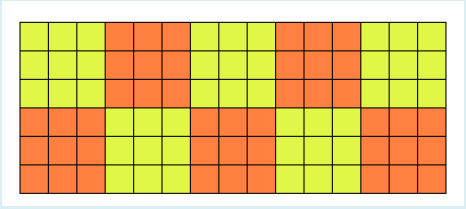
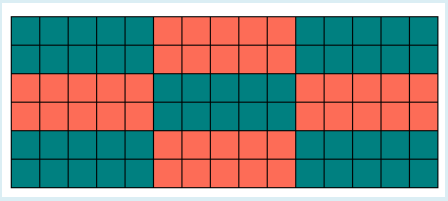
Divisibilidad





Edición 2024

Colección Hojamat.es

http://www.hojamat.es

BREVE ESQUEMA TEÓRICO

CONTENIDO

INTRODUCCIÓN

El tema de divisibilidad se trata aquí sobre el conjunto de 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 primeros. 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.

En algunos apartados se incluirá la traducción a hojas de cálculo de algunas operaciones. Podrá haber también referencias a algún lenguaje de programación, calculadora especializada o programa de Matemáticas.

DIVISIÓN ENTERA Y EXACTA

División entera

Dados dos números naturales **a** y **b**, llamaremos *división entera* (o *euclídea*) 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*.

En hojas de cálculo el cociente entero se representa como **ENTERO(A/B)** y el resto con la función **RESIDUO(A;B)**. En casi

todos los lenguajes de programación el cociente entero se representa también como **A\B**.

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. En Excel y Calc nos vale la función **RESIDUO**.

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.**

También podemos decir que en este caso la división exacta y la entera coinciden, o que el resto es 0. Esto se traduce en varias formas de expresar la relación múltiplo-divisor. Así, para expresar que **B** divide a **A** podemos usar, por ejemplo:

En hojas de cálculo: **RESIDUO(A;B)=0**, es decir, que el resto es igual a 0.

En algunos lenguajes: **a mod b = 0** o **mod(a,b)=0**

Otras: **A/B = A\B** (si lo admite la herramienta que se use)

A/B=INT(A/B) Expresa que A/B es un entero.

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** (Reflexiva)
- 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 **k|a** y **k|b** entonces **k|(a+b)** y **k|(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** (Transitiva)
- 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**.
- Si **a|b** y **b|a,** ambos positivos, entonces **a=b**

La relación de divisibilidad como orden parcial

La relación cumple las tres propiedades

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

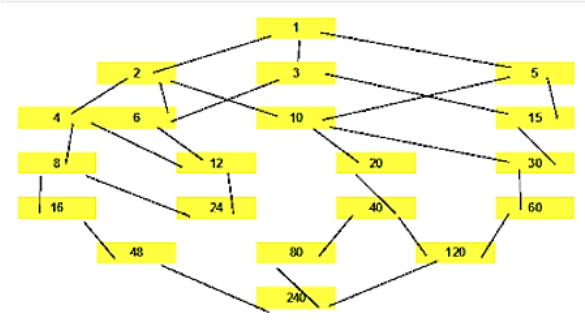
Por ellas es **una relación de orden**. Al existir elementos no comparables (7 no divide a 8, ni 8 divide a 7), este orden es **parcial**, por lo que los elementos se pueden ordenar mediante diagramas de árbol.

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 (reflexiva) y de la unidad.
- **0** 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** (transitiva).
- Si **a** es múltiplo de **b**, y **b** es múltiplo de **a** y ambos son positivos, entonces **a=b**

La relación de "ser múltiplo" representa el **orden parcial inverso** al de la relación de "ser divisor". Estas relaciones se pueden representar en forma de *retículo*, como el de la imagen



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 de 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.** Indirectamente se deduce que todo divisor de **a** y **b** también lo es del **MCD** de ambos.
- 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.

Cálculo del MCD con ordenador

En las hojas de cálculo usuales se usa la función M.C.D, que hay que escribirla bien, con los dos puntos intermedios y sin un punto al final. Solo sirve para dos números, por ejemplo:

M.C.D(842;964)=2

Si actúa sobre varios números, habrá que anidar. Por ejemplo, el M.C.D. de 832, 2024 y 3000 será:

M.C.D(832;M.C.D(2024;3000))=8

En lenguajes de programación como PARI se usan las iniciales en inglés ***gcd***, que también actúa sobre dos parámetros y necesita anidamiento para más de dos.

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, mutuamente primos 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.

Si una fracción a/b se simplifica hasta llegar a una reducida, el numerador y el denominador serán primos entre sí.

