DIVISIBILIDAD

BREVE ESQUEMA TEÓRICO

CONTENIDO

INTRODUCCIÓN

El tema de divisibilidad se trata sobre los números naturales, aunque se sabe que sus resultados son válidos en Z. Sin embargo, para cuestiones de unicidad es más claro restringir el estudio a los números naturales. En las propiedades en las que intervengan números enteros se advertirá sobre este carácter.

No se demuestra ningún resultado, ya que el objetivo de esta página es tan solo mostrar un recorrido breve por los aspectos teóricos más interesantes.

DIVISIÓN ENTERA Y EXACTA

División entera

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

a = b.q + r con r<b, o lo que es lo mismo, b.q<= a < b(q+1)

Se demuestra que **q** y **r** son únicos y que siempre existen.

Si esta situación la expresamos como **a =b.q+r**, llamaremos a **q** *cociente por defecto* y a **r** *resto por defecto*.

También podemos expresarla como **a=b(q+1)-r'**. llamando a **r'** *resto por exceso*.

Propiedades

- Se cumple siempre que **r + r' = b**
- Si el dividendo y el divisor se multiplican (o dividen) por un mismo número, el cociente no varía, pero el resto queda multiplicado (o dividido) por ese número.

En la división entera podemos definir la operación "módulo". Dados dos números a y b naturales llamaremos **a MOD b** al resto por defecto que resulta al dividir a entre b.

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.**

MÚLTIPLOS Y DIVISORES

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**. Expresado de otra forma, la división entre **b** y **a** ha de ser exacta.

La relación de "*ser divisor*" o de divisibilidad se representa con el símbolo **|**. Así, "*a divide a b*" se escribe como **a|b**

Propiedades

- Todo número natural es divisor de sí mismo. **a|a**
- La unidad es divisor de todos los números naturales **1|a**
- El cero no es divisor de ningún número.
- Si un número es divisor de otros dos, también lo es de suma y diferencia: si **a|a** y **a|b** entonces **a|(a+b)**
- Si **a** es divisor de **b**, y **b** es divisor de **c**, entonces **a** es divisor de **c:** si **a|b** y **b|c** entonces **a|c**
- Si a divide a b, también divide a bx, siendo x natural.
- **Si a|b** y ambos son positivos (naturales), **a≤b**
- Si **d** divide a **a** y a **b**, también divide al resto de dividir **a** entre **b**.

La relación de divisibilidad como orden parcial

La relación por cumplir las tres propiedades

Reflexiva: a|a
Antisimétrica: a|b y **b|a,** ambos positivos, entonces **a=b**
Transitiva: a|b y **b|c** entonces **a|c**

es **una relación de orden**. Al existir elementos no comparables (7 no divide a 8, ni 8 divide a 7), este orden es **parcial**, por lo que los elementos se pueden ordenar mediante diagramas de árbol.

Diremos que un número natural **a** es *múltiplo* de **b** cuando existe otro número natural **k** que multiplicado por **b** da por resultado **a**. Expresado de otra forma, **b** ha de ser divisor de **a**.

Propiedades

- Todo **n** es múltiplo de sí mismo y de la unidad.
- Cero es múltiplo de todos los números.
- La suma o diferencia de dos múltiplos de un número también es múltiplo de dicho número.
- Si **a** es múltiplo de **b**, y **b** es múltiplo de **c**, entonces **a** es múltiplo de **c**.

La relación de "ser múltiplo" representa el **orden parcial inverso** al de la relación de "ser divisor".

CRITERIOS DE DIVISIBILIDAD

Criterios más comunes

Llamaremos criterio de divisibilidad a toda regla u operación que nos permita conocer si un número es múltiplo (o divisible) entre otro dado. Los criterios que todos conocemos se basan en los restos potenciales del la base 10 respecto al número fijado. Puedes consultar esta relación en la Teoría de las Congruencias.

Se recogen aquí los más populares:

Divisibilidad entre 2: Un número es divisible entre 2 si termina en cifra par: 0,2,4,6,8.
Entre 5: Si termina en 0 o 5
Entre 10, 100, 1000, ...: Si termina respectivamente en 0, 00, 000, ...
Entre 4: Si las dos últimas cifras del número forman otro número divisible entre 4. Por ejemplo 236, 132, 448,...
Entre 25: Similar al anterior: si termina en 00, 25, 50 o 75.
Entre 8 o 125: Son similares a los dos anteriores, pero observando las tres últimas cifras.
Entre 3 o 9: Un número es divisible entre 3 o 9 cuando también lo sea la suma de sus cifras.
Entre 11: Se suman las cifras de orden par y las de orden impar por separado. Se restan después ambas sumas y ha de resultar un múltiplo de 11 (incluido el cero).

Otros criterios menos eficientes

Divisibilidad entre 7 o 13: Este criterio también es válido para el 11, aunque no es útil. Consiste en separar el número en bloques consecutivos de tres cifras, e ir sumando cada bloque con signos alternados + y -. El resultado ha de ser múltiplo de 7 o de 13 en su caso (o entre 11 si se estudia este número). Por ejemplo, el número 1707069 es múltiplo de 13, porque 1-707+069 = -637 = -13*49

Divisibilidad entre números compuestos: Para ver si un número es divisible entre otro compuesto, basta estudiar la divisibilidad respecto a sus factores primos. Así, un número es divisible entre 6 si lo es entre 2 y 3.

Criterios recursivos

Últimamente se han hecho populares los criterios de tipo recursivo, en los que se reitera una misma operación varias veces hasta conseguir la seguridad de si es divisible o no. Vemos un ejemplo para el 7:

Para ver si un número es divisible entre 7 se apartan su última cifra de la derecha, se multiplica por 2 y se resta el resultado del resto de número formado por las cifras que quedan. Si se obtiene un número múltiplo de siete, el número primitivo también lo es. Podemos probarlo con el número 191548, que se transforma en 19154 - 2*8 = 19138. Si no sabemos si es múltiplo de 7, reiteramos la operación: 1913 - 2*8 = 1897, Podemos continuar: 191 - 2*3 =

175, que es múltiplo de 7 por ser 7*15. Según este criterio, también será múltiplo de 7 el primitivo número.

Criterios para ordenador

Todo lo anterior ha perdido eficacia ante el uso de las funciones ENTERO, COCIENTE y RESIDUO de las hojas de cálculo y programas similares.

ENTERO: Todos los programas de cálculo y lenguajes de programación disponen de la función parte entera, que, en los números positivos, que son los que nos interesan ahora, truncan los decimales de un número y devuelven la parte entera. Según la herramienta usada, se puede representar como ENTERO, ENT, E, INT, etc.

