^{p-1} \equiv 1 \pmod{p}$ si p es primo.

Congruencia de Euler:

$A^{f(n)} \equiv 1 \pmod{n}$ donde n no ha de ser necesariamente primo y $f(n)$ es el indicador de Euler de dicho número.

Congruencia de Wilson:

$(p-1)! + 1 \equiv 0 \pmod{p}$ con p primo.

Conjetura

Una conjetura es una afirmación que parece ser cierta en muchos casos, pero que no se ha podido demostrar.

Son conjeturas famosas las de: [Bertrand](#), [Fermat](#), [Girard](#), [Goldbach](#), [Hardy - Littlewood](#), [Polignac](#), [Primos gemelos](#), [Waring](#), etc.

Coprimos

Sinónimo de [primos entre sí](#)

Criterio

Criterio de divisibilidad

Un número natural **a** divide a otro **b** si todos los factores primos de **a** lo son también de **b** con exponentes iguales o mayores.

Criterios de primalidad

Existen muchos criterios para ver si un número N es primo. Destacaremos:

Clásico: Ir probando posibles divisores entre 2 y la raíz cuadrada N . Si ninguno es divisor, N es primo.

Fermat: Basado en el pequeño teorema de Fermat, si 2^{N-1} no es congruente con 1 módulo N, el número es compuesto. Si es congruente, no se sabrá si es primo o no.

ARCLP: Test basado en el anterior, pero que es totalmente fiable.

Lucas-Lehmer: Criterio especializado en candidatos a primos que sean números de Mersenne.

Cubano

Primos cubanos

Se llaman así (Cunningham (1923)) aquellos números primos que son iguales a una diferencia de cubos consecutivos. Lo de “cubano” viene de cubo, no de Cuba. No es un nombre afortunado, pero así quedó. Al ser los cubos consecutivos, se da por supuesto que X es entero.

Cullen

Números de Cullen

Son enteros de la forma $n \cdot 2^n + 1$

Los primeros números de Cullen son 3, 9, 25, 65, 161, 385, ...

Para todo número primo p distinto de 2 existe una infinidad de naturales n tales que p divide al número de Cullen correspondiente.

El número primo más pequeño de Cullen es $141 \cdot 2^{141} + 1$.

Los siguientes números primos de Cullen son los generados por 4713, 5795, 6611, 18496, 32292, ... Existe la conjetura de que haya infinitos números de Cullen que sean primos.

Cunnigham

Cadenas de Cunnigham

Las cadenas de este tipo se generan así:

- Elegimos un número primo cualquiera.
- Lo sometemos a la recurrencia $p_{i+1} = 2 p_i + 1$ (cadena de Cunnigham de primera especie) o bien a la recurrencia $p_{i+1} = 2 p_i + 1$ (cadena de Cunnigham de segunda especie) .
- Interrumpimos la recurrencia cuando el resultado no sea primo.

Todos los términos de la cadena (en el caso de primera especie) son [primos de Sophie Germain](#).

D

De la Vallé Pousin

Ver [Hadamard](#)

Deficiente

Número deficiente

Un número se llama *deficiente* cuando es mayor que la suma de sus divisores propios. Por ejemplo: $21 > 1+3+7$

Derivada aritmética

Este original concepto fue presentado por el matemático español José Mingot Shelly en 1911 con el título "Una cuestión de la teoría de los números", trabajo presentado en el Tercer Congreso Nacional para el Progreso de las Ciencias, Granada.

Como su nombre indica, esta derivada se basa en una operación similar a la de la derivada de un producto, y

aplicada a números naturales. Podemos concretarla de esta forma:

$D(0)=D(1)=0$ (para completar la definición)

$D(p)=1$ si p es primo

$D(ab)=aD(b)+bD(a)$ $a>1, b>1$ (Regla del producto)

Descomposición

Descomposición en factores primos

Todo número natural se puede descomponer de forma única como producto de factores primos.

Dirichlet

Teorema de Dirichlet

En toda sucesión aritmética $a+b.n$ con a y b primos entre sí existen infinitos números primos.

Por tanto, hay infinitos primos del tipo $4n+1$ y también del tipo $4n-1$.

Distribución

Distribución de los números primos

Hechos referentes a la distribución de los números primos:

- Los números primos son infinitos
- Dado un número natural, siempre existe un número primo entre él y su doble.
- Es posible encontrar números primos cuya diferencia sea mayor que un número fijado previamente.
- El número de primos menores o iguales que n es asintóticamente igual a $n/\ln(n)$.

Divisibilidad

Parte de la Aritmética que estudia los [múltiplos](#) y [divisores](#)

Relación de divisibilidad

Es la relación que existe entre dos números cuando uno es [múltiplo](#) del otro.

Divisible

Sinónimo de [Múltiplo](#)

Divisor

Divisor de un número

Diremos que un número natural a es *divisor* de b cuando existe otro número natural k que multiplicado por a da por resultado b .

Divisor propio

Es aquel que es menor que el número al que divide

Conjunto de divisores de un número

Todo número mayor que 1 tiene al menos dos divisores. El conjunto de todos los divisores posibles de un número natural se obtiene a partir de su descomposición factorial $a^n \cdot b^m \cdot c^p \cdot d^q \dots$ mediante técnicas combinatorias y el número total de divisores es $(n+1)(m+1)(p+1)(q+1) \dots$

Divisor común a varios números

Es un número que es *divisor* de todos ellos.

Función divisor

Recibe este nombre y también el de [tau](#), el número de divisores de un número N.

Divisor unitario

Un divisor d de N se llama unitario si $MCD(d, N/d) = 1$

Divisorial

Llamaremos *divisorial* de un número al producto de sus divisores. Su cálculo es muy sencillo, porque los divisores de N se presentan por pares cuyo producto es N. Por ejemplo, en 45 se da que $45 \cdot 1 = 15 \cdot 3 = 9 \cdot 5 = 45$. El producto total, o divisorial, será $45^3 = 91125$.

Si $TAU(N)$ es el número de sus divisores, se tendrá que el número de pares será $TAU(N)/2$ si TAU es par y

$(\tau(N)+1)/2$ si es impar, porque este último caso se dará en los cuadrados, y la RAIZ(N) se contaría repetida.

Duffiniano

Los números duffinianos, llamados así por Richard Duffy, son números compuestos que son primos con la suma de sus divisores, es decir, con el valor de la función SIGMA (σ). En ellos no existe ningún divisor común entre N y $\sigma(N)$.

E

Eratóstenes

Criba de Eratóstenes

Algoritmo que encuentra la serie de números primos inferiores a uno dado mediante supresiones ordenadas de números compuestos.

Esfénico

Número esfénico

Es aquel número que es producto de tres números primos diferentes, como $110=2*5*11$.

Euclides

Algoritmo de Euclides

Algoritmo para el cálculo del máximo común divisor de dos números mediante las propiedades del resto de la división euclídea.

Teorema de Euclides o de Gauss

Si un número natural **n** divide a un producto de otros dos **a** y **b** y es primo con **a**, entonces debe ser divisor de **b**.

Euler

Indicador de Euler (o indicatriz, o en inglés Function totient. O PHI(N))

Es una función $f(n)$ que indica la cantidad de números inferiores a n y menores que él.

Si un número natural m se descompone en factores primos: $m=p_1, p_2, p_3 \dots$ su indicatriz de Euler vendrá dada por:

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

Extraño

Número extraño

Es aquel que es abundante, pero no perfecto ni pseudoperfecto. El menor número extraño es el 70.

Números extraños

Dos números son *extraños* o *primos entre sí* cuando no poseen divisores comunes.

F

Factor

Sinónimo de [divisor](#).

Factor primo

Todo número se puede descomponer en producto de factores primos de forma única.

Factorización

Es la operación de calcular todos o algunos factores de un número. En especial es importante la [factorización mediante números primos](#) y la de Fermat. Existen técnicas especiales para factorizar números muy grandes.

