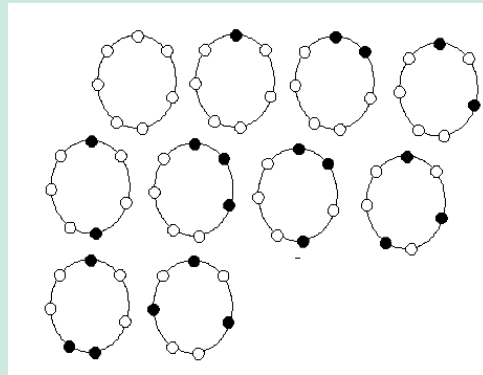
Temas de Matemáticas discretas básicas



Edición 2026

PRESENTACIÓN

Esta publicación unifica las cuatro sobre teoría incluidas en la página web *hojamat.es*:

Aritmética,
Divisibilidad,
Congruencias,
Combinatoria.

Cuando se creó esa página, la velocidad de Internet no era muy alta, y el formato PDF aún no estaba tan al alcance de un usario medio como ahora. Por eso era conveniente manejar archivos que no tuvieran un tamaño grande. Ahora, que han cambiado las circunstancias, parece interesante poder disponer de todos los contenidos de Matemática Discreta en una sola publicación.

En esta edición se han añadido temas nuevos y eliminado o reducido otros que carecían de interés.

CONTENIDO

ARITMÉTICA

En este capítulo trataremos de los números naturales. Los definiremos mediante los axiomas de Peano, para evitar recurrir a la teoría de conjuntos. Tradicionalmente se comenzó su definición a partir del 1, y así los copiaremos. Modernamente se tiende a incluir el cero, con lo que se tendría que cambiar el axioma 1. Los dejaremos así, y cuando se tenga que considerar el cero se advertirá. Se suelen representar como N si se incluye el 0 y como N× si no se incluye. La inclusión del cero es un tema de permanente discusión.

Se han incluido temes generales que no pertenecen a otros capítulos, como

Fundamentos

Sucesiones

Números poligonales y piramidales

Cuestiones diofánticas

Curiosidades

FUNDAMENTOS

AXIOMAS DE PEANO

Existe un conjunto N compuesto por elementos llamados *números naturales*, relacionados entre sí por la relación "ser siguiente o sucesor" **m= sg(n)** que cumple estos cinco axiomas.

1. **1** es un número natural.

2. Si **a** es un número natural, entonces **sg(a)** también es un número natural

3. 1 no es siguiente de ningún número natural. (El 1 es el primero, no tiene precedentes)

4. De la igualdad **sg(a)=sg(b)** se deduce que **a=b** (Dos números diferentes no pueden tener el mismo siguiente)

5. Axioma de inducción: si un conjunto C de números naturales contiene al 1 y a los siguientes de cada uno de sus elementos entonces C=N (es decir, pertenecerían a él todos los números naturales)

Estos axiomas cumplen la compatibilidad, independencia y completitud. También garantizan que N es un conjunto infinito. Se suelen representar como

puntos equidistantes en una recta, a partir (generalmente hacia la derecha) de un punto origen, que representa el 0 o el 1.

También garantizan que entre un número natural y su siguiente no existe otro número intermedio.

OPERACIONES CON NÚMEROS NATURALES

Operaciones básicas

A partir de los axiomas de Peano se define la suma de dos números naturales **a+b** mediante las definiciones

a+1 = sg(a) y **a+sg(b) = sg(a+b)**.

A partir de esta definición se demuestra que es una operación interna con las propiedades

Asociativa: a+(b+c) = (a+b)+c
Conmutativa: a+b=b+a
Cancelativa: Si a+c = b+c, entonces a=b

La propiedad asociativa permite definir sumas de más de dos números de forma unívoca.

Esta última propiedad permite definir *la resta*, como **a-b=x** si y solo si **b+x=a**. Esta operación no es cerrada,

porque si **a** es menor que **b**, no se pueden restar. Hay quien no la considera operación en sentido estricto.

La multiplicación de dos números naturales se define a partir de: **a×1 = a** y **a×sg(b) = a×b+a.** De esta definición se puede deducir la clásica de que la multiplicación es una suma de un elemento sumado consigo mismo **n** veces.

Esta operación posee las propiedades

Asociativa: a×(b×c) = (a×b)×c
Conmutativa: a×b = b×a
Elemento neutro: a×1 = 1×a = a
Distributiva respecto a la suma: a×(b+c) = a×b + a×c
Cancelativa: Si a×c = b×c y c>0, entonces a = b

Aquí también la propiedad asociativa permite definir productos de más de dos números de forma unívoca.

Estas propiedades dotan al conjunto N de la estructura algebraica de *anillo conmutativo con unidad*.

La propiedad cancelativa permite definir la división exacta como **a/b = x** con **b>0** si y solo si **b×x=a**. Esta operación tampoco es cerrada. Si un número admite la división entre 2 se llama *par*, y en caso contrario, *impar*.

Se define también la división entera como la operación, para dos números naturales **a** y **b**, que encuentra un cociente **q** y un resto **r<b** tales que **a=b×q+r**. Se puede

demostrar que esta operación siempre es posible. Existe también la *división por exceso*, definida como a=b×(q+1)-r', donde r' es el *resto por exceso*, y se cumple que r +r' = b.

Operaciones derivadas

Potenciación

De la operación de multiplicar derivamos la *potenciación*:

La potencia de *exponente* k de un número natural (*base*) es el resultado de multiplicar por sí misma la base **a** tantas veces como indique el exponente k:

$$a^k = a \times a \times a \times a \ldots \times a \ (k \ veces)$$

Propiedades:

Destacamos:

Es $a^0=1$ y $a^1=a$ por definición
Potencias de la misma base: $a^m \times a^n = a^{m+n}$
Potencias del mismo exponente: $a^m \times b^m = (a \times b)^m$
Potencia de una potencia: $(a^m)^n = a^{m \times n}$

Radicación

Diremos que **b** es la raíz **k-ésima** de **a** si **b** elevado al exponente **k** da como resultado **a**.

$$\sqrt[k]{a} = b \; equivale \; a \; que \; b^k = a$$

No siempre es posible esta operación ni es cerrada en el conjunto de los números naturales. Cuando lo es, al número **a** se le da el título de *potencia perfecta*. En caso contrario, se puede acudir a la **raíz entera** de a, que es un número r tal que

$$r^k < a < (r+1)^k$$

Según esto, el resto de esta operación no puede llegar a 2r+1.

Jerarquía de operaciones

Cuando se combinan varias operaciones en un mismo cálculo, se deberán resolver en primer lugar las de mayor orden jerárquico, según estos principios:

- Se comienza calculando las operaciones encerradas entre paréntesis.
- Después, potencias y raíces
- A continuación, multiplicaciones y divisiones
- Finalmente, sumas y restas.

Aunque las distintas medias o promedios suelen darse más en números racionales y reales, como intervienen en algunas propiedades y curiosidades sobre números enteros, se incluyen aquí:

Media aritmética

La media aritmética de un conjunto de números a_1, a_2, a_3, a_4,…a_k es el cociente entre su suma y el número de elementos:

$$\bar{a} = \frac{a_{1+}a_{2+}a_{3+\cdots+}a_k}{k}$$

Aquí nos interesarán tan solo los conjuntos con media aritmética entera. Por ejemplo, dos números con media entera han de ser ambos pares o impares.

Media geométrica

Es mucho menos usada que la anterior entre números naturales. La incluimos solo para completar. Es la raíz de orden k del producto de k números enteros:

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

Si la media geométrica de dos números es entera, se pueden visualizar como las dimensiones de un rectángulo de lados enteros que se puede transformar en un cuadrado con su lado también entero.

Media armónica

Es la inversa de la media aritmética de los inversos. Como la anterior, solo tiene utilidad aquí si es entera.

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

Media contraarmónica

En el caso de dos números naturales a y b, al cociente $(a^2+b^2)/(a+b)$ se le suele llamar *media contraarmónica* de a y b

Esta media y la media armónica son equidistantes de la media aritmética, siendo la armónica la de menor valor:

$$\frac{a^2 + b^2}{a + b} \geq \frac{a + b}{2} \geq \frac{2ab}{a + b}$$

Si se resta cada una de la anterior esa diferencia equivale a

$$\frac{(a-b)^2}{2(a+b)}$$

Se puede repasar con un ejemplo, a=30, b=20. Los valores de estas medias serían:

Contraarmónica: $(30^2+20^2)/(30+20)=26$ (hemos elegido el ejemplo con valor entero)
Aritmética: (30+20)/2=25
Armónica: 2×20×30/(20+30)=24

Hemos comprobado que los tres valores son equidistantes.

ORDEN EN N

Dados dos números naturales **a** y **b**, diremos que **a** es menor que **b** si existe otro número natural **x** tal que **a+x=b**

Igualmente, diremos que **a** es menor o igual que **b** si **a** es o bien menor o bien igual que b (en modo texto lo representamos como **a<=b**)

Esta relación es de orden, porque presenta las propiedades

Reflexiva: a<=a para cualquier a natural
Antisimétrica: Si a<=b y b<=a , entonces a=b
Transitiva: Si a<=b y b<=c, entonces a<=c

Este orden *es total*, porque dados dos números naturales **a** y **b**, se cumple siempre o que **a<=b** o que **b<=a** (Ley de tricotomía: se cumple siempre que a<b o a>b o a=b)

El orden establecido por la relación <= posee la propiedad monótona respecto a la suma y el producto: Si **a<=b**, entonces **a+c<=b+c** y **a×c<=b×c**

Igualmente, el conjunto N está *bien ordenado* para la relación <=, porque todo subconjunto de N no vacío posee un elemento mínimo.

El conjunto de los números naturales no tiene máximo para este orden, por ser infinito. Esto permite representar N en una recta numérica, situando los naturales a intervalos iguales en longitud.

SISTEMAS DE NUMERACIÓN

Los números naturales, por su infinitud, necesitan un sistema de representación a partir de un número finito de símbolos. Para eso se inventaron los sistemas de numeración, como el romano, el decimal, etc.

Sistemas posicionales

Un sistema de numeración basado en la *posición relativa* usa la llamada *base* del sistema, que es el *número de unidades de orden inferior necesarias para obtener una unidad de orden inmediato superior*. A estos órdenes les llamamos *unidades*, *decenas*, *centenas*,…De esta forma, existirán tantos sistemas de numeración como bases distintas sean posibles, es decir, infinitas. Los más populares son los de bases 10 (decimal), 2 (binario), 8 (octal) y 16 (hexagesimal). La expresión de un número en una base se termina con un paréntesis y la base: $111010_{(2}$, $66523_{(8}$

La base de la expresión de un número N en una base B es lograr el desarrollo polinómico

$N = C_0B^k + C_1B^{k-1} +\ldots+ C_{k-1}\times B + C_k$ en el que los coeficientes C_i sean todos más pequeños que la base, positivos o nulos.

Según esto, el verdadero valor de C_0 es C_0B^k, el de C_1 será C_1B^{k-1} y así con todas. Por eso se llama sistema posicional. Además, así se cumple que cada unidad es B veces mayor que la anterior, porque son potencias todas de B.

Para poder usar los sistemas de numeración hay que admitir el número 0, como representante de un lugar vacío en la expresión de un número.

En un sistema de numeración en base B se necesitan B símbolos para las distintas cifras, pues son el cero y todos los posibles restos menores que B, así {0,1} para el binario, {0,1,2} para la base 3…Si la Base es mayor que 10 se añaden letras mayúsculas A, B, C, D…como cifras. Si no bastan las letras, se pueden usar números de varias cifras bien separados. Por ejemplo, 7722 se expresaría así en base 81: 1, 14, 27 (81, que equivale a la igualdad 7722=1×81^2+14×81^1+27×81^0

La expresión de un número N en un sistema de base B se logra por el método de las divisiones sucesivas:

- Mientras N sea mayor que la base B
  - Dividir de forma entera N entre B
  - El resto se toma como nueva cifra a la derecha
  - El cociente como nuevo valor de N
- Cuando N llegue a ser menor que B, él será la primera cifra de la expresión.

Por ejemplo, para expresar 2013 en base 7: 2013\7=287 y resto **4**; 287/7=41 y resto **0**; 41/7=5 y resto **6**. Como primera cifra tomamos el último cociente **5**, luego la expresión sería: 2013(10 = 5604(7

Efectivamente, así se cumple el desarrollo polinómico $2013=5\times7^3+6\times7^2+0\times7+4$, como se puede comprobar con facilidad.

La operación inversa, de pasar de una expresión en una base a la expresión decimal usual se hará cambiando la división por multiplicación y los restos por sumas:

Para pasar 45541(6 a base diez: 4×6+5=29; 29×6+5=179; 179×6+4=1078; 1078×6+1=6469

Sistemas no posicionales

Los sistemas de numeración aditiva son aquellos en los que los valores de los símbolos se suman, sin que influya la posición relativa, como el sistema romano.

Números especiales según sus cifras

Llamamos ***reverso*** o ***simétrico*** de un número natural a otro número que contiene las mismas cifras pero en orden opuesto, en una base dada. Si no indicamos lo contrario, nos referiremos a la base decimal. Por ejemplo, 345 es el simétrico de 543.

Número palindrómico o capicúa es aquel que es igual a su reverso. Los números de una sola cifra se consideran palindrómicos. Por ejemplo, el número 238832 es capicúa.

Número pandigital es aquel que contiene en su expresión decimal las diez cifras 0123456789 en cualquier orden. A veces no se exige que entre el 0, y

hay quien admite que se repita alguna cifra. Es pandigital 3672510984.

Repituno, **repunit** o **repuno** es el número que sólo contiene la cifra 1, como 11 o 111. **Repidígito** es aquel en el que todas sus cifras son iguales, como el 7777. Se le puede llamar también *monocifra*.

Equilibrado se le llama al número que contiene todas sus cifras con la misma frecuencia en una expresión respecto a una base dada. En esta categoría entran los que tienen todas sus cifras distintas. Por ejemplo, el número 5722 es equilibrado al menos en tres bases: 5722(10 =21211221(3 = 1A67(15 = 165A(16

Ondulado es el número cuyas cifras siguen la pauta ababab…en una base dada, como 23232 en base 10.

Periódico en sus cifras sería, por ejemplo, 283228322832.

Automórfico es aquel número que al elevarlo al cuadrado, está contenido en las últimas cifras del mismo. Por ejemplo, el 9376, que al elevarlo al cuadrado se convierte en 8790**9376**

Anagramáticos son dos números que poseen las mismas cifras con igual frecuencia y distinto orden. Por ejemplo, 27761 y 17672.

Se llaman así los procesos por los que reiteramos una misma operación sobre las cifras de un número hasta llegar a un punto de no avance de resultados. Podemos considerar:

Persistencia aditiva

Consiste en ir sumando las cifras de un número de forma reiterada hasta llegar a un número de una cifra, a partir del cual se estabiliza el proceso. Por ejemplo, el proceso con el número 6512 consistiría en

6+5+1+2=14; 1+4=5, 5=5

El número en el que se detiene la reiteración se llama *raíz digital*, en este caso, el 5. El número de iteraciones que son necesarias para obtener esa raíz recibe el nombre de *índice de persistencia aditiva*, que en el ejemplo es 2.

Persistencia multiplicativa

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

Se multiplican las cifras del número y se reitera esta operación con los números obtenidos. Estos productos formarán una sucesión decreciente, y se cuentan las iteraciones necesarias hasta llegar a un producto de una

sola cifra. Al número de esos pasos se le denomina *índice de persistencia multiplicativa*, y al número final resultante, *raíz digital multiplicativa* del número.

Por ejemplo, iniciamos con el número 762. El producto de sus cifras es 84. Multiplicamos cifras de nuevo, resultando 32, y reiteramos:
762 – 84 – 32 – 6.
Se puede razonar que los productos serán decrecientes hasta llegar a una cifra.

Los procesos de persistencias son invariantes al orden de las cifras, y el caso aditivo, al número de cifras 0 existentes en el número, mientras que en el multiplicativo, al número de cifras 1.

POTENCIA DE UN NÚMERO NATURAL

Llamaremos potencia de *exponente* **k** de un número natural **n**, y la representaremos por $\mathbf{n^k}$, al producto **n.n.n….n** de k factores iguales a n, al que llamaremos *base*. Se añaden las definiciones $n^0=1$ y $n^1=n$, en las que no existe producto.

Propiedades:

- $n^0=1$
- $n^1=n$

- $n^k.n^h=n^{k+h}$
- $n^k.m^k=(nm)^k$
- $n^k/n^h=n^{k-h}$ (k>=h)
- $n^k/m^k=(n/m)^k$
- $(n^k)^h = n^{kh}$

Dado un exponente k, llamaremos *raíz exacta* de índice **k** de un número **n** a otro número natural **r** tal que $\mathbf{r^k=n}$. Si esta operación es posible, calificaremos a **n** como *potencia perfecta*. Si no lo es, llamaremos raiz entera **q** de índice k a un número tal que

$$q^k < n < (q+1)^k$$

En este caso, llamaremos *resto* a la diferencia $\mathbf{n-q^k}$**.**

PRINCIPIO DE INDUCCIÓN COMPLETA

Es el método de demostración de propiedades referentes a números naturales consistente en:

a. Demostrar la propiedad para **n=1** (o el cero).

b. Demostrar que si la propiedad es cierta para **n**, también lo es siempre para **n+1** (es decir, **sg(n)**)

Con esto quedará demostrado que es cierto para todo n natural, en virtud del quinto axioma de Peano.

Con esta y otras técnicas, se demuestran fórmulas muy interesantes sobre sumas de los primeros números naturales de cierto tipo. Por ejemplo:

Suma de los primeros números naturales

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Suma de los primeros impares

$$1 + 3 + 5 + \cdots (2n + 1) = n^2$$

Suma de los primeros pares

$$2 + 4 + 6 + 8 + \cdots + 2n = n(n + 1)$$

Suma de los primeros cuadrados

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Suma de los primeros cubos

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$

Identidad de Nicómaco

$$(1 + 2 + 3 + \cdots + n)^2 = 1^3 + 2^3 + 3^3 + \cdots + n^3$$

FÓRMULA DE FAULHABER

Una alternativa a la inducción completa en las sumas anteriores es el uso de la fórmula de Faulhaber

(https://es.wikipedia.org/wiki/F%C3%B3rmula_de_Faulhaber),

que da el resultado de cualquier suma de potencias de los primeros números enteros. Solo incluimos su resultado para las primeras potencias, copiado de Wikipedia.

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}=\frac{n^2+n}{2}$$

$$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}=\frac{2n^3+3n^2+n}{6}$$

$$1^3+2^3+3^3+\cdots+n^3=\left(\frac{n^2+n}{2}\right)^2=\frac{n^4+2n^3+n^2}{4}$$

$$1^4+2^4+3^4+\cdots+n^4=\frac{6n^5+15n^4+10n^3-n}{30}$$

$$1^5+2^5+3^5+\cdots+n^5=\frac{2n^6+6n^5+5n^4-n^2}{12}$$

$$1^6+2^6+3^6+\cdots+n^6=\frac{6n^7+21n^6+21n^5-7n^3+n}{42}$$

FACTORIALES

Llamamos factorial de un número N al producto N(N-1)(N-2)(N-3)…1 si N>0 y la unidad si N=0. Lo representamos por n!, notación incómoda para la computación, por lo que es preferible FACT(N), que es la usada en Excel.

Los primeros factoriales serán, pues, contando 0!, 1, 1, 2, 6, 24, 120, 720, 5040,…

Su significado más importante es que coincide con las formas de ordenar los elementos de un conjunto de N de ellos (permutaciones), por lo que lo encontraremos en muchas fórmulas de Combinatoria.

Es evidente su definición por recurrencia: $N!=N\times(N-1)!$ Si N>0 y 0!=1

Es claro que la sucesión de factoriales es estrictamente creciente y que si m<n, m! divide a n!.

Doble factorial

Si en el producto del factorial sustituimos los factores consecutivos por otros descendientes de 2 en 2, obtendremos el doble factorial N!!, que se definirá como N(N-2)(N-4)…hasta finalizar en 1 o en 2.

Su fórmula de recurrencia será $N!!=N\times(N-2)!!$ Si N>0 y 0!!=1

Los primeros son:

1, 1, 2, 3, 8, 15, 48, 105, 384, 945, 3840, …En otro capítulo se estudiará el *primorial*, similar al factorial, pero formado como producto de los primeros primos.

CUADRADO MÁGICO

Un cuadrado mágico es una matriz cuadrada de números (normalmente consecutivos y a partir de 1) en la que las sumas por filas, columnas y diagonales son todas iguales. Esta suma, si los números son 1,2,...n, deberá ser igual a $n(n^2+1)/2$

Es famoso el cuadro Lo-Chu, formado por los números 1 al 9 dispuestos en tres filas y tres columnas y cuyas sumas son siempre 15

4	9	2
3	5	7
8	1	6

Este cuadrado mágico posee muchas propiedades curiosas. Algunas de ellas son:

42+92+22 = 82+12+62
42+32+82 = 22+72+62
4922+3572+8162 = 2942+7532+6182
4382+9512+2762 = 8342+1592+6722

También es clásico el cuadrado de 16 números llamado Melancolía, por haber aparecido en un cuadro del mismo título de Alberto Durero. Todas sus filas y columnas suman 34. Además, en la parte inferior contiene la fecha de su realización 1514. Este cuadrado, grabado en una placa de plata, se usaba para protegerse de enfermedades.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Este cuadrado mágico también es hipermágico, porque sigue siendo mágico cambiando entre sí algunas filas o columnas.

También suman 34 sus cuatro vértices 16+13+4+1 y sus vecinos 5+8+9+12, 15+14+3+2. También los números centrales 10+11+6+7 y los "saltos de caballo" 5+2+12+15.