Para ver si un número A es divisible entre un número B, basta plantear esta condición:

Si A/B = ENTERO(A/B) es divisible, y en caso contrario, no.

En hoja de cálculo se puede representar así:

=SI(A/B=ENTERO(A/B);"Es divisible";"No es divisible")

COCIENTE: La función COCIENTE, a veces representada con el signo \, devuelve el cociente entero entre dos números. Por tanto, el criterio de divisibilidad es similar al anterior:

=SI(A/B=COCIENTE(A;B);"Es divisible";"No es divisible")

RESIDUO: Esta función devuelve el resto de la división entera de A entre B. También se usan los símbolos MOD, MÓDULO, %, según los programas o lenguajes. Con esta función basta averiguar si el RESIDUO es igual a cero para decidir si es divisible un número entre otro:

=SI(RESIDUO(A;B)=0;"Es divisible";"No es divisible")

Máximo común divisor y Mínimo común múltiplo

Divisores y múltiplos comunes

Un número natural **k** es *divisor común* de otros cuando es divisor de todos ellos. Igualmente se define el *múltiplo común*.

MÁXIMO COMÚN DIVISOR (MCD)

El máximo común divisor de varios números naturales es el mayor de sus divisores comunes. Se representa como MCD(a, b, , e, …) En el caso de dos números se puede representar como (a,b)

Si su valor es 1, diremos que los números son ***primos entre sí*** o ***coprimos***.

Propiedades:

- Si **a** es múltiplo de **b**, entonces el MCD de ambos es **b: (a,b)=b**
- El MCD de dos números **a** y **b** coincide con el MCD de **b** y el resto de la división de **a** entre **b**. En esta propiedad se basa el Algoritmo de Euclides: Se divide a entre b. Si el cociente es exacto, tendremos que b será el MCD. En caso contrario se divide b entre el resto. Si obtenemos un nuevo resto nulo, el primer resto es el MCD. Si no, reiteramos hasta conseguir resto 0, y el último divisor será el MCD.

	0	1	1	1	2	1	11	0	0
328	516	328	188	140	48	44	4	0	0
328	188	140	48	44	4	0	0	0	0

- Si varios números naturales se multiplican (o dividen exactamente) por otro natural **m**, su MCD queda también multiplicado (o dividido exactamente) por **m**. En concreto, si se dividen entre su MCD, los resultados son primos entre sí:

$$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$$

- Si **d** divide al producto **ab** y es primo con **a**, entonces divide a **b** (Lema de Euclides)
- Igualmente, si **m** es el MCD de **a** y **b**, existen dos números enteros **p** y **q** tales que se verifica: **m = p.a+q.b** (Teorema de Bezout). Además **m** tiene el menor valor absoluto entre todos los del conjunto de ese tipo **p.a+q.b**
- La operación de calcular el MCD es conmutativa y asociativa. Por eso se puede hallar el MCD de varios números encontrando el correspondiente a cada dos de forma progresiva.

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*.

Según el Teorema de Bezout, si **a** y **b** son primos entre sí, existirán dos números enteros **p** y **q** tales que se verifique: **p.a+q.b = 1.**

Es importante este concepto para el Lema de Euclides, visto en el anterior apartado, y también en esta propiedad:

Si **a** es múltiplo de **m** y **n** y estos son coprimos, entonces **a** es múltiplo de **mn**.

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.

MÍNIMO COMÚN MÚLTIPLO (MCM)

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

Propiedades:

- Si **a** es múltiplo de **b**, entonces el MCM de ambos es **a.**
- Si varios números naturales se multiplican (o dividen exactamente) por otro natural **m**, su MCM queda también multiplicado (o dividido exactamente) por **m**.
- Si **m** es el MCD de dos números **a** y **b** y **n** su MCM, se cumple la igualdad: **m.n = a.b**

NÚMEROS PRIMOS Y COMPUESTOS

Número primo

Un número natural mayor que 1 se llama primo si sólo es divisible entre sí mismo y la unidad. En caso contrario le llamaremos compuesto.

Existen infinitos números primos (se sabe desde Euclides), aunque su densidad es cada vez menor y se ha demostrado que converge de la siguiente forma:

Si denominamos p (x) al número de números primos inferiores o iguales a x, se cumple el teorema:

Teorema de los números primos

El cociente ***p(x)/x*** es asintóticamente equivalente al cociente ***1/ln(x)*** para valores de x muy grandes (versión de Gauss) o bien a **1/(ln(x)- 1.08366)** (versión de Legendre). Este teorema lo expresó Gauss como conjetura. Un tiempo más tarde sustituyó estas funciones por el logaritmo integral **Li(x),** conjeturando que **p(x)** se aproxima asintóticamente a esta función:

$$Li(x) = \int_2^x \frac{dx}{\log x}$$

El matemático ruso Chebychev acotó mediante dos constantes esta aproximación.

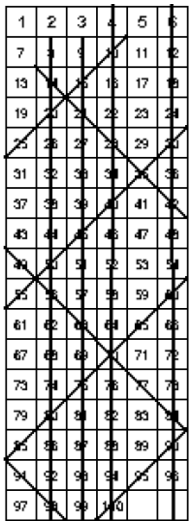
Riemann usó la función zeta x (s) = $1 + 1/2^s + 1/3^s + 1/4^s + 1/5^s$ … para lograr una gran aproximación entre p(x) y Li(x), aunque no llegó a demostrar su convergencia, cosa que lograron por separado los matematicos De la Vallée Pousin y Hadamard, al final del siglo XIX, y en el siguiente siglo (1949), demostraron el teorema Selberg y Erdös usando técnicas elementales.

La serie S (1/p) , donde **p** recorre todos los números primos, es divergente.

No obstante, si limitamos la serie a una suma parcial de todos los números primos inferiores o iguales a 5.10^7, dicha suma es menor o igual que 4.

Criba de Eratóstenes

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



En primer lugar se tachan los pares a partir del 4. Después, a partir del 9, se tachan de 3 en 3
Desde el 25, de 5 en 5, y así sucesivamente.

En la figura se observa un modo muy atractivo de tachado de números compuestos entre 1 y 100, debido a K.P.Swallow.

En este esquema se comprueba que todos los números primos son de la forma 6n+1 o 6n-1. También se ve fácilmente que son de la forma 4n+1 o 4n-1.

Criterio para saber si un número es primo

Un número es primo si no es divisible entre ninguno de los números primos menores o iguales a su raíz cuadrada. Como el número de esos primos es finito, esto proporciona un algoritmo para descubrir si un número es primo o no.