En lenguaje de ordenador bastará exigir que su MCD valga 1: *M.C.D(A;B)=1* (en Excel y Calc) o *gcd(a,b)==1* en PARI y lenguajes similares.

En Aritmética Modular, un número coprimo con el módulo *m* es una unidad o elemento inversible en el anillo Z/m.

Una propiedad interesante de un par de coprimos es que su MCM, que veremos más adelante, equivale a su producto.

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**

En las hojas de cálculo usuales se suele representar como M.C.M(a;b), y actúa sobre dos números, por lo que para trabajar con más, hay que anidar la función M.C.M, al igual que se procedió con el M.C.D. En el lenguaje PARI y afines se usa *lcm(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.

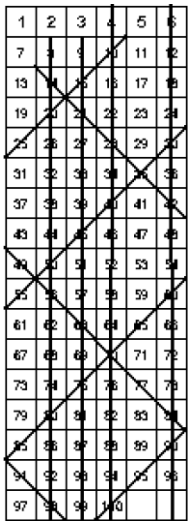
Riemann usó la función zeta x(s) = 1 + $1/2^s$ + $1/3^s$+ $1/4^s$ + $1/5^s$ … para lograr una gran aproximación entre p(x) y Li(x), aunque no llegó a demostrar su convergencia, cosa que lograron por separado los matematicos De la Vallée Pousin y Hadamard, al final del siglo XIX, y en el siguiente siglo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

Es el 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:

-Un número primo es suma de cuadrados de dos números naturales si y sólo si es de la forma 4n+1.

-El producto de dos números que son suma de cuadrados también es otra suma de cuadrados, en virtud de la identidad

$(a^2 + b^2)(c^2 + d^2) = (ac-bd)^2 + (ad+bc)^2$

-Por tanto el producto de potencias de números del tipo 4n+1 también equivale a una suma de cuadrados.

Si una suma de cuadrados se multiplica por otro cuadrado, resulta una nueva suma de cuadrados:

$(a^2 + b^2)c^2 = (ac)^2 + (bc)^2$

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.

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.

Llamaremos *semiprimos* a aquellos números que sólo poseen dos divisores primos, iguales o distintos. A los de tres divisores distintos se les suele llamar *esfénicos*. Los que poseen k factores primos se nombran en algunos textos como *k-casiprimos*, pero esta denominación es discutida.

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

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

Luego el número de divisores será

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

El conjunto de divisores se puede visualizar muy bien en una tabla de doble entrada creada en una hoja de cálculo, en la que tanto filas como columnas pueden contener productos del tipo $1+p+p^2+\dots p^k$:

	180=2^2*5*3^2					
	1	2	4	5	10	20
1	1	2	4	5	10	20
3	3	6	12	15	30	60
9	9	18	36	45	90	180

SD(N)=(1+2+4)(1+5)(1+3+9)=32*13=546
D(N)=(1+2)(1+1)(1+2)=18

En la imagen hemos construido con orden todos los divisores de 180, calculando su suma SD(N) y su número, D(N)

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 $n = p_1^{a1}.p_2^{a2}.p_3^{a3...}$ basta considerar que son los términos del producto

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

Esta operación equivale a formar todos los productos posibles del tipo $p_1^{b1}.p_2^{b2}.p_3^{b3...}$ 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

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

También se usan las funciones

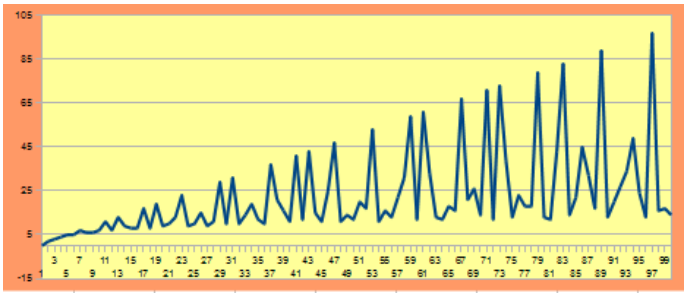
OMEGA: Cuenta los factores primos de un número sin tener en cuenta las multiplicidades. Así, omega(60)=3

BIGOMEGA: Cuenta los factores primos con multiplicidad, como biomega(60)=4.

SOPF: Suma los factores primos de un número sin contar multiplicidad. Por ejemplo Sopf(48)=2+3=5, porque sus divisores primos son 2 y 3, o sopf(60)=2+3+5=10

SOPFR: Idéntica a la anterior, pero contando multiplicidades. En los ejemplos anteriores, sopfr(48)=2+2+2+2+3=11 y sopfr(60)=2+2+3+5=12

Sopfr también recibe el nombre de **logaritmo entero** 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).