Existen 880 cuadrados mágicos de orden 4 y 275305224 de orden 5

Es notable el cuadrado mágico formado por números primos de Henry Dudeney

67	1	43
13	37	61
31	73	7

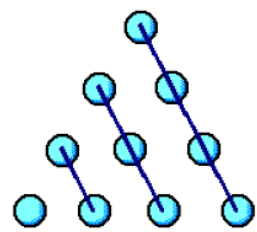
NÚMEROS FIGURADOS

Son números que se pueden disponer en forma de figura geométrica. Los más populares son:

NÚMEROS POLIGONALES

Número triangular

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



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

En la figura se observa la generación de cada número triangular:

$t_1 = 1 = 1$
$t_2 = 1+2 = 3$
$t_3 = 1+2+3 = 6$
$t_4 = 1+2+3+4 = 10$

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

Los números triangulares terminan en 0, 1, 3, 5, 6 u 8.

Otro resultado muy interesante es el de que la suma de los inversos de los números triangulares tiende a 2. Si quieres desarrollarlo basta que pienses que 1/3 = (2/2 - 2/3), 1/6 = (2/3 - 2/4) y así sucesivamente. Desarrolla la suma y verás anularse términos.

Comprueba lo siguiente: El número T(n) coincide con el número de soluciones positivas de la ecuación x+y+z=n+2.

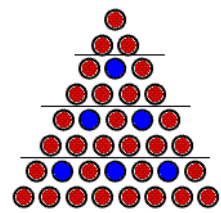
Triangulares de lado par

Los números triangulares 3, 10, 21, 36,…son aquellos cuyo número de orden es par: 3=T(2)=2×3/2; 10=T(4)=4×5/2; 21=T(6)=6×7/2,…Si aplicamos la

expresión algebraica de un número triangular, la de estos será

$T(2n)=2n(2n+1)/2=n(2n+1)=2n^2+n$

Los podemos representar como formados por filas de triángulos de 3 elementos separados por otros elementos aislados. En la imagen hemos representado el 36, es decir T(8)



Observa que está formado por 10 triángulos de tres elementos y 6 puntos aislados. Nos sugiere que un número triangular de orden par equivale a triangular de orden mitad multiplicado por 3 más su triangular anterior, es decir:

$T(2n)=3T(n)+T(n-1)$

Es fácil demostrarlo por inducción:
$T(2)=3\times T(1)+T(0)=3\times 1+0=3$;
$T(4)=3\times T(2)+T(1)=3\times 3+1=10$…

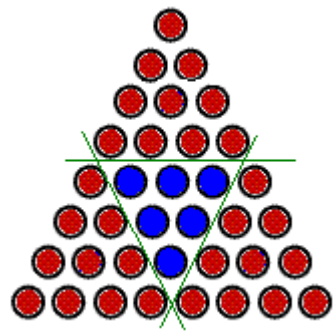
Probemos con $T(2(n+1))=T(2n)+(2n+1)+(2n+2)$ por definición de número triangular. Si aceptamos la hipótesis para n, tendremos:

T(2(n+1))=3×T(n)+T(n-1)+(n+1+n+1+n+1)+n=3×T(n)+3×(n+1)+T(n-1)+n=3×T(n+1)+T(n), luego la hipótesis se cumple para n+1.

La fórmula T(2n)=3T(n)+T(n-1) es válida

Adaptamos una demostración visual contenida en

http://math.berkeley.edu/~rbayer/09su-55/handouts/ProofByPicture-printable.pdf



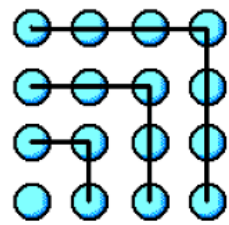
Así se ve mejor la relación.

En realidad, estos números **son los triangulares que no pueden ser hexagonales**. Se sabe que todo hexagonal es triangular, porque su expresión es H(n)=n(2n-1)=2n(2n-1)/2=T(2n-1), pero el número de orden del triangular es 2n-1, impar, luego los que no son hexagonales formarán la sucesión que estamos

estudiando: 3, 10, 21, 36…, que está contenida en http://oeis.org/A014105

Número cuadrado

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



Los primeros números cuadrados son: 1, 4, 9, 16, 25, …

En la figura se observa la generación de cada número cuadrado:

$C_1 = 1 = 1$
$C_2 = 1+3 = 4$
$C_3 = 1+3+5 = 9$
$C_4 = 1+3+5+7 = 16$

Los números cuadrados terminan en 0, 1, 4, 5, 6 o 9

Todos siguen la fórmula n^2, como es evidente.

Todo número cuadrado es suma de dos triangulares consecutivos. Compruébalo o intenta demostrarlo.

También se forma un cuadrado con 8 números triangulares, sumándoles una unidad. Con un dibujo lo puedes lograr fácilmente.

Los números triangulares y cuadrados cumplen tres propiedades:

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

Triangulares cuadrados

Números que son a la vez triangulares y cuadrados

Son los números 1, 36, 1225, 41616, 1413721, 48024900, ...

Siguen las fórmulas de recurrencia:

$C_{n+1} = 34 \times C_n - C_{n-1} + 2$

$$C_{n+1} = \frac{(C_n - 1)^2}{C_{n-1}}$$

Fórmula directa:

$$\frac{\left(17+12\sqrt{2}\right)^{n}+\left(17-12\sqrt{2}\right)^{n}-2}{32}$$

Estos números están publicados en OEIS, y los primeros son:

0, 1, 36, 1225, 41616, 1413721, 48024900, 1631432881,… (http://oeis.org/A001110)

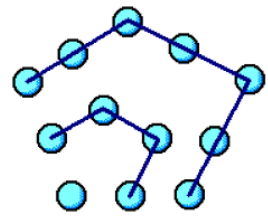
Evidentemente, estos números tienen en común el ser triangulares y cuadrados a la vez.

Una propiedad similar es que la media geométrica entre un término y el siguiente es también un número triangular

A(n)	RAIZ(A(n)*A(n+1))	Orden como triangular
0		
1		
36	6	3
1225	210	20
41616	7140	119
1413721	242556	696
48024900	8239770	4059
1631432881	279909630	23660

Número pentagonal

Se definen de la misma forma que los cuadrados y los triangulares, como números que forman pentágonos, hexágonos, etc.



La fórmula que siguen los pentagonales 1, 5, 12, ... es n(3n-1)/2

Los hexagonales 1, 6, 14, siguen la fórmula n(4n-2)/2 = $2n^2$ - n

En general, de k lados la fórmula adecuada es (n×(2+(n-1)×(k-2))/2

Número poligonal en general

Aunque estos números se tratan en documento aparte, se incluyen aquí sus conceptos y propiedades generales.

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

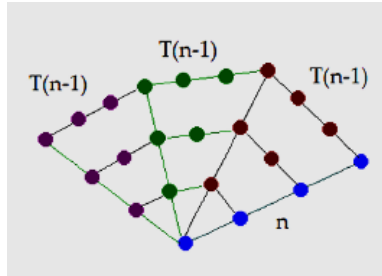
La expresión general de un número poligonal de k lados y orden n es

$$P_{n.k} = \frac{n(n(k-2)-(k-4)}{2}$$

o lo que es equivalente

$$P_{n.k} = n + (k-2)T_{n-1}$$

siendo T_{n-1} el triangular de una dimensión menos. La siguiente imagen demuestra esta propiedad:



Las unidades azules representan a n, y las de los otros tres colores a los números triangulares que terminan de engendrar el pentagonal.

También son válidas las descomposiciones

Teorema de Nicómaco:

Todo número poligonal es igual al de su mismo orden pero con una dimensión menos sumado con el triangular de una dimensión menos:

$$P_{n.k} = P_{n-1,k} + T_{n-1}$$

Descomposición triangular de Fermat

$$P_{n.k} = T_n + (k-3)T_{n-1}$$

Según Fermat, todo número natural se puede expresar como la suma de n números poligonales de n lados. Gauss lo demostró para los triangulares y Cauchy para todo tipo de polígonos.

Poligoriales

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

Un número poligorial de orden k equivale al producto de los primeros números poligonales de orden k. Por ejemplo, 180 es poligorial de orden 3, porque es el producto de los cuatro primeros números triangulares: 180=1×3×6×10. 518400 lo es de orden 4, porque equivale al producto de los cuadrados 1, 4, 9, 16, 25 y 36.

En el caso de los factoriales los factores son números naturales, y no hay que calcularlos previamente al producto, pero en el caso de los poligoriales, cada factor posee su propia fórmula, que hay que evaluar.

OTROS NÚMEROS FIGURADOS

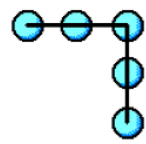
Un número **rectangular** es aquel cuyas unidades se pueden ordenar en forma de rectángulo de lados mayores que uno. Es sinónimo de compuesto.

Lo llamaremos **oblongo** si es posible elegir sus dimensiones como números consecutivos, como 12 = 3×4, 42 = 6×7, etc.

Los primeros números oblongos son 2, 6, 12, 20, 30, 42,

La fórmula de los números oblongos es n(n+1) lo que nos hace ver que son dobles de los triangulares. También equivalen a la suma de los k primeros números pares.

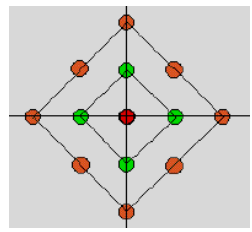
Un número natural constituye un **gnomon** cuando se puede dibujar como una escuadra de brazos iguales. Es equivalente a un número impar. En efecto, basta observar la figura:



Todo número cuadrado es suma de gnomones.

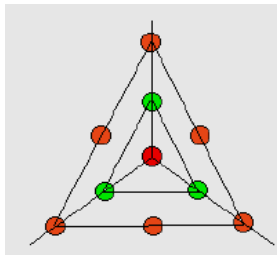
Números poligonales centrados

Los números poligonales anteriores crecen a partir de un vértice, y no tienen centro. Podíamos formarlos a partir de un punto (centro) rodeando después con triángulos, cuadrados o pentágonos con número creciente de puntos. Así, la imagen siguiente es un cuadrado centrado de orden 3 que equivale al número 13. Si suprimimos el perímetro más lejano nos resultaría el cuadrado centrado 5.



De igual forma se pueden definir los triángulos o polígonos centrados.

Así, los números 1, 4, 10, 19, 31,… son triangulares centrados.



1, 5, 13, 25, 41... son cuadrados centrados y

1, 6, 16, 31, 51... pentagonales centrados

Las fórmulas de generación de estos números son:

$TC_n = (3n^2-3n+2)/2$

$CC_n = 2n^2-2n+1$

$PC_n = (5n^2-5n+2)/2$

como puede verse en esta tabla generada con hoja de cálculo:

	Triangulares	Cuadrados	Pentagonales
N	(3*n^2-3*n+2)/2	2*n^2-2*n+1	(5*n^2-5*n+2)/2
1	1	1	1
2	4	5	6
3	10	13	16
4	19	25	31
5	31	41	51
6	46	61	76
7	64	85	106
8	85	113	141

Existe una fórmula general para la obtención del valor de un poligonal centrado:

$$POLC(n,k) = \frac{nk^2 - nk + 2}{2}$$

En ella n representa el número de lados y k su longitud. Así los triangulares tendrían como expresión

$TC_n = (3n^2-3n+2)/2$

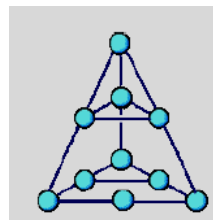
como vimos más arriba. Igual se deducen las de cuadrados, pentagonales y siguientes.

NÚMEROS PIRAMIDALES

Son aquellos números cuyas unidades se pueden representar como puntos en los lados de una pirámide.

Al igual que los poligonales se generan añadiendo a cada uno de ellos lados nuevos, los piramidales se forman mediante **números poligonales nuevos** que van haciendo el papel de bases de una pirámide.

Tomemos, por ejemplo, los números triangulares, 1, 3, 6, 10,… Imaginemos que comenzamos por 1 (siempre se comienza con él), que hará el papel de vértice, y después le adosamos como base el siguiente triangular, 3, y después el siguiente, 6, y así hasta que obtengamos el orden deseado. Lo puedes ver en la imagen.



A los números poligonales de orden 3 (triangulares) les llamaremos **tetraédricos**, a los de orden 4, **piramidales cuadrados**, y al resto, pentagonales, hexagonales, y así hasta el orden que deseemos. Usamos la palabra *orden* para no crear confusión con la calculadora que ofrecemos. Llamaremos *lado* al número de poligonales que se acumulan.

El número piramidal de orden k y lado n (PIR(n,k)) equivale a la suma del piramidal de idéntico orden y un lado menos y el poligonal de mismo orden y lado.

Fórmula de los piramidales

Existe una expresión general para calcular **PIR(N,K)**. De todas las versiones publicadas nos quedamos con la siguiente:

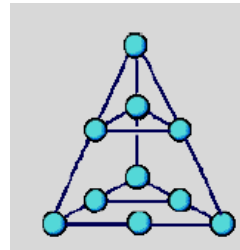
$$PIR(n,k) = \frac{3n^2 + n^3(k-2) - n(k-5)}{6}$$

Es un polinomio de tercer grado, al igual que los poligonales se expresan con uno de segundo.

Tetraedros.

A los números piramidales triangulares se les conoce también como tetraédricos, o simplemente tetraedros (abreviado, TET), en recuerdo del primer poliedro

regular. Todos ellos se forman a partir del 1 adosando los distintos números triangulares, 3, 6, 10, 15, 21, 28… por lo que también podemos decir que los tetraédricos equivalen a las sumas parciales de los triangulares.



TET(1)=1
TET(2)=1+3=4
TET(3)=4+6=1+3+6=10
TET(4)=10+10)1+3+6+10=20
…

La lista de los primeros será, pues:

1, 4, 10, 20, 35, 56, 84, 120, 165, 220, 286, 364, 455, 560, 680, 816, 969, 1140, 1330, 1540, 1771, 2024, 2300, 2600, 2925,… http://oeis.org/A000292

Representan pirámides formadas por números triangulares, como las balas esféricas amontonadas en capas triangulares.

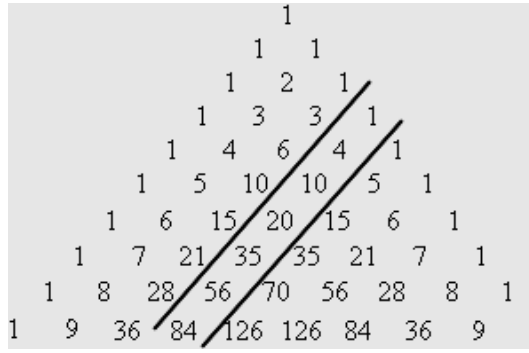
Su expresión algebraica es:

$$TET(n) = PIR(n,3) = \frac{3n^2 + n^3 + 2n}{6} = \frac{n(n+1)(n+2)}{6}$$

Esta expresión nos suena familiar, y es que equivale al número combinatorio n+2 sobre 3:

$$TET(n) = \binom{n+2}{3}$$

Por ser números combinatorios de orden 3, los tetraedros se situarán en la cuarta fila del triángulo de Pascal:



(Imagen adaptada de otra contenida en Wikipedia.es)

Piramidales cuadrados

Los piramidales cuadrangulares se forman al apilar números cuadrados consecutivos.

Los primeros números piramidales cuadrados son:

0, 1, 5, 14, 30, 55, 91, 140, 204, 285, 385, 506, 650, 819, 1015, 1240, 1496, 1785, 2109, 2470, 2870, 3311, 3795,

4324, 4900, 5525, 6201, 6930, 7714, 8555, 9455, …(http://oeis.org/A000330)

Según su definición, cada piramidal cuadrado será equivalente a la suma 1+4+9+16+…, pero se conoce, y es muy popular, la fórmula de la suma de los n primeros cuadrados, que es igual a n×(n+1)×(2×n+1)/6, luego, si llamamos PCUAD(n) al enésimo piramidal cuadrado tendremos:

$$PCUAD(n) = \frac{n(n+1)(2n+1)}{6}$$

Si descomponemos 2n+1 en (n+2)+(n-1) resulta

$$PCUAD(n) = \binom{n+2}{3} + \binom{n+1}{3}$$

Al igual que un cuadrado se descompone en dos triángulos consecutivos, aquí serían dos tetraedros: ***Todo número piramidal cuadrado es suma de dos piramidales triangulares consecutivos.***

Piramidales pentagonales

Se forman añadiendo a la unidad (el vértice de la pirámide) distintos números pentagonales como si fueran cortes poligonales de la pirámide. Para nosotros es preferible ver los piramidales como suma de

pentagonales sucesivos. Así, si estos forman la sucesión 1, 5, 12, 22, 35, 51, 70, 92, 117, 145,… http://oeis.org/A000326, los piramidales correspondientes coincidirán con sus sumas parciales: 1, 6, 18, 40, 75, 126, 196, …

Los primeros piramidales pentagonales son:

1, 6, 18, 40, 75, 126, 196, 288, 405, 550, 726, 936, 1183, 1470, 1800, 2176, 2601, 3078, 3610, 4200, 4851, 5566, 6348, 7200, 8125, 9126, 10206, 11368, 12615, 13950, 15376, 16896, 18513, 20230, 22050, 23976, 26011, 28158, 30420, 32800, 35301, 37926, 40678, …http://oeis.org/A002411

Los números piramidales pentagonales (PPENT) siguen una expresión polinómica muy sencilla:

$$PPENT(n) = \frac{n^2(n+1)}{2} = \frac{n^3 + n^2}{2}$$

Esta fórmula se obtiene particularizando para 5 la general de los piramidales:

$$PIR(n,k) = \frac{3n^2 + n^3(k-2) - n(k-5)}{6}$$

$$PPENT(n) = \frac{3n^2 + n^3(5-2) - n(5-5)}{6} = \frac{3n^3 + 3n^2}{6} = \frac{n^3 + n^2}{2}$$

Por tanto, podemos afirmar que los piramidales pentagonales son **los promedios entre el cuadrado y el cubo de un número**.

PIRAMIDALES DE CUATRO DIMENSIONES

Al igual que la acumulación de números poligonales da lugar a los piramidales (de tres dimensiones), si encontramos las sumas parciales las podemos llamar **números piramidales de cuatro dimensiones.** No podemos dibujarlos, pero sí estudiar su fórmula y algunos ejemplos concretos.

Fórmula

El valor de los números piramidales de cuatro dimensiones se encuentra con la expresión

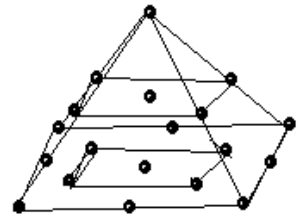
$$PIRK_4(n) = \frac{n(n+1)(n+2)((k-2)n+(6-k))}{24}$$

En ella **n** es el número de orden y **k** el valor del lado.

PIRAMIDALES CENTRADOS

En el caso de tres dimensiones sí se pueden dibujar y poseemos una expresión para ellos. Se forman

acumulando, mediante sumas parciales, los números poligonales centrados.



En la imagen se representa el número piramidal centrado de orden 4 (cuatro lados) y longitud 3 (tres niveles)

Su expresión general es:

$$PIRC_m(n) = \frac{mn^3 + (6-m)n}{6}$$

(Elena Deza y Michel Deza)

En ella **m** es el número de lados y **n** su longitud.

TERNAS PITAGÓRICAS

Definiciones

Una terna de números enteros positivos se llama pitagórica si es solución de la ecuación $x^2 + y^2 = z^2$

Llamaremos ternas pitagóricas primitivas x_0, y_0 y z_0 a aquellas que no tienen divisores comunes. Por tanto, los

tres números no pueden ser pares, luego alguno será impar. Los tres impares tampoco pueden ser, porque z sería suma de impares y por tanto par. Tampoco puede haber un sólo impar, porque la suma no tendría la paridad adecuada, luego z_0 es impar y las otras dos, una par y otra impar.

En lo que sigue sólo nos referiremos a las ternas pitagóricas primitivas.

Fórmulas de generación

(1) $Z = m^2 + n^2$; $Y = m^2 – n^2$; $X = 2mn$ con m y n primos entre sí y de distinta paridad, con m>n.

Son pitagóricas, porque $(m^2 + n^2)^2 = (m^2 - n^2)^2 + 4m^2n^2$

Son primitivas, porque todo divisor de $m^2 + n^2$ y $m^2 – n^2$ es distinto de 2 (son impares) y divide a su suma y diferencia, luego divide simultáneamente a m y a n, lo que es imposible por ser coprimos. Luego ambos son primos entre sí y también con 2mn.

El perímetro tendrá como fórmula $2m^2 + 2mn$, el semiperímetro $m(m+n)$, el área $mn(m^2 - n^2)$ y por tanto, el radio del incentro $r = mn(m^2 - n^2)/(m(m+n)) = n(m-n)$

Esta propiedad del radio nos lleva a la fórmula generadora (4)

(2) $Z=(m^2 + n^2)/2$; $Y=(m^2 - n^2)/2$; $X=mn$ con m y n impares u coprimos y m>n

Esta es la primitiva fórmula de los pitagóricos.

(3) $X = 2n+1$; $Y = 2n(n+1)$; $Z = 2n(n+1)+1$

En efecto: $X^2+Y^2 = 4n^2+4n+1+4n^4+8n^3+4n^2$
$Z^2= (2n^2+2n+1)^2 = 4n^4+4n^2+1+8n^3+4n^2+4n$

Esta fórmula no genera todas las ternas primitivas. Sólo genera aquellas en las que el cateto mayor y la hipotenusa son números consecutivos.