Algunas propiedades de los números primos

- El menor divisor (distinto de 1) de un número N es un número primo. Si ese divisor es N, este será primo. Si no, el divisor no sobrepasará la raíz cuadrada de N.

Esta propiedad nos permite encontrar rápidamente los factores primos de un número. Consiste en un algoritmo voraz, con estos pasos:

(a) Si N es mayor que 1, se busca su menor divisor d, que será primo, y por tanto factor primo de N. Si no, termina el proceso.

(b) Se divide N entre d y al resultado se le vuelve a llamar N

(c) Se vuelve al paso (a)

Este algoritmo es muy útil para implementarlo en calculadoras u hojas de cálculo, pues es relativamente rápido para números grandes.

- Como consecuencia de lo anterior, un número es primo o un producto de primos.

- Dados un número N cualquiera y un número primo P se verificará o que N sea divisible entre P o que N sea primo con P. Como consecuencia, un primo P es primo con todos los números menores que él.

- Si un producto de números es divisible entre un primo P, uno al menos de los factores también lo será. Por tanto, si el producto es entre primos distintos, P coincidirá con alguno de ellos.

- Hay infinitos números primos de la forma ***4n+3***
- Si p_n es el n-ésimo primo, será menor o igual que ***2*** elevado a 2^{n-1}
- Todo número primo mayor que 3 es de la forma 6n+1 o de la forma 6n-1
- Todo número primo mayor que 2 es de la forma 4n+1 o de la forma 4n-1.

Un número primo tiene las siguientes propiedades respecto a una suma de cuadrados:

a. Un número primo es suma de cuadrados de dos números naturales si y sólo si es de la forma 4n+1.
b. El producto de dos números que son suma de cuadrados también es otra suma de cuadrados, en virtud de la identidad
c. $(a^2 + b^2)(c^2 + d^2) = (ac-bd)^2 + (ad+bc)^2$
d. Por tanto el producto de potencias de números del tipo 4n+1 también equivale a una suma de cuadrados.
e. Si una suma de cuadrados se multiplica por otro cuadrado, resulta una nueva suma de cuadrados:

f. $(a^2 + b^2)c^2 = (ac)^2 + (bc)^2$
g. De las propiedades anteriores se deduce que son suma de cuadrados los números que contienen factores primos del tipo 4n+1 y factores de otro tipo cualquiera pero con potencia par.

NÚMEROS K-CASIPRIMOS

A un número se le llama ***k*-casi primo** si es el producto de k números primos, no necesariamente distintos. Por ejemplo, 210 es 4-casiprimo, porque equivale al producto 2*3*5*7. Si sólo son dos, recibe el nombre de semiprimo, como 6=2*3 o 9=3*3. En el caso de tres factores, si son distintos, al número le llamaremos esfénico, como por ejemplo 110=2*5*11.

DESCOMPOSICIÓN EN FACTORES PRIMOS

La descomposición en factores primos se basa en el siguiente teorema

Teorema Fundamental de la aritmética

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

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

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

Las potencias del tipo $\mathbf{p^a}$, potencias de un número primo, reciben el nombre de *números primarios*.

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.

Por tanto, todos los divisores de N se obtendrán combinando de todas las formas posibles los factores primos tomados con repetición. Son los términos de este producto

$$\sigma(N) = \prod \frac{{p_i}^{s_i+1} - 1}{p_i - 1} = \prod (1 + p_i + {p_i}^2 + \cdots {p_i}^{s_i})$$

Luego el número de divisores será

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

Como consecuencia de lo anterior, todo divisor d posee un complementario N/d que contiene todos los factores primos que faltan en d.

Según esto, el producto de todos los divisores de N se puede descomponer en pares D*N/D=N, luego su valor será

$$P = \sqrt{N^{D(n)}}$$

Cálculo del MCD y el MCM mediante factores primos

Una vez descompuestos dos números **a** y **b** en factores primos, su MCD se obtiene como producto de los *factores comunes tomados con el menor exponente* y el MCM como producto de *todos los factores con el mayor exponente*.

Como consecuencia, dos números serán *primos entre sí* si no tienen factores primos comunes.

Factorización de Fermat

La factorización de Fermat siempre se ha presentado como una técnica para representar un número impar como producto de dos de sus factores sin usar la lista de números primos. En efecto, la factorización de Fermat no se basa en los factores primos, sino en representar un número impar N como una diferencia de dos cuadrados y después expresar la misma como el producto de una suma por una diferencia, con lo que se logra la factorización:

$N=y^2-x^2=(x+y)(y-x)$, $y>x$

En el caso impar esta operación siempre es posible, porque $N=(N+1)^2/4-(N-1)^2/4$, que da lugar a la factorización N=N.1

FÓRMULA DE POLIGNAC

Es relativamente sencillo encontrar los divisores primos del factorial de un número natural n. Simplemente son todos los primos inferiores o iguales a n. El problema reside en calcular los exponentes a los que están elevados. Por ejemplo, la descomposición factorial de 22! Es

$$22! = 2^{19}*3^9*5^4*7^3*11^2*13*17*19$$

Para obtener los exponentes Polignac propuso esta fórmula

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

En la que el exponente r de cada factor primo p viene dado por la suma de los cocientes enteros del número n entre las sucesivas potencias de p.

Puedes usar esta fórmula para resolver las cuestiones siguientes:
¿Cuál es el mayor divisor del factorial 12! que es cuadrado perfecto? (Solución 2073600, cuadrado de 1440)
¿En cuántos ceros termina el cociente 100!/50!? (Solución en 12 ceros)
¿Cuál es la máxima potencia de 56 que divide a 56!? (Solución 56 elevado a 9)

CONJUNTO DE DIVISORES DE UN NÚMERO

Divisor propio: Un divisor de un número N se llama propio si es menor que N. También recibe el nombre de **parte alícuota**.

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

NÚMERO Y SUMA DE DIVISORES

Consideremos el conjunto formado por todos los divisores de un número. Generalmente sólo se consideran los positivos. En nuestro caso lo haremos así, por restringirnos a los números naturales.