Fermat

Factorización de Fermat

Consiste en representar un número natural como diferencia de cuadrados y después aplicar que $a^2 - b^2 = (a+b)(a-b)$

Número de Fermat

Es aquel que es de la forma

$$2^{2^n} + 1$$

Fórmula

Fórmulas para generar números primos

La fórmula n^2+n+17 produce números primos desde $n=1$ hasta $n=16$

$2n^2+9$ produce primos desde $n=1$ hasta $n=8$

y n^2-n+41 , de $n=1$ a $n=40$

Número de Fortune

Si llamamos primorial $N\#$ al producto de los N primeros números primos y número de Euclides a un primorial aumentado en una unidad, diremos que un número es de Fortune si es el siguiente primo posterior a un número de Euclides y se diferencia en un número primo del primorial correspondiente. Por ejemplo, 37 es el primer primo

posterior a $2 \cdot 3 \cdot 5 + 1$ (número de Euclides) y su diferencia con $2 \cdot 3 \cdot 5 = 30$ (primorial) es 7, que es primo.

Fósil de un número

Dado un número natural N , se multiplican todas sus cifras. Se repite el proceso con el resultado obtenido, hasta obtener un número de una cifra únicamente; a ese número se le llama el **fósil de N** . Por ejemplo, el fósil de 327 es 8.

Frobenius

Sabemos que dados dos números a y b primos entre sí, existirán dos números enteros x e y tales que se cumpla $x \cdot a + y \cdot b = 1$, y, por tanto, existirán otros dos m y n tales que $m \cdot a + n \cdot b = N$, siendo N cualquier entero positivo.

La cuestión que planteó Frobenius (problema de las monedas) es para qué números enteros no negativos estos números m y n pueden ser también no negativos, o existirá alguno en el que esto sea imposible. Por ejemplo, $5m + 7n$ nunca es igual a 23 si m y n son mayores o iguales a cero.

Se puede demostrar que para números grandes siempre es posible esta expresión de un número como suma de dos o más múltiplos de otros que sean primos entre sí. Existirá, por tanto, un número **que sea el mayor para el**

que no se cumpla. Este es el llamado **número de Frobenius**

Fuerte

Número primo fuerte

Si ordenamos y numeramos los números primos, diremos que el primo número n , P_n es fuerte, cuando es mayor que la media aritmética de su primo anterior P_{n-1} y su siguiente P_{n+1}

Funciones

Funciones importantes en teoría de números

f (n): (Indicador de Euler) Representa cuántos números naturales inferiores a n son primos con él.

s (n): Representa la suma de todos los divisores de n incluido él mismo (es la función *sigma de Gauss*).

p (n): Representa cuántos números primos hay no superiores a n (también llamada *función de números primos*)

$\Omega(n)$: Esta función devuelve el número total de factores primos **no necesariamente distintos** que figuran en su descomposición factorial. Equivale a la suma de los exponentes con los que figuran los factores primos en dicha descomposición.

$\omega(n)$: Representa número total de factores primos **distintos** que figuran e su descomposición factorial.

G

Gauss

Teorema de Gauss o de Euclides

Si un número natural **n** divide a un producto de otros dos **a** y **b** y es primo con **a**, entonces debe ser divisor de **b**.

Polígonos regulares construibles con regla y compás

Para que un polígono regular pueda dibujarse con regla y compás, ha de tener un número de lados del tipo: $n=2^r \cdot p_1 \cdot p_2 \cdot p_3 \dots p_s$, siendo $p_1, p_2, p_3 \dots p_s$ números de [Fermat](#).

Entero de Gauss

Es un número primo del tipo $4n+1$, con **n** natural. Este tipo de números se puede descomponer en una suma de cuadrados enteros.

Primo de Gauss

Es un número primo del tipo $4n+3$, con n natural. Este tipo de números no se puede descomponer en una suma de cuadrados enteros.

Gemelos

Números primos gemelos

Dos números primos se llaman gemelos si su diferencia es 2. Por ejemplo, los pares 5 y 7, 17 y 19, 311 y 313,

Se ignora si el número de primos gemelos es infinito, pero se conjetura que así es.

Erdős demostró que existe una constante $c < 1$ e infinitos primos p tales que $p' - p < c \cdot \ln(p)$, donde p' denota el número primo que sigue a p .

Chen mostró que existen infinitos números primos p tales que $p+2$ es un producto de, a lo más, dos factores primos.

Si dos números son primos gemelos, se demuestra que han de tener la forma $6n-1$ y $6n+1$ respectivamente.

Se ha demostrado también que dos números n y $n+2$ son primos gemelos si y sólo si $4((n-1)!+1) \equiv -n \pmod{n(n+2)}$

Números primos gemelos capicúas

Son aquellos que son ambos primos y capicúas y sólo se diferencian en la cifra central, que en uno de ellos es consecutiva de la del otro. Por ejemplo, son gemelos capicúas los pares de números 181 - 191, 373-383, 13831-13931.

Girard

Conjetura de Girard

Todo número primo de la forma $4n+1$ puede expresarse de forma única como suma de dos cuadrados.

Esta conjetura fue demostrada por Fermat

Goldbach

Conjeturas de Goldbach

Todo número par mayor que 2 es suma de dos primos

Fue propuesta por Goldbach en 1742, en una carta dirigida a Euler. Ha sido comprobada hasta 10^{14} , pero no se ha podido demostrar.

Todo número impar N mayor que 5 es suma de tres primos

Es consecuencia de la anterior.

(Demostrada por Vinogradov (para un número suficientemente grande), tiene como consecuencia que

todo número par suficientemente grande es suma de a lo sumo cuatro primos)

Ramaré demostró que todo número par es suma de seis o menos números primos.

H

Hadamard

Teorema de Hadamard

Llamando $p(n)$ al número de primos no superiores a n , se cumple

$$\lim_{n \rightarrow \infty} p(n) \cdot \ln(n)/n = 1$$

(Demostrado también por De la Vallé Pousin)

Hamming

Recibe el nombre de sucesión de Hamming la formada por el 1 y los números naturales que son divisibles entre 2,3 y 5 y ningún otro factor primo: 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25, 27, 30, 32, 36, 40, 45, 48,...

Hardy - Littlewood

Conjetura de Hardy - Littlewood

Si llamamos $p_2(x)$ al número de parejas de primos gemelos menores o iguales que n , se cumple:

$$p_2(x) \approx 0,660161 \cdot 2 \cdot \int_2^x \frac{dt}{(\ln t)^2}$$

que es una expresión similar a la de la distribución de los números primos.

Harshad

Un número de Harshad (también conocido como número de Niven), es un número entero divisible entre la suma de sus cifras. Este concepto depende de la base usada. Un número puede ser de Harshad en una base, pero no en otra. Los números de una cifra son todos de Harshad.

Por ejemplo, son números de Harshad 12, 42, 111, 133, 153, etc.

Heterogéneo

Números heterogéneos

Dos números naturales se llaman heterogéneos cuando no tienen sus divisores primos iguales.

Por ejemplo, son heterogéneos 15 y 20.

Hoax

Números hoax

En un número "hoax" (engañoso) la suma de sus cifras coincide con la de las de sus factores primos sin repetir, como $424=2^3 \cdot 53$ y las sumas de cifras son: $4+2+4=10$. $2+5+3=10$, tomando el 2 una sola vez

Homogéneo

Números homogéneos

Dos números naturales se llaman homogéneos cuando tienen los mismos divisores primos, como, por ejemplo, 24 y 36.

HP (Home prime)

Son números tales que al concatenar en orden creciente sus factores primos (incluso repetidos) y reiterar la operación, alcanzan un número primo. Por ejemplo, $42=2 \cdot 3 \cdot 7$ lo convertimos en 237, que es compuesto, $237=3 \cdot 79$. Reiteramos y formamos el número 379, que es primo, luego 42 es home prime.