(4) $Y = 2pq+q^2$; $X = 2pq+2p^2$; $Z = 2pq+2p^2+q^2$

En efecto, tomando m y n de la primera fórmula, si llamamos p=n q=m-n, m=p+q, obtendremos: r=n(m-n)=pq; $Z = m^2 + n^2 = (p+q)^2 + p^2 = 2pq+2p^2+q^2$; $Y = m^2 – n^2 = (p+q)^2 - p^2 = 2pq+q^2$; $X = 2mn = 2(p+q)p = 2pq+2p^2$

Este desarrollo demuestra fácilmente la primera de las propiedades que incluimos a continuación

Propiedades

- La diferencia entre la hipotenusa y el cateto par es un cuadrado perfecto, y su diferencia con el otro el doble de otro cuadrado perfecto.

- Por ejemplo, en la terna 35, 12, 37, la diferencia 37-12 = 25 y 37-35 = 2×1. Puedes comprobarlo con cualquiera de las fórmulas de generación.
- El cateto par es múltiplo de 4
  En efecto, si los otros dos son impares, se cumplirá que $m^2 = (2p+1)^2 - (2q+1)^2$ y desarrollando $m^2 = 4(p-q)(p+q+1)$, pero uno de los paréntesis es par. luego m^2 es divisible entre 8, y al ser cuadrado perfecto, entre 16, luego m es múltiplo de 4.
- La hipotenusa es congruente con 1 módulo 4
  Según la primera fórmula de generación, es suma de dos cuadrados, uno par y otro impar, luego no puede tener la forma 4K+3. Ha de ser del tipo 4K+1

Primos pitagóricos

Los primos pitagóricos son los del tipo 4K+1, es decir, que poseen resto 1 al dividirlos entre 4. Estos primos se caracterizan por poder ser expresados mediante una suma de dos cuadrados **de forma única**.

Por ejemplo, $13=4\times3+1=2^2+3^2$

Relacionando estos números con el estudio sobre el número de ternas pitagóricas de las que un número es hipotenusa, podemos afirmar que estos primos sólo pueden ser hipotenusa de una sola terna. Así, el ejemplo del 13 se traduce en la terna única $13^2=12^2+5^2$.

Los primeros primos son sencillos de identificar. La terna que producen es siempre primitiva, pues su carácter de primos impide su simplificación.

Según lo aprendido anteriormente, sus potencias serán hipotenusas de tantas ternas como indique su exponente. Por ejemplo, 13^5=371293 lo es de las cinco siguientes:

$371293=3107^2+371280^2=139932^2+343915^2=142805^2+342732^2=145668^2+341525^2=261443^2+263640^2$

Números de Saint-Exupéry

Reciben este nombre en la página OEIS (http://oeis.org) aquellos números que coinciden con el producto de los tres lados de una terna pitagórica. El primero, como era de esperar, es 60, que es el producto de 3, 4 y 5, elementos de la terna más sencilla que conocemos. El segundo, 480, es el producto de sus dobles, 6×8×10. Siguen infinitos de este tipo (porque también es infinito el número de ternas.

TRIÁNGULOS HERONIANOS

Estos triángulos están relacionados con las ternas pitagóricas, porque también representan conceptos geométricos mediante números naturales.

Un triángulo se califica de *heroniano* si las longitudes de sus lados y el valor de su área son números enteros. Es un concepto aritmético, por lo que se supone que esto ocurre con una unidad de medida adecuada. Consecuencia de esto es que también es entero el perímetro.

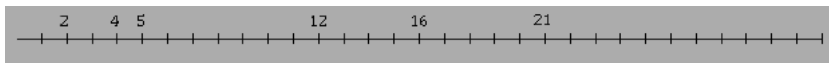
El nombre que les aplicamos es un recuerdo de Herón de Alejandría, autor de la popular fórmula para el área de un triángulo conocidos los lados a, b y c:

$$A = \sqrt{p(p-a)(p-b)(p-c)}$$

En esta fórmula, p es el semiperímetro. Si A y los lados son todos enteros, el triángulo será heroniano. Esto exige que p(p-a)(p-b)(p-c) sea un cuadrado perfecto.
Una primera clase de este tipo de triángulos lo constituyen los pitagóricos, ya que en una terna pitagórica (a, b, c), el área equivale a **a×b/2**, y en estas ternas siempre existe un cateto par

Regla de Golomb

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



Las seis marcas presentan las quince diferencias 1,2,3,4,5,7,8,9,10,11,12,14,16,17 y 19 distintas. Se llama orden de la regla al número de marcas, en este caso 6, y longitud a la mayor diferencia entre ellas, 19 en el ejemplo.

Como lo importante del tema son las diferencias, se suele hacer coincidir la primera marca con el 0. De esta forma, la anterior regla quedaría así:

Estas marcas poseen las mismas diferencias, pero no abarcan todas las posibles medidas. Por ejemplo, con esta regla no se podría medir una distancia (diferencia) de 13. Una regla que mida todas las longitudes posibles

recibe el nombre de perfecta, y si es la más corta dentro de su orden, óptima. Por ejemplo, {0,1,4.6} forman una regla perfecta, pues se pueden medir con ellas las longitudes

1,2,3,4,5 y 6.

Conjunto de Sidon

Un conjunto de números naturales se llama de Sidon cuando todas las sumas posibles entre sus elementos son distintas. Por ejemplo {3,5,8,9} produce las sumas

8,11,12,13,14 y 17.

Se puede demostrar que un conjunto finito de Sidon es también una regla de Golomb, y a la inversa (si se prescinde del convenio de comenzar por cero). Por tanto, un conjunto finito es de Sidon si produce diferencias entre sus elementos todas distintas. Intenta demostrarlo, que no es difícil.

DERIVADA ARITMÉTICA

Este original concepto fue presentado por el matemático español José Mingot Shelly en 1911 con el título "Una cuestión de la teoría de los números", trabajo presentado

en el Tercer Congreso Nacional para el Progreso de las Ciencias, Granada. Es interesante su biografía, condicionada totalmente por la Guerra Civil española.

Como su nombre indica, esta derivada se basa en una operación similar a la de la derivada de un producto, y aplicada a números naturales. Podemos concretarla de esta forma:

D(0)=D(1)=0 (para completar la definición)
D(p)=1 si p es primo
D(ab)=aD(b)+bD(a) a>1, b>1 (Regla del producto)

Por ejemplo, D(10)=D(2×5)=2D(5)+5D(2)=2×1+5×1=7
Como la definición formal es similar a la de la derivada de una función, podemos extenderla a más factores, a potencias y a todos los números en general.
Así, en un número esfénico N=p×q×r, se tendrá

D(N)=p×q+q×r+r×p

Por ejemplo, D(30)=D(2×3×5)=2×3+3×5+5×2=31

Se generaliza fácilmente a las potencias de primos:

$D(p^k)=k\times p^{k-1}$
$D(8)=D(2^3)=3\times 2^2=12$
$D(16)=D(2^4)=4\times 2^3=32$

Como todo número equivale a una potencia o a un producto de potancias de números primos, con estas operaciones podemos derivar cualquier número entero positivo.

NÚMEROS DE LÖSCH

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

Aparecen como las normas de los números enteros de Eisenstein, pero no seguiremos por ahí porque es un tema de números complejos. Estos números son cerrados para la operación de multiplicar, por lo que si **m** y **n** pertenecen a este tipo, también lo serán **mn**, $\mathbf{m^k}$ y $\mathbf{n^k}$. Al poder ser **x** o **y** iguales a cero, estos números presentarán algunos subtipos. Por ejemplo, entre ellos estarán el cero y todos los cuadrados enteros, si elegimos y=0 o y=-x. Esto demuestra que existen infinitos números de este tipo.

SUCESIONES

Sucesión de números naturales

Es toda función definida de N (conjunto de los números naturales) en N o en subconjunto suyo, al que llamaremos conjunto imagen.. A los elementos orígenes de la función les llamaremos **índices**, y a las imágenes **elementos** o **términos** de la sucesión.

En la práctica es una secuencia ordenada de números naturales del tipo 2, 4, 7, 11, 12,....representada por los símbolos a_1, a_2, a_3, a_4, ...a_n ... en la que $\mathbf{a}_n$ es el elemento y **n** el índice o subíndice.

El término general **a(n),** o **b(n)** o **c(n)** es una fórmula dependiente de **n** que permite reproducir, si es posible, cualquier elemento de la sucesión.

Las sucesiones más útiles suelen ser infinitas, sin último término. En el caso finito se llama **longitud** a su número de términos, ya que estos formarán un conjunto imagen finito,

Las sucesiones se pueden representar como {a(n)} , (b(n)), e incluso como [c(n)]. Es un detalle sin importancia. Una sucesión **{b(n)}** es **subsucesión** de otra **{a(n)}** cuando el conjunto imagen de **{b(n)}** está incluido en el de **{a(n)}**

Por último, una sucesión es **creciente** si cada término es mayor o igual que el anterior, y **decreciente** si se cumple la condición opuesta. Será acotada superiormente si todos los elementos son iguales o menores que una cota K. Simétricamente se defina acotada inferiormente y simplemente acotada (con cotas superior e inferior) Las desigualdades también pueden ser estrictas. Hay deficiniciones orientadas a las curiosidades, como **oscilante, ondulada** y otras**.**

Sucesión o progresión aritmética

Es aquella en la que cada término es igual al anterior sumado con un número constante llamado *diferencia*. Su fórmula de recurrencia es: $\mathbf{a_1 = a;\ a_n = a_{n-1} + d,}$ donde **a** (valor inicial) y **d** (diferencia) son constantes.

La fórmula del término general es

$$a_n = a_1 + (n-1)d$$

La suma de n términos viene dada por la fórmula

$$S_n = \frac{n(a_1 + a_n)}{2}$$

Sucesión o progresión geométrica

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

La fórmula del término general es

$$a_n = a_1 r^{n-1}$$

Suma de los primeros términos:

$$a_n = a_1 \frac{r^n - 1}{r - 1}$$

SUCESIONES RECURRENTES

Una sucesión se llama *recurrente* o *recursiva* cuando todos sus términos, salvo los primeros, que se definen directamente, dependen de los valores de los anteriores inmediatos. El número de esos términos de los que dependen se denomina el ***orden*** de la sucesión. La ecuación que relaciona estos términos se denomina también **de recurrencia**. Un ejemplo de segundo orden es el siguiente:

$x_1=1$, $x_2=2$, $x_n=2\times x_{n-1}+x_{n-1}\times x_{n-2}$

Si la relación entre un término y los anteriores se basa en una fórmula lineal, diremos que la recurrencia es también de tipo *lineal*. Añadiremos el calificativo de *homogénea* si en esa fórmula no existen términos constantes.

Esta sería lineal homogénea de tercer orden:

$x_1=1$, $x_2=2$, $x_3=0$, $x_n=2\times x_{n-1}+2\times x_{n-2}-x_{n-3}$

Y esta, lineal no homogémea de segundo orden:

$x_1=1$, $x_2=2$, $x_n=2\times x_{n-1}+2\times x_{n-2}+7$

Recurrencia lineal de primer orden

Es la del tipo $x_n=a\times x_{n-1}+b$**.** Si b=0 es la que llamamos en la sección anterior *progresión geométrica*, y a ella nos remitimos. Si a=1 y $b\neq 0$ será *aritmética*. Si a=1 y b=1 la sucesión coincidirá con los *números naturales*. Si ambos son no nulos, será *no homogénea*, pero veremos que es convertible en homogénea de segundo orden.

Recurrencia lineal de segundo orden

Llamaremos relación de recurrencia lineal de segundo orden a la que existe entre los términos de una sucesión si reviste esta forma:

$$x_n=a_1x_{n-1} + a_2x_{n-2} + a_3$$

Interpretamos que cada término a partir uno de ellos equivale al anterior multiplicado por un número más el anterior del anterior por otro y sumado un tercer número. Nos dedicaremos tan sólo al caso en el que $a_3=0$, es decir, a *relaciones lineales de segundo orden homogéneas*, pues en ellas encontraremos bastantes hechos curiosos.

Lo normal es definir directamente los primeros términos, llamados *valores iniciales*, y después dar los *coeficientes*

de la recurrencia, que supondremos constantes. Por ejemplo, en la sucesión de Fibonacci, definimos directamente $x_0=1$, $x_1=1$ y usamos los coeficientes $a_1=1$ y $a_2=1$, con lo que la relación de recurrencia vendrá dada por $x_n = x_{n-1} + x_{n-2}$, constituyendo una recurrencia lineal de segundo orden homogénea, y entrando así en nuestro estudio.

Una sucesión definida por recurrencia vendrá dada así por el conjunto de valores iniciales y el de coeficientes, siendo conveniente fijar también el número de términos.

Tal como se anunció anteriormente, las recurrencias no homogéneas de primer grado se pueden convertir en este tipo:

Tomamos dos términos consecutivos $x_n=a\times x_{n-1}+b$, $x_{n-1}=a\times x_{n-2}+b$. Restamos miembro a miembro: $x_n - x_{n-1}= a(x_{n-1} - x_{n-2})$, y de ahí:

$$x_n = (a+1)x_{n-1} - ax_{n-2}$$

Suma de una sucesión recurrente

Las sucesiones recurrentes de orden **h** se pueden sumar mediante la siguiente fórmula, también recurrente,que procede de la publicación *Sucesiones recurrentes* de A.I.Markushevich – Editorial Mir. La demostración de ella no es difícil, pero resulta larga para esta publicación:

$$s_{n+h+1}=(1+a_1)s_{n+h}+(a_2-a_1)\, s_{n+h-1}+ \ldots +(a_h-a_{h-1})\, s_{n+1}-a_h s_n$$

Por ejemplo, en la sucesión de Fibonacci $a_1=1$ y $a_2=1$, luego la fórmula se aplicará así $s_{n+3}=(1+a_1)s_{n+2}+(a_2-a_1)s_{n+1}-a_2s_n$, es decir:

$$s_{n+3}=2s_{n+2}-s_n$$

Se puede comprobar fácilmente:

$54=2\times33-12=66-12=54$, $88=54\times2-20=108-20=88$

Ecuación característica

Existe un procedimiento simple para intentar expresar **X(n)** en función de **n** en sucesiones definidas por recurrencias de segundo orden: *la ecuación característica*. Puedes estudiarla en cualquier manual o página web específica, como

(http://people.uncw.edu/tompkinsj/133/recursion/homogeneous.htm)

En esencia este método consiste, para recurrencias homogéneas, en:

(1) Dada la relación

$x_n=a_1x_{n-1}+a_2x_{n-2}$

planteamos la ecuación de segundo grado

$x^2-a_1x-a_2=0$

(2) Si las soluciones de esa ecuación son distintas, $\mathbf{x_1}$ y $\mathbf{x_2}$, la expresión buscada será

$x(n)= (x_1)^n$ o $x(n)= (x_2)^n$

o bien una combinación lineal de ambas:

$x(n)= C_1(x_1)^n+C_2(x_2)^n$

A veces uno de los sumandos tiende a cero al crecer n, y esto da lugar a propiedades interesantes, ya que X(n) sólo dependería aproximadamente del primer sumando.

(3) Si las soluciones son iguales, $\mathbf{x_1=x_2=x,}$ la solución vendrá dada por

$x(n)= (C_1+C_2n)x^n$

(4) Con soluciones complejas conjugadas, caso bastante frecuente, la solución viene dada por

$x(n)=r^n(C_1sen(n\alpha))+C_2cos(n\alpha))$

Está expresada en coordenadas polares r y α.

En el caso de ecuaciones no homogéneas, se resuelve, en primer lugar, como si fuera homogénea, y después se realizan ajustes en la expresión resultante.

En casos complejos es preferible usar la función generatriz.

Función generatriz

Es una función tal que al desarrollarla como polinomio, los coeficientes del mismo reproducen los términos de la sucesión. Veremos varias en los siguientes ejemplos.

Ejemplos de sucesiones recurrentes

Números de Fibonacci

Es la más popular de todas. Se define como $x_0=1$, $x_1=1$ y la relación de recurrencia viene dada por $x_n=x_{n-1}+x_{n-2}$. Sus elementos son:

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377,…

Su ecuación característica será $x^2-x-1=0$ con soluciones

$$x = \frac{1 \pm \sqrt{5}}{2}$$

Ellas dan lugar a la fórmula explícita para esta sucesión:

$$f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Como el segundo sumando tiende a cero para n tendiendo a infinito, los números de Fibonacci se aproximarán al primero, y, de hecho, el cociente entre dos consecutivos tiende al número de oro.

Su función generatriz es

$$f(x) = \frac{1}{1-x-x^2}$$

Si se inicia la sucesión en 0 en lugar de en 1, puede cambiar esta función generatriz.

Sumas de Zeckendorf

Cada entero positivo puede expresarse de manera única como una suma de números distintos de Fibonacci no consecutivos. Este resultado se denomina teorema de Zeckendorf y la secuencia de números de Fibonacci que se suman se denomina representación de Zeckendorf. Se llaman así en honor al médico belga y matemático aficionado E. Zeckendorf.

Para descomponer un número en sumandos de la sucesión de Fibonacci, se ha demostrado que el mejor procedimiento es el de ir restando al número el término de Fibonacci mayor posible (algoritmo voraz), hasta llegar a una diferencia que sea también de Fibonacci, con lo que se termina en un cero. El teorema correspondiente afirma que siempre se llegará a este término en las diferencias.

Sucesión de Jacobsthal

Esta sucesión es poco conocida, pero tiene alguna propiedad interesante. Se define como $x_0=1$, $x_1=1$ y la relación de recurrencia viene dada por $x_n=x_{n-1}+2x_{n-2}$. Sus elementos son:

0, 1, 1, 3, 5, 11, 21, 43, 85, 171, 341, 683, 1365, 2731, 5461, 10923, 21845, 43691,…

(la tienes en http://oeis.org/A001045)

Su término general viene dado por

$$X(n) = \frac{2^n - (-1)^n}{3}$$

Números de Pell

Tomamos como coeficientes de recurrencia $X_0=2$ y $X_1=1$. Es decir, que $X_{n+1}=2X_n+X_{n-1}$. Si como valores iniciales tomamos 0 y 1 resultan los números de Pell o números lambda http://oeis.org/A000129. Son estos:

0, 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, 5741, 13860, 33461, 80782, 195025, 470832, …

Su fórmula general viene dada por

$$P(n) = \frac{1}{2\sqrt{2}}\left(\left(1+\sqrt{2}\right)^n - \left(1-\sqrt{2}\right)^n\right)$$

Como consecuencia, por tender a cero el segundo sumando, el cociente entre dos números de Pell consecutivos es:

$$\frac{P(n+1)}{P(n)} \to 1+\sqrt{2}$$

Su función generatriz es

$$\frac{x}{1-2x-x^2}$$

Para que un número de Pell P(n) sea primo es necesario que n sea primo. Los valores de n que producen esos primos son 2, 3, 5, 11, 13, 29, 41, 53, 59, 89, 97, 101, 1,… que producen los **números de Pell primos**

2, 5, 29, 5741, 33461, 44560482149, 1746860020068409, …

Números de Lucas

Los números de Lucas se pueden engendrar con los coeficientes A=1 y B=1 comenzando con X_0=2 y X_1=1 Su definición es, por tanto $X_n=X_{n-1}+X_{n-2}$

Son estos: 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, 2207, 3571,…

Su expresión general viene dada por

$$L(n) = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n = \varphi^n + (-\varphi)^{-n}$$

Y su función generatriz:

$$L(x) = \frac{x_0 + (x_1 - a_1 x_0)x}{1 - a_1 x - a_2 x^2} = \frac{2 + (1 - 1 * 2)x}{1 - 1x - x^2} = \frac{2 - x}{1 - 2x - x^2}$$

Recurrencia lineal de tercer orden

Definición

Las recurrencias de tercer orden son idénticas a las de segundo, pero con un término más en la fórmula (nos referiremos tan sólo a las homogéneas). Su recurrencia vendrá definida por

$$x_n = Ax_{n-1} + Bx_{n-2} + Cx_{n-3}$$

El resto de cuestiones es similar a las de segundo orden.

Sucesión de Perrin

Condiciones iniciales: $\mathbf{x_0=3}$ $\mathbf{x_1=0}$ $\mathbf{x_2=2}$ Ecuación de recurrencia: $\mathbf{x_n=x_{n-2}+x_{n-3}}$

Es como una sucesión del tipo Fibonacci pero “con retraso”, pues los que se suman no son los dos anteriores, sino los que están un paso más atrás.

Esta popular sucesión la tienes disponible en

http://oeis.org/A001608, donde les llaman números skiponacci, quizás por los saltos o retardos que presentan: 3, 0, 2, 3, 2, 5, 5, 7, 10, 12, 17, 22, 29, 39, 51, 68, 90, 119, 158, 209, 277, 367, 486, 644, 853, …

Ecuación característica

La ecuación característica correspondiente será X^3-x-1=0. Con la suma de potencias de sus tres soluciones obtenemos la expression del término general:

La solución real 1,32471…(aquí sólo aproximada) es el ***número plástico*** ψ, cuyo nombre se eligió como afín al número de oro o el de plata. Como en casos anteriores, los cocientes entre términos consecutivos tienden a él.

Función generatriz

$$F(x) = \frac{3 - x^2}{1 - x^2 - x^3}$$

Sucesión de Perrin y números primos

La propiedad más conocida de estos números es que si **p** es primo, **p** divide a **X(p).** Por ejemplo, X(11)=22, que es múltiplo de 11. A pesar de su carácter algo extraño, la propiedad ha sido demostrada para todos los números primos. La contraria no es cierta. X(n) puede ser múltiplo de n sin que este sea primo. A estos términos se les suele llamar pseudoprimos de Perrin

(http://oeis.org/A013998):

271441, 904631, 16532714, 24658561, 27422714, 27664033, 46672291, …

Sucesión de Narayana

Esta sucesión fue ideada por el hindú Narayana (siglo XIV), e intentaba calcular con ella generaciones de vacas, al igual que Fibonacci lo hacía con conejos. Planteó lo siguiente:

Una vaca tiene anualmente una cría. Cada una de ellas, cuando ya es novilla a los cuatro años, también tiene una cría anual ¿Cuántas vacas habrá a los 20 años?