NÚMERO DE DIVISORES

Para obtener todos los divisores de un número cuya descomposición es $n = p_1^{a1}.p_2^{a2}.p_3^{a3\ldots}$ basta considerar que son los términos del producto

$(1 + p_1 + p_1^2 + \ldots p_1^{a1})(1 + p_2 + p_2^2 + \ldots p_2^{a2})(1 + p_3 + p_3^2 + \ldots p_3^{a3})$

Esta operación equivale a formar todos los productos posibles del tipo $p_1^{b1}.p_2^{b2}.p_3^{b3\ldots}$ en los que los exponentes b_i recorren todos los valores enteros que van de 0 a a_i. Como esta es una operación de combinar elementos de conjuntos distintos se calculará su número por la ley del producto y nos quedará que el número de divisores de N, o función **divisor** o **TAU** vendrá dada por la fórmula

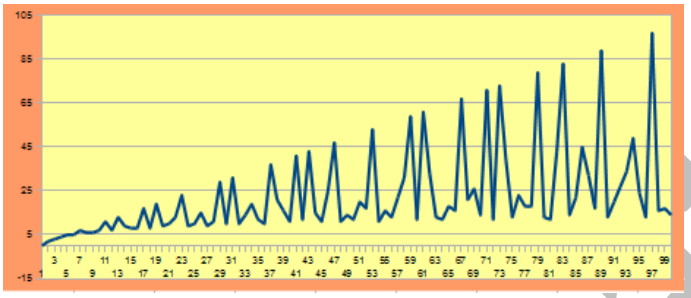
$$D(N) = (1 + a_1) * (1 + a_2) \ldots (1 + a_k)$$

También se usan las funciones

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

BIGOMEGA: Cuenta los factores primos con multiplicidad, como biomega(60)=4. También recibe el nombre de **logaritmo entero** o función **sofpr(N)**

Se suele representar por la función sopfr(n). Así, sopfr(28)=2+2+7=11. El valor más pequeño corresponde a sopfr(1)=0 y los mayores coinciden con los números primos, como es evidente. Aquí tienes la gráfica de esta función para los primeros números, en la que se perciben los máximos correspondientes a los primos:



Se le llama logaritmo porque posee la propiedad 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).

S(N) (SUMA DE DIVISORES FUNCIÓN SIGMA)

Representa la suma de todos los divisores de n incluido él mismo.

Si **n** es primo, s (n)=n+1. Si es perfecto, s (n)=2n. Si es un número primario, la función s (n) tiene como fórmula:
$s(p^r) = (p^{r+1}-1)/(p-1)$ que nos permite evaluar la función s (n) para un número compuesto si se conocen sus factores primos:

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

Si a y b son primos entre sí se verifica que s (a.b)=s (a).s (b). Diremos que esta función es multiplicativa

OTRAS FUNCIONES SIMILARES A SIGMA

USIGMA**:** Es la suma de todos los divisores propios de un número N. Se calcula con la fórmula siguiente, en la $\mathbf{p_i}$ son los factores primos y $\mathbf{k_i}$ sus exponentes.

$$\sigma^*(N) = \prod (1 + {p_i}^{k_i})$$

SIGMA_K: Es la suma de todos los divisores de un número elevados todos al exponente k. Su cálculo se efectúa a través de la fórmula, siendo $\mathbf{e_i}$ los exponentes de los factores primos $\mathbf{p_i}$

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

ANTISIGMA:

Al igual que se ha definido la función SIGMA(N) como la suma de todos los divisores de N (incluido él mismo), podemos definir la ANTISIGMA(N), que es la suma de los números menores que N y que no lo dividen, Por ejemplo, la antisigma de 8 sería la suma de 3+5+6+7=21, y sigma(8) es igual a 1+2+4+8=15.

Los valores de esta función antisigma son los siguientes, que están incluidos en https://oeis.org/A024816

0, 0, 2, 3, 9, 9, 20, 21, 32, 37, 54, 50, 77, 81, 96, 105, 135, 132, 170, 168, 199, 217, 252, 240, 294, 309, 338, 350,…

La suma de SIGMA(N) y ANTISIGMA(N) es muy fácil de calcular, ya que se trata de sumar todos los números desde 1 hasta N, y esto sabemos que es igual a N(N+1)/2.

Relación fundamental: **SIGMA(N)+ANTISIGMA(N)=N(N+1)/2**

NÚMEROS ESPECIALES

En este apartado se irán explicando algunas clases curiosas de números sin un orden predeterminado, pudiéndose añadir tipos nuevos en sucesivas ediciones.

NÚMEROS PERFECTOS, ABUNDANTES O DEFICIENTES

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.

Todos los números perfectos son también triangulares y todos los conocidos hasta ahora son pares. Se ignora si existe algún número perfecto impar, aunque se sabe que de existir debería ser mayor que 10^{150}.

Tampoco se sabe si existen infinitos números perfectos.

Euclides demostró que si el número 2^k-1 es primo (número de Mersenne), el número $N=2^{k-1}(2^k-1)$ es perfecto.

Euler demostró el recíproco (evidentemente, sólo para perfectos pares), con lo que quedó establecida una correspondencia biunívoca entre los números perfectos pares y los números de Mersenne primos.

Número abundante

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

- Todos los números múltiplos de 6 mayores que 6 son abundantes. Intenta demostrarlo.
- El menor abundante impar es 945. Puedes comprobarlo con el Buscador de Naturales.
- Todo número abundante mayor que 83.160 es suma de otros dos abundantes. También todo número par mayor que 46 es suma de dos abundantes.

Número deficiente

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

Curiosidades numéricas sobre números perfectos, abundantes o deficientes

- Los inversos de los divisores de un número perfecto suman siempre 2:

- Divisores del 6: 1/1 +1/2 +1/3 + 1/6 = 2
- Divisores del 28: 1/1 + 1/2 +1/4 + 1/7 + 1/14 + 1/28 = 2
- Todos los números perfectos, salvo el 6, coinciden con sumas parciales de la serie
- $1^3 + 3^3 + 5^3 + 7^3 + 9^3 + \ldots$ Así: $28 = 1^3 + 3^3$; $496 = 1^3 + 3^3 + 5^3 + 7^3$

Concepto de abundancia

Llamamos ***abundancia*** del número A al S(A)/A, siendo S(A) la suma de los divisores de A, o sigma de A. Es claro que que el cociente S(N)/N vale 2 en los números perfectos, más de 2 en los abundantes y menos en los deficientes. Se puede demostrar lo siguiente:

La abundancia de un número múltiplo de A es mayor que la abundancia de A: Si M=A*k, (M, A y K enteros positivos), entonces S(M)/M > S(A)/A

Para demostrarlo basta considerar el caso en el que k es primo, porque por reiteración la propiedad se iría repitiendo en cada factor primo de k si fuera compuesto. Recordemos la fórmula de la función sigma S:

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

En la que p_i son los factores primos de A y e_i sus multiplicidades. Si el nuevo primo k es uno de ellos con multiplicidad p, su cociente $(k^{p+1}-1)/(k-1)$ se convertiría en $(k^{p+2}-1)/(k-1)$, que es mayor que $(k^{p+1}-k)/(k-1)=k(k^{p+1}-1)/(k-1)$. Por tanto, ese factor $(k^{p+1}-1)/(k-1)$ de la función sigma quedaría multiplicado por un número mayor que k. Por tanto, la abundancia aumenta, porque S(M)/M > kS(A)/M=kS(A)/(kA)=S(A)/A.