DE I A O

I

Indicador de Euler

Ver [Euler](#)

Indicatriz

Sinónimo del anterior

Infinitud de los números primos

Desde Euclides se sabe que los números primos son infinitos. La demostración de este hecho es una de las más elegantes de la Historia de las Matemáticas.

Ingham

Teorema de Ingham

Para todo n natural suficientemente grande existe un número primo entre n^3 y $(n+1)^3$

Interprimo

Un número interprimo es aquel que es media de dos primos consecutivos, como el 15, que es media entre el 13 y el 17.

Intocable

Se llaman así a aquellos números que no pueden ser el resultado de la suma de las partes alícuotas de otro número, es decir, de la suma de sus divisores propios.

L

Lagrange

Teorema de Lagrange

Todo número natural es suma de a lo más cuatro números cuadrados.

Legendre

Conjetura de Legendre

Esta conjetura afirma que entre dos cuadrados consecutivos n^2 y $(n+1)^2$ existe siempre un número primo.

$$n < \sqrt{p} < n + 1$$

Lemoine

La conjetura de Lemoine afirma que todo número impar mayor que 5 se puede expresar como la suma $p+2q$, donde p y q son números primos. Se ha comprobado para $N < 10^{13}$, y no se ha demostrado cuando escribimos esto.

Esta conjetura es más fuerte que la segunda de Goldbach, que afirma que todo número impar mayor que 5 puede expresarse como suma de tres números primos. Aquí no se exige que dos de los primos sean iguales.

Logaritmo entero

Llamaremos **logaritmo entero** de un número natural a la suma de todos sus factores primos, contando sus repeticiones.

Se suele representar por la función **sopfr(n)**. Así, **sopfr(28)=2+2+7=11**. El valor más pequeño corresponde a $\text{sopfr}(1)=0$ y los máximos coinciden con los números primos, como es evidente.

Se le llama logaritmo porque posee la propiedad completamente aditiva: **sopfr(a*b)=sopfr(a)+sopfr(b)**. Se cumple por el hecho de contar las repeticiones de los factores primos. Si se contaran una sola vez, esta propiedad sólo se verificaría si los números fueran

primos entre sí y daría lugar a otra función que se representa por **sopf(n)**.

K

Kempner

Los números de Kempner son los valores de la función de [Smarandache](#).

M

Máximo común divisor

El máximo común divisor de varios números es el mayor de sus divisores comunes.

MDI

Mayor divisor impar de un número entero, como $MDI(20)=5$

Menor múltiplo cuadrado (MMC)

Es el menor múltiplo cuadrado que posee un número. Por ejemplo $MMC(12)=36=6^2$.

Mersenne

Número de Mersenne

Número del tipo $2^p - 1$ con p primo.

Mínimo común múltiplo

El mínimo común múltiplo (MCM) de varios números es el menor de sus múltiplos comunes.

Moebius

La función de Moebius $\mu(n)$ se define así:

Si n no es libre de cuadrados, $\mu(n) = 0$

Si no contiene ningún cuadrado como divisor, $\mu(n) = 1$ si posee un número par de factores primos distintos y $\mu(n) = -1$ si ese número es impar.

Moran

Un número de [Hashard](#) se llama número de Moran cuando el cociente entre él mismo y la suma de sus cifras es un número entero primo.

Múltiplo

Múltiplo de un número

Diremos que un número natural **a** es *múltiplo* de **b** cuando existe otro número natural **k** que multiplicado por **b** da por resultado **a**.

Múltiplo común a varios números

Es un número que es múltiplo de todos ellos.

N

N^2+1

Conjetura: Existen infinitos primos de la forma n^2+1

Niven

Sinónimo de [Harsard](#)

Número

Ver Número [Abundante](#), [de Cullen](#), [Deficiente](#), [Extraño](#), [Feliz](#), [de Fermat](#), [de Harshad](#), [de Mersenne](#), [Narcisista](#), [de Ore](#), [Perfecto](#), [Primario](#), [Primo](#), [Pseudoprimo](#)

Ver Números

[Amigos](#), [Primos entre sí](#), [Primos Gemelos](#), [Heterogéneos](#), [Homogéneos](#), [Sociables](#)

O

Omega

Familia de funciones que cuentan los divisores de un número.

Omega: Cuenta los factores primos de un número sin tener en cuenta las multiplicidades. Así, $\omega(60)=3$

Biomega: Cuenta los factores primos con multiplicidad, como $\Omega(60)=4$

Omipr

Un número primo recibe el nombre de *omipr* si su simétrico (el que tiene sus mismas cifras pero invertidas, en base 10) también es primo. Son números **omipr** 3, 17, 31, 37, 71, 73, 79, 97, 107, 113,...

Ormiston

Se llaman pares de Ormiston a los formados por dos números primos consecutivos que presentan las mismas cifras, como 1913 y 1931

Oppermann

Conjetura de Oppermann

Fue establecida por Opperman en 1882. Afirma lo siguiente:

Para todo número entero $x > 1$, existe al menos un número primo entre $x(x - 1)$ y x^2 , y otro primo entre x^2 y $x(x + 1)$.

Ore

Un número entero positivo N se llama de Ore cuando la media armónica de todos sus divisores es un número entero.

DE P A Z

P

Palprimo

Según se deduce del nombre, los palprimos son números primos capicúas o palindrómicos (nos limitaremos al sistema de numeración en base 10 por ahora), es decir, que se leen igual de izquierda a derecha que de derecha a izquierda.

Partes cuadrada y libre

Todos los números naturales contienen un cuadrado en alguna de sus descomposiciones factoriales (eventualmente valdría 1) y otro factor libre de cuadrados (quizás también 1).

Así, tendríamos, por ejemplo: $80=42*5$, $121=112*1$, $90=32*10$, $15=12*15$

Podemos llamar parte cuadrada $PC(N)$ a la primera y parte libre $PL(N)$ a la segunda.

Perfecto

Número perfecto

Diremos que un número es perfecto cuando equivale a la suma de todos sus divisores propios (menores que él).

Los primeros números perfectos son 6, 28, 496 y 8128, ya conocidos en la antigüedad.

Número perfecto por múltiplos

Diremos que un número es perfecto (doblemente, triplemente,...) cuando la suma de sus divisores propios es múltiplo de dicho número. Igualmente, se puede afirmar que la función $s(n)$ es el triple, cuádruple, etc. del número.

Por ejemplo: La suma de los divisores de 120 es su doble, 240. Lo mismo les ocurre a los números 672 y 523776.

P(N) primos hasta N

Representa cuántos números primos hay no superiores a n . Para n tendiendo a infinito, coincide asintóticamente con la expresión $n/\ln(n)$.

Poderoso

Un número natural es poderoso cuando todos sus factores primos están elevados al menos al cuadrado. Por ejemplo el $72=2^3 \cdot 3^2$

Polidivisible

Un número natural escrito en sistema decimal es polidivisible si cumple:

Su primera cifra es distinta de cero

El número formado por las dos primeras cifras es múltiplo de 2

El número formado por las tres primeras cifras es múltiplo de 3

El número formado por las cuatro primeras cifras es múltiplo de 4

Y así sucesivamente.

Por ejemplo, 2012, pues 20 es par. 201 múltiplo de 3 y 2012 múltiplo de 4.

Polignac

Conjetura de Polignac

Para todo número natural k , existen infinitos pares de primos tales que su diferencia es $2k$

Fórmula de Polignac

Es una fórmula muy sencilla para encontrar los divisores primos del factorial de un número natural n . Estos divisores son todos los números primos inferiores a n elevados al exponente r dado por la fórmula

$$r = \sum \left[\frac{n}{p^i} \right]$$

siendo p^i las potencias del número.