Este proceso es recurrente:

En efecto, supongamos que nace la vaca en el año 1. Se pasará tres años sin parir, por lo que la sucesión deberá comenzar con 1, 1, 1,… Al cuarto año tiene una cría, luego ya serán 2 vacas, y, como pare cada año, los siguientes números serán 3 y 4. Cuando la cría tiene 4 años, tendrá otra a su vez, y serán 6. En general, en cada generación habrá tantas vacas como las que haya actuales, más todas aquellas que ya tengan cuatro años, lo que nos lleva a que $\mathbf{x_n=x_{n-1}+x_{n-3}}$

Según esto, la sucesión de Narayana es recurrente de tercer orden.

La definición de la sucesión, como todas las de su clase, se basa en dar la fórmula de recurrencia y las

condiciones iniciales. Según lo explicado más arriba, son estas:

Condiciones iniciales: $\mathbf{x_0=1\ x_1=1\ x_2=1}$ Ecuación de recurrencia: $\mathbf{x_n=x_{n-1}+x_{n-3}}$

Coincide con la sucesión publicada en
http://oeis.org/A000930

1, 1, 1, 2, 3, 4, 6, 9, 13, 19, 28, 41, 60, 88, 129, 189, 277, 406, 595, 872, 1278, 1873, 2745, …

Ecuación característica

La ecuación característica correspondiente es $X^3-x^2-1=0$. Al resolverla obtenemos una raíz real, 1,46557, y como ocurre en casos similares. El cociente X(n+1)/X(n) se acercará a ese valor 1,46557.

Función generatriz

Al igual que en las sucesiones recurrentes que ya hemos estudiado, podemos considerar una función generatriz para esta. Es la siguiente:

$$F(x) = \frac{1}{1 - x - x^3}$$

Los coeficientes de su desarrollo en polinomio coinciden con los términos de la sucesión.

1 + x + x^2 + 2×x^3 + 3×x^4 + 4×x^5 + 6×x^6 + 9×x^7 + 13×x^8 + 19×x^9 + 28×x^10 + 41×x^11 + 60×x^12 +

88×x^13 + 129×x^14 + 189×x^15 + 277×x^16 + 406×x^17 + 595×x^18 + 872×x^19 +…

Cálculo directo de un término

Se puede demostrar que los términos de esta sucesión vienen dados por una suma de números combinatorios:

$$X(n) = \sum_{i=0}^{n/3} \binom{n-2i}{i}$$

Sucesión de Padovan

Esta sucesión es similar a la de Perrin, pero con condiciones iniciales distintas. En ambas la recurrencia viene definida por $\mathbf{x_n=x_{n-2}+x_{n-3}}$, pero mientras que en la de Perrin son $\mathbf{x_0=3\ x_1=0\ \ x_2=2,}$ en la de Padovan $\mathbf{x_0=1\ x_1=1\ \ x_2=1.}$

Sus primeros términos son: 1, 1, 1, 2, 2, 3, 4, 5, 7, 9, 12, 16, 21, 28, 37, 49, 65, 86, 114, 151, 200, 265, 351, 465, 616, 816, 1081, 1432 (http://oeis.org/A134816)

En el resto de características es muy parecida a la anterior.

Números "Tribonacci"

Los números "tribonacci" son análogos a los de Fibonacci, pero generados mediante recurrencias de tercer orden homogéneas. Existen muchas sucesiones

con este nombre, según sean sus condiciones iniciales. Aquí comenzaremos con la contenida en

http://mathworld.wolfram.com/TribonacciNumber.html,

pero podemos cambiar más tarde si surgen propiedades interesantes para su estudio con hoja de cálculo.

En estos números la fórmula de recurrencia posee todos sus coeficientes iguales a la unidad

$x_n = A \times x_{n-1} + B \times x_{n-2} + C \times x_{n-3}$ se convertiría en $x_n = x_{n-1} + x_{n-2} + x_{n-3}$

Al igual que en el caso de Fibonacci, los dos valores iniciales también valen 1, y el tercero, 2: $\mathbf{x_0=1\ x_1=1\ x_2=2}$

Los primeros términos son:

1, 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, 504, 927, 1705, 3136, 5768, 10609, 19513, 35890, 66012, 121415, 223317, 410744, … http://oeis.org/A000073

Ecuación característica

Al igual que en otras sucesiones recurrentes, su ecuación característica se formará a partir de sus coeficientes, en este caso todos iguales a 1, luego será $\mathbf{x^3-x^2-x-1=0}$

Recordemos que los elementos de las sucesiones recurrentes se pueden expresar como suma de potencias de las tres soluciones, pero con estos números ocurre como con algunos similares (los de Fibonacci, Perrin o Narayana), y es que las raíces complejas, al

tener módulo inferior a la unidad, tienden a cero si prolongamos la sucesión. Por ello, las potencias de la raíz real, 1,839286…generan con bastante aproximación los números Tribonacci, y, lo que es lo mismo, esta constante coincidirá aproximadamente con el cociente entre dos de estos números consecutivos.

Función generatriz

Todas las variantes de las sucesiones Tribonacci comparten los mismos coeficientes de recurrencia, y por tanto también el denominador de su función generatriz. La que estamos estudiando, de inicio 1, 1, 2, se genera con la siguiente:

$$F(x) = \frac{x}{1 - x - x^2 - x^3}$$

Números de Catalan

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

Fueron descubiertos por Euler al estudiar las particiones de los polígonos convexos en triángulos que no se intersecten. Así, el cuadrado se puede dividir en triángulos de dos formas distintas, el pentágono de 5, y así con todos. Intenta dibujar las particiones.

Su generación mediante un procedimiento recursivo se obtiene de esta forma:

Añadimos un 1 a la sucesión y, entonces, basta hacer $C_{n+1} = C_n \times (4n-6)/n$

Otra recursión:

$$C_1 = 1 \quad C_n = C_{n-1}\frac{2(2n-1)}{n+1}, para\ n > 1$$

Para n>2 su fórmula explícita es

$$C_n = \frac{2 \times 6 \times 10 \times \ldots (4n-10)}{(n-1)!}$$

Existen también tres fórmulas directas para calcular el enésimo número de Catalan.

$$C_n = \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{(n+1)!\,n!} = \frac{2^n(2n-1)!!}{(n+1)!}$$

También es útil esta otra:

$$C_n = \binom{2n}{n} - \binom{2n}{n-1}$$

Estos números también equivalen a las formas de introducir paréntesis (que todos encierren dos elementos) dentro de n símbolos. Por ejemplo, para los símbolos abcd existen 5 formas (número de Catalan para n=4) de introducir paréntesis.

((ab)(cd)) (((ab)c)d) (a(b(cd))) (a((bc)d)) ((a(bc)d)

También coinciden, en la Teoría de Grafos, con el número de árboles plantados trivalentes.

Unas recurrencias muy útiles

Quienes usamos a menudo los números poligonales nos encontramos con esta relación de recurrencia de tercer orden:

$$x_n= 3x_{n-1}-3x_{n-2}+x_{n-3}$$

El origen de esta presencia es que se pueden generar con ella los números naturales y sus cuadrados:

Números naturales

Se pueden generar mediante

$$x_1=1,\ x_2=2,\ \ x_3=3,\ x_n= 3x_{n-1}-3x_{n-2}+x_{n-3}$$

En efecto, aquí x_n es **n**, x_{n-1}, **n-1**, luego

$3(n-1)-3(n-2)+n-3=3n-3-3n+6+n-3=n$

Esto demuestra que la recurrencia con estos coeficientes es verdadera.

Constantes

Una constante K sometida a esa recurrencia sigue teniendo el valor de K: $3\times K-3\times K+K=K$

Números cuadrados

En ellos también es válida esta recurrencia. Lo vemos:

$x_{n+1}=(n+1)^2=n^2+2n+1=x_n+2n+1$

$x_{n+2}=(n+2)^2=(n+1)^2+2(n+1)+1=x_{n+1}+2n+3$

Luego, despejando:

$x_{n+2} - x_{n+1} = x_{n+1} - x_n + 2$

$x_{n+2} = 2x_{n+1} - x_n + 2$

De igual forma

$x_{n+3} = 2x_{n+2} - x_{n+1} + 2$

Restamos las dos igualdades y agrupamos:

$x_{n+3} - x_{n+2} = 2x_{n+2} - x_{n+1} + 2 - 2x_{n+1} + x_n - 2$

Despejando:

$x_{n+3} = 3x_{n+2} - 3x_{n+1} + x_n$

Con esto se demuestra la validez de la recurrencia. Por ejemplo:

$11^2=121=3\times10^2-3\times9^2+8^2=300-243+64=364-243=121$

También nos vale un desarrollo directo:

$(n+3)^2=3(n+2)^2-3(n+1)^2+n^2=3n^2+12n+12-3n^2-6n-3+n^2$

$n^2+6n+9=n^2+6n+9$

Identidad que demuestra la recurrencia.

Números oblongos

Siguen la fórmula $n(n+1)=n^2+n$, y al ser la recurrencia propuesta de tipo lineal, también será válida en esa suma de un cuadrado con un natural.

Lo podemos comprobar con los primeros oblongos: 2, 6, 12, 20, 30, 42, …Por ejemplo, 30=3×20-3×12+6=60-36+6=24+6=30

Números triangulares

Al tener un número triangular la fórmula $n(n+1)/2=(n^2+n)/2$, es la mitad de un oblongo, luego admitirá la misma recurrencia. Lo vemos con un ejemplo tomado de la sucesión de números triangulares:

1 , 3 , 6 , 10 , 15 , 21, 28 , 36 , 45 , 55, …

45=3×36-3×28+21=108-84+21=129-84=45

Polinomios de segundo grado

También se generarán de la misma forma. Lo vemos con $P(x)=2x^2-3x+2$:

P(1)=1, P(2)=4, P(3)=11, P(4)=22, P(5)=37, P(6)=56 y P(7)=79

Observamos que P(7)=3×56-3×37+22=168-111+22=190-111=79

Números poligonales

Todo número poligonal es suma de triangulares. Basta ver la imagen:

Esta descomposición hace válida la recurrencia en ellos. En mi publicación sobre estos número se incluye una demostración con la fórmula general, que es un polinomio de segundo grado sin término independiente: $P(n,k)=((k-2)n^2-(k-4)n)/2$

https://www.hojamat.es/publicaciones/poligonales.pdf

En esa publicación figuran otras recurrencias que a veces son más rápidas que la propuesta.

También siguen esta recurrencia los poligonales centrados, de fórmula $POLC(n,k)=(kn^2-kn+2)/2$, por ser también polinomio de segundo grado.

Números piramidales

Si a esta recurrencia que estamos estudiando le aplicamos la fórmula de la suma que se presentó anteriormente, nos permitirá encontrar una recurrencia para números piramidales, que son sumas de poligonales.

Tomamos a1=3, a2=-3 y a3=1 para aplicarlo a la fórmula de la suma

$s_{n+h+1}=(1+a_1)s_{n+h}+(a_2-a_1)\ s_{n+h-1}+ \ldots +(a_h-a_{h-1})\ s_{n+1}-a_h s_n$

$s_{n+4}=4s_{n+3}-6s_{n+2}+4s_{n+1}-s_n$

Lo aplicamos a los números piramidales pentagonales, 1, 6, 18, 40, 75, 126, 196, 288, 405, 550, ...

550=4×405-6×288+4×196-126=550

SUCESIONES CURIOSAS

Sucesión de Recamán

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

(ver https://www.youtube.com/watch?v=h3qEigSSuF0).

Su definición es la siguiente (versión con $a_1=1$):

$a_1=1$

$a_n = a_{n-1} – n$, si este valor es positivo y no figura ya en la sucesión

$a_n = a_{n-1} +n$, en caso contrario.

Sus primeros términos son: 1, 3, 6, 2, 7, 13, 20, 12, 21, 11, 22, 10, 23, 9, 24, 8, 25, 43, 62, 42, 63, 41, 18, 42, 17, 43, 16, 44, 15, 45, 14, 46, 79, 113, 78, 114, … (existe

otra versión que comienza en 0, idéntica a esta en todo lo demás http://oeis.org/A005132)

Sucesión de Golomb

Se trata de esta:

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

http://oeis.org/A001462

También se la conoce como sucesión de Silverman. Es no-decreciente.

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

Lo verás mejor si acompañamos cada valor con su índice:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15														
a(n)	1	2	2	3	3	4	4	4	5	5	5	6	6	6	6	7	7	7	7	8	8	8	8	9	9	9	9	9	10	10	10

La imagen de 1 es 1 por definición. La de 2 es 2 porque en la sucesión figura ese valor dos veces. También el 3

aparece repetido, por lo que a(3)=2. A(4)=3 debido a que aparecen tres cuatros, y así con todos.

Este es un ejemplo muy elegante de *autorreferencia*, pues se define un objeto como si ya estuviera construido, pero sólo lo podemos formar si seguimos la definición.

Si aceptamos la condición de que cada valor ocupe el primer número de orden que esté libre, y que cada nueva imagen es la menor que cumple a(n)>=a(n-1), esta sucesión es única. En efecto, nos ponemos a razonar:

A(1)=1 por definición, luego sólo existirá un 1 en la sucesión, por lo que la imagen de 2 no podrá ser 1. Según las condiciones, ha de ser 2, luego en la sucesión deberá haber un par de 2. Como hemos quedado en que se ocupan los menores números de orden, deberá quedar:

	1	2	3
	1	2	2

Esto significa que a(3)=2, luego también repetiremos el 3 dos veces:

	1	2	3	4	5
	1	2	2	3	3

Obligamos así a que el 4 y el 5 figuren tres veces:

1	2	3	4	5	6	7	8	9	10	11
1	2	2	3	3	4	4	4	5	5	5

Números belgas

Estos números han sido introducidos por Eric Angelini y publicados en el año 2005 en http://oeis.org/A106039. Hay varios tipos, por lo que comenzaremos con los 0-Belgas. Estos números tienen la propiedad de que si a partir del número 0 vamos sumando reiteradamente las cifras (por orden) del número dado, se forma una sucesión que contiene a ese número. Por ejemplo, el 18 es 0-belga, porque a partir del 0 vamos a ir sumando sucesivamente 1, 8, 1, 8,…hasta llegar o sobrepasar el 18: 0, 1, 9, 10, 18, resultando que el mismo 18 es término de la sucesión. Sin embargo, el 19 no lo es, porque se forma la sucesión 0, 1, 10, 11, 20, 21, 30,…al ir sumando sucesivamente 1, 9, 1, 9,… y el mismo 19 es sobrepasado sin pertenecer a la sucesión. Se llaman 0-belgas porque la sucesión la comenzamos en 0, y los primeros son estos:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 17, 18, 20, 21, 22, 24, 26, 27, 30, 31, 33, 35, 36, 39, … http://oeis.org/A106039

Si un número posee 3, 4 o más cifras, estas se irán también sumando de forma sucesiva y ordenada.

Llamaremos *n-belgas* a aquellos números que pertenecen a la sucesión formada al sumar cifras, pero comenzando en el número **n**, siendo n menor que el número dado. Así, estos son los 1-belgas:

1, 10, 11, 13, 16, 17, 21, 23, 41, 43, 56, 58, 74, 81, 91, 97, 100, 101, 106, 110,… http://oeis.org/A106439

Por ejemplo, el 23, comenzando en 1, genera con las cifras 2 y 3 la sucesión 1, 3, 6, 8, 11, 13, 16, 18, 21, 23,…a la que él mismo pertenece.

Se han publicado también los 2-belgas (A106518), los 3-belgas (A106596) y otros.

Sucesión de Mian-Chowla

Esta sucesión se define por recurrencia de dos formas equivalentes:

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

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

Aquí trabajaremos con la primera.

Pertenece al rango de problemas y conjuntos de Sidon, matemático que estudió las cuestiones sobre sumas o diferencias todas distintas, Puedes leer nuestra entrada

http://hojaynumeros.blogspot.com.es/2010/03/jugamos-con-sidon-y-golomb.html

Los primeros elementos son 1, 2 , 4, 8, 13, 21, 31, 45, 66,... http://oeis.org/A005282

Comprobemos la definición con el 8: Los términos anteriores (1, 2, 4) producen las siguientes sumas 2, 3, 4, 5, 6, 8. Deberíamos ahora probar con el siguiente número, el 5, pero este produce la suma 1+5=6, que ya está en la lista, luego no es válido. Probamos el 6, y la suma 2+6=8 lo invalida. El 7 tampoco pertenece a la sucesión, ya que 1+7=8 pertenece a la lista de sumas. Probamos el 8, que produce las sumas 9, 10 y 12, no incluidas en la lista, luego el 8 es válido y se incorpora a la lista.

La permutación Yellowstone

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

factores primos con el 2 pero no con el 3. Tenemos ya 1, 2, 3 y 4.

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

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

Esta sucesión no es creciente, y algunos números tardan en aparecer, como el 10. Se llama permutación porque se ha demostrado que todos los números naturales aparecen una vez

(Ver https://cs.uwaterloo.ca/journals/JIS/VOL18/Sloane/sloane9.pdf)

Hipotenuseando

Se presenta en este apartado la sucesión http://oeis.org/A104863

10, 30, 31, 43, 53, 68, 86, 109, 138, 175, 222, 282, 358, 455, 578, 735, 935, 1189,…

En ella, a partir de los valores a(1)=10 y a(2)=30, se van formando los siguientes como **la parte entera de la raíz**

cuadrada de la suma de cuadrados de los dos anteriores.

Así, el tercer elemento es igual a

ENTERO(RAIZ(10^2+30^2))=ENTERO(RAIZ(1000))=ENTERO(31,62)=31.

Prueba a justificar que el siguiente es 43.

Esta definición equivale a que cada término es la hipotenusa truncada correspondiente a los términos anteriores tomados como catetos. Por eso le hemos llamado a esta sucesión la de “hipotenusear”. Su expresión recurrente sería:

$$a_n = Int\left(\sqrt{{a_{n-2}}^2 + {a_{n-1}}^2}\right)$$

Esta sucesión presenta algunas características que le hacen merecer este estudio:

(1) El uso de la parte entera obliga a renunciar a las fórmulas teóricas. De hecho, en términos avanzados de la sucesión, el cumplimiento del Teorema de Pitágoras es deplorable. Observa este ejemplo, en el que a(n-2)=8348, a(n-1)= 10618 y a(n)=13506. Si elevamos al cuadrado obtenemos:

13506^2=182412036

8348^2+10618^2=182431028

Restamos y nos queda un error de 18992 unidades. Así que las hipotenusas que obtengamos con esta recurrencia **no son tales**, aunque seguiremos llamándolas así.

(2) Como también ocurre en las recurrencias lineales, el cociente entre dos términos consecutivos se va estabilizando y tiende a un límite. Esto nos permite "razonar en el límite", aunque sepamos que es una técnica aproximada, que sólo nos valdrá para explicar (y no demostrar) algunas conjeturas que se han afirmado para esta sucesión y otras similares.

(3) La sucesión presentada es sólo un caso particular de toda una familia en la que podemos fijar a(1) y a(2) como deseemos. La mayoría de las propiedades se mantendrán. Vemos la primera:

Conjetura: El límite del cociente a(n+1)/a(n) es la raíz cuadrada del número áureo.

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \sqrt{\emptyset} = 1{,}27201965\ldots$$

La llamamos conjetura por causa de la parte entera, que nos impide mejores razonamientos.

Números de Ulam

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

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

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

Puedes ampliar este concepto en las páginas

https://es.wikipedia.org/wiki/N%C3%BAmeros_de_Ulam

http://www.grupoalquerque.es/mate_cerca/paneles_2014/221_Numeros%20de%20Ulam.pdf

https://www.gaussianos.com/feliz-ano-2012/

El 1 y el 2 se toman de forma arbitraria. El siguiente deberá ser el 3, ya que 3=1+2 de forma única. También está claro que el cuarto debe ser 4=1+3, pues 4=2+2 no sería válido por ser iguales los sumandos.

Deberíamos rechazar el 5, pues 5=1+4=2+3. El 6 sí nos vale, pues 6=2+4, siendo no válida la suma 6=3+3.

Por tanto, los primeros términos de la sucesión de Ulam serán 1, 2, 3, 4, 6. Es sencillo buscar los siguientes: 8, 11, 13, 16, 18, 26,…

SUCESIONES COMPLETAS

Este concepto se relaciona con la posibilidad de que los elementos de una sucesión de números naturales, finita o infinita, generen otros números, a partir de sumas, con o sin repetición.

Una sucesión de números naturales se llama **completa** cuando cualquier otro número natural se puede escribir como suma de elementos de esa sucesión sin repetir ninguno.

El ejemplo básico más popular es el de las potencias de 2, que da lugar al sistema binario de representación de los números. En efecto, la sucesión 1, 2, 4, 8, 16, … permite representar cualquier número como suma de algunos términos, sin repetición.

Vemos un ejemplo: representar el número 53:

Buscamos el término de la sucesión más cercano a 53 y menor que él, que es el 32, tomamos nota y restamos: 53-32=21. Reiteramos: 21-16=5, 5-4=1, con lo que obtenemos 53=32+16+4+1, que da lugar a la representación binaria 110101.

Este ejemplo nos abre camino para caracterizar las sucesiones completas. Podemos dar tres condiciones para que una sucesión sea de este tipo:

- El primer término ha de ser 1, $a_1=1$

- Aunque no es imprescindible, pero sí algo operativo, la sucesión debe presentar un orden creciente.
- Si llamamos s_n a la suma de los n primeros términos de la sucesión, se debe cumplir: $s_{n-1} \geq a_n - 1$ para todo $n \geq 1$

La primera condición es imprescindible para poder generar todos los números y que los algoritmos tengan parada. Por ejemplo, los números pares no son completos, pues nunca pueden generar un impar.