Si k es un número primo que no divide a A, entonces su función sigma, al pasar a M, quedaría multiplicada por (k+1) y tendríamos: S(M)/M=S(A)*(k+1)/(A*k)= S(A)/A*((k+1)/k)>S(A)/A, es decir, la abundancia quedaría multiplicada por un número mayor que la unidad.

Si k fuera compuesto, iríamos multiplicando por cada uno de sus factores primos, con lo que la abundancia crecería aún con más razón.

Lo importante es que estos crecimientos son estrictos: nunca se da la igualdad de abundancias entre un número y sus múltiplos. De esto se desprende lo siguiente, que es muy fácil de razonar:

- Los divisores de un número perfecto son todos deficientes.
- Si un número es no deficiente (perfecto o abundante), sus múltiplos serán todos abundantes.

Nos podemos imaginar que si N es no deficiente, entre los divisores de N encontraremos deficientes (quizás no todos) y entre los múltiplos, todos abundantes. ¿Dónde está la frontera?

Dickson (1913) llamó **no deficientes primitivos** a aquellos números no deficientes cuyos divisores propios sí son todos deficientes. Es evidente que entre esos números estarán los

perfectos y quizás alguno más. Pues sí, hay más: 6, 20, 28, 70, 88, 104, 272, 304, 368, 464, 496, 550, 572, 650, 748, 836, 945, 1184…

NÚMEROS DE ORE

Un número entero positivo N se llama de **Ore** o **armónico** cuando la media armónica de todos sus divisores es un número entero. Por ejemplo, es armónico 140, porque sus 12 divisores son 1, 2, 4, 5, 7, 10, 14, 20, 28, 35, 70 y 140 y por tanto su media armónica es

$$m_a = \frac{12}{\frac{1}{1}+\frac{1}{2}+\frac{1}{4}+\frac{1}{5}+\frac{1}{7}+\frac{1}{10}+\frac{1}{14}+\frac{1}{20}+\frac{1}{28}+\frac{1}{35}+\frac{1}{70}+\frac{1}{140}}=5$$

Parece muy pesado este cálculo para números grandes, pero existe una simplificación. Para ello basta observar que cada divisor d posee un complementario d′ tales que d.d′=N. Este hecho permite ir sustituyendo cada cociente del tipo 1/d por d′/N, con lo que todos los denominadores resultará iguales a N y se podrán sumar los cocientes con facilidad:

$$m_a = \frac{12}{\frac{140}{140}+\frac{70}{140}+\frac{35}{140}+\frac{28}{140}+\frac{20}{140}+\frac{14}{140}+\frac{10}{140}+\frac{7}{140}+\frac{5}{140}+\frac{4}{140}+\frac{2}{140}+\frac{1}{140}}=\frac{140.12}{336}=5$$

Este procedimiento es fácilmente generalizable: basta multiplicar N por su número de divisores y dividir después entre la suma de los mismos:

$$m_a = \frac{N.d(N)}{\sigma(N)}$$

Representamos el número de divisores mediante d(N) y su suma por s(N). Basta observar la fórmula para poder interpretarla de otra manera: La media armónica de los divisores equivale al cociente entre el número y la media aritmética de dichos divisores.

Los primeros números de Ore son: 1, 6, 28, 140, 270, 496, 672, 1638, 2970, 6200, 8128, 8190…Entre ellos se incluyen los números perfectos 6, 28, 496, 8128,...y otros más que no lo son. Todo número perfecto se puede demostrar que también es armónico. Esto es interesante, porque si se lograra demostrar la Conjetura de Ore de que no existen armónicos impares, también se habría logrado demostrar que tampoco hay perfectos impares.

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 (conocido por los griegos), 17296 y 18416 (Fermat) y 9363584 con 9437056 (Descartes). Euler encontró 64 pares, entre ellos 2620 y 2924, y 5020 con 5564. Paganini descubrió un par relativamente pequeño que había permanecido inadvertido durante siglos: 1184 y 1210

- Parece que su cociente tiende a 1
- No se conocen pares de amigos uno par y otro impar ni se ha podido demostrar que no existan.
- Todas las parejas de números amigos impares son múltiplos de 3.
- No hay fórmulas para encontrar todos los números amigos, aunque existen para construir algunos (Ver Thabit idn Qurra)
- No se sabe si su número es finito o infinito.

Los primeros pares de números amigos son:

220	**284**
1184	**1210**
2620	**2924**
5020	**5564**
6232	**6308**
10744	**10856**
12285	**14595**
17296	**18416**
63020	**76084**
66928	**66992**

NÚMEROS SOCIABLES

Son similares a los anteriores, pero sin reciprocidad: Un conjunto de números sociables es una sucesión de números en la que cada término es igual a la suma de los divisores propios del término anterior. En el caso de los números sociables, la sucesión es cíclica. Por ejemplo, el conjunto 1264460, 1547860, 1727636, 1305184 está formado por números sociables, porque

cada uno (y el último con el primero) coincide con la suma de los divisores propios del siguiente.

Al número de elementos del conjunto lo llamaremos ***periodo*** u ***orden*** del mismo. Existe un conjunto de orden 5 formado por los números más sencillos: 12 496, 14 288, 15 472, 14 536, 14 264

Según lo anterior, un número perfecto forma un ciclo de orden 1, y un par de números amigos de orden 2.

No se sabe si todos los enteros o bien son sociables, o su conjunto acaba en un primo y sigue con 1, o bien para algún número el conjunto de los sociables con él nunca acaba.

NÚMEROS DE MERSENNE

Son los números del tipo 2^p -1 con p primo.

Si 2^n -1 es primo, n también es primo, pero no al revés. Por ejemplo, 2^{67}-1 es divisible entre 193.707.221. También 2^{11} – 1 es compuesto e igual a 23*89

Mersenne afirmó que son primos tan sólo los correspondientes a los valores de **p** 2, 3, 5, 7, 13, 19, 31, 67, 127 y 257, pero falló en el 61, que también es primo, y en el 67, que no lo es (Cole 1903).

Se ignora si hay infinitos números primos de Mersenne.