Número de Polignac

Llamaremos número de Polignac a aquel número impar que no pueda expresarse como $p+2x$. Se supone implícitamente que x puede valer 0, porque en ningún listado se toma el 3 como número de Polignac, ya que $3=2+2^0$. Los primeros números de Polignac son 1, 127, 149, 251, 331, 337,...

Primario

Número primario

Se llaman números primarios a aquellos que son potencias de primos, como 9, 16, 49 o 169.

Primo

Número primo

Un número natural se llama primo si sólo es divisible entre sí mismo y la unidad.

Números primos gemelos

Ver [Gemelos](#)

Números primos entre sí

Son aquellos números naturales (no necesariamente primos) que no tienen divisores comunes.

Su MCD es 1. También se les llama *extraños*, *primos relativos* o *coprimos*.

Números primos entre sí dos a dos

Los elementos de un conjunto de números naturales se dicen *primos entre sí dos a dos*, cuando tomados por parejas, son siempre primos entre sí. Los números 5, 15 y 9 son primos entre sí, pero no *dos a dos*. Sin embargo 4, 9, 25 y 49 sí lo son.

Números primos permutables

Un número primo es ***permutable*** cuando todas sus permutaciones de cifras dan lugar a números primos. Por ejemplo el 337.

Función primo

Es la que relaciona un número primo con su número de orden. Se suele escribir como *prime(N)*. Así, $\text{prime}(5)=11$

Primorial

La palabra primorial se suele usar con tres significados distintos:

(1) Un número es primorial si es igual al producto de los k primeros números primos. Por ejemplo, $210=2*3*5*7$.

(2) Llamaremos primorial de un número N y lo representaremos por $N\#$ al producto de todos los números primos menores o iguales que él. Los primeros valores de esta función son (están incluidos $n=0$ y $n=1$)

(3) Llamaremos primo primorial o primo de Euclides al que tiene la forma $p\#+1$, siendo p primo. Esta definición recuerda que son estos los números usados por Euclides en su demostración de la infinitud del conjunto de primos.

Problema

Problemas no resueltos en la Teoría de Números

Los siguientes problemas sobre números naturales no han sido resueltos en el momento de redactar esta página:

- ¿Hay infinitos números primos de Mersenne y, por tanto, infinitos números perfectos?
- ¿Existen números perfectos impares?
- ¿Hay infinitos pares de números amigos?
- ¿Hay más números de Fermat primos además de 3, 5, 17, 257 y 65.537?
- ¿Hay infinitos pares de números primos gemelos?
- ¿Existen progresiones aritméticas formadas por números primos, tan grandes como queramos?
- ¿Es cierta la conjetura de Golbach?

- ¿Es cierta la conjetura de Polignac?
- ¿Existen infinitos números primos de la forma n^2+1 ?
- ¿Existe siempre un número primo entre n^2 y $(n+1)^2$?
- ¿Es cierta la conjetura de Catalán?
- ¿Hay algún entero mayor que 1 que figure más de 8 veces en el triángulo de Pascal? (problema de Singmaster)
- ¿Existen números amigos, uno de ellos par y el otro impar?
- La sucesión de Fibonacci ¿contiene infinitos primos?

Pseudoperfecto

Número pseudoperfecto

Es un número n es pseudoperfecto cuando equivale a la suma de algunos de sus divisores, como $20=10+5+4+1$. Si se tomaran todos los divisores se llamaría [perfecto](#).

Pseudoprimo

Número pseudoprimo

Es un número n que cumple que 2 elevado a n es congruente con 2 módulo n Hay infinitos, como 645 o 161038

Pseudoprimo de Perrin

En la sucesión de Perrin, si n es primo, divide a $P(n)$, pero la propiedad contraria no es verdadera: un compuesto puede dividir o no a $P(n)$. La gran mayoría de los compuestos no lo dividen. Los valores de n compuestos que dividan a $P(n)$ son denominados como pseudoprimos de Perrin, como el número 271441.

R

Radical

Radical de un número natural

Radical de N es el mayor divisor de N libre de cuadrados. Equivale al producto de todos sus factores primos elevados a la unidad. Por ejemplo, el radical de 48 es $6=2 \cdot 3$

Raíz interna y externa

Raíz interna de N es la raíz cuadrada de su parte cuadrada. Por ejemplo, la parte cuadrada de 11400 es 100, luego su raíz interna será 20. La representaremos como $RI(N)$. En este caso $RI(11400)=10$

Raíz externa de N es la raíz cuadrada de su menor múltiplo cuadrado. En el caso de 11400 podríamos escribir $RE(11400)=1140$, que es la raíz cuadrada de Menor múltiplo cuyadrado de 11400.

Ramaré

Teorema de Ramaré

Todo número par es suma de 6 o menos números primos.

Rassias

Conjetura de Rassias

Para cada número primo $p > 2$ existen dos primos p_1 y p_2 , con $p_1 < p_2$ tales que

$$(p-1)p_1 = p_2 + 1$$

Es decir, que si el primer primo lo multiplicamos por $p-1$, conseguimos un número al que precede otro número primo

Refactorizable

Número refactorizable o “tau”

Un número se llama refactorizable o tau si es múltiplo del número de sus divisores.

Regular

Número regular

Es aquel número natural cuya descomposición en factores primos tiene la forma $2^m 3^n 5^p$. Se pueden expresar también como aquellos que dividen a alguna potencia de 30.

Relación

Relación de divisibilidad

Diremos que **a** es divisible entre **b** cuando **b** es divisor de **a** (que por tanto será múltiplo de **b**)

Esta relación es reflexiva, antisimétrica y transitiva, por lo que constituye un **orden**. Como no siempre dos números están relacionados por ella, el orden es de tipo **parcial**.

Relación de congruencia

Dos números están relacionados por una congruencia cuando son congruentes respecto a un módulo dado. Esta relación es reflexiva, simétrica y transitiva y produce, por tanto, **clases de equivalencia**, llamadas también clases de restos o residuales.

Repunit

Un número se llama repunit (o repuno o repituno) cuando se puede representar como $11111\dots(N\dots)$ en el sistema de numeración decimal o en otros. Todo primo distinto de 2 y 5 posee un múltiplo repunit en el sistema decimal.

Los cuadrados de los repunit hasta $N=9$ unos, se llaman números de Demlo, y la suma de sus cifras es igual al cuadrado de N .

Riemann

Función zeta de Riemann

La función de Riemann sobre un número s viene dada por la serie

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} \dots$$

Se demuestra que coincide con el producto infinito

$\prod_p (1 - p^{-s})$, donde p recorre todos los números primos.

Ruth-Aaron

Un par del tipo Ruth-Aaron está formado por dos números naturales consecutivos que comparten el mismo valor en su logaritmo entero

S

Schinzel

Conjetura de Schinzel

Schinzel conjeturó que para $x > 8$, existe al menos un número primo entre x y $x + (\ln x)^2$.

Semiperfecto

Sinónimo de [Pseudoperfecto](#)

Semiprimo

Un número natural es *semiprimo* cuando es producto de dos números primos iguales o distintos. Son semiprimos 4, 6, 9, 10, 14, etc. Se usan en Criptografía con números primos muy grandes.

Sexy

Números primos sexy son los que forman un par del tipo $(p, p + 6)$, es decir que su diferencia es seis. Por ejemplo, 31 y 37

Sigma

Con este nombre se conocen todas las funciones que provienen de la suma de los divisores de un número.

Sigma: Llamamos función Sigma a aquella que relaciona cada número con la suma de sus divisores.

Su fórmula más popular respecto a sus factores y exponentes es:

$$\sigma(N) = \prod \frac{p_i^{e_i+1} - 1}{p_i - 1}$$

Sigma_k: Idéntica a la anterior, suma todos los divisores de un número elevados a la potencia k, por lo que la anterior equivale a sigma_1.

$$\sigma_k(N) = \prod \frac{p_i^{(e_i+1)k} - 1}{p_i^k - 1}$$

Sigma* (o *usigma*): Suma sólo los [divisores unitarios](#).