La segunda se incluye para que tengan sentido los algoritmos.

La tercera es fundamental, porque garantiza que se pueda avanzar en descubrir sumandos hasta llegar, si es necesario al 1.

CUESTIONES DIOFÁNTICAS

Ecuación diofántica

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

Sistema diofántico

Es aquel que está formado por ecuaciones diofánticas.

ECUACIÓN DIOFÁNTICA LINEAL

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

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

Efectivamente, si consultas la teoría de fracciones continuas verás que la diferencia entre dos reducidas consecutivas equivale a una fracción de numerador la

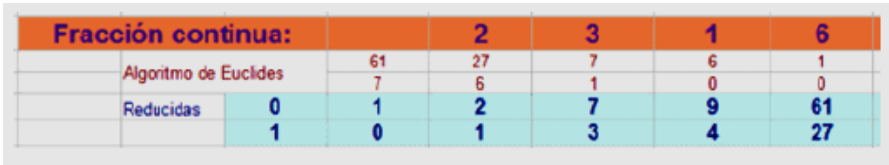
unidad y de denominador el producto de sus denominadores. Esta propiedad también se cumple entre la última reducida y la fracción dada.

Vemos cómo se aprovecha esta propiedad para resolver la ecuación diofántica lineal

Sea, por ejemplo, la ecuación 244X+108Y=112.

Simplificamos: 61X+27Y=28, con MCD(61,27)=1

Buscamos las reducidas de la fracción 61/27 y elegimos la última 9/4



Fracción continua:			2	3	1	6
Algoritmo de Euclides		61	27	7	6	1
		7	6	1	0	0
Reducidas	0	1	2	7	9	61
	1	0	1	3	4	27

Se cumplirá, según la propiedad citada, que 61×4-27×9=1, luego 4 y -9 serán las soluciones de 61X+27Y=1. Bastará multiplicar por el término independiente 28 para obtener una solución: X=4×28 = 112 e Y=-9×28 = -252

Las demás soluciones se obtienen mediante las paramétricas

X=112-27v
Y=-252+61v

Si se desean soluciones positivas deberemos ajustar el parámetro v

ECUACIÓN PITAGÓRICA

Es la que tiene la forma $x^2 + y^2 = z^2$

Llamaremos soluciones primitivas x_0, y_0 y z_0 a aquellas que no tienen divisores comunes. Se puede demostrar que z_0 es impar y las otras dos, una par y otra impar.

Las soluciones primitivas se obtienen mediante las fórmulas

$X = m^2 + n^2$
$Y = m^2 – n^2$
$Z = 2mn$

con m y n primos entre sí y de distinta paridad, con m>n.

Si multiplicamos cualquier conjunto de soluciones primitivas por un mismo número, obtendremos infinitas soluciones.

FRACCIONES CONTINUAS

Definición

Llamamos fracción continua a la expresada de esta forma:

$$a+\cfrac{1}{b+\cfrac{1}{c+\cfrac{1}{d...}}}$$

donde a es entero y b, c…son enteros positivos llamados cocientes (o cocientes parciales). Toda fracción ordinaria se puede expresar de esta forma, y todo número irracional admite aproximaciones mediante desarrollos de este tipo. Si se exige que el último cociente sea distinto de 1 esta representación es única.

Las fracciones continuas también se expresan mediante el conjunto ordenado de los cocientes: [a, b, c, d...]

Fracción ordinaria

Los cocientes a, b, c,… son los que aparecen en el algoritmo de Euclides para el cálculo del m.c.d. de dos números. Así, por ejemplo, para encontrar el m.c.d. de 345 y 1280, en el algoritmo se obtienen los siguientes cocientes:

	3	1	2	2	4	2	0	0	0
1280	345	245	100	45	10	5	0	0	0
245	100	45	10	5	0	0	0	0	0

En el desarrollo mediante fracciones continuas de 1280/345 vuelven a aparecer los mismos cocientes 3,1,2,2,….¡porque se trata del mismo algoritmo orientado de forma diferente! En la siguiente imagen, capturada de la hoja de cálculo **fraccont.ods**,

Numerador	1280	Fracción continua:	3	1	2	2	4	2
Denominador	345		3	4	11	26	115	256
			1	1	3	7	31	69

puedes comprobar la evidente igualdad de la serie de

cocientes. Comprueba que, efectivamente, es válido este desarrollo:

$$\frac{1280}{345} = 3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{4 + \frac{1}{2}}}}}$$

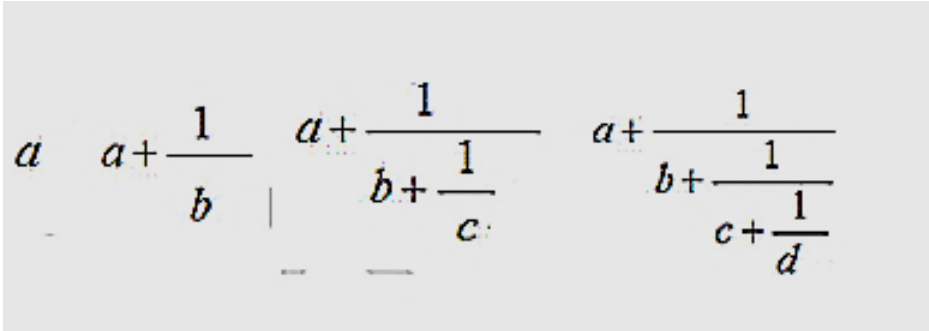
Estos desarrollos son finitos, porque así lo es el conjunto de los coeficientes del algoritmo de Euclides. Veremos más adelante que en el caso de irracionales son infinitos. En ambos casos se puede demostrar que son únicos.

Convergentes

Para un desarrollo cualquiera en fracción continua

$$a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d...}}}$$

se llaman reducidas o convergentes a los desarrollos



a los que nombraremos como C_0, C_1, C_2, C_3... En el caso del ejemplo obtendríamos:

3=3; 3+1/1=4; 3+1/(1+1/2)=11/3…

Cumulantes

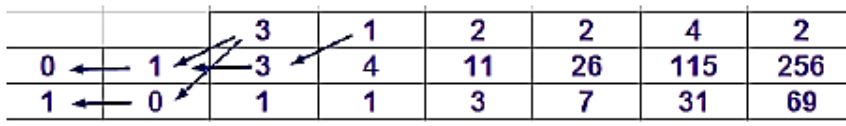
Los convergentes son fundamentales en los desarrollos de las funciones continuas, como se verá más adelante. El algoritmo más sencillo para crearlos consiste en comenzar con el cálculo de los cocientes mediante el algoritmo de Euclides y después añadir dos filas de numeradores y denominadores para las convergentes tal como se ve en la imagen, comenzando con 0 y 1 para los numeradores y 1, 0 para los denominadores. En el ejemplo 1280/345 quedaría así

		3	1	2	2	4	2
0	1						
1	0						

Después las fracciones reducidas o convergentes se obtienen mediante un algoritmo clásico llamado de “los cumulantes”. Consiste en construir dos sucesiones recurrentes del tipo

$P_n = p_{n-1} \times a_n + p_{n-2}$

Se multiplica cada cociente superior por el último numerador o denominador, sumando posteriormente el penúltimo:



		3	1	2	2	4	2
0	1	3	4	11	26	115	256
1	0	1	1	3	7	31	69

En realidad lo que se hace es "deshacer" las operaciones del Algoritmo de Euclides.

Las convergentes o reducidas poseen varias propiedades importantes. Destacamos alguna:

- Todas las reducidas son fracciones irreducibles.
- Las de índice par (comenzando por el cero) forman una sucesión creciente y las de orden impar decreciente, siendo cota de ambas la fracción ordinaria que se desarrolla. Por tanto, las de orden par son mayores que las de orden impar.
- La última reducida equivale a la fracción original simplificada. Así 1280/345 = 256/69. Las demás son aproximaciones por exceso o defecto.

- La diferencia entre dos reducidas consecutivas equivale a la unidad positiva o negativa dividida entre el producto de sus denominadores. También podemos expresarlo como que el producto en cruz de sus numeradores y denominadores es igual a 1 o a -1.

Aproximación diofántica

Es evidente que las reducidas aproximan la fracción que se haya expresado en forma continua. Así, 115/31 es una aproximación a 256/68 en el ejemplo anterior, Lo interesante es que también pueden aproximare a los números irracionales. Por ejemplo, la fracción 3650401/2107560 es una muy buena aproximación de la raíz cuadrada de 3 (coinciden en los trece primeros decimales)

Cualquier número expresado en forma decimal puede representarse mediante una fracción continua. Si el número es racional, ésta será finita, pero si es irracional no podrá serlo, y tendríamos que prolongar el desarrollo de la fracción continua hasta el infinito. En los siguientes párrafos veremos cómo.

Un caso muy interesante es el de los irracionales cuadráticos, que, como demostró Lagrange, presentan desarrollos periódicos.

¿Cómo desarrollar un decimal cualquiera en fracción continua exacta (caso racional) o aproximada (si es

irracional)?

La idea es: separamos la parte entera y la parte decimal del número N=e+d, y la decimal la expresamos así: N=e+1/(1/d). Volvemos a separar parte entera y decimal de 1/d y reiteramos, con lo que irán apareciendo los cocientes enteros de una fracción continua.

Probamos con la raíz cuadrada de 3. Los cálculos serían:

1,73205080757 = 1+ (1/(1/1,73205080757) =
1+ 1/1,36602540378 = 1+ 1/(1+1/2,73205080760) =
1+1/(1+1/(2+1/1,36602540378) = ….

Al salir este último número se descubre la periodicidad, luego 1,73205080757 equivale a la fracción continua

[1,1,2,1,2,1,2,….] que es periódica por tratarse de un irracional cuadrático.

A continuación destacamos algunos desarrollos importantes:

$$\sqrt{2} = [1,2,2,2,2...]$$

Se llaman números de Pell a los denominadores de este desarrollo en fracciones continuas de la raíz cuadrada de 2.

Números metálicos

Son soluciones de ecuaciones cuadráticas del tipo $x^2 - bx - 1 = 0$

Número de oro

$$\phi = \frac{\sqrt{5}+1}{2} = [1,1,1,1,1...]$$

Es solución de la ecuación $x^2-x-1 = 0$

Número de plata

$$\varphi = 1+\sqrt{2} = [2,2,2,2...]$$

Es solución de la ecuación $x^2-2x-1 = 0$

Número de bronce

$$\psi = \frac{\sqrt{13}+3}{2} = [3,3,3,3...]$$

Es solución de la ecuación x^2-3x-1 = 0

Ecuación de Pell

Una aplicación importante de las fracciones continuas es la resolución de la ecuación de Pell

Se llama ecuación de Pell (por error, porque Pell no la estudió) a la ecuación diofántica cuadrática $X^2 - DY^2 = 1$, con X e Y variables enteras y D número entero positivo no cuadrado perfecto. Existe una variante con el segundo miembro -1 que se resuelve de forma similar, con algunas restricciones, y también se consideran los casos en los que se trate de cualquier número entero.

En su resolución hay que distinguir dos problemas:

Primera solución

Una primera solución no es difícil de encontrar en general.

(a) Puedes acudir a un simple tanteo entre cuadrados perfectos. Por ejemplo, una solución de $X^2 - 6Y^2 = 1$ es

$X_0=5$ $Y_0=2$. Con una hoja de cálculo no es tarea muy complicada.

(b) Las fracciones continuas también son útiles en la resolución de esta ecuación. Basta para ello desarrollar la raíz cuadrada de D mediante ellas y, según vimos en una sección anterior, aprovechar la periodicidad del desarrollo. En el caso de la ecuación de Pell basta tomar las reducidas anteriores a la finalización del primer periodo.

En la imagen observarás que la solución $X_0=5, Y_0=2$ aparece antes del final del primer periodo [2,4] en el desarrollo por fracciones continuas. Después siguen otras: X=49, Y=20, X=485, Y=198, etc.

En nuestro modelo de hoja de cálculo que recomendamos más abajo basta escribir el valor de D y el segundo miembro +1 ó -1 y la hoja se encarga de desarrollar la raíz cuadrada de D mediante fracciones continuas:

Siguientes soluciones

Según la teoría del anillo Q(√D), que no podemos desarrollar aquí, las primeras soluciones, escritas como X0+Y0 (√D) constituyen una unidad del anillo, y también lo serán todas sus potencias, por lo que las siguientes soluciones provendrán de los desarrollos de las expresiones

$$\left(X_0 + Y_0\sqrt{D}\right)^n$$

agrupando después los términos que no contienen el radical como valor de Y y los que sí lo contienen como valor de X. Este método puede ser fatigoso, por lo que es mejor ir obteniendo las distintas soluciones por recurrencia. En efecto, de la anterior consideración se deduce que

$$\left(X_n + Y_n\sqrt{D}\right) = \left(X_{n-1} + Y_{n-1}\sqrt{D}\right)\left(X_0 + Y_0\sqrt{D}\right)$$

O bien, separando términos:

$$X_n = X_{n-1}X_0 + Y_{n-1}Y_0D$$

$$Y_n = X_{n-1}Y_0 + Y_{n-1}X_0$$

Estas son las fórmulas que hemos usado en la hoja de cálculo.

Puedes consultar la búsqueda de la primera solución por fracciones continuas y la recurrencia para las siguientes en las hojas de cálculo pell.ods para Calc y pell.xls para Excel

Por ejemplo, intenta resolver esta cuestión: ¿Qué cuadrado perfecto de diez cifras, al quitarle una unidad se puede descomponer en cinco cuadrados perfectos idénticos?

SUMAS DE CUADRADOS

CONDICIONES DE FERMAT

Hay números que se pueden descomponer en suma de dos cuadrados, pero ¿de cuántas formas?

Para conseguir una respuesta a la pregunta formulada se necesitaron esfuerzos de varios matemáticos, pero todo comenzó con Fermat y su Teorema de Navidad (lo comunicó a Mersenne el 25 de Diciembre de 1640, pero no lo demostró), y que actualmente expresamos así:

Un número primo se puede descomponer en suma de dos cuadrados x^2+y^2 de números enteros si y sólo si es el número 2 o bien es congruente con 1 módulo 4 (es decir, si es de la forma 4n+1).

El teorema directo es difícil de demostrar, y lo ha sido a lo largo de siglos mediante diversas técnicas (descenso infinito, enteros gausianos, etc.), siendo Euler el primero que lo logró. El inverso está a nuestro alcance. Inténtalo:

Un número primo congruente con 3 módulo 4 no puede descomponerse en suma de dos cuadrados de números enteros.

Gauss, en la sección 182 de sus Disquisitiones arithmeticae destacó que esa descomposición es única,

salvo orden y signo. Los dos números x e y han de ser primos entre sí ¿por qué?

De este hecho podemos obtener un criterio marginal: Si un número de la forma 4n+1 no se puede descomponer en dos cuadrados o bien lo puede de más de una forma, no es primo.

Esta propiedad de poder descomponerse en suma de dos cuadrados se mantiene si multiplicamos dos números primos de este tipo, y además se puede duplicar el número de posibles sumas. Así, si 13 = 2^2+3^2 y 5 = 2^2+1^2, al multiplicarlos obtenemos:

65 = 13×5 = 8^2+1^2 = 7^2+4^2

Esta propiedad se desprende de la famosa identidad:

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

que nos viene a decir que este producto también es suma de dos cuadrados y además de dos formas distintas (si los sumandos son distintos):

65 = $(2\times2+3\times1)^2$ +$(2\times1-3\times2)^2$ = 7^2+4^2 (obsérvese que en el cálculo se ha obtenido -4 y no 4)

65 = $(2\times2-3\times1)^2$ +$(2\times1+3\times2)^2$ = 8^2+1^2

Ocurre lo mismo si se multiplica el número primo por 2 (elemental ¿no?)

Estas propiedades se resumen en un criterio que no vamos a desarrollar aquí, y es que sólo se pueden descomponer en cuadrados los números en los que los factores primos del tipo 4n+3 figuren en su descomposición con exponente par. Gauss fue más allá en esa sección 182, pues dio una fórmula para contar el número de formas diferentes en las que se descompone un número en suma de dos cuadrados con base no negativa:

$$N = ES[(\alpha+1)(\beta+1)\ldots(\delta+1)/2]$$

donde ES significa “mínimo entero igual o superior” y los factores que le siguen se corresponden con los exponentes de los factores del tipo 4n+1 aumentados en una unidad. La fórmula, como advierte Gauss, sólo es válida si los factores del tipo 4n+3 forman un cuadrado perfecto.

Así, por ejemplo, el número 325=52×13 se deberá descomponer en

N=ES((2+1)(1+1)/2)=ES(3×2/2)=ES(3)=3

En efecto, $325=1^2 + 18^2 = 6^2 + 17^2 = 10^2 + 15^2$ (tres formas distintas)

Y el número 6664 sólo de una forma, pues 6664 = 23×72×17 y aplicando la fórmula nos daría

N=ES(1+1)/2 = ES(1)=1, y su descomposición única es $6664=42^2+70^2$

Actualmente se prefiere considerar todas las sumas de cuadrados posibles, incluyendo bases negativas y teniendo en cuenta el orden. Esto multiplica por 8 el número de soluciones cuando x es distinto de y y ambos son no nulos, y por 4 en caso contrario. Así, el 13 presentaría ocho soluciones:

$13= 2^2+3^2 = (-2)^2+3^2 = 2^2+(-3)^2 = (-2)^2+(-3)^2 = 3^2 +2^2 =(-3)^2 +2^2 = 3^2 +(-2)^2 = (-3)^2 +(-2)^2$

Y el 16, cuatro: $16 = 4^2+0^2 = (-4)^2+0^2 =0^2 + 4^2 = 0^2 + (-4)^2$

Igualmente, 8 presentaría también 4: $8 = 2^2+2^2 = (-2)^2+2^2 =2^2 + (-2)^2 = (-2)^2 + (-2)^2$

DIVISIBILIDAD

FUNDAMENTOS

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.

Todo este tema se puede extender a números enteros.

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 (o entero).
- **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**
- El conjunto de divisores de un número es finito.

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.

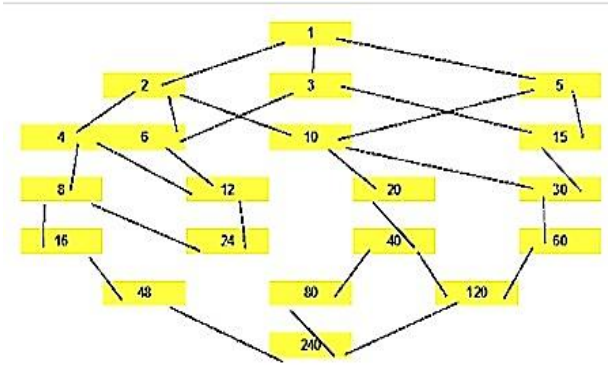
Múltiplo

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**
- El conjunto de múltiplos es infinito.

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



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

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.

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

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) 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).*

RETÍCULOS DE LOS DIVISORES DE UN NÚMERO

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∧b=b** y que **1∨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∨a'=E y a∧a'=Φ.

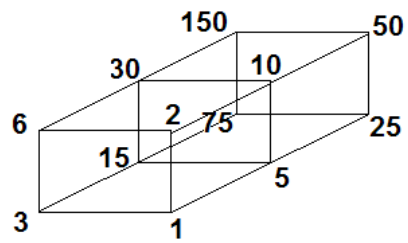
El retículo de los divisores de N es complementado si y sólo si N es libre de cuadrados.

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:



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:

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

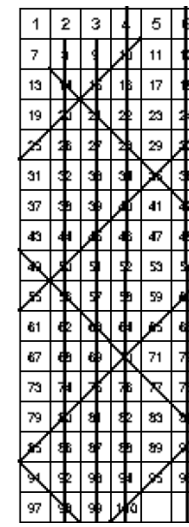
El matemático ruso Chebychev acotó mediante dos constantes esta aproximación.

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.

Teorema de Euclides sobre la infinitud de los primos

Para demostrar que el conjunto de números primos es infinito, Euclides acudió a la demostración por el absurdo: supuso lo contrario, que el conjunto fuera finito, es decir, p_1, p_2, p_3,…p_k. En ese caso, formó el número

$P= p_1 \times p_2 \times p_3 \times ,\ldots \times p_k+1$

Este número no sería divisible entre ningún primo conocido, pues siempre existiría un resto igual a 1. O sería primo, o tendría un divisor primo distinto de los conocidos y mayor que ellos. En ambos casos, existiría un número primo mayor que los conocidos, por lo que su conjunto tendría un primo más. Reiterando, nunca se llegaría a un último primo.

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, es decir, compuesto.

- 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

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

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* si los factores son distintos. 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

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

Luego el número de divisores será

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

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 $1+p+p^2+\ldots p^k$:

	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

Valuación de un número primo

Este concepto se refiere a la *p-adic valuation*, ya que existen otras definiciones en contextos diferentes. Nos referiremos a ella simplemente como *valuación*.

*Llamaremos valuación de un número primo **p** respecto a otro número natural **N** no nulo al máximo exponente **e** de p tal que $\boldsymbol{p}^{\boldsymbol{e}}$ sea divisor de N.*

El cociente entre N y valuacion(p) será primo con p. Es una forma de apartar las potencias de p de entre los divisores de N.

Por ejemplo, valuación de 2 respecto a 48 es 3, porque 8=23 es la máxima potencia de 2 que divide a 48.

Es fácil razonar que será una función aditiva, por ser un exponente: la valuación de un producto coincidirá con la suma de valuaciones.