σ(N) (SUMA DE DIVISORES O FUNCIÓN SIGMA)

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

Si **n** es primo, σ(n)=n+1. Si es perfecto, σ(n)=2n. Si es un número primario p^e, la función σ(n) tiene como fórmula:

$$\sigma(n) = \sigma(p^e) = \frac{p^{e+1} - 1}{p - 1}$$

$\sigma(p^r)= (p^{r+1}-1)/(p-1)$ que nos permite evaluar la función σ(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 σ(a.b)=σ(a).σ(b). Diremos que esta función es multiplicativa

OTRAS FUNCIONES SIMILARES A SIGMA

USIGMA**:** Es la suma de todos los divisores unitarios 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.

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

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 e_i los exponentes de los factores primos 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**

PARTES CUADRADA Y LIBRE

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

Así, tendríamos, por ejemplo: $80=4^2*5$, $121=11^2*1$, $90=3^2*10$, $15=1^2*15$

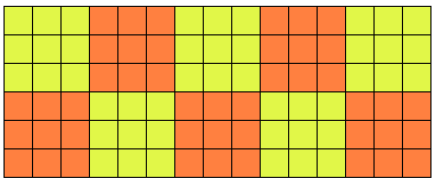
Podemos llamar parte cuadrada PC(N) a la primera y parte libre PL(N) a la segunda (se llama *core* en inglés y podemos traducir por “núcleo”) No se debe confundir con el *radical* de N, que es el mayor divisor de N que está libre de cuadrados.

Tendremos que:

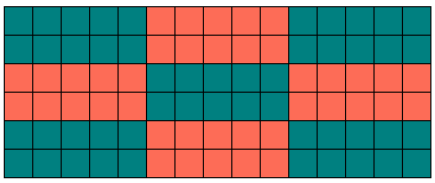
En un cuadrado perfecto PL(N)=1, en un número libre de cuadrados PC(N)=1 y en el resto de números ambos serán mayores que la unidad. En este caso los podemos llamar “cuadrables”, porque admiten su representación como un embaldosado de estructura cuadrada (las mismas filas que columnas), o bien como uno rectangular con baldosas cuadradas.

Así, el número $90=3^2*10$ es cuadrable, y admite estas dos estructuras:

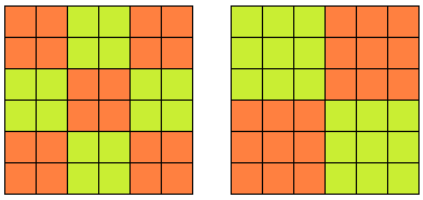
Rectangular con baldosas cuadradas



Mismo número de filas y columnas con baldosas rectangulares



Los cuadrados, como el 36, es evidente que admiten estructuras cuadradas con baldosas cuadradas, y tal vez de varias formas. Son totalmente cuadrables.



Por último, los libres de cuadrados solo admitirán estructuras rectangulares con baldosas también rectangulares. No son nada cuadrables.

Para encontrar la parte cuadrada basta seleccionar los factores primos que figuren con exponente par. La parte libre se calcularía

entonces dividiendo el número entre su parte cuadrada. Estará formada por factores primos elevados todos a la unidad.

Otras funciones

A la raíz cuadrada de PC(N) la llamaremos ***Raíz interna*** de N. Así, en el número 3500 PC(3500)=100, luego su raíz interna será 10. Es fácil ver que el número de divisores de la parte cuadrada coincide con el de la raíz interna.

Otra función que se puede definir en este contexto es **MMC(N),** Menor múltiplo cuadrado MMC(N), que, como indica su nombre, es el menor cuadrado divisible entre N. Para calcularlo, basta incrementar todos los exponentes de los factores primos hasta convertirlos todos en pares.

Llamaremos función **Q(N)** al resultado de contar los factores primos de la parte cuadrada. Así, por ejemplo, en el número $2520=2^3\times3^2\times5\times7$ tendríamos:

Q(2520)= 2, porque la parte cuadrada contiene dos primos distintos, el 2 y el 3.

De igual forma, definiremos como **P(N)** al resultado de contar los factores primos de la parte libre. Por ejemplo, P(140)=P(2^2*5*7)=2, porque la parte libre es 35=5*7, con dos primos distintos. En los cuadrados P(N)=0, porque su parte libre es 1.

Como los factores pueden pertenecer a ambas partes, libre y cuadrada, se tendrá que $P(N)+Q(N)\geq OMEGA(N)$.