Signatura

Signatura prima

Es el conjunto de los exponentes que figuran en la factorización de un número en factores primos. Se

escriben las repeticiones y se suelen ordenar los exponentes de menor a mayor. Por ejemplo, 60 tiene como signatura $\{1,1,2\}$, porque $60=2^2 \cdot 3 \cdot 5$

Smarandache

Función de Smarandache

La función de Smarandache se define, para un número natural n , como el menor entero tal que su factorial es divisible entre n .

Smith

Número de Smith

Es aquel en el que la suma de sus cifras coincide con la de la suma de las de sus factores primos tomados con repetición, como el 666, cuyas cifras suman 18 y las de su desarrollo en factores primos $2 \cdot 3 \cdot 3 \cdot 37$ también: $2+3+3+3+7=18$.

Si se usan los cuadrados de las cifras, se llamará número de Smith de segundo orden. Por ejemplo, $822=2 \cdot 3 \cdot 137$ y se cumple $8^2+2^2+2^2 = 72$ y $2^2+3^2+1^2+3^2+7^2=72$.

Sociable

Un conjunto de números se llaman sociables si cada uno de ellos es igual a la suma de los factores propios

del anterior hasta llegar de nuevo al primero, es decir, formando una [sucesión alícuota](#) cíclica. El periodo de esta sucesión se llama orden del conjunto de números sociables.

Si el periodo es 1, el número es perfecto. Si es 2, es que se trata de números amigos.

Los números sociables más sencillos son 12 496, 14 288, 15 472, 14 536 y 14 264

Sophie Germain

Primo de Sophie Germain

Es aquel número primo P tal que $2P+1$ es también primo.

Identidad de Sophie Germain

$$x^4+4y^4=(x^2+2y^2+2xy)(x^2+2y^2-2xy)$$

Teorema de Sophie Germain

Todo número del tipo a^4+4 , con a natural y distinto de 1, es compuesto.

Sucesión de Sophie Germain

Es la formada por los números primos p tales que 2^*p+1 también es primo: 2, 3, 5, 11, 23, 29, 41, 53, 83, 89,...

SOPF

Suma de los factores primos de un número sin repetición. Así, si $12=2*2*3$, $SOPF(12)=2+3=5$

SOPFR

Suma de los factores primos de un número con repetición. Así, si $60=2*2*3*5$,

$$SOPFR(60)=2+2+3+5=12$$

Submúltiplo

Sinónimo de [divisor](#).

T

Tau

Recibe el nombre de función **tau** de un número N al número de sus divisores. También se la denomina función **divisor**.

Su fórmula más popular es

$$D(N) = (1 + a_1) * (1 + a_2) \dots (1 + a_k)$$

Los a_i son los exponentes de los factores primos.

Teorema

Ver Teoremas de [Bezout](#), [Chen](#), [Dirichlet](#), [Euclides](#), [Gauss](#), [Hadamard](#), [Ingham](#), [Lagrange](#), [Ramaré](#), [Sophie Germain](#), [Vaughan](#), [Vinogradov](#), [Wilson](#).

Teorema de los números primos

El cociente $p(x)/x$ (ver [p\(x\)](#)) es asintóticamente equivalente al cociente $1/\ln(x)$ para valores de x muy grandes.

Teorema Fundamental de la aritmética

Sea N un número mayor que 1. Entonces existen números primos p_1, p_2, p_3, \dots y unos exponentes a_1, a_2, a_3, \dots tales que

$$N = p_1^{a_1} \times p_2^{a_2} \times p_3^{a_3} \times \dots \times p_k^{a_k}$$

A estos números primos les llamaremos *factores primos* de n y siempre existen y son únicos, así como sus exponentes.

Teoría de Números

Parte de las Matemáticas que estudia las propiedades de los números naturales y enteros. Se considera que la fundó Gauss en sus *Disquisitiones arithmeticae* (Leipzig 1801) en la parte llamada Teoría de Números

Aritmética. Más tarde, Galois fundó la parte algebraica y Minkowski la geométrica.

Thabit idn qurra

Fórmula de Thabit idn qurra

Permite encontrar pares de números amigos. Se basa en lo siguiente:

Para $n > 1$, si los tres números $a = 3 \cdot 2^n - 1$, $b = 3 \cdot 2^{n-1} - 1$ y $c = 9 \cdot 2^{2n-1} - 1$ son primos, entonces los números $p = 2^n \cdot a \cdot b$ y $q = 2^n \cdot c$ son amigos

Por ejemplo, para $a=11$, $b=5$ y $c=71$ resultan 220 y 284.

Los números del tipo $3 \cdot 2^n - 1$ se llaman números de **Thabit** y en el sistema de numeración binario vienen representados por las cifras 1, 0 seguidas de la cifra 1 repetida hasta terminar la expresión. Por ejemplo, el número de Thabit 786431 viene representado por 10111111111111111111

Tchebychev

Demostró en 1851 la conjetura de Bertrand

Triplete

Triplete de números primos

Es el formado por tres números primos de la forma p , $p+2$, $p+4$. Sólo existe el triplete 3, 5, 7, pues otro mayor contendría un múltiplo de 3.

Truncable

Números primos truncables

Reciben este nombre los números primos que siguen siendo primos aunque se les vayan eliminando las cifras una a una. Unos números permiten esa operación por la izquierda, como 167, que se transforma en 67, también primo, y después en 7. Otros presentan esta propiedad por la derecha, como 599, que pasa a 59 y después a 5. Por último, otros, como el 373, pueden reducirse por ambos lados.

U

Ulam

Espiral de Ulam

Si los números naturales se sitúan en espiral alrededor del 1, los números primos producen pautas que siguen muy a menudo líneas rectas.

Números de Ulam

Se llaman números de Ulam a los que forman una sucesión construida de la siguiente forma:

Se declara $u(1)=1$ y $u(2)=2$ (veremos que esto se puede alterar) y después definiremos $u(n+1)$ como el primer número que se pueda expresar como suma de dos números de Ulam anteriores distintos, de forma única.

Los creó el matemático polaco Stanislaw Ulam y los publicó en SIAM Review en 1964.

Unicidad

Unicidad de la descomposición en factores primos

La [descomposición](#) de un número natural en factores primos es única, lo que constituye el teorema fundamental de la Divisibilidad.

Usigma

La función usigma asigna a cada número entero positivo la suma de sus [divisores unitarios](#).

V

Vaughan

Teorema de Vaughan

Todo número par es suma como máximo de 26 números primos.

Vinogradov

Teorema de Vinogradov

Todo número impar N suficientemente grande es suma de tres primos

W

Waring

Conjeturas De Waring

- a. Todo número impar o es primo o es suma de tres primos
- b. Para todo número natural k existe otro $r=g(k)$ tal que cualquier número natural n se puede escribir como una suma de r sumandos de potencias de orden k de números naturales adecuados.

- c. Casos particulares:

Para $k=2$ y $r=4$ resulta el teorema de Lagrange: Todo número natural es suma de cuatro números cuadrados.

- d. Todo entero positivo se puede expresar como suma de no más de 9 cubos (esto está demostrado) o como suma de no más de 16 cuartas potencias.

Hilbert probó que existe $g(k)$ pero no dio un método para calcularlo.

Hardy y Littlewood descubrieron un método que funciona casi siempre.

Wilson

Teorema de Wilson

Para que n divida a $(n-1)!+1$ es necesario y suficiente que n sea primo.

Por tanto, para $p>0$ primo tendremos que $(p-1)!$ Es congruente con -1 módulo p

Z

Zuckerman

Número de Zuckerman

Es aquel número entero que es divisible entre el producto de sus cifras (Ver [Niven](#)).