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

$22! = 2^{19}\times3^{9}\times5^{4}\times7^{3}\times11^{2}\times13\times17\times19$

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)

FUNCIONES SOBRE DIVISORES

TAU: 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

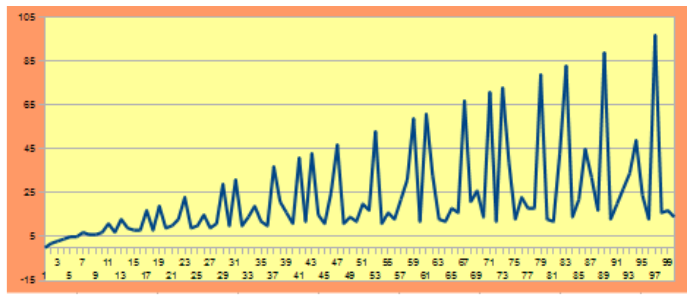
OMEGA: Cuenta los factores primos de un número sin tener en cuenta las multiplicidades. Así, omega(60)=3

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).

SIGMA $\sigma(n)$ (Suma de divisores)

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

Si **n** es primo, $\sigma(n)=n+1$. Si es perfecto, $\sigma(n)=2n$. Si es un número primario p^e, la función $\sigma(n)$ 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 $\sigma(n)$ 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 $\sigma(a.b)=\sigma(a).\sigma(b)$. 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 de cuadrados

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: $80=4^2\times5$, $121=11^2\times1$, $90=3^2\times10$, $15=1^2\times15$

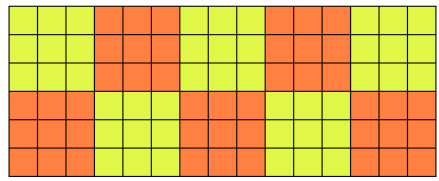
Podemos llamar parte cuadrada PC(N) a la primera y parte libre PL(N) a la segunda (se llama *core* en inglés y podemos traducir por “núcleo”) No se debe confundir con el *radical* de N, que es el mayor divisor de N que está libre de cuadrados.

Tendremos que:

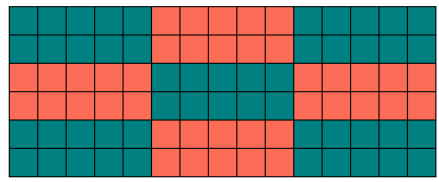
En un cuadrado perfecto PL(N)=1, en un número libre de cuadrados PC(N)=1 y en el resto de números ambos serán mayores que la unidad. En este caso los podemos llamar “cuadrables”, porque admiten su representación como un embaldosado de estructura cuadrada (las mismas filas que columnas), o bien como uno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

Así, el número $90=3^2\times10$ es cuadrable, y admite estas dos estructuras:

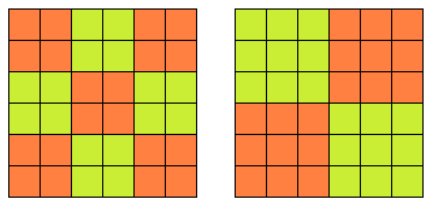
Rectangular con baldosas cuadradas



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)≥OMEGA(N).

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.

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: $S(M)/M=S(A)\times(k+1)/(A\times k)= S(A)/A\times((k+1)/k)>S(A)/A$, 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,

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

aunque existen para construir algunos (Ver Thabit idn Qurra)

- No se sabe si su número es finito o infinito.

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

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

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, …

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

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.

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

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 $N=36=2^2\times3^2$, 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 $2^2\times5^2\times3^3$. 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, …

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, …

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 $\mathbf{N=(a'\times k)^2b^3} = (a'^2\times b^3)\times k^2$. 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 esta sucesión:

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, …

(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, …

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.

Números esfénicos

Los números esfénicos (del griego sphen, “cuña”) son aquellos naturales que equivalen a un producto de tres números primos diferentes, como 42=2×3×7. Si los factores son distintos, el número será “libre de cuadrados” y su número de divisores (función TAU) será 8, porque se calcula multiplicando los exponentes de sus factores primos aumentados todos en una unidad. Así, TAU(42)=(1+1)(1+1)(1+1)=2×2×2=8.

Todos los números esfénicos tienen ocho divisores.

Así, los divisores de 42 son: 42, 21, 14, 7, 6, 3, 2 y 1

La afirmación inversa no es cierta. Por ejemplo, 24 no es esfénico ($24=2^3\times3$) y tiene ocho divisores, pues TAU(24)=(3+1)(1+1)=8.

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

$390 = 364+16+8+2 \equiv 81 \times 81 \times 9 \times 9 \equiv 1 \pmod{91}$;

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, …

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,…

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, …

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, …

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, …

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,…)

“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, …

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, 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 $N=2^i\times3^j$ con $i,j\geq0$.

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 $1=2^0\times3^0$ 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.

N**úmeros 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 primeros son:

1, 1, 2, 6, 24, 1, 720, 3, 80, 12, 3628800, 2, 479001600, 360, 8, 45, 20922789888000, 40, 6402373705728000, 6, 240, 1814400, 1124000727777607680000, 1, 145152, 239500800, 13440, 180, 304888344611713860501504000000, …

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, $\sigma(p)=1+p$, 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.

También recibe el nombre de *totiente* o *totient* en inglés.

p(n) (Primos hasta n)

Representa cuántos números primos hay no superiores a **n**. También se representa como **π(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 publicación:

- ¿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?

COMPLEMENTOS Y CURIOSIDADES

ANTIDIVISORES

Todo número entero positivo N (he excluido los negativos porque no tienen interés en este estudio) posee divisores. Si es primo, serán el 1 y él mismo, y, en otro caso, presentará todo un conjunto de divisores.

Siempre existirán números enteros positivos menores que N que no sean divisores de él (salvo el caso de 2). A estos números les llamamos *no divisores* de N, como sería, por ejemplo, N-1.

Podemos considerar un divisor de N como un número K tal que al conjunto K, 2K, 3K, 4K, ... pertenece N. Esto parece trivial, pero si aplicamos la idea a un no divisor, esa sucesión sobrepasará N, y alguno de los múltiplos de K será el más cercano a N. Unos quedarán muy "cerca" de N, como, por ejemplo, si N=21, su no divisor 5, acercará un múltiplo a una unidad de él, ya que $21=4\times5+1$.

Un antidivisor K de N se define como el no divisor que se "acerca" a N dejando intervalos iguales entre N y dos múltiplos consecutivos de K. Por ejemplo, 10 es un antidivisor de 55, porque no es divisor de él, pero 55 equidista de dos de sus múltiplos: $50<55<60$, con 55-

50=60-55. Una ligera reflexión nos indica que, si K es impar, no es posible la equidistancia, y se permite una diferencia de 1.

La aproximación intuitiva anterior se puede concretar en la siguiente definición, que se aplica de forma distinta si K es par o si es impar:

Si K es par y no divisor de N, será antidivisor si N MOD K=K/2

Si K es impar, diremos que es antidivisor de N si N MOD K=(K±1)/2

Por esta simetría en los dos intervalos, también se llama no divisores insesgados a los antidivisores.

Unos ejemplos: 14 es antidivisor de 147, porque los múltiplos de 14 140 y 154 rodean a 147 con 7 unidades a cada lado: 147-14×10=14×11-147. Más directo, 147 MOD 14=14/2

El número impar 7 es antidivisor de 25, porque lo rodea con un intervalo de 3 y otro de 4: 25-7×3=4 y 7×4-25=3. También; 25 MOD 7 = INT(7+1).

POLIDIVISIBLES

Un número se llama polidivisible (aquí se limitará el estudio a base 10) cuando al recorrer sus cifras de

izquierda a derecha, las dos primeras forman un múltiplo de 2, las tres primeras, de 3, las cuatro de 4, y así sucesivamente. Por ejemplo, 126006 es polidivisible, porque 12=2×6, 126=3×42, 1260=4×315, 12600=5×2520, 126006=6×21001. Se supone que no se han escrito ceros a la izquierda, o lo que es lo mismo, que la primera cifra es no nula.

Puedes comprobar la afirmación de Wikipedia de que 381654729 es polidivisible.

DIVISORIAL

Llamaremos *divisorial* de un número al producto de sus divisores, (según OEIS WIKI, sin revisar). Su cálculo es muy sencillo, porque los divisores de N se presentan por pares cuyo producto es N. Por ejemplo, en 45 se da que 45×1=15×3=9×5=45. El producto total, o divisorial, será 45^3=91125.

Si TAU(N) es el número de sus divisores, se tendrá que el número de pares será TAU(N)/2 si TAU es par y (TAU(N)+1)/2 si es impar, porque este último caso se dará en los cuadrados, y la RAIZ(N) se contaría repetida. Por ejemplo, el divisorial de 36 será 36×18×12×9×6×4×3×2×1=10077696, pero si lo ordenamos por pares, la raíz cuadrada estaría repetida:

36	1
18	2
12	3
9	4
6	6
60466176	

Nos resultaría un producto seis veces mayor. Habría que suprimir el 6 sobrante, con lo que resultaría ese 6 multiplicado por los pares restantes, que forman TAU(N). Tendríamos $6\times36\times36\times36\times36=36^{9/2}$

Por tanto, en el caso par y en el caso impar la fórmula adecuada es

$$\pi(n) = n^{\tau(n)/2}$$

Hemos seguido la nomenclatura usual de π(n) para el divisorial.

En el caso de 45 nos daría $45^{6/2}=45^3=91125$

En el caso de 36 existen 9 divisores, luego tendríamos $36^{9/2}$= 10077696.

NÚMEROS PRIMOS DE PIERPONT

Definición y primeras consecuencias

Un **número primo de Pierpont** es un número primo de la forma $\mathbf{2^u3^v+1}$, donde u y v han de ser enteros no negativos. Esto nos lleva a consideraciones muy sencillas:

El exponente **u** no puede ser cero, pues la expresión sería par y, por tanto, no representaría a un número primo. De hecho, si v=0, deberá ser potencia de 2. La razón está en que una suma de potencias impares es divisible entre la suma de sus bases. Por ejemplo, $(X^5+y^5)/(x+y)=x^4-x^3y+x^2y^2-xy^3+y^4$. Si el exponente poseyera un factor primo distinto de 2, podríamos descomponer la potencia como "potencia de potencia", y aislar el número impar. Por ejemplo 2^{12} se podría expresar como 2^2 y luego elevado a 3, con lo que construiríamos una suma de potencias impares, y no podría ser primo. Todo este razonamiento nos lleva a que si v=0, **los primos de Pierpoint serían también de Fermat**.

NÚMEROS BOGOTÁ

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

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

PRIMOS BRASILEÑOS

Se llaman así porque se popularizaron en Brasil. Se trata de números primos que se pueden formar con la suma de las primeras potencias de un número, es decir, cuándo una suma del tipo $1+n+n^2+n^3+n^4+n^5+\ldots$es un número primo. No consideraremos el caso en el que un primo **p** sea igual a **1+n**, ya que esto lo cumplen todos los primos.

Esta cuestión equivale a la búsqueda de números primos que sean “repitunos” (formados sólo con la cigfra 1), en una base de numeración dada. Por ejemplo, 31(10=111(5, ya que las tres cifras 1 provienen de la igualdad $31=1+5+5^2$.

NÚMEROS REFACTORIZABLES

Estudiando el número 2025 se descubre que tiene 15 divisores, y que este número 15 es divisor de 2025. Por eso, cumple la definición de **número refactorizable o “tau”**, porque si llamamos función TAU al número de divisores de N, en estos números se cumple que N/TAU(N) es un entero. En el caso de 2025 se cumple que 2025/15=135.

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

Para descubrir si un número es de este tipo, habrá que calcular TAU y efectuar el cociente N/TAU(N) para analizar si es entero.

El cálculo de TAU es bastante simple:

$TAU(N)=(1+a_1)(1+a_2)\ldots(1+a_k)$, donde a_1, a_2, …a_k son los exponentes de los factores primos de N.

PRIMOS CUBANOS

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

Los primeros primos cubanos son *7, 19, 37, 61, 127, 271, 331, 397, 547, 631, 919, 1657…*

Por ejemplo, $7=2^3-1^3$, $37=4^3-3^3$

ARITMÉTICA MODULAR

CONGRUENCIAS

NÚMEROS CONGRUENTES

Definición

Dos números enteros **a** y **b** se llaman **congruentes** respecto a un número natural **m** llamado **módulo**, cuando **a - b** es divisible entre **m**, y se escribe **a ≡ b (mod m)**

También se puede expresar esta situación como que ambos números dan el mismo resto al dividirlos entre m.

A la relación que se establece entre ambos la llamaremos **congruencia**. Por ejemplo, son válidas las congruencias 8 ≡ 13 (mod 5) 129 ≡ 229 (mod 100)

Este concepto fue introducido por K.F. Gauss en su obra Disquisitionae Arithmeticae

Propiedades

- Para que sea **a ≡ b (mod m)** es necesario y suficiente que exista un **h** entero tal que **a = b + hm**.
- Todos los múltiplos de m son congruentes con 0.
- Si **a≡b (mod m)** y **a** es primo con **m**, también lo será **b**.
- Si **a≡b (mod m)**, entonces **an≡bn (mod m)**
- Ley de simplificación: si **ac≡bc (mod m)** y es **d** el MCD de c y m, se cumple que **a≡b (mod m/d)** *(un factor se puede simplificar si el módulo se divide entre su MCD con ese factor)*

Esta ley tiene casos particulares interesantes:

- Si n divide a a,b y m, y a≡b (mod m), se tiene que **a/n ≡ b/n (mod m/n)**
- Si n divide a a y b y es primo con m, y además a≡b (mod m), se tiene que **a/n ≡ b/n (mod m)**
- Si n divide a a y b y el MCD(n,m)=d, y además ≡b (mod m), se tiene que **a/n ≡ b/n (mod m/d)**
- Si **a≡b (mod m)** y **c≡d (mod m)**, entonces:
- a+b ≡ c+d (mod m)
- a-b ≡ c-d (mod m)
- a×b ≡ c×d (mod m)

- $ab \equiv cd \pmod{m}$
- Si dos números **a** y **b** son congruentes respecto a varios módulos, también lo serán respecto a su mínimo común múltiplo.
- Dos números congruentes respecto a un módulo presentan el mismo MCD respecto a él.
- Si dos números **a** y **b** son congruentes respecto a un módulo **m**, también lo serán respecto a todos los divisores de m.
- La congruencia **es una relación de equivalencia**, porque es:
- Reflexiva: $a \equiv a \pmod{m}$
- Simétrica: Si $a \equiv b \pmod{m}$ entonces $b \equiv a \pmod{m}$
- Transitiva: Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$ entonces $a \equiv c \pmod{m}$
- Si en un polinomio con indeterminada x y coeficientes todos enteros, se sustituyen todos los elementos dos veces mediante pares de valores congruentes respecto a un módulo, los valores numéricos resultantes también serán congruentes respecto a ese módulo. Así: $2.2^2+3.2+7= 21$ es congruente con $2.7^2+3.7+2=121$ respecto al módulo 5.

Esta propiedad resume muchas anteriores y permite, por ejemplo, la prueba del 9 en las operaciones aritméticas.

CLASES DE RESTOS

Si la congruencia es una relación de equivalencia, permitirá clasificar a los números enteros (y por tanto a los naturales) en clases de equivalencia, conjuntos formados por cada número entero y todos sus congruentes. En este caso se llaman **clases de restos o residuales**, porque cada clase se puede representar por el resto que resulta al dividir cualquier elemento entre el módulo m.

Las clases módulo m se representan por **Z/mZ**, o por $\mathbf{Z_m}$. Así:

Z_2 = {0, 1}, que son los dos restos producidos al dividir entre 2. El elemento 0 representa a los números pares y el 1 a los impares.

Z_5 = {0, 1, 2, 3, 4}, en la que, por ejemplo el elemento 3 representa a los números 3, 8, 13, 18, 23, ... que dan resto 3 al dividirlos entre 5

La clase Z_m contiene exactamente m elementos: {0, 1, 2, 3,... m-1}. A veces se usan restos mínimos, admitiendo números positivos y negativos, mediante la elección entre **a** y **a-m** del número con menor valor absoluto. Por ejemplo, $\mathbf{Z_5}$ se podría representar como {0, 1, 2, -2, -1}

Vimos en el apartado anterior la compatibilidad de la suma y el producto con la relación de congruencia:

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

$a+b \equiv c+d \pmod m$

$a \times b \equiv c \times d \pmod m$

Estas dos propiedades nos permiten definir **la suma** y **el producto** entre clases de restos: sumar o multiplicar dos clases equivaldrá a efectuar la operación entre los restos correspondientes a cada clase.

En Informática la función MOD convierte un número en su resto respecto a un módulo dado. En las hojas de cálculo se usa la función RESIDUO.

Estructura algebraica

Las clases de restos tienen **estructura de anillo conmutativo con unidad** (la clase de resto 1) para la suma y el producto. El grupo aditivo de ese anillo es cíclico, pues puede ser engendrado por sucesivas sumas de la unidad.

No todos los elementos tienen inverso. En caso afirmativo, se llaman **inversibles**, y su conjunto coincide con las clases representadas por **números primos con m**, incluyendo el 1. En efecto:

- **Un elemento A de Z_m es inversible si existe otro elemento X de Z_m tal que $A \times X \equiv 1 \pmod m$.** Esta ecuación tiene solución única siempre que **A sea primo con el modulo m**

(ver más adelante). **Luego los restos primos con m son inversibles**.

- Por el contrario, si A y m tienen un divisor común, para que la ecuación tuviese solución debería ser divisor también de 1, lo que es imposible. **Si el elemento A tiene divisores comunes con m, entonces A no es inversible.**

Los elementos no primos con el módulo m no serán, pues, inversibles, pero sí son **divisores del cero**.

Llamamos divisor de cero en un anillo a aquel elemento A que multiplicado por cierto elemento no nulo C del anillo, da un producto nulo: A×C=0. En este caso en el que A **tiene factores comunes con m, es un divisor de cero**, porque si D=MCD(A,m), tendremos que A=A'×D y m=m'×D. Multiplicando A por m' resulta Am'=A'D×m/D=A'm, que es congruente con cero, luego A×m'≡0 (mod m y por tanto divisor de cero.

Los divisores de cero no son inversibles, porque si A fuera inversible y divisor de cero, se daría una igualdad del tipo A×C=0 con C distinto de cero, pero multiplicando por el inverso resultaría: A-1×A×C=C=A-1×0 lo que daría C=0 en contra de lo supuesto.

Por tanto, el número de inversibles respecto a un módulo coincide con la **indicatriz φ(m) de Euler** del módulo y el de divisores del cero con **m - φ(m)**

Una fórmula para calcular el inverso de un número a es $\mathbf{a^{-1}=a^{\varphi(m)-1}}$, siendo φ (m) la indicatriz del módulo m (ver los teoremas de Fermat y Gauss más adelante)

Otra forma es acudir a la identidad de Bezout, pues si **p** y **m** son coprimos, existen dos enteros A y B tales que **Ap+Bm=**1 (Estos números A y B se calculan mediante el algoritmo de Euclides extendido) Despejando, Ap=1-Bm será congruente con 1 módulo m, luego A será el inverso pedido.

Los elementos inversibles forman un grupo multiplicativo, al que representaremos por $\mathbf{Z\times_m}$ (grupo de las unidades). Basta considerar que el producto, el inverso y la unidad pertenecen a él. Las siguientes líneas lo demuestran

- $(B^{-1}\times A^{-1})\times A\times B=B^{-1}\times(A^{-1}\times A)\times B=B^{-1}\times 1\times B=1$
- $1\times 1=1$
- $A^{-1}\times A=1$

Así, en Z_{12}, son inversibles las clases 1, 5, 7 y 11. Sus inversos se pueden encontrar por ensayo y error. He aquí la tabla de multiplicar del grupo:

	1	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Este carácter de grupo da lugar a una propiedad muy sencilla:

Si a es inversible en Z_m, existe un número natural r tal que $a^r=1$

El número **r** mínimo que cumple la anterior igualdad se llama, como en todos los grupos, **orden, índice o gaussiano de a.**

Es fácil ver que si $\mathbf{a^x =1}$ (mod m, el exponente x deberá ser múltiplo del orden r.

Otra consecuencia es que si a es primo con m y se cumple que

$a^x = a^y$, entonces han de ser x = y.

Si m es primo, serán inversibles todos los elementos y **constituirán un cuerpo.**

Exponenciación modular

Existe una técnica que simplifica las potencias grandes en Zm. Consiste en ir dividiendo el exponente entre 2 de forma entera y simultáneamente elevar sucesivamente al cuadrado la base. Después se multiplican las potencias de exponente impar que hayan resultado.

Por ejemplo, para calcular 7^{13} en Z podríamos proceder así:

13	7	7
6	49	
3	2401	2401
1	5764801	5764801
		96889010407
	7^13=	96889010407

Para el conjunto Z la potenciación desemboca pronto en números grandes, pero no así en Z_m, pues los resultados siempre tendrán como cota m y este método puede ser muy útil. Incluso se puede intentar mentalmente. Por ejemplo, calcular 7^{63} (mod 5): $7 \equiv 2 \pmod 5$; $7^2 \equiv 4 \pmod 5$; $7^4 \equiv 1 \pmod 5$; $7^8 \equiv 1 \pmod 5$ y ya todos valen 1, luego

$7^{63}=7^{32+16+8+4+2+1} \equiv 2\times4\times1\times1\times1\times1 \equiv 8 \equiv 3$, luego $7^{63} \equiv 3 \pmod 5$

Esta sería la exponenciación modular o binaria, que resulta imprescindible en cálculos con grandes números, porque sólo utiliza un número de multiplicaciones del

orden del logaritmo de **n**, y no de **n** como el algoritmo clásico.

A continuación se copia la versión recursiva que aparece en Wikipedia (para Z)

$$x^n = \begin{cases} x & \text{si } n = 1 \\ \left(x^{\frac{n}{2}}\right)^2 & \text{si } n \text{ es par} \\ x \times x^{n-1} & \text{si } n \text{ es impar} \end{cases}$$

SISTEMAS DE RESTOS

Un conjunto de números enteros forma un sistema de números incongruentes respecto a un módulo m, cuando **cada uno de ellos produce un resto distinto** al dividirlo entre m (son incongruentes dos a dos). Por ejemplo, 13, 26, 36 y 78 forman un sistema de números incongruentes módulo 12, pues producen los restos 1, 2, 0 y 6 respectivamente.