RETÍCULOS EN EL CONJUNTO DE DIVISORES

El conjunto de divisores de un número natural N está ordenado parcialmente mediante la relación de orden a|b ("a divide a b") que es reflexiva, simétrica y transitiva, pero en la que dos elementos pueden no ser comparables: ni 6 divide a 13 ni 13 a 6. Por ello decimos que se trata de un orden parcial. En cualquier texto o página específica puedes leer más detalles.

Quizás sepas que el conjunto de los divisores de un número tiene estructura de retículo. Como aquí no estudiamos cuestiones de Álgebra, sólo daremos una noción de este concepto en su variante de orden (existe otra definición algebraica y ambas son equivalentes)

Definimos

Se dice que un conjunto ordenado **es filtrante superiormente** si para cada par de elementos a y b del mismo **existe al menos otro elemento del conjunto que es mayorante de ellos** (en nuestra relación de divisibilidad se traduciría como "múltiplo común"). Lo será **inferiormente** si existe un **minorante** de ambos (aquí sería un "divisor común").

El conjunto de los divisores de N está filtrado superior e inferiormente, y además, para cada par de elementos existe **un supremo**, que es el mayorante mínimo (el mínimo común múltiplo), que representaremos como $a \vee b$ y **un ínfimo** (el máximo común divisor), representado como $a \wedge b$. Por estas dos propiedades recibe el nombre de retículo. Sería semirretículo si sólo cumpliera una. Investiga en un tratado de Álgebra las propiedades de estas operaciones (conmutativa, asociativa, absorbente, idempotente…). Si sólo se garantiza la existencia de un supremo, el retículo se convertiría en un sup_semirretículo, y sub_semirretículo en el caso del ínfimo.

Un retículo puede ser acotado si existe **un máximo E que es mayorante de todos los demás elementos, y un mínimo Φ que**

es minorante de todos ellos. Es claro que en nuestro ejemplo N es el máximo E y 1 es el mínimo Φ. Se cumple que $N \wedge b=b$ y que $1 \vee b=b$. A los elementos que sólo tienen como minorante Φ (y distintos de él) les llamaremos átomos, y en nuestro caso son los factores primos de N. Por el contrario, si su único mayorante es E, reciben el nombre de coátomos.

Estos dos elementos E y Φ nos valen para la siguiente definición: un retículo acotado es complementado si para todo elemento a existe otro a', su complemento, tal que $a \vee a'=E$ y $\mathbf{a \wedge a'=\Phi}$. Aunque no nos extenderemos en esta dirección, el complemento no tiene que ser único.

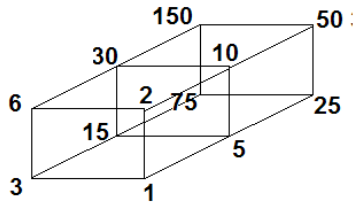
Puedes investigar cuándo un retículo se convierte en un álgebra de Boole. No trataremos esto.

El retículo de los divisores de N es complementado si y sólo si N es libre de cuadrados.

En efecto: Si N es libre de cuadrados, todos sus factores primos estarán elevados a la unidad, por lo que cada divisor a se caracterizará tan sólo por su colección de factores primos, y bastará tomar para a' el número formado por el producto de los primos que no son divisores de a, que cumplirá trivialmente lo exigido. Por ejemplo, entre los divisores de 210 (libre de cuadrados porque 210=2*3*5*7), el complemento de 35 es 14.

Por el contrario, si no es libre de cuadrados, un divisor p se presenta elevado a una potencia con exponente r mayor que 1. Busquemos el complemento q de p (sin elevar a r). En primer lugar deberá cumplir que $p \wedge q=\Phi$ o expresado mejor en este caso, p y q han de ser coprimos. Entonces q sólo podrá contener factores primos distintos de p. Pero al calcular $p \vee q$ el resultado no podrá coincidir con N, ya que el MCM(p, q) contendrá a p elevado a la unidad, mientras que N lo contiene elevado a $r>1$. Así que ningún candidato a complemento cumple las dos propiedades. Hemos encontrado un contraejemplo que invalida la propiedad.

Este carácter de retículo se suele expresar mediante un diagrama de Hasse, en el que cada dos elementos relacionados se unen mediante una línea, no teniendo en cuenta la propiedad reflexiva y aprovechando la transitiva para eliminar líneas. Aquí tienes el correspondiente a 150:



Se comprende que hay otras formas de ordenarlo y dibujarlo. Es un buen ejercicio identificar el carácter de un número según su diagrama de divisores (potencia de un primo, semiprimo, libre de cuadrados…)

NÚMEROS ESPECIALES

En este apartado se irán explicando algunas clases curiosas de números con propiedades relacionadas con la Divisibilidad, 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.