Los primeros números de Mersenne primos son:

p	2^p-1
2	3
3	7
5	31
7	127
13	8191
17	131071

NÚMEROS DE FERMAT

Son aquellos de la forma $2^{2^n}+1$

Todo primo de la forma 2^k+1 es de Fermat, pues es fácil demostrar que si k es impar, o contiene un factor impar, el resultado es un número compuesto.

Pero cualquier número de Fermat no es necesariamente primo.

Los primeros números de Fermat, para n=0,1,2,3 y 4, los números 3, 5, 17, 257, 65537, ...son primos.

Euler demostró que para n=5 El número resultante no es primo, sino divisible entre 641: 4.294.967.297 = 641*6.700.417

Next, en 1880 demostró que el número de Fermat correspondiente a n=6 se descompone en los factores 18.446.744.073.709.551.617 = 274.177 * 67.280.421.310.721

No se sabe si existen más números de Fermat primos.

Gauss relacionó estos números con los polígonos regulares que se pueden dibujar con regla y compás.

NÚMEROS DE AQUILES

Un número natural se llama ***poderoso*** cuando todos los exponentes de sus factores primos son mayores o iguales a 2. Expresado de otra manera: si N es poderoso y un número p primo divide a N, entonces p^2 también divide a N.

Esta definición tiene una consecuencia muy curiosa: todos los números poderosos se pueden expresar así: $\mathbf{N=a^2b^3}$ con a y b naturales. ¿Te atreves a demostrarlo? Antes de que te pongas a ello, recuerda que no hemos dicho que a y b tengan que ser primos.

Los números de Aquiles son números poderosos que no pueden representarse como potencias perfectas, es decir, no equivalen a m^n con m y n naturales. Esto significa que el máximo común divisor de los exponentes ha de ser 1. En efecto, si en la descomposición de un número los exponentes tuvieran un factor común se podría efectuar la siguiente transformación:

$$N = p^{tk}q^{tl}r^{tm}\ldots = \left(p^k q^l r^m \ldots\right)^t$$

Esto convertiría N en una potencia, en contra de lo supuesto.

Por ejemplo, el número 2700 es de Aquiles, porque equivale a $2^2*5^2*3^3$. El m.c.d de los exponentes es 1. Son coprimos, aunque no dos a dos.

La descomposición $N=a^2b^3$ que vimos más arriba exige que en el caso de los números de Aquiles ni **a** ni **b** sean iguales a la unidad.

Los primeros números de Aquiles son

72, 108, 200, 288, 392, 432, 500, 648, 675, 800, 864, 968, 972, 1125, 1152, 1323, 1352, 1372, 1568, 1800,… (http://oeis.org/A052486)

Se han descubierto interesantes propiedades de estos números. Por ejemplo:

* 3087 y 7803 son ambos de Aquiles y sus cifras ordenadas en orden inverso

* Los números de Aquiles consecutivos más pequeños son

$5425069447 = 7^3 \times 41^2 \times 97^2$

$5425069448 = 2^3 \times 26041^2$

* Hay números de Aquiles "fuertes", en los que ellos son de Aquiles y su indicatriz de Euler también. Son estos:

500, 864, 1944, 2000, 2592, 3456, 5000, 10125, 10368, 12348, 12500, 16875, 19652, 19773, (https://oeis.org/A194085)

Existen números de Aquiles cuyos divisores propios no son de ese tipo, como el 72. ¿Qué caracteriza a esos números? Vamos a demostrar que son aquellos cuya signatura prima es (2,3), es decir, que son de la forma p^2q^3 con p y q ambos primos.

Son números de Aquiles minimales los que tienen la forma p^2q^3 con p y q ambos primos.

Vimos que todo número de Aquiles se puede expresar como $\mathbf{N=a^2b^3}$ con a y b naturales mayores que la unidad. Si uno de ellos es compuesto, por ejemplo a, sea a=a'*k con a' mayor que 1 y N se puede expresar como $\mathbf{N=(a'*k)^2b^3} = (a'^2*b^3)*k^2$. El paréntesis es un número de Aquiles y divisor de N, luego es necesario que a y b sean primos para que N sea minimal.

Inversamente, si a y b son primos mayores que 1, los únicos divisores propios de N estarían en este conjunto: 1, a, b, a^2, b^2, b^3, ab, ab^2, a^2b, ab^3, a^2b^2, y ninguno cumple lo exigido a un número de Aquiles.

Según esto, los números de Aquiles minimales son los contenidos en la secuencia https://oeis.org/A143610

72, 108, 200, 392, 500, 675, 968, 1125, 1323, 1352, 1372, 2312, 2888, 3087, 3267, 4232, 4563, 5324, 6125, 6728, 7688, 7803, 8575, 8788, 9747, 10952, 11979, 13448...

Todo número de Aquiles posee un divisor (no necesariamente propio) que tiene el carácter de número de Aquiles minimal

Si en un número N de Aquiles presenta un mayor divisor propio también de Aquiles, tendrá un cociente por la izquierda equivalente a un número primo. Los números que tienen esa propiedad son estos:

864 1944, 3888, 4000, 5400, 6912, 9000, 10584, 10800, 10976, 17496, 18000, 21168, 21600, 24696, 25000, 26136, 30375, 31104, 32000, 34992, 36000, 36504, 42336, 42592, 43200, 48600, 49000, 49392, 50000…(los hemos publicado en http://oeis.org/A203662)

En ellos se cumplen dos propiedades:

- El exponente del menor factor primo de cada uno de ellos es mayor que 2.
- Todos tienen los mismos factores primos (salvo los exponentes) que su mayor divisor propio.

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. Los primeros primoriales son

1, 2, 6, 30, 210, 2310, 30030, 510510, 9699690, 223092870, 6469693230, 200560490130, 7420738134810, 304250263527210, 13082761331670030,… (https://oeis.org/A002110)

(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)

1, 1, 2, 6, 6, 30, 30, 210, 210, 210, 210, 2310, 2310, 30030, 30030, 30030, 30030, 510510, 510510, 9699690, 9699690, 9699690, 9699690, 223092870, 223092870,… (https://oeis.org/A034386)

(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. Los primeros son

2, 3, 7, 31, 211, 2311, 30031, 510511, 9699691, 223092871, 6469693231, 200560490131, 7420738134811, 304250263527211,

(https://oeis.org/A006862)

También se suelen llamar primos primoriales a los de la forma p#-1

Al cociente entre el factorial de un número y su primorial se le suele llamar el "***compositorial de n***".

Dos primoriales consecutivos se corresponden con el mismo compositorial.