Los restos módulo m sólo pueden ser los elementos del conjunto {0, 1, 2,... m-1} que constituyen **un sistema completo de restos**. Por analogía, llamaremos sistema completo de números incongruentes a un conjunto de m números enteros que produzcan **todos los restos posibles** desde 0 hasta m-1. Por ejemplo, {21, 6, 15, 4} forman ese tipo de sistema respecto al módulo 4.

Un conjunto de m elementos incongruentes siempre es completo.

Si se forma un conjunto sólo con los números primos con m (inversibles), el sistema formado se llama **reducido**. Su número es la **indicatriz φ(m) de Euler**

La propiedad fundamental de estos conjuntos es:

Si los elementos de un sistema de números incongruentes (mod m) se multiplican todos por un mismo número primo con m y se les suma después un mismo número a todos, el resultado será otro sistema de números incongruentes.

Es evidente que si el primer sistema es completo, también lo será el segundo. Por ejemplo, el sistema {3, 4, 5, 6, 7}, completo respecto a 5, se transforma mediante la función 3.n+2 en {11, 14, 17, 20, 23}, que produce los restos {1,4,2,0,3}, por cierto que en distinto orden.

Mediante estos sistemas (no lo haremos aquí), se pueden demostrar dos teoremas fundamentales:

Si llamamos φ**(m) a** la **indicatriz de Euler** de m, se cumplirá que

$\mathbf{a}^{\varphi(m)} \equiv 1 \pmod{m}$

para todo **a** primo con m. (Teorema de Euler)

Si m es primo, la igualdad anterior se puede expresar como

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

(Teorema de Fermat)

También es interesante formular el Teorema de Fermat, o Pequeño Teorema, como

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

El recíproco no es cierto. Si para un a primo con m se cumple $a^{m-1}=1 \pmod{m}$, entonces m no tiene que ser necesariamente primo. A estos números compuestos que cumplen el teorema les llamaremos pseudoprimos. Hay algunos pseudoprimos que cumplen la condición $a^{m-1}=1 \pmod{m}$ para todos los números primos con él. A estos números se les llama de números de Carmichael o pseudoprimos absolutos. En el siguiente apartado daremos más detalles sobre ellos.

Otro teorema destacable en la teoría de las congruencias es el de **Wilson**:

Si p es un número primo, se cumple la congruencia:

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

El recíproco también es cierto: si se cumple la congruencia, el módulo p es primo, con lo que este teorema es útil en algunos criterios de primalidad, pero resulta costoso.

El inverso afirma que si n es compuesto mayor que 5, entonces divide a (p-1)!

RESTOS POTENCIALES

Llamaremos **Restos potenciales** del número natural **n** respecto a un módulo dado **m** a los restos producidos por las distintas potencias naturales de n.

Por ejemplo, los restos potenciales de 5 respecto al módulo 3 son:

De 5^0 el resto es 1, de 5^1 el resto es 2, de 5^2 el 1, de 5^3 el 2, etc. y así siguen de forma periódica.

El conjunto de restos potenciales sigue unas pautas muy sencillas:

1. Si m sólo contiene factores primos con n, se llegará a cierta potencia de n que será múltiplo de m y por tanto, a partir de ella, todos los restos potenciales serán nulos.

2. Si m es primo con n, los restos son periódicos de periodo el **índice o gausiano** de n respecto a m. El resto 1 se producirá en los múltiplos de ese gausiano.

3. Por último, si MCD(n, m)=d, siendo d mayor que 1, los restos potenciales tendrán una parte no periódica y otra periódica.

Aplicación a los decimales periódicos

Si lo anterior lo aplicamos a los restos potenciales módulo 10, sus factores primos serán 2 y 5, las pautas expuestas se convertirían en estas otras, aplicables al caso del desarrollo en decimales de la fracción D/d

*Si **d** sólo contiene los factores 2 y 5, el proceso de generación de decimales termina con un r_k=0 (cuando la potencia de 10 del primer miembro contenga 2 y 5 con exponentes mayores o iguales a los de **d)** y se obtendrá un desarrollo **decimal exacto**.*

*Si el divisor d no contiene como factores ni el 2 ni el 5 se producirá un **decimal periódico puro** en la que todos los restos se repetirán a partir del primero, con periodo igual al gausiano de 10 respecto al divisor d*

*Si **d** contiene además del 2 o 5 otros factores, el desarrollo comenzará con k decimales no periódicos (el anteperiodo), siendo k el mayor exponente tomado entre los del 2 y el 5 que figuran en la factorización prima de **d**, seguidos de un periodo con tantas cifras como indique el*

*gausiano de 10 respecto a la parte de **d** que no contiene 2 ni 5. Se formaría un **decimal periódico mixto.***

LOS PSEUDOPRIMOS

En un apartado anterior presentamos los pseudoprimos. Añadimos ahora más cuestiones sobre ellos:

Identificación de pseudoprimos

No es nada complicado identificar un pseudoprimo respecto a una base dada. Las operaciones son sencillas, pero pueden alcanzar números muy grandes, por lo que tendremos que usar técnicas de Aritmética Modular en algunos casos, para abreviar cálculos y datos.

La primera operación es la de obtener el resto de una potencia respecto a un módulo, lo que hemos llamado ***resto potencial***.

La teoría sobre restos potenciales también la puedes consultar en apartados anteriores.

Aquí partiremos de una función que actuará sobre tres datos:

•Base de la potencia b

•Exponente p

•Módulo m

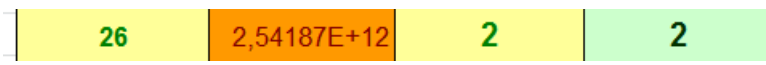
Sobre ellos actuará la función RESTOPOT para Excel y LibreOffice Calc, que irá construyendo la potencia mediante multiplicaciones, pero convirtiendo cada resultado en resto módulo m, con lo que no se disparará la magnitud de los datos. Este es su listado:

Función RESTOPOT

```
Function restopot(b, p, n)
Dim r, m, i

r = b Mod n ‘Resto de la base respecto a m
m = 1
For i = 1 To p ‘Se construye la potencia con restos
m = m × r Mod n ‘m irá recorriendo los restos potenciales
Next i
restopot = m
End Function
```

Por ejemplo, el resto de 3^26 respecto al módulo 7 sería RESTOPOT(3;26;7)=2, como puedes comprobar en la hoja potenciales.xls:



Con esta función podemos averiguar si am-1 □1 (mod m) y si m es compuesto, con lo que tendría el carácter de pseudoprimo.

Contando con la función RESTOPOT es fácil exigir que se cumplan las condiciones para ser pseudoprimo en una base dada.

Public Function espseudo(m, b) As Boolean

If Not esprimo(m) And mcd(m, b) = 1 And restopot(b, m - 1, m) = 1 Then espseudo = True Else espseudo = False

End Function

Nos limitamos a exigir que

•Sea compuesto

•Primo con la base

•El resto potencial b^m-1 respecto a m sea 1

Con esta función y un bucle de búsqueda podemos reproducir muchas sucesiones de pseudoprimos ya publicadas en OEIS. Por ejemplo, para b=23 obtenemos esta lista:

Pseudoprimos en base 23

22, 33, 91, 154, 165, 169, 265, 341, 385, 451, 481,…

La puedes comprobar en http://oeis.org/A020151

En base 11

Obtenemos: 10, 15, 70, 133, 190, 259, 305, 481, 645, 703, 793, 1105, 1330, 1729, 2047, 2257, …

Números de Carmichael

Si un número es pseudoprimo con base todos los números coprimos con él, se llama “de Carmichel”.

Los primeros son:

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633,…

Bastará recorrer los números coprimos con uno de ellos y comprobar que es pseudoprimo con todos ellos.

Números de Sarrus o Poulet

Estos son los pseudoprimos en base 2, también llamados números de Sarrus, Poulet o simplemente psudoprimos, sin especificar el módulo.

El primer pseudoprimo módulo 2 es el 341, porque es compuesto (341=11×31) y cumple que

$\mathbf{2^{340}} \equiv 1 \pmod{341}$

Esta condición se verifica fácilmente, ya que 210=1024=3×341+1 presenta resto 1 respecto al módulo 341, por lo que todas sus potencias, entre ellas 2340 también tendrán ese mismo resto.

El segundo pseudoprimo módulo 2 es 561, que es compuesto (561=3×11×17) y se verifica que

$\mathbf{2^{560}} \equiv 1 \pmod{561}$

La sucesión de números de Poulet comienza con:

341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911, 10261, 10585, 11305, 12801, 13741, 13747, 13981, 14491, 15709, 15841, 16705, 18705, 18721, 19951, 23001, 23377, 25761, 29341, …

Aquí nos hemos limitado a presentar conceptos básicos y facilitar la búsqueda de pseudoprimos. Se podría extender más su estudio, pero superaría los objetivos de este documento.

RESTOS CUADRÁTICOS

Un elemento **a** de unas clases de restos de módulo **m**, con **a** primo con **m**, es **resto cuadrático** cuando es resto potencial de algún cuadrado, es decir, que existe un n tal que $n^2 \equiv a \pmod{m}$.

En caso contrario diremos que **a** es **no resto cuadrático**. Bastará ensayar los cuadrados de los números 0, 1, 2, 3... m-1 para ver si alguno de ellos produce de resto **a**. En realidad sólo hay que probar la mitad, pues **r** produce el mismo resto cuadrático que **m-r**. Intenta demostrarlo.

Por ejemplo, con módulo 8, son restos cuadráticos 0, 1 y 4 y son no restos cuadráticos 2, 3, 5, 6 y 7.

El caso más interesante se presenta cuando **m es primo impar**. En este caso se verifican estas propiedades:

× El número de restos cuadráticos es (m-1)/2, que son congruentes con 1^2, 2^2, 3^2… $((p-1)/2)^2$ y por tanto, este también es el número de no-restos.

× El producto de dos restos o de dos no-restos siempre da un resto, y el de resto con no resto produce un no-resto. Es decir, poseen estructura alternada, por lo que es fácil representar los restos mediante el signo + y los no restos con el -, y así poder usar la regla de los signos.

× El conjunto de restos cuadráticos forma un grupo multiplicativo en Z_p, de índice 2.

Por ejemplo, si m=11, los restos son 1, 3, 4, 5 y 9 y los no restos 2, 6, 7, 8 y 10 (o bien -1, -3, -4, -5 y -9). Los restos forman un grupo, como se puede verificar fácilmente.

Si a es un resto cuadrático respecto a p se cumple

$$a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$$

Y si no lo es

$$a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$$

Símbolo de Legendre

Si **m** es primo, y **a** primo con él (es decir, no múltiplo, en este caso) usaremos el símbolo **(a/m)** (símbolo de Legendre) para indicar si **a** es resto cuadrático o no respecto a m.

Si lo es, declararemos que **(a/m)=1**, y si no lo es, que **(a/m)=-1** (Escribimos el símbolo de forma inclinada, pero se suele escribir verticalmente como una fracción)

Según se vio en el apartado anterior, podremos escribir

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod\ p)$$

El símbolo de Legendre presenta varias propiedades interesantes:

$$\left(\frac{1}{p}\right) = 1$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) * \left(\frac{b}{m}\right)$$

La asignación de +1 o -1 **es un verdadero homomorfismo entre Z_p y el grupo multiplicativo {+1,-1}**, tal como se anunció en párrafos anteriores.

LEY DE RECIPROCIDAD CUADRÁTICA

*Si **p** y **q** son primos impares, y uno de ellos tiene la forma **4n+1**, entonces **p** es resto cuadrático respecto de **q** si y solo si **q** es resto cuadrático de de **p**.*

*Si ambos presentan la forma **4n+3**, si **p** es resto cuadrático de **q**, entonces **q** no lo es de **p**, y a la inversa.*

Si se usa el símbolo de Legendre, la ley se puede expresar así:

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

En ese caso, si uno de los dos, p o q, tienen la forma 4n+1, la potencia tiene el valor de 1, por lo que si p es resto cuadrático de q, ocurrirá también que q lo será de p. Si ambos tienen la forma 4n+3, la potencia valdrá -1, y si p es resto de q, q no lo será de p.

Criterio de Euler

Los símbolos de Legendre nos ayudan a expresar un criterio debido a Euler para saber si un entero es resto cuadrático:

Sea **m** primo y **a** entero coprimo con él. Entonces se cumple:

$$a^{\frac{m-1}{2}} \equiv \left(\frac{a}{m}\right) \bmod m$$

Lo podemos comprobar, por ejemplo, con los restos respecto a 11.

$5^5 = 3125 \equiv 1 \pmod{11}$, luego 5 sí es resto cuadrático.

$7^5 = 16807 \equiv 10 \pmod{11} \equiv -1 \pmod{11}$, luego 7 no es resto cuadrático.

El algoritmo extendido de Euclides

Llamamos algoritmo extendido de Euclides al algoritmo clásico de ese nombre en el que se continúa con el desarrollo en fracciones continuas y del cálculo de convergentes o reducidas. También se puede interpretar como el recorrido inverso del algoritmo hasta llegar a la Identidad de Bezout.

El algoritmo extendido supone tres fases de calculo:

(1) El algoritmo para el cálculo del MCD. Lo recordamos en esta imagen:

	q_1	q_2	q_3	q_4	…	q_t
D	d	r_1	r_2	r_3	…	MCD
r_1	r_2	r_3	r_4	r_5	…	0

(2) Se despejan los restos a partir de las identidades de la división entera:

$$r_1=D-d*q_1$$

$$r_2=d-r_1*q_2$$

$$r_3=r_1-r_2*q_3$$

$$r_4=r_2-r_3*q_4$$

….

(3) Sustituimos $\mathbf{r_1}$ en la fórmula de $\mathbf{r_2}$, con lo que éste dependerá sólo de **D** y **d**. Proseguimos sustituyendo $\mathbf{r_2}$ en $\mathbf{r_3}$, éste en $\mathbf{r_4}$ y así hasta llegar al **MCD** que dependerá entonces sólo de **D** y **d** y habremos obtenido la identidad de Bezout: $\mathbf{MCD=m\times D+n\times d}$

Este proceso puede complicarse algebraicamente, por lo que se sustituye por cálculos más automáticos, como el algoritmo de las reducidas (Ver la teoría de fracciones continuas en nuestro documento teorarit.pdf)

Ecuación lineal en congruencias

Llamaremos ecuación lineal a la de forma $\mathbf{a\times x \equiv b \pmod m}$. Los tipos de solución que presenta son:

1. Si **a** es primo con **m**, existe una sola solución $\mathbf{x \equiv b\times a^{-1} \pmod m}$, por ser **a** inversible en el anillo Zm

2. Si **MCD(a,m)=d**, con d mayor que 1, para que exista solución ha de ser b múltiplo de d. En ese caso se simplifican los tres números a,b y m con lo que se pasa al primer caso. Se puede encontrar una primera solución $\mathbf{x_0= b\times a^{-1} \pmod m}$ y existirán en total d soluciones, que vienen dadas por la fórmula $\mathbf{x_r = x_0+r\times m/d}$

Para resolver esta ecuación deberemos encontrar el inverso a^{-1}. Esto se puede conseguir de las dos formas explicadas más arriba:

- Una fórmula para calcular el inverso de un número a es $\mathbf{a^{-1}=a^{\varphi\ (m)-1}}$, siendo φ (m) la indicatriz del módulo m
- Otra forma es acudir a la identidad de Bezout, pues si a y m son coprimos, existen dos enteros p y q tales que ap+mq=1 (Estos números p y q se calculan mediante el algoritmo de Euclides extendido) Despejando, ap=1-mq será congruente con 1 módulo m, luego A será el inverso pedido.

Caso homogéneo

Si **b** es cero, esta ecuación queda como $a \times x \equiv 0 \pmod m$ por lo que además de la solución trivial x=0 existirán otras si M.C.D(a,m)>1, y entonces **a** se confirmará como divisor de cero. Por ejemplo, si se resuelve $6 \times x \equiv 0 \pmod 9$ y obtendrás las soluciones 0, 3 y 6, ya que M.C.D(6,9)=3>1. Sin embargo, resuelve $6 \times x \equiv 0 \pmod 7$ y sólo obtendrás x=0, ya que en este caso 6 es inversible.

Las diferencias existentes entre las soluciones de la ecuación $A \times x \equiv B \pmod m$ son soluciones de la homogénea $A \times x \equiv 0 \pmod m$. Inversamente: dada una solución de $A \times x \equiv B \pmod m$, si le vamos sumando por separado las soluciones de la homogénea, resulta el conjunto de todas las soluciones de $A \times x \equiv B \pmod m$

Sólo se incluye el caso del llamado **Teorema Chino de los restos**:

Si M_1, M_2, M_3…M_n son números enteros primos entre sí dos a dos y B_1, B_2, B_3,…B_n, otros números enteros cualesquiera, existe otro número natural N único que cumple $N \equiv B_i$ (mod M_i para todo i entre 1 y n.

$$N \equiv B_1 \pmod{M_1}$$

$$N \equiv B_2 \pmod{M_2}$$

$$N \equiv B_3 \pmod{M_3}$$

...

$$N \equiv B_n \pmod{M_n}$$

Todas las demás soluciones del sistema son congruentes con N respecto a un módulo H igual al producto de los módulos.

Esta solución es única. Su fundamento está en que si dos números son congruentes respecto a módulos primos entre sí, también lo serán congruentes respecto al producto de los módulos. Así, en este caso, si N_1 y N_2 fueran dos soluciones distintas, serían congruentes respecto a todos los módulos M_1, M_2, M_3…M_n y por tanto congruentes respecto a H, que es lo que garantiza su unicidad.

Para calcular ese número se sigue el proceso, llamado algoritmo de Gauss:

Llamemos H al producto de todos los módulos M_i y sea $M'_i = H/M_i$.

Se buscan unas m_i tales que $m_i.M'_i=1 \pmod{M_i}$, es decir, sus inversos, y entonces la solución será:

$$N = \sum_{i=0}^{n} M_i\, m_i B_i = \sum_{i=0}^{n} E_i\, B_i$$

Se han destacado los coeficientes $E_i=M_i \times m_i$ porque sólo dependen de los módulos, y no de las B_i, lo que significan que se pueden seguir usando para esos módulos aunque cambiemos otros datos.

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

$H=9.10 = 90$; $A'_1=9$; $A'_2=10$; $m_1=9$; $m_2=1$ y por último:

$N=9.7.9+10.3.1= 81\times7+10\times3=597$. Si reducimos a módulo 90 nos quedará 57, que es la solución única en Z_{90}.

Para encontrar las demás soluciones bastará con ir sumando H=90: 147, 237,327, ...

El caso de dos ecuaciones

Si la solución de este problema es única, podríamos definir una función $\Psi(a,b,m,n)$ tal que a cada par de enteros **a** y **b** y dos módulos **m** y **n** primos entre sí les asignara la solución N tal que $N \equiv a \pmod m$ y $N \equiv b \pmod n$. Si los módulos no fueran primos entre sí le podríamos asignar el valor de alarma, por ejemplo el cero.

Por otra parte, para todo entero N existen dos enteros únicos a y b tales que $N \equiv a \pmod m$ y $N \equiv b \pmod n$. Por tanto, tenemos delante una correspondencia biunívoca entre el conjunto $\mathbf{Z_m \times Z_n}$ y el conjunto $\mathbf{Z_{mn}}$. (Recuerda que **m** y **n** han de ser coprimos)

Por tanto, nuestra función Ψ quedará como un isomorfismo entre anillo $\mathbf{Z_m \times Z_n}$ y el anillo $\mathbf{Z_{mn}}$ si la aplicamos a módulos **m** y **n** coprimos, cumpliendo

$\Psi(a+a', b+b') = \Psi(a, b) + \Psi(a', b')$ y $\Psi(a \times a', b \times b') = \Psi(a, b) \times \Psi(a', b')$

Correspondencia entre inversibles

Si el resto **p** es inversible en $\mathbf{Z_m}$, será porque no tiene factores primos comunes con **m**. De igual forma, si **q** es inversible en $\mathbf{Z_n}$, no compartirá factores con **n**. Si aplicamos la función $\Psi(p,q)=N$ (si suponemos que m y n son coprimos), este resultado N será coprimo con m y con n, pues en caso contrario produciría divisores de

cero tanto en $\mathbf{Z_m}$ como en $\mathbf{Z_n}$. Por tanto, N es inversible en $\mathbf{Z_{mn}}$

La correspondencia $\Psi(p,q)=N$ convierte inversibles en inversibles.

ECUACIONES POLINÓMICAS EN Z_M

Al ser Z_m un anillo, será posible definir polinomios con una indeterminada. Esto permite definir ecuaciones polinómicas como la siguiente:

$$\mathbf{f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0 \equiv 0 \pmod m}$$

Para este tipo de ecuaciones es cierto el Teorema de Lagrange

Si en la ecuación polinómica $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0 \equiv 0 \pmod m$ el módulo m no divide a todas las a_i , entonces el número de soluciones de la ecuación no puede ser superior a m.

Índice o gaussiano de un resto en Zn

Teoría previa

Resumimos brevemente la teoría previa que es conveniente conocer antes de seguir esta serie de temas:

Comenzamos con la estructura $\mathbf{Z_m}$ formada por los restos posibles al dividir un número entre m. Ya sabes que este conjunto es la base de la Aritmética Modular (o del reloj)

Este conjunto $\mathbf{Z_m}$ con la suma y la multiplicación forma un **anillo cíclico de m elementos**. Por esta estructura cíclica se pensó en llamarles ***anillos*** por primera vez. Es un anillo con unidad, por lo que puede contener elementos inversibles. De ellos trataremos aquí.