Por ejemplo, 28 coincide con la suma de sus divisores propios:

$28=14+7+4+2+1$

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 (12<1+2+3+4+6):

- Todos los números múltiplos de 6 mayores que 6 son abundantes. Intenta demostrarlo.
- El menor abundante impar es 945.
- 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 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 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.

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

En la imagen se presentan los primeros pares de números amigos.

NÚMEROS CASI AMIGOS

Los llamados números comprometidos o casi amigos son dos números m y n tales que 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.

Esta idea de divisores no triviales se recoge en la función de Chowla, que se puede definir como

CHOWLA(n)=SIGMA(n)-n-1.

Así que en estos números se cumple

CHOWLA(48)=75 y CHOWLA(75)=48

Es evidente que esta función tiene valor 0 si un número es primo. Esto confirma que estos números que estudiamos son todos compuestos.

Es trivial también que la función SIGMA coincide en ambos números m y n del par (en el ejemplo, 124) y que su valor es m+n+1. Este hecho se toma también como definición de números comprometidos.

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: 12496, 14288, 15472, 14536, 14264

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.

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 ALTAMENTE COMPUESTOS

Estos números fueron estudiados por Ramanujan, que ya tenía ideas sobre ellos antes de su colaboración con Hardy. Su definición es muy sencilla:

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, ... (http://oeis.org/A002182)

La sucesión contiene infinitos términos, porque si N es NAC, el número 2N tiene los mismos factores primos que N y uno más, luego al menos existe un número con más divisores que N y recorriendo N+1, N+2, N+3,…N+N=2N bastará quedarse con el primer número que presente un máximo de divisores respecto a los anteriores (puede ser el mismo 2N).

Podemos expresarlo mediante la función ***divisor*** o ***sigma***, que cuenta los divisores de un número. En los NAC esta función presenta un valor superior al de cualquier otro número entero menor que él.

Pero si recordamos que la expresión de la función divisor es

$$D(N) = (a_1 + 1)(a_2 + 1)(a_3 + 1) \dots (a_k + 1)$$

siendo a_i los exponentes en su descomposición en factores primos

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

comprenderemos que lo que debemos estudiar son los máximos de esta expresión, que sólo dependen de la signatura prima de N (esto es, el conjunto de los exponentes en la factorización. Esto es importante: si sustituimos uno de los números primos de la factorización por otro, el valor de la función divisor no se altera. Esta idea tan simple nos lleva a la primera propiedad de los NAC:

Todo número altamente compuesto tiene como factores primos los primeros de la lista, de forma consecutiva: 2, 3, 5, 7, 11, …

$$N = 2^{e_1}3^{e_2}5^{e_3}7^{e_4}\ldots$$

Es sencillo demostrarlo. Imagina que en su desarrollo no figuraran todos los primeros números primos. Por ejemplo, que figurara el 11 y no el 7. Entonces, si sustituyéramos el 11 por un 7, el valor de N disminuiría, pero el de su función *divisor*, tal como vimos en el párrafo anterior, se mantendría igual, lo que contradice lo afirmado de que N presenta más divisores que cualquier otro número menor.

Esto recuerda a los *primoriales*. Los tienes en

http://hojaynumeros.blogspot.com.es/2012/02/el-primorial.html

No sólo han de figurar los primeros primos, sino que sus exponentes deberán ser no crecientes si ordenamos las potencias mediante bases crecientes: $e_1 \geq e_2 \geq e_3 \geq e_4 \geq e_5 \geq \ldots$

También es fácil demostrarlo: si un par de exponentes se presentaran en orden inverso, intercambiando sus bases obtendríamos un número menor que N con sus mismos divisores, luego N no es NAC.

Por último, salvo en los casos de $N=4=2^2$ y $N=36=2^2*3^2$, el último de los exponentes debe ser 1. No he encontrado demostración de este hecho.

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

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.

PRIMOS DE SOPHIE GERMAIN

Son aquellos primos p en los que 2p+1 también es primo. A este último se le suele llamar "primo seguro".

Reciben este nombre porque Sophie Germain demostró el último teorema de Fermat para estos números. Con estos primos se pueden formar cadenas de Cunningham:

Cadenas de Cunningham

Este tipo de cadenas se construye de esta forma:

- 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 Cunningham de segunda especie) .
- Interrumpimos la recurrencia cuando el resultado no sea primo.

En el caso de primera especie, todos los elementos de una de estas cadenas serán primos de Sophie Germain salvo el último y todos serán primos seguros salvo el primero.