PSEUDOPRIMOS

El Pequeño teorema de Fermat afirma que si m es primo, se cumple que para todo a coprimo con m es verdadera esta congruencia:

$a^{m-1} \equiv 1 \pmod{m}$

En cualquier manual puedes estudiarlo y seguir su demostración.

El recíproco no es cierto. Si para un a primo con m se cumple $a^{m-1} \equiv 1 \pmod{m}$, entonces m no tiene que ser necesariamente primo. A estos números compuestos que cumplen el teorema les llamaremos pseudoprimos de Fermat para ese número a (hay otros, como los de Euler y los de Poulet, pero los dejamos para otra ocasión)

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.

Vemos algún ejemplo de lo explicado:

91 pasa la prueba con 3 pero no es primo Es pseudoprimo para el 3. En efecto, lo vemos por duplicación de exponentes: $3 \equiv 3 \pmod{91}$, luego $3^2 \equiv 9 \pmod{91}$; $3^4 \equiv 81 \pmod{91}$; $3^8 \equiv 9 \pmod{91}$; $3^{16} \equiv 81 \pmod{91}$; $3^{32} \equiv 9 \pmod{91}$; $3^{64} \equiv 81 \pmod{91}$ y queda
$390 = 364+16+8+2 \equiv 81*81*9*9 \equiv 1 \pmod{91}$;

Sin embargo, 91 no es primo, porque equivale a 7*13. Es pseudoprimo para el 3

Hemos presentado los números de Carmichael o primos absolutos. Son estos:

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361, 101101,… (http://oeis.org/A002997)

En ellos la prueba de primalidad basada en el teorema de Fermat falla siempre. Por ejemplo, el 561 se daría como primo y resulta que es 561= 3* 11* 17.

ALTAMENTE COMPUESTOS

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

Así, el 12 tiene 6 divisores, mientras que todos los números menores que él tienen (del 1 al 11) 1, 2, 2, 3, 2, 4, 2, 4, 3, 4 y 2 respectivamente, luego 12 es altamente compuesto (lo expresaremos como NAC)

Los primeros son:

1, 2, 4, 6, 12, 24, 36, 48, 60, 120, 180, 240, 360, 720, 840, 1260, 1680, 2520, 5040, ...

INTERPRIMOS

Se llaman “interprimos” a los números naturales que son media de dos primos consecutivos. El conjunto de estos números es amplísimo, y se puede descomponer en diversos subconjuntos interesantes, la mayoría ya publicados. Los primeros interprimos son

4, 6, 9, 12, 15, 18, 21, 26, 30, 34, 39, 42, 45, 50, 56, 60, 64, 69, 72, 76, 81, 86, 93, 99, 102, 105, 108, 111, 120, 129, 134, 138, 144,…

Interprimos entre primos gemelos

Entre ellos son interesantes los que son media de dos primos gemelos:

4, 6, 12, 18, 30, 42, 60, 72, 102, 108, 138, 150, 180, 192, 198, 228, 240, 270, 282, 312, 348,…

Salvo el primero, todos son múltiplos de 6, ya que los primos gemelos han de tener la forma 6k-1 y 6k+1 (salvo 3 y 5), con lo que la media será 6k. Este mismo hecho demuestra también que el interprimo es la raíz cuadrada del producto de los dos primos más una unidad.

Interprimos entre primos “cousin” y “sexy”

Los primos “cousin” son los que se diferencian en 4 unidades. Sus promedios son estos:

5, 9, 15, 21, 39, 45, 69, 81, 99, 105, 111, 129, 165, 195, 225, 231, 279, 309, 315, 351, 381, 399, 441,… https://oeis.org/A087679

Si los anteriores eran todos múltiplos de 6, salvo los primeros, estos lo serán de 3 y no de 6. La razón es que los primos que se diferencian en 4 unidades han de tener la forma 6k+1 y 6k+5, con lo que el promedio será (12k+6)/2=6k+3.

Si el par de primos es “sexy”, es decir, que se diferencian en 6 unidades, sus interprimos son:

26, 34, 50, 56, 64, 76, 86, 134, 154, 160, 170, 176, 236, 254, 260, 266, 274, 334, 356, 370, 376, 386,… https://oeis.org/A072571

En este caso, para que diferencien en 6, los primos han de ser 6k+1 y 6(k+1)+1 o bien 6k+5 y 6(k+1)+5. Y los promedios 6k+4 o 6(k+1)+2, luego estos interprimos son todos pares, pero no múltiplos de 3.

PRIMOS EQUILIBRADOS

Un número primo es equilibrado si es promedio de sus dos primos contiguos. Por ejemplo, 257 es media de su anterior 251 y el posterior 263, que por cierto también es primo equilibrado. Los tres primos componentes de la terna formarán, pues, una progresión aritmética.

Los primeros primos equilibrados son:

5, 53, 157, 173, 211, 257, 263, 373, 563, 593, 607, 653, 733, 947, 977, …

FUNCIONES IMPORTANTES EN TEORÍA DE NÚMEROS

F(N) (INDICATRIZ O INDICATRIZ DE EULER, FUNCIÓN PHI)

Representa cuántos números naturales inferiores a **n** son primos con él, contando el 1.

Si **n** es primo, f(n)= n-1. Si es primario (tipo $\mathbf{p^r}$ con p primo), su indicatriz viene dada por la fórmula $\mathbf{f(n)=p^{r-1}(p-1) = p^r(1-1/p)}$

Es una función multiplicativa. La indicatriz de un producto de números primos dos a dos es el producto de las indicatrices de éstos. Con esta propiedad podemos calcular la indicatriz de cualquier número compuesto

Si un número natural m se descompone en factores primos: $m=p^a.q^b.r^s$.... su indicatriz de Euler vendrá dada por:

$f(m) = m\ (1- 1/p)(1 - 1/q)(1- 1/r)....$

Por ejemplo, si $12 = 2^2*3$, su indicatriz será $f(12) = 12*(1-1/2)*(1-1/3) = 4$, y , efectivamente los 4 números 1, 5, 7 y 11 son primos con él

El indicatriz de Euler coincide con el número de elementos inversibles de un grupo cíclico de orden **n**

Una curiosa propiedad de esta función es que si sumamos su valor en los divisores de N, esa suma coincide con N.

Π(N) (PRIMOS HASTA N)

Representa cuántos números primos hay no superiores a **n**. Por eso se le llama también contador de números primos y se representa por π(n). Es una de las funciones más estudiadas en Teoría de Números, ya que sobre ella trata el

Teorema de los números primos:

Para **n** tendiendo a infinito, π(n) coincide asintóticamente con la expresión **n/ln(n).**

Según expresa la Wikipedia, esto no significa que la diferencia entre π(x) y x/ln x se aproxime a cero, sino que su cociente se aproxima a 1.