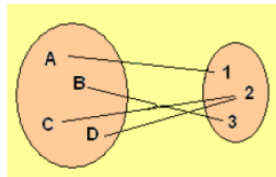
COMBINATORIA

A A M

A

Aplicación

Una **aplicación** es una correspondencia en la que cada elemento del primer conjunto le corresponde un elemento del segundo conjunto y solo uno



Aritmético

Triángulo aritmético

Nombre dado también al triángulo de [Pascal](#) o Tartaglia.

Arreglo

Llamaremos **arreglo** en un conjunto finito a cualquier sucesión también finita formada por elementos de ese conjunto. Al ser el arreglo una sucesión, intervendrá en él el orden, y se podrán repetir elementos.

B

Binomial

Número binomial

Sinónimo de [número combinatorio](#).

C

Ciclo

Es una parte de una permutación que aplica un subconjunto en sí mismo. Por ejemplo

(3 4 5 6)

(5 3 6 4) $s(3)=5$ $s(5)=6$ $s(6)=4$ $s(4)=3$ (regresa al primero, el 3)

Circular

Una permutación es circular o cíclica si es ella misma un ciclo, o que se puede descomponer en un solo ciclo.

Clase

Clase de una permutación

Es su carácter par o impar.

Combinación

Una de las distintas formas de elegir subconjuntos de **n** elementos dentro de otro conjunto de **m** elementos. Es claro que cada elección se distingue de otras por los elementos elegidos, no por el orden en el que son elegidos.

Fórmulas

Sin repetición:

$$C_{m,n} = \frac{n!}{m!(n-m)!}$$

Con repetición:

$$CR_{m,n} = C_{m+n-1,n} = \binom{m+n-1}{n} = \binom{m+n-1}{m-1}$$

Combinatoria

Parte de las Matemáticas que estudia las formas de ordenar o elegir elementos en los conjuntos. Se considera fundada por Santiago Bernoulli en su tratado *Ars Conjectandi* en 1713.

Combinatorio

Número combinatorio

Es el número de combinaciones posibles de **n** elementos en un conjunto de **m** elementos.

Fórmula:

$$\binom{m}{n} = \frac{m!}{n! (m - n)!}$$

Contar

Contar ordenadamente

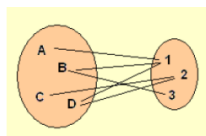
En Combinatoria es esencial el saber contar ordenadamente los elementos de un conjunto o un arreglo. Para ello se suele usar

- Contar directamente los elementos
- Uso del producto cartesiano de dos conjuntos
- Diagramas de árbol
- Tablas de contingencia
- Los grandes principios combinatorios
-

Correspondencia

Una **correspondencia** entre dos conjuntos es cualquier subconjunto de su producto cartesiano. En la práctica

consiste en asignar una pareja o varias a todos o algunos elementos del conjunto.



D

Desarreglo

Llamaremos **desarreglo** a una permutación de un conjunto en sí mismo en el que no coincide ningún origen con su imagen (no hay puntos fijos). El número de desarreglos posibles en un conjunto de n elementos viene dado por la expresión

$$D_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} \dots + \frac{(-1)^n}{n!} \right)$$

El resultado de esta fórmula recibe también el nombre de *subfactorial*, y se representa por $!n$.

Descomposición

Descomposición de un número en sumas

Ver [Partición](#)

F

Ferrers

Diagrama de Ferrers

Es un diagrama en el que se adosan símbolos formando tantas filas como sumandos entran en la partición, y columnas, siendo la longitud de cada una el valor del sumando. Así, la partición $8=4+2+1+1$ se puede representar así:

G

Generatriz

Función generatriz

La función generatriz de arreglos, sucesiones o particiones es una función polinómica cuyos coeficientes coinciden con valores numéricos obtenidos en ellas, especialmente el número total de casos posibles.

Grado

Grado u orden de un ciclo en una permutación o sustitución

Es el número de veces que hay que aplicarlo sobre un conjunto para que el resultado sea la identidad. Se puede expresar como potencia: $S^g = I$, donde **S** es el ciclo, **g** su grado e **I** la identidad.

Grado de una sustitución

Vale la misma definición anterior: $S^g = I$, donde **S** es el ciclo, **g** su grado e **I** la identidad.

Si **S** está descompuesta en ciclos, su grado será el m.c.m. de los grados de esos ciclos.

Grupo

Grupo de permutaciones (o sustituciones)

Todas las sustituciones que operan sobre un conjunto forman un grupo para la operación $S * T$, que consiste en aplicar sobre ese conjunto, de forma sucesiva, las dos sustituciones **S** y **T**. Su elemento neutro es la Identidad **I**. Se le llama *grupo simétrico* y se representa por S_n , siendo **n** el cardinal del conjunto.

I

Impar

Permutación impar

Una permutación es *impar* cuando posee un número impar de inversiones (o transposiciones). El número total de permutaciones impares de orden n es $n!/2$

Inversión

Inversión de una permutación

Diremos que dos elementos **a** y **b** de una permutación presentan una inversión si están ordenados de forma inversa al orden principal prefijado. Por ejemplo, los números 5 y 2 presentan una inversión en 15342 respecto al orden natural de los números.

Si el número de inversiones de una permutación es par, dicha permutación también se llama par, e igualmente si es impar.

Así la permutación del ejemplo 15342 presenta las inversiones 53, 54, 52, 32 y 42, luego es impar.

L

Lah

Los números de Lah sin signo cuentan el número de formas en que un conjunto de n elementos puede dividirse en k subconjuntos ordenados.

Un caso particular, los de segundo índice igual a 2, representa el número de aplicaciones sobreyectivas que se pueden construir entre un conjunto de n elementos y otro de $n-1$.

M

Multinomial

$$\binom{n}{n_1, n_2, n_3, \dots, n_k}$$

Coeficiente n_1, n_2, \dots, n_k , multinomial de índice superior n e inferiores a, b, \dots, h , con $k > 2$ es una forma de expresar el número de [permutaciones](#) de n elementos con elementos repetidos en grupos de a, b, \dots, h elementos. Su valor equivale a

$$P_{n,a,b,c} = \frac{n!}{a! b! c!}$$

N A Z

N

N-pla

Sinónimo de [Arreglo](#) o de Selección ordenada

Número

Número combinatorio: Ver [Combinatorio](#)

Número de Bell: Se llama **número de Bell** de un conjunto finito de n elementos, y se representa por B_n al número de [particiones](#) distintas que se pueden definir en ese conjunto.

Números de Stirling

Existen dos sucesiones distintas de números de Stirling, que son

Números de Stirling de primera clase

Dado el grupo de permutaciones S_n sobre un conjunto de n elementos, llamaremos **Número de Stirling de primera clase**, $S_1(n,k)$, al número de permutaciones de S_n que se pueden descomponer exactamente en k ciclos.

Números de Stirling de segunda clase

Dado un conjunto de n elementos, llamaremos **número de Stirling de segunda clase $S_2(n,k)$** al número de particiones distintas de k conjuntos que se pueden definir en ese conjunto de n elementos.

O

Orden

El orden en Combinatoria: El orden es un elemento de definición en las [combinaciones](#) y [permutaciones](#).

Orden de un ciclo o de una permutación: Sinónimo de [grado](#)

P

Par

Permutación par

Una permutación es *par* cuando posee un número par de inversiones. El número total de permutaciones pares de orden n es $n!/2$

Paridad

Paridad de una permutación o una sustitución

Es el carácter par o impar de esa permutación.