Por ejemplo, la cadena de primera especie creada a partir del 5 es (5, 11, 23, 47), porque los tres primeros son primos de Sophie Germain, pero el 47, aunque primo, no es de este tipo, ya que 2*47+1=95, que es compuesto.

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)

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...

NÚMEROS DE KEMPNER

La función de Smarandache se define, para un número natural **n**, como el menor entero tal que su factorial es divisible entre **n**. La designaremos como S(n). Por ejemplo, para n=12, el menor valor de **k** tal que **k!** sea divisible entre 12 es el 4, ya que 4!=24 es el menor factorial divisible entre 12. Lo expresaremos como S(12)=4. Es fácil entender que S(6)=3 o que S(7)=7.

Esta función fue estudiada por Lucas y Kempner antes de que Smarandache le asignara su propio nombre. Por eso, la sucesión de sus valores recibe el nombre de “números de Kempner”, y es esta:

1, 2, 3, 4, 5, 3, 7, 4, 6, 5, 11, 4, 13, 7, 5, 6, 17, 6, 19, 5, 7, 11, 23, 4, 10, 13, 9, 7, 29, 5, 31, 8, 11,… (http://oeis.org/A002034)

NÚMEROS ARITMÉTICOS Y AFINES

Los números aritméticos son aquellos en los que el promedio de sus divisores positivos es un número entero. Expresado de otra forma, aquellos en los que su función TAU (número de divisores) divide a su función SIGMA (suma de divisores).

Por ejemplo, 14 es aritmético, porque la suma de sus divisores es 1+2+7+14=24, y, por tanto, el promedio de ellos es 24/4=6, un número entero.

Los primeros son:

1, 3, 5, 6, 7, 11, 13, 14, 15, 17, 19, 20, 21, 22, 23, 27, 29, 30, 31, 33, 35, 37, 38, 39, 41, 42, 43, 44, 45, 46, 47, 49, 51, 53, 54, 55, 56, 57, 59, 60,…

Al ser SIGMA y TAU funciones multiplicativas, ocurrirá que si dos aritméticos son primos entre sí, su producto también será aritmético. Por ejemplo, 3 y 19, presentan un producto, 57, que es también aritmético. Llamaremos *números aritméticos primitivos* a los que no sean producto de otros.

Todos los números primos **p** mayores que 2 son aritméticos, ya que son impares, su función Sigma(p) equivale a 1+p, par, y su función Tau(p) es 2, luego su cociente es entero. También, todo número libre de cuadrados impar ha de ser aritmético.
Existen muchos números aritméticos que no son libres de cuadrados, como, por ejemplo, 20, 27, 44, 45, y 49.

Aritméticos con promedio primo

Podemos exigir que el promedio de los divisores no sólo sea entero, sino también primo. Los primeros aritméticos que cumplen esto son:

3, 5, 6, 13, 20, 37, 45, 49, 61, 73, 150, 157, 169, 193, 277, 313, 361, 397,…(https://oeis.org/A048968)

Por ejemplo, los divisores de 45 son 45, 15, 9, 5, 3 y 1. Su suma es 78, su número, 6, y dividiendo: 78/6=13, que es un número primo.

Si el número es un primo **p**, deberá ser también primo **(p+1)/2**, que es el cociente entre SIGMA(P) Y TAU(p). Esta situación recuerda a los primos de Sophie Germain, pero en ellos es primo (q-1)/2, siendo q el asociado de p.

Números de Ore

Si en lugar de estudiar la media aritmética de divisores usamos la armónica, obtendremos los 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.

Aritméticos unitarios

Un número natural **d** es un divisor unitario de otro número natural **N** cuando **d** y **N/d** son coprimos. Por ejemplo, 33 es divisor unitario de 66, ya que 33 es coprimo con 66/33=2. Es evidente que N/d también es unitario. **Los divisores unitarios aparecen por parejas.**

Su suma se llama USIGMA, y podemos buscar con ella el promedio de los divisores unitarios. Si ese promedio es entero, diremos que el número es aritmético unitario.

Damos un ejemplo:

Los divisores unitarios de 84 son 1, 3, 4, 7, 12, 21, 28 y 84 (los pares de unitarios son 1*84, 3*28, 4*21 y 7*12), en total $8=2^3$. Y su suma es 160. Dividimos: 160/8=20, que es entero, luego 84 es aritmético unitario.

Los primeros aritméticos unitarios son: 1, 3, 5, 6, 7, 9, 11, 12, 13, 14, 15, 17, 19, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 33, 35, 37, 38, 39, 41, 42, 43, 44, 45, 46,,,,(https://oeis.org/A103826)

LOS 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,…y están publicados en https://oeis.org/A024675.