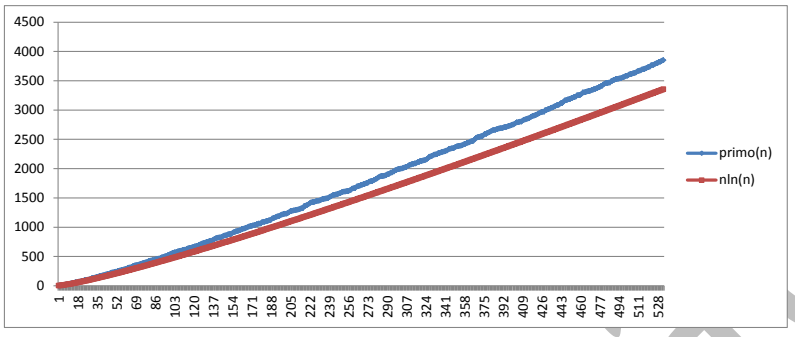
Este resultado fue presentado por Gauss y después de mucho tiempo, los matemáticos Jacques Hadamard y Charles de la Vallée-Poussin consiguieron, de forma independiente, una demostración definitiva.

P(N) PRIMO NÚMERO N

Es la función inversa de la anterior: dado un número natural n, P(n) (o PRIMO(n)) representa el número primo que ocupa el lugar n en la lista de ellos.

Es evidente que $P(\pi(n))=\pi(P(n))=n$

Esta función presenta un crecimiento casi lineal, y es siempre mayor que nln(n), como puedes observar en este gráfico:



D(N) (DISTANCIA AL PRÓXIMO PRIMO)

Su valor es la distancia entre un número cualquiera y el número primo más pequeño que es mayor o igual que él.

M(N) (FUNCIÓN DE MÖBIUS)

Se define para todos los números naturales según sean múltiplos o no de números cuadrados. A cada uno se le hace corresponder uno de los valores -1, 0 o +1,de la siguiente forma:

M(n)= 1 si n no es múltiplo de cuadrados y tiene un número par de factores primos distintos
M(n)=-1 si n no es múltiplo de cuadrados y tiene un número impar de factores primos distintos
M(n)=0 si n es divisible entre algún cuadrado.

Es una función es muy importante en Teoría de Números y Combinatoria.

FUNCIONES MULTIPLICATIVAS

Funciones aritméticas

Son funciones reales o complejas definidas sobre el conjunto de los números naturales.

Por tanto, toda función aritmética admite una representación como una sucesión de números (enteros, reales, complejos…)

Funciones multiplicativas

Una función aritmética es multiplicativa cuando para todo par a y b de números naturales primos entre sí se cumple que

F(a*b)=F(a)*F(b) (si (a,b)=1, siendo (a,b) el MCD de ambos números)

Si esto se cumple aunque los números no sean coprimos, llamaremos a la función completamente multiplicativa. Por ahora no las consideraremos.

Propiedades de las funciones multiplicativas

(1) Si una función es multiplicativa se dará que **F(a*1)=F(a)*F(1),** luego deberá ser **F(1)=1**

A veces esta propiedad no está clara en alguna función, porque puede que no acabe de tener mucho sentido aplicarla a la unidad. En ese caso se suele definir directamente: F(1)=1.

(2) Si una multiplicativa está definida para cada potencia de un primo, lo estará para todo número natural, pues aplicando la función a la factorización

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

Por su carácter multiplicativo se tendrá

$$F(N) = F({p_1}^{a_1} * {p_1}^{a_2} * \dots {p_k}^{a_k}) = F({p_1}^{a_1}) * F({p_1}^{a_2}) * \dots F({p_k}^{a_k})$$

Puedes seguir los detalles en los documentos teóricos. En ellos también se demuestra lo siguiente, que es fundamental para manejar funciones multiplicativas:

Si una función aplicada a N actúa de igual forma e independientemente para cada factor de N del tipo pr, siendo p un factor primo de N y r su exponente (factor primario) y después multiplica los resultados, esa función será multiplicativa

(3) El producto de dos multiplicativas también es también multiplicativo

(4) Si g(x) es una función multiplicativa, entonces, la función f(n) definida por

$$f(n) = \sum_{(d|n)} g(d)$$

CONJETURAS

Conjeturas de Goldbach

Todo número par mayor que 2 es suma de dos primos

Fue propuesta por Goldbach el 7 de Junio de 1742, en una carta dirigida a Euler. En realidad, su propuesta se refería a la conjetura ternaria: " *Todo número impar es la suma de tres primos*" y Euler le respondió con la propuesta binaria que todos conocemos.

Ha sido comprobada hasta 10^{14}, pero no se ha podido demostrar.

No obstante, se han logrado resultados provisionales:

Cualquier número par es suma de 6 o menos números primos.(Ramaré 1995)

Todo número par suficientemente grande es suma de un primo y del producto de dos primos.(Chen 1966)

Todo número impar N mayor que 5 es suma de tres primos. (Demostración de la conjetura ternaria a cargo de Vinogradov en 1937).

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)

Conjetura de Legendre

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

Se considera básica e importante, por lo que se incluyó en los Problemas de Landau

(http://en.wikipedia.org/wiki/Landau%27s_problems)

Otra formulación

Si usamos la función π, que da la distribución de los números primos ($\pi(200)$ equivaldría a los primos que existen menores o iguales a 200), la conjetura de Legendre se podría expresar así:

$$\pi((n+1)^2) - \pi(n^2) > 0$$

Conjetura de Andrica

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

Si representamos por p_n el número primo que aparece en el lugar n de su lista, la conjetura se expresa como

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

Si la conjetura de Andrica es cierta, de ella se deduce la de Legendre.

Conjetura de Brocard

Parecida a la anterior, la conjetura de Brocard dice que existen al menos cuatro números primos comprendidos entre $(p_n)^2$ y $(p_{n+1})^2$, para n > 1, donde p_n es el n-ésimo primo.

*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.*

Conjetura n^2+1

Es uno de los problemas de Landau, y en el momento de redactar este texto sigue sin conocerse si es verdadera o no la siguiente conjetura:

Existen infinitos primos de la forma n^2+1

Conjetura de Polignac

Se llama Conjetura de Polignac a la enunciada por Alphonse de Polignac in 1849 y que se puede expresar así:

Hay un número infinito de números primos (p, q) tales que p - q = k, siendo k un número par.

Últimamente se ha hablado más de ella por algunos avances que se han producido y que pudieran llevar a su demostración

PROBLEMAS NO RESUELTOS

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?