Partición

Partición de un número natural

Es cada una de las representaciones de ese número como suma de otros naturales no nulos, sin tener en cuenta el orden. Se representa con el símbolo $p(n)$ y se calcula mediante la identidad de Euler

$$(1-x)^{-1} \cdot (1-x^2)^{-1} \cdot (1-x^3)^{-1} \dots = 1+p(1)x+p(2)x^2+p(3)x^3+\dots$$

Pascal

Triángulo de Pascal

Disposición en triángulo de los números combinatorios o binomiales.

$$\begin{array}{cccccc} & & & & & & 1 \\ & & & & & & & 1 & & 1 \\ & & & & & & & & 1 & & 2 & & 1 \\ & & & & & & & & & 1 & & 3 & & 3 & & 1 \\ & & & & & & & & & & 1 & & 4 & & 6 & & 4 & & 1 \\ & & & & & & & & & & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \end{array}$$

Permutación

Se llama permutación sin repetición a cualquiera de las distintas formas posibles de ordenar un conjunto. El número de permutaciones de un conjunto de n elementos es el [factorial](#) de n , $n!$.

También se define como una aplicación biyectiva del conjunto en sí mismo.

En los distintos órdenes posibles quizás se desee admitir la repetición de algunos elementos un número determinado de veces. Por ejemplo, en la palabra CATAPULTA, si quisiéramos ordenar sus letras, deberíamos admitir que la A se repitiera tres veces y la T dos. Llamaremos permutaciones con repetición a estas ordenaciones.

También se pueden definir estas permutaciones como las formas de distribuir n objetos en k cajas, de forma que cada caja contenga siempre un mismo número determinado de objetos.

Igualmente, coincide con el número de aplicaciones (o funciones) existente entre un conjunto de n elementos y otro de k elementos, en el que el número de antiimágenes de cada elemento está prefijado.

Para calcular el número de permutaciones de este tipo bastará dividir el factorial del número total de símbolos,

contando sus repeticiones, entre el número de veces que se repite cada uno.

$$P_{n,a,b,c} = \frac{n!}{a!b!c!}$$

Este número recibe el nombre de **coeficiente multinomial**.

Principios combinatorios

Principio de Adición

Dados los conjuntos A_1, A_2, \dots, A_k , disjuntos dos a dos, se cumple que

$$\text{Card}(A_1 \cup A_2 \dots A_k) = \text{Card}(A_1) + \text{Card}(A_2) + \dots + \text{Card}(A_k)$$

Es decir, que para contar los elementos de la unión de varios conjuntos disjuntos, deberemos **sumar**.

Principio de multiplicación

Si los conjuntos A_1, A_2, \dots, A_k , son no vacíos, se cumple que

$$\text{Card}(A_1 \cap A_2 \cap \dots A_k) = \text{Card}(A_1) * \text{Card}(A_2) * \dots * \text{Card}(A_k)$$

Podemos traducir este principio a la idea de que al combinar mediante pares, ternas, etc. varios conjuntos, el número total de elementos resultantes equivale al producto de los cardinales de los conjuntos que se combinaron.

Principio de distribución

Este principio se conoce también como *Principio de las cajas, del palomar o de Dirichlet*

Lo desarrollaremos en dos versiones equivalentes:

(a) Si repartimos m objetos en n cajas, y $m > n$, entonces, al menos una caja deberá contener 2 objetos o más.

(b) Si se reparten $np+m$ objetos en n cajas, entonces alguna caja deberá contener al menos $p+1$ objetos.

Principio de inclusión y exclusión

Se llama así a la fórmula obtenida anteriormente

$$\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B) - \text{Card}(A \cap B)$$

y a su generalización para más de dos conjuntos. Por ejemplo, para tres sería

$$\text{Card}(A \cup B \cup C) = \text{Card}(A) + \text{Card}(B) + \text{Card}(C) - \text{Card}(A \cap B) - \text{Card}(A \cap C) - \text{Card}(B \cap C) + \text{Card}(A \cap B \cap C)$$

En el caso de varios conjuntos aparecerían signos - en las intersecciones de un número par de conjuntos y signo + en las de número impar:

$$\text{Card}(\cup S_i) = \sum \text{Card}(S_i) - \sum \text{Card}(S_i \cap S_j) + \sum \text{Card}(S_i \cap S_j \cap S_k) + \dots + (-1)^n \sum \text{Card}(S_i \cap \dots \cap S_n)$$

R

Rachas

En Combinatoria es interesante el problema de las rachas, conjuntos de elementos consecutivos iguales. Por ejemplo, el conjunto AABBCDDDDEE posee cinco rachas; AA, BB, C, DDDD y EE. No se impone ninguna condición a la longitud de cada racha.

Reducida

Permutación reducida

Una permutación es reducida si no deja fijo ningún elemento. En su descomposición en ciclos ninguno de ellos tiene orden 1.

S

Selección ordenada

Sinónimo de [Arreglo](#) y de [n-pla](#)

Signatura

Signatura de una permutación

Llamaremos *signatura* de una permutación al número +1 si es de tipo [par](#) o al número -1 si es de tipo [impar](#).

Stirling

Números de Stirling de primera clase (o primera especie)

Número de Stirling de primera clase $S1(n,k)$ indica, dado el grupo de permutaciones S_n sobre un conjunto de n elementos, cuántas permutaciones se pueden descomponer exactamente en k ciclos.

La propiedad fundamental de estos números, y que permite generarlos en una tabla, es la siguiente:

$$S1(n,r) = (n-1)*S1(n-1,r)+S1(n-1,r-1)$$

Números de Stirling de segunda clase (o segunda especie)

Número de Stirling de segunda clase $S2(n,k)$ representa cuántas particiones distintas de k conjuntos se pueden definir en un conjunto de n elementos.

La propiedad que permite generar estos números es:

$$S2(n,r) = r*S1(n-1,r)+S1(n-1,r-1)$$

Subfactorial

Subfactorial de un número natural

Llamaremos ***subfactorial*** de n al número de [desarreglos](#) de un conjunto de n elementos.

Sustitución

Una sustitución aplicada a un conjunto es cualquier [correspondencia](#) definida entre los elementos de dicho conjunto. Su número total es el [factorial](#) del cardinal de ese conjunto. Es sinónimo de [permutación](#).

T

Transposición

Se llama **transposición** en el grupo de permutaciones de un conjunto, a todo ciclo de orden 2. Todas las permutaciones se pueden descomponer en transposiciones, pero no de forma única, aunque se conserva la paridad.

V

Variación

Una de las distintas formas de elegir subconjuntos de otro conjunto, de forma que cada elección se distinga de otras por los elementos o bien por el orden en el que son elegidos.

Fórmulas:

Con repetición:

$$VR_{m,n} = m^n$$

Sin repetición:

$$Vm,n = m(m-1)(m-2)\dots(m-n+1) = m!/(m-n)!$$

ARITMÉTICA MODULAR

A

Aritmética Modular

Aritmética modular

Comprende el estudio de las [clases de restos](#) Z/nZ de los enteros respecto a un módulo n . Ver [Congruencias](#).

C

Clase

Clases de restos (de congruencia, o residuales)

Son las clases que se forman al aplicar la relación de [congruencia](#) en el conjunto de los números enteros Z .

Se representan por Z/nZ , Así: $Z/5Z = \{0, 1, 2, 3, 4\}$

Congruencia

Relación de congruencia

Diremos que a y b (números enteros) son congruentes módulo n (natural), si la diferencia $b-a$ es un múltiplo de n . Representaremos la relación de congruencia como $a \equiv b \pmod{n}$.

La relación de congruencia es reflexiva, simétrica y transitiva, y por tanto da lugar a clases de equivalencia, llamadas también [residuales](#).

Congruencias famosas

Congruencia de Fermat:

$A^{p-1} \equiv 1 \pmod{p}$ si p es primo.

Congruencia de Euler:

$A^{f(n)} \equiv 1 \pmod{n}$ donde n no ha de ser necesariamente primo y $f(n)$ es el indicador de Euler de dicho número.

Congruencia de Wilson:

$(p-1)! + 1 \equiv 0 \pmod{p}$ con p primo.