Basta estudiar la lista para darse cuenta de que hay entre ellos cuadrados (A075190), como 81 y 144, pares (A072568) e impares (A072569), triangulares (A130178), como el 6 y el 15, semiprimos (A078443), como el 21, y muchos más tipos. Sólo los que son potencias ocupan muchas páginas de OEIS (A075190, A075191, A075192, A075228, A075229,…)

Visita la página http://oeis.org/wiki/Interprimes y te abrumará la cantidad de variantes que presentan los interprimos.

"PALPRIMOS" (PRIMOS PALINDRÓMICOS)

Tomamos la palabra *palprimo* directamente del inglés, pero si te apetece, nómbralos como *primos palindrómicos*.

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.

Los números de una sola cifra se suelen considerar palindrómicos (en realidad, cumplen la definición), por lo que es fácil entender que los primeros *palprimos* son

2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919, 929, 10301, 10501, 10601, 11311, 11411, 12421, 12721,…(https://oeis.org/A002385)

NÚMEROS 3-FRIABLES

Son los números que sólo poseen como factores primos el 2 y el 3. De nuevo nos inspiramos en una sucesión de OEIS. Esta vez en la A003586 (http://oeis.org/A003586), que presenta los que llama “3-smooth numbers”, que se puede traducir como “liso o alisado (o regular) de grado 3”. En francés se les denomina 3-friables, y en nuestro idioma “friable” equivale a “fácilmente desmenuzable”. Si alguien conoce otra denominación española puede comunicármelo. Mientras tanto, utilizaré una denominación similar a la francesa. Hendrik Lenstra les llama *armónicos*, en recuerdo de un texto de Phillipe de Vitry, obispo de Meaux, compositor del siglo XIV.

Me quedaré con la nomenclatura francesa: Un número es B-friable si todos sus factores primos son menores o iguales a B. En nuestro caso los números que estudiaremos son 3-friables.

Simplemente son números cuyos únicos factores primos son el 2 o el 3 (o ambos), es decir, que tienen la forma N=2^i*3^j con i,j≥0.

Los primeros son estos:

1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 32, 36, 48, 54, 64, 72, 81, 96, 108, 128, 144, 162, 192, 216, 243, 256, 288, 324, 384, 432, 486,…

Es fácil ver que desde el 1=2^0*3^0 hasta el final, todos tienen como únicos factores primos el 2 y/o el 3.

Existe una prueba muy sencilla para averiguar si un número es de este tipo. Consiste en dividir entre 2 y entre 3 mientras sea posible, es decir, mientras el número y los cocientes sucesivos sean múltiplos de uno de los dos. Si al final del proceso nos queda un 1, es que los únicos factores son 2 y 3, como se pide.

NÚMEROS DE POLIGNAC

Estos números se definen a partir de la conjetura de Polignac, que pronto se descubrió que era falsa. Afirma que todo número impar es suma de un primo y de una potencia de 2. Números tan pequeños como 127 no la cumplen, por lo que duró poco como conjetura.

Llamaremos número de Polignac a aquel número impar que no cumpla la conjetura explicada, que no pueda expresarse como $p+2^x$. Se supone implícitamente que x puede valer 0, porque en ningún listado se toma el 3 como número de Polignac, ya que $3=2+2^0$

Son números de Polignac el 1 y el ya citado 127.

Los primeros números de Polignac son 1, 127, 149, 251, 331, 337, 373, 509, 599, 701, 757, 809, 877, 905, 907, 959, 977, 997, 1019, 1087,…

NÚMEROS DE FORTUNE

A estos números se les suele llamar afortunados, pero esa denominación puede confundirse con otras parecidas, como “números felices” o “de la suerte”. Por ello los nombraremos según el primer matemático que los estudió, que fue Reo Franklin 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*3*5+1 (número de Euclides) y su diferencia con 2*3*5=30 (primorial) es 7, que es primo.

Los resultados de esta operación los tienes en

http://oeis.org/A007672

1, 1, 2, 6, 24, 1, 720, 3, 80, 12, 3628800, 2, 479001600, 360, 8, 45, 20922789888000, 40, 6402373705728000, 6, 240, 1814400, 112400072777607680000, 1, 145152, 239500800, 13440, 180, 30488834461171386050150400000000…

NÚMEROS DUFFINIANOS

Estos números, 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 σ(N).

Por ejemplo, es duffiniano el 111, que es compuesto, ya que 111=3*37, y la suma de sus divisores es σ(111)=111+37+3+1=152, cuya descomposición factorial es 2^3*19. Los factores primos de 111 son 3 y 37, mientras que los de la suma de sus divisores son 2 y 19, luego son primos entre sí y 111 es duffiniano.