Criterio de Congruencia

Criterio de congruencia

Dos números enteros a y b son congruentes módulo n , si y sólo si la diferencia $b-a$ es un múltiplo de n

CH

Chino

Teorema chino de los restos

Si A_1, A_2, \dots, A_n son números primos entre sí dos a dos y $a_1, a_2, a_3, \dots, a_n$, enteros cualesquiera, existe un número entero N que cumple $N \equiv a_i \pmod{A_i}$ para todo i entre 1 y n .

Para calcular ese número llamemos H al producto de todas las A_i y sea $A'_i = H/A_i$.

Se buscan unas m_i tales que $m_i \cdot A'_i = 1 \pmod{A_i}$ y entonces la solución será:

$$N = \sum A_i \cdot m_i \cdot a_i$$

Por ejemplo: Encontrar un número n tal que al dividirlo entre 10 nos dé de resto 7, y al dividirlo entre 9 obtengamos un resto de 3.

$H=9 \cdot 10 = 90$; $A'_1=9$; $A'_2=10$; $m_1=9$; $m_2=10$ y por último:

$$N=9 \cdot 7 \cdot 9 + 10 \cdot 3 \cdot 10 = 867$$

E

Ecuación

Ecuación de congruencias

Es toda ecuación definida sobre el anillo de las clases de restos $\mathbb{Z}/m\mathbb{Z}$

Euler

Indicador de Euler

Es una función $f(n)$ que indica la cantidad de números inferiores a n y primos con él.

Si n es primo, su indicador será $n-1$

Una fórmula para esta función es

$f(n) = n(1-1/p_1)(1-1/p_2)(1-1/p_3)\dots$ siendo p_1 p_2 p_3 los factores primos de n

Así, $f(7) = 6$, $f(8) = 3$ porque sólo son primos con él 3, 5 y 7.

Criterio de Euler

Si p es un número primo impar, y a es coprimo con p , entonces si

$$a^{(p-1)/2} = 1 \pmod{p}$$

será a resto cuadrático respecto a p , y no lo será si

$$a^{(p-1)/2} = -1 \pmod{p}$$

F

Fermat

Teoremas de Fermat

Teorema núm. 1 (pequeño teorema): Si p positivo es primo, entonces para todo n extraño con p se cumple que $n^p = n \pmod{p}$

Es equivalente afirmar que

Teorema núm. 2

Si p es primo y a es primo con p se cumple que $a^{p-1} = 1 \pmod{p}$

Fue generalizado por Euler así: Si a y n son extraños, se cumple que $a^{f(n)} = 1 \pmod{n}$, siendo $f(n)$ el [indicador de \$n\$](#)

G

Gausiano

Gausiano de un número respecto a un módulo.

Es el mínimo exponente al que hay que elevar ese número para que produzca resto 1 al dividirlo entre el módulo. Por ejemplo, el gausiano de 3 respecto a 4 es 2, porque $3^2=1 \pmod{4}$

I

Incongruente

Números incongruentes

Varios números son incongruentes módulo **m**, cuando dan todos restos *distintos* al dividirlos entre m.

Indicador de Euler

Ver [Euler](#)

Índice modular

Si **n** es una [raíz primitiva](#) respecto a un módulo primo **p**, diremos que el número **a** es *índice modular* de otro número **b** respecto a la base **p**, cuando $n^a=b \pmod{p}$

Inversible

Número inversible

Un número es inversible si posee inverso para una operación determinada

Inverso

Inverso de un número natural en $\mathbb{Z}/m\mathbb{Z}$

Dos números naturales **a** y **b** son inversos respecto al módulo **m**, si se cumple que **$a \cdot b = 1 \pmod{m}$**

L

Ley de reciprocidad cuadrática (ya descubierta por Legendre)

Si **p** y **q** son primos impares se cumple que el sistema de ecuaciones $x^2 = q \pmod{p}$ y $x^2 = p \pmod{q}$ tiene solución siempre, excepto si tanto **p** como **q** tienen la forma $4n+3$, en cuyo caso, una tiene solución y la otra no.

Logaritmo discreto

Si una raíz primitiva engendra todo el grupo de inversibles, cada uno de estos vendrá representado por su exponente respecto a esa raíz primitiva. Es decir,

que si **a** es raíz primitiva y **b** un elemento inversible, existirá un exponente **g** tal que $a^g = b$. A ese número **g** le llamaremos **logaritmo discreto** o **índice** de b con base a.

M

Módulo

Módulo en una congruencia

Es el número **m** que tiene el papel de divisor en la definición de [congruencia](#)

P

Prueba

Prueba del 9

Consiste en sustituir cada número en una operación por su resto al dividirlo entre 9 y someter los restos a las mismas operaciones para ver si son congruentes respecto a 9. El resto se calcula fácilmente sumando las cifras del número y restando 9 cuando sea posible. Por ejemplo:

Comprobar mediante restos respecto a 9 la corrección de esta operación:

$$568 \cdot 899 + 23 = 510655$$

Pasando a restos: $1 \cdot 8 + 5 = 13$ que es congruente con 4, resto del resultado.

Pseudoaleatorio

Números naturales pseudoaleatorios

Son sucesiones de números, procedentes de fórmulas, que sin embargo parecen haber sido generados al azar. Para ello usan las propiedades de las congruencias.

R

Raíz

Raíz digital de un número entero positivo (en base 10)

La raíz digital de un número entero positivo es el dígito, entre 0 y 10, que resulta al sumar las cifras de su expresión decimal, volviendo a sumar reiteradamente los resultados de esa suma y de las siguientes hasta que la suma sea un número de una cifra, al que llamaremos raíz digital del número. Por ejemplo, la raíz digital del número 23451 es 6, porque $2+3+4+5+1 = 15$ y sumando las cifras del 15 resulta 6.

Se obtiene el mismo resultado calculando el resto módulo 9 de ese número, pero en caso de ser 0 se sustituye por 9.

Raíz primitiva respecto a un módulo primo

Un número n constituye una *raíz primitiva* respecto a un módulo primo p , cuando el [gausiano](#) de n respecto a p es exactamente $p-1$

Relación

Relación de congruencia

Dos números están relacionados por una congruencia cuando son *congruentes* respecto a un módulo dado. Esta relación es reflexiva, simétrica y transitiva y produce, por tanto, **clases de equivalencia**, llamadas también clases de restos o [residuales](#).

Residual

Ver [Clases](#)

Resto

Resto potencial

Llamaremos restos potenciales de un número natural z respecto a un módulo m a los restos de dividir las potencias de z entre m . Por ejemplo, los restos potenciales del número 7 respecto a 5 son:

$$r_0=1 \quad r_1=2 \quad r_2=4 \quad r_3=3 \quad \dots$$

Resto cuadrático

Un elemento a de unas clases de restos es **resto cuadrático** cuando es resto potencial de algún cuadrado, es decir, que existe un n tal que $n^2 = a \pmod{m}$. En caso contrario diremos que a es **no resto cuadrático**.

S

Sistema

Sistema de ecuaciones en congruencias

Es un conjunto de ecuaciones de congruencia con soluciones comunes.

Ver [el Teorema Chino](#)

Sistema de números incongruentes

Es un conjunto de números naturales cuyos restos respecto a un módulo dado son todos diferentes.

Por ejemplo: los números 13, 24 y 31 forman un sistema de números incongruentes respecto al 5.

Sistema completo de números incongruentes

Un sistema de números incongruentes se llama **COMPLETO** cuando sus restos completan todo el conjunto de los posibles respecto a un módulo.

Por ejemplo: El sistema 2,7,8,13 es completo respecto a 4, porque produce los restos 2,3,0 y 1.

T

Teorema

Ver Teoremas [Chino](#), [Fermat](#),

W

Wilson

Teorema de Wilson

Para que n divida a $(n-1)!+1$ es necesario y suficiente que n sea primo.

Por tanto, para $p>0$ primo tendremos que $(p-1)!$ es congruente con -1 módulo p