Se excluyen los primos porque cumplen la condición de forma trivial: si p es primo, σ(p)=1+p, y dos números consecutivos siempre son primos entre sí (intenta calcularles el M.C.D.).

Los primeros son

4, 8, 9, 16, 21, 25, 27, 32, 35, 36, 39, 49, 50, 55, 57, 63, 64, 65, 75, 77, 81, 85, 93, 98, 100, 111, 115, 119, 121, 125, 128, 129, 133, 143, 144, 155, 161, 169, 171,

NÚMEROS INTOCABLES

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. Por ejemplo, el 88 no coincide con el resultado de sumar los divisores propios de ningún número natural. Si efectuamos un barrido de los N primeros números y anotamos el resultado de esa suma, ningún resultado coincidirá con 88.

Los primeros números intocables son 2, 5, 52, 88, 96, 120, 124, 146, 162, 188, 206, 210, 216, 238, 246, 248, 262, 268, 276, 288,…

NÚMEROS ADMIRABLES

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 sus divisores propios suman de esta forma:

652=325+130+65+50+26+25+13+10+5+2+1

La diferencia entre 650 y la suma de los divisores propios es 2, luego bastará cambiar de signo al 1:

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

NÚMEROS DE ZUMKELLER

Son un subconjunto de los anteriores. En ellos los divisores se pueden clasificar en dos conjuntos de la misma suma. Por ejemplo:

El número 25122 posee los siguientes divisores:

1+2+3+6+53+79+106+158+159+237+318+474+4187+8374+12561 +25122 = 51840

Esta suma de 51840 se puede repartir entre dos particiones de los divisores, de forma que sus sumas sean iguales. Serían estas:

1+2+3+53+79+106+158+159+237+4187+8374+12561 = 25920

6+318+474+25122 = 25920

Le daremos a 25122 el título de número de Zumkeller. No es una condición difícil de cumplir, y la prueba es que estos números aparecen entre los naturales con frecuencias altas. Estos son los primeros:

6, 12, 20, 24, 28, 30, 40, 42, 48, 54, 56, 60, 66, 70, 78, 80, 84, 88, 90, 96, 102, 104, 108,…

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 estos. 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:

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

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.

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)** (Teorema de los números primos).

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.

Por ejemplo, D(25)=4 porque el siguiente primo es 29, y 29-25=4

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.

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 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

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

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.

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

La conjetura de Legendre es equivalente a la afirmación de que entre dos números consecutivos n y n+1 siempre existe un número que es la raíz cuadrada de un número primo.

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

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

Hardy y Littlewood supusieron que la conjetura era verdadera, y aproximaron el número de tales primos menores que n, P(n), asintóticamente a

$$P(n) = C\frac{\sqrt{n}}{\ln(n)}$$

Con C una constante adecuada.

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

Dentro de esta conjetura, y para k=2 se incluye la de los primos gemelos:

Existen infinitos pares de primos gemelos (p, p+2)

Primos de Fibonacci

Existen infinitos números de Fibonacci que son primos.

Así que si construimos la sucesión de Fibonacci y elegimos los términos que sean primos, encontraremos uno de ellos que sea mayor que cualquier otro entero que imaginemos.

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).

CONJETURA DE SCHINZEL

Se puede afinar más la conjetura de Opperman. Schinzel conjeturó que *para x>8, existe al menos un número primo entre x y x+(lnx)^2.*

CONJETURA DE RASSIAS

Esta conjetura recibe el nombre de su autor, M. Th. Rassias, que la enunció siendo muy joven, mientras preparaba una Olimpiada Matemática. Se puede formular de varias formas, pero la que preferimos es la siguiente:

Para cada número primo p>2 existen dos primos p1 y p2, con p1<p2 tales que

(p-1)p1=p2+1

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

Para el número 17, el par de primos puede ser 2 y 31, porque (17-1)*2=32=31+1. Para el primo 47 los primos pueden ser 3 y 137, porque (47-1)*3=138=137+1

La conjetura afirma que siempre se pueden encontrar esos dos primos para uno dado.

CONJETURA DE COLLATZ

Para quienes no conozcan esta conjetura recordaremos su planteamiento:

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 le suma 1.

En el caso del 13, como es impar, se le aplicará la segunda, y quedará 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 COLL(40)=20 (por ser par), COLL(20)=10, COLL(10)=5, COLL(5)=3*5+1=16, COLL(16)=8, COLL(8)=4, COLL(4)=2, 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.

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?