Un elemento A de Z_m es inversible si existe otro elemento X de Z_m tal que $A \times X \equiv 1 \pmod m$. Esta ecuación se sabe que tiene solución única siempre que A sea primo con el modulo m. **Luego los restos primos con m son inversibles**.

Por el contrario, si **A** y **m** tienen un divisor común, para que la ecuación tuviese solución debería ser divisor también de 1, lo que es imposible. **Si el elemento A**

tiene divisores comunes con m, entonces A no es inversible.

Llamamos **divisor de cero** en un anillo a aquel elemento A que multiplicado por cierto elemento no nulo C del anillo, da un producto nulo: A×C=0. Si que A tiene factores comunes con m, **es un divisor de cero**, porque si D=MCD(A,m), tendremos que A=A'×D y m=m'×D. Multiplicando A por m' (que es no nulo) resulta Am'=A'D×m/D=A'm, que es congruente con cero, luego A×m'≡0 (mod m) y por tanto divisor de cero.

Los divisores de cero no son inversibles, porque si A fuera inversible y divisor de cero, se daría una igualdad del tipo A×C=0 con C distinto de cero, pero multiplicando por el inverso resultaría: A^{-1}×A×C=C=A^{-1}×0 lo que daría C=0 en contra de lo supuesto.

Así que:

- **Si el elemento A es primo con el módulo m, entonces es inversible**, es decir, que existe algún otro elemento B tal que A×B=B×A=1. Anteriormente vimos cómo encontrarlo mediante el algoritmo extendido de Euclides

(http://hojaynumeros.blogspot.com.es/2012/06/la-herencia-de-euclides-1-el-algoritmo.html).

- **Si el elemento A no es primo con m, es un divisor de cero, y por tanto no inversible**.

Grupo de inversibles

El producto de dos inversibles A y B también lo es, y su inverso es $B^{-1}\times A^{-1}$, ya que

$(B^{-1}\times A^{-1})\times A\times B=B^{-1}\times(A^{-1}\times A)\times B=B^{-1}\times 1\times B=1$

Como el 1 es inversible trivialmente y el inverso también, tenemos que **los inversibles forman grupo abeliano** para la multiplicación**, llamado grupo de las unidades $Z\times_m$**

Como es conocido, la función indicatriz de Euler cuenta los números menores que m y primos con él, por tanto, **el cardinal del grupo $Z\times_m$ coincide con la indicatriz o función φ(x) de Euler**.

Se cumple el llamado Teorema de Euler

$\mathbf{a}^{\varphi(m)} \equiv 1 \pmod m$

para todo **a** primo con m o *unidad*.

Orden multiplicativo, índice o gaussiano de un elemento

Dado un elemento inversible **a**, llamaremos ***orden*** de ese elemento al mínimo número entero tal que $\mathbf{a}^r\equiv\mathbf{1}$. Según el teorema anterior, ese valor existe y puede ser φ(m) y todos sus múltiplos. Si es menor, ha de ser un divisor suyo. En efecto, supongamos que φ(m) no fuera múltiplo del orden r. Entonces efectuando la división entera entre ambos quedaría $\varphi(m)=qr+s$, con $s<r$. Aplicamos esa potencia al elemento **a** y obtendríamos

$1 \equiv a^{\varphi(m)} \equiv a^{qr+s} \equiv a^{qr} \times a^s \equiv a^s$, luego $a^s \equiv 1$ en contra del carácter mínimo de r.

Así que el orden ha de ser un divisor de la función **φ(m)**. Toda potencia que sea igual a 1 tendrá un exponente múltiplo de ese orden. Hay muchas formas de representar el orden o gaussiano. Aquí por comodidad tipográfica representaremos el gaussiano de N respecto al módulo M como G(N,M)

Podíamos habernos ahorrado el razonamiento anterior recordando el Teorema de Lagrange para grupos, que afirma que el orden de un subgrupo H es divisor del orden del grupo G. En este caso este último es **φ(m)** y como las potencias de **a** forman un grupo monógeno, su orden será divisor de **φ(m)**.

Vemos algunos ejemplos:

Orden de 5 módulo 8: Como 5 es primo con 8 y φ(8)=4, el orden podrá ser 2 o 4: 5^2=25≡1(8, luego el orden de 5 con módulo 8 es 2, o G(5,8)=2

Orden del 3 respecto al 7: φ(7)=6, luego el orden podrá ser 2, 3 o 6. Probamos: 3^2=9≡2(7, 3^3=27≡6(7, 3^6=729≡1 (7luego el orden o gaussiano de 3 es 6, G(3,7)=6

Gaussiano de las potencias de un resto

Supongamos que un resto a tiene como gaussiano t, es decir g(a)=t. Es fácil demostrar que el gaussiano de una potencia de a, sea por ejemplo a^k, equivale a

$$g(a^k) = \frac{t}{MCD(k,t)}$$

Por ejemplo, G(4,29)=14 y si elevamos el 4 a la sexta se tendrá G(4^6,29)=14/MCD(6,14)=14/2=7

Se puede razonar así: t divide a MCM(k,t), luego se cumplirá que $a^{MCM(k,t)} \equiv 1$, por ser t el menor exponente con esa propiedad. Efectuamos unos cambios en la expresión:

$a^{MCM(k,t)} = (a^k)^{MCM(k,t)/k} = (a^k)^{t/MCD(k,t)} \equiv 1$, luego t/MCD(k,t) puede ser el gaussiano de a^k. Sólo falta demostrar que es el más pequeño con esa propiedad. En efecto, si $(a^k)^m \equiv 1$, será $a^{km} \equiv 1$, con lo que km será múltiplo de t, pero como también es múltiplo de k, lo será del MCM(k,t), luego m>= MCM(k,t)/k=t/MCD(k,t), luego esta expresión t/MCD(k,t) es la menor con esta propiedad, lo que la convierte en el gaussiano de a^k.

En esta tabla tienes un ejemplo de lo demostrado. El resto 4 tiene un gaussiano igual a 14 respecto al módulo 29, luego el gaussiano de sus potencias será un divisor de 14, precisamente el MCD de 14 y el exponente. Estúdialo bien:

Exponente K	Potencia	Gaussiano	MCD(K,14)
1	4	14	1
2	16	7	2
3	6	14	1
4	24	7	2
5	9	14	1
6	7	7	2
7	28	2	7
8	25	7	2
9	13	14	1
10	23	7	2
11	5	14	1
12	20	7	2
13	22	14	1

Observamos 6 potencias con el mismo gaussiano 14, que se corresponden con los exponentes primos con 14, que son 6, porque **φ(14)**=6

Otras seis potencias tienen gaussiano igual a 7. Se trata de los números pares, en los que MCD(2N,14)=2, y por la fórmula anterior su gaussiano será 14/2=7

Por último, la potencia de exponente 7 presenta un gaussiano igual a 14/7=2.

Hemos descubierto que en el grupo monógeno engendrado por las potencias de un elemento de Zm no tienen que poseer el mismo valor del gaussiano, pero eso era de esperar, porque ocurre lo mismo en todo el grupo Zm.

Subgrupos cíclicos en $Z_m\times$

Según el tema anterior, todo elemento **a** perteneciente a $Z_m\times$ (conjunto de inversibles del grupo multiplicativo Z_m)

posee un ***orden g(a)***, que es el mínimo número entero tal que $\mathbf{a^r \equiv 1}$. Ese orden siempre es divisor de la indicatriz de Euler de m, φ(m), o igual a ella.

$$a^{g(a)} \equiv 1 \ (mod\ m$$

Sabemos que las potencias de un mismo elemento **a** forman siempre un grupo cíclico **< a >**. En el caso de un elemento de $Z_m\times$ estos grupos tendrán el mismo orden que el elemento que los genera, es decir g(a). En efecto, las potencias a^0, a^1, a^2,…$a^{g(a)-1}$ son todas distintas (si dos fueran iguales, al dividirlas resultaría una potencia del elemento igual a la unidad con exponente menor que g(a), en contra de la definición de g(a)). Sus productos pertenecen al conjunto, ya que si sobrepasan $a^{g(a)}$, al ser este la unidad, se puede eliminar de dicho producto.

Por ejemplo, con módulo 13, el orden o gaussiano de 5 es 4, luego $5^0 \equiv 1$ (mod 13, $5^1 \equiv 5$ (mod 13, $5^2 \equiv 12 \equiv -1$ (mod 13 y $5^3 \equiv 8 \equiv -5$ (mod 13 formarán un subgrupo de Z_{13}. Lo podemos representar así: < 5 > = {1, 5, -1, -5}

Así que el concepto de orden de un elemento coincide aquí con el de orden del grupo cíclico que engendra. Este grupo es el más pequeño que contiene ese elemento. Según la teoría general de grupos cíclicos, será abeliano (conmutativo) y ***único***, para un valor dado del orden.

Según los párrafos anteriores, en un subgrupo de potencias de un elemento de gaussiano g, existen φ(g) elementos con el mismo gaussiano, pero como hemos

señalado que este grupo es único para ese valor de g, podremos afirmar:

El conjunto de elementos pertenecientes a $Z_m\times$ con un gaussiano concreto g tiene un cardinal de φ(g).

Si volvemos al ejemplo concreto del módulo 29 que vimos más arriba, esta sería la descomposición de los elementos de Z_{29} según su gaussiano. Cada uno de los elementos engendrará un subgrupo de orden idéntico a su gaussiano, y todos los que compartan el mismo valor g de ese gaussiano formarán un subconjunto de φ(g) elementos:

Gaussiano	Conjunto con el mismo gaussiano			Función de Euler	
28	2, 3, 8, 10, 11, 14, 15, 18, 19,26, 27			ϕ(28)=12	
14	4, 5, 6, 9, 13,22			ϕ(14)=6	
7	7, 16, 20, 23, 24, 25			ϕ(7)=6	
4	12, 17			ϕ(4)=2	
2	28			ϕ(2)=1	
1	1			ϕ(1)=1	
			Suma	28	

Esta tabla es muy útil para repasar lo que hemos explicado hasta ahora:

29 es primo, luego $Z\times_{29}$ contendrá 28 elementos inversibles, y poseerán como gaussiano uno de los divisores de 28: 28, 14, 7, 4, 2 y 1. Según lo explicado, cada conjunto de elementos con el mismo gaussiano k tendrá un cardinal de φ(k). En la tabla vemos que aparecen 12 elementos con gaussiano 28, y φ(28)=12. Luego, tenemos 6 con gaussiano 14 y otros 6 con el valor 7. Finalmente, otros cuatro presentan los gaussianos 4,

2 y 1. Si los sumamos todos, obtenemos 28= φ(29), que es el cardinal de $Z\times_{29}$.

Con esta tabla hemos comprobado la expresión de 28 en suma de φ(28)+φ(14)+φ(7)+φ(4)+ φ(2)+φ(1), que es un caso de la fórmula general:

$$n = \sum_{d:n} \varphi(d)$$

Un número entero coincide con la suma de las indicatrices de sus divisores.

Periodicidad de las potencias

Si en lugar de considerar sólo las potencias de exponente menor que g(a) las estudiamos todas, es evidente que son periódicas, pues $a^{k+tg(a)}=a^k\times a^{tg(a)}=a^k\times 1=a^k$

Exponente	Resto
1	5
2	25
3	13
4	9
5	17
6	1
7	5
8	25
9	13
10	9
11	17
12	1
13	5
14	25
15	13
16	9
17	17
18	1

De paso hemos demostrado que el periodo de las potencias de a es precisamente g(a). Lo puedes comprobar con la hoja de cálculo que presentamos en anteriores párrafos.

En la tabla figuran las potencias de 5 respecto al módulo 28. El orden de $Z_{28}\times$ es 12 (φ(28)), el orden del 5 respecto a 28 es 6 (divisor de 12), y se produce,

como puedes comprobar, una periodicidad de periodo 6.

Además, los integrantes de cada ciclo son los elementos del grupo engendrado por el elemento 5: {5, 25, 13, 9, 17, 1} En el anterior apartado descubrimos que cada elemento de este tipo de grupos tiene un gaussiano diferente, como puedes ver en la siguiente tabla:

Exponente K	Potencia	Gaussiano
1	5	6
2	25	3
3	13	2
4	9	3
5	17	6
6	1	1

Todos los gaussianos son divisores de 12 (φ(28)).

Subgrupos generados

Ha quedado claro que las potencias de un elemento no tienen que compartir el mismo gaussiano, luego los subgrupos que vamos a recorrer ahora no tienen por qué coincidir con los conjuntos estudiados más arriba. Lo que sí queda claro es que, dentro del subgrupo engendrado por un elemento, pueden aparecer subgrupos formados a partir de una potencia con un gaussiano menor.

Más adelante estudiaremos los elementos que engendran todo $Z\times_n$, pero ahora los repasaremos todos. Para entenderlo mejor, estudia esta primera tabla que hemos creado, con módulo 13 y resto 11:

Subgrupo de potencias								
Exponente	*G0*	*Gaussiano*	*Subgrupos*					
1	11	12						
2	4	6	4	3	12	9	10	1
3	5	4	5	12	8	1		
4	3	3	3	9	1			
5	7	12						
6	12	2	12	1				
7	2	12						
8	9	3	9	3	1			
9	8	4	8	12	5	1		
10	10	6	10	9	12	3	4	1
11	6	12						
12	1	1	1					

En la primera columna figuran las potencias de 11, que como su gaussiano es 12, posee ese número de elementos. Este es G0, el subgrupo creado por las potencias de 11 en $Z\times_{13}$. Tal como vimos anteriormente, los elementos de ese grupo no han de tener gaussiano 12. De hecho aparecen todos los divisores de 12: 6, 4, 3, 2 y 1. También vimos que las potencias de cada uno de ellos forman subgrupos del principal. Según la teoría de grupos, estos son únicos para cada orden, aunque se engendren con elementos distintos. Compruébalo:

- G6: Grupo de orden 6: {4, 3, 12, 9, 10, 1} Engendrado en la tabla por 4 y 10.
- G4: Grupo de orden 4: {5, 12, 8, 1} con generadores 5 y 8
- G3: Grupo de orden 3: {3, 9, 1} engendrado por 3 y 9.
- G2: Grupo de orden 2: {12, 1} con generador 12.
- GE: Grupo trivial: {1}

Obsérvese que el número de generadores de cada subgrupo coincide con el valor de su indicatriz de Euler.

Así tenemos φ(6)= φ(4)=φ(3)=2 y por eso los primeros subgrupos poseen dos generadores. Sin embargo, como φ(2)=1, el penúltimo tiene un solo generador.

Como son grupos de potencias, se cumple que si el gaussiano de **a** es divisor del de **b**, el grupo engendrado por **a** es subgrupo del engendrado por **b**.

Todas las potencias de 11 pertenecen a un grupo, y algunas a varios.

Aquí tienes otro ejemplo, con módulo 15 y elemento 7:

			Subgrupos engendrados con potencias					
				Módulo	14		Su gaussiano es	6
				Número	5		Número válido	
				(Menor que el módulo y primo con él)				
Subgrupo de potencias								
Exponente	***G0***	***Gaussiano***	***Subgrupos***					
1	5	6						
2	11	3	11	9	1			
3	13	2	13	1				
4	9	3	9	11	1			
5	3	6						
6	1	1	1					

Indicador de un elemento

Dado cualquiera de los subgrupos que estamos estudiando, cualquier elemento de $Z\times_n$ posee una potencia perteneciente a cada uno de ellos. En efecto, dado un subgrupo S, si un elemento **a** pertenece a él, bastará elevarlo a 1. Si no pertenece, lo elevamos a **n** para engendrar la unidad, pero hay casos en los que existen otros enteros positivos k<n tales que a^k pertenece a S. Al menor de ellos le llamaremos *indicador de **a*** con respecto a S. Hemos visto que puede valer **1** o **n**. Observa la tabla anterior: el indicador de 5 respecto al

subgrupo {11, 9, 1} es 2, porque $5^2=11$ es la potencia positiva más pequeña que pertenece al subgrupo. Igualmente, el 3 es el indicador respecto a {13, 1}

Raíces primitivas

En los apartados anteriores estudiamos el grupo multiplicativo $Z\times_n$ de las unidades en Z_n (números coprimos con **n**). Su orden coincide con φ(n). Cualquier elemento **a** de ese grupo engendrará a su vez un subgrupo cíclico **< a >** mediante sus potencias. Por el Teorema de Lagrange, el orden de ese subgrupo será un divisor de φ(n) y recibe el nombre de gaussiano g de ese elemento. Recordemos que esto implica que $\mathbf{a^g \equiv 1 \pmod n}$. También vimos que el número de generadores de < a > coincide con φ(g).

En este apartado estudiaremos **las raíces primitivas**, que son aquellos elementos que engendran todo $Z\times_n$, o lo que es equivalente, aquellos cuyo gaussiano coincide con **φ(n)**. Según lo que hemos recordado, el número de esas raíces primitivas puede coincidir con φ(φ(n)), y de hecho es así **si $Z\times_n$ es cíclico**. Usamos la palabra "puede" pues, como ya veremos, **no todos los módulos poseen raíces primitivas**.

Aquí tienes la tabla correspondiente al módulo 14

Módulo	14
Indicatriz	6
Núm. Posible de raíces	2

Inversibles	Gaussiano	Es raíz primitiva
1	1	
3	6	Raíz primitiva
5	6	Raíz primitiva
9	3	
11	3	
13	2	

Explicamos la tabla: El módulo es 14, luego existirán tantos inversibles como indique φ(14)=6. En efecto, $Z\times_{14}$ = {1, 3, 5, 9, 11, 13}, conjunto de 6 elementos, como puedes comprobar en la tabla. Ahora bien, las raíces primitivas son generadores de todo $Z\times_{14}$, y su número ha de ser φ(φ(14)) = φ(6) = 2.

Esto es así porque si una raíz primitiva se eleva a un exponente primo con φ(m), resulta otra raíz primitiva, en virtud de la fórmula que estudiamos anteriormente

$$g(a^k) = \frac{t}{MCD(k,t)}$$

En efecto, aparecen las dos raíces primitivas 3 y 5. Recorre sus potencias y comprobarás que engendran todo el grupo: $3^0\equiv1$, $3^1\equiv3$, $3^2\equiv9$, $3^3\equiv13$, $3^4\equiv11$ y $3^5\equiv5$. Igualmente, $5^0\equiv1$, $5^1\equiv5$, $5^2\equiv11$, $5^3\equiv13$, $5^4\equiv9$ y $5^5\equiv3$.

Es fácil comprender entonces que si $Z\times_k$ admite raíces primitivas tendrá carácter de cíclico, ya que está generado por las potencias de un mismo elemento. Según esto, en virtud de una propiedad general de estos grupos, $Z\times_k$ estaría engendrado por cualquier potencia

de una raíz primitiva cuyo exponente fuera coprimo con φ(k), ya que, en caso contrario engendraría sólo un subgrupo propio de $Z\times_k$. Todas esas potencias serían también raíces primitivas, luego su número será φ(φ(k)), como ya comprobamos más arriba. Observa esta tabla y comprueba que todas las raíces primitivas tienen exponentes coprimos con la indicatriz:

Módulo	19	
Indicatriz	18	
Núm. Posible de raíces	6	
Potencias de 2		Gaussiano
1	2	18
2	4	9
3	8	6
4	16	9
5	13	18
6	7	3
7	14	18
8	9	9
9	18	2
10	17	9
11	15	18
12	11	3
13	3	18
14	6	9
15	12	6
16	5	9
17	10	18
18	1	1

El módulo es 19, su indicatriz 18, 2 es una raíz primitiva, con gaussiano 18, y observa hacia abajo que las demás raíces primitivas son potencias del 2 con exponentes coprimos con 18: {1, 5, 7, 11, 13, 17}, seis en total.

Otros módulos no tienen raíces primitivas, como el 30:

				Módulo	30
				Indicatriz	8
				Núm. Posible de raíces	4
	Inversibles	Gaussiano	Es raíz primitiva		
	1	1			
	7	4			
	11	2			
	13	4			
	17	4			
	19	2			
	23	4			
	29	2			

Vemos en la tabla que ningún elemento presenta gaussiano máximo 8 (φ(30)=8), luego con módulo 30 no existen raíces primitivas. Se puede demostrar (no es simple, es un conjunto de teoremas que puedes consultar en los textos especializados) que sólo poseen raíces primitivas **los módulos 2, 4, p^k y $2p^k$, siendo p primo impar y k>=1**. El 30=2×3×5 no es de ninguno de estos cuatro tipos, y carece de raíces primitivas. El 14 es del tipo **$2p^k$** y sí tiene raíces primitivas.

Criterio de los factores de la indicatriz

Si buscamos la indicatriz del módulo, φ(m), y la descomponemos en factores primos, sean estos p_1, p_2, p_3,…(escritos sin exponentes), un resto **a** será raíz primitiva si se cumple

$$a^{\varphi(m)/p_i} \equiv r, con\ r \neq 1\ \forall i$$

Si todas las potencias presentan restos distintos de 1, **a** será raíz primitiva, y si por el contrario, alguna de las

potencias es congruente con 1, ese resto **a** no será raíz primitiva. La justificación no es muy complicada:

Si una de las potencias es congruente con 1, el gaussiano de a sería menor que φ(m), y no podría ser raíz primitiva. Por el contrario, si ninguna es congruente con 1, sí ha de serlo, ya que, en caso contrario, existiría un divisor propio de φ(m), sea **g**, que sería el gaussiano de a y $a^g \equiv 1$. Además, como los cocientes $\varphi(m)/p_i$ son los divisores maximales de φ(m), uno al menos de ellos sería múltiplo o igual al gaussiano, con lo que la potencia $a^{\varphi(m)/pi} \equiv 1$ en contra de lo supuesto.

Índices modulares

En el apartado anterior estudiamos las raíces primitivas, elementos del grupo multiplicativo $Z\times_n$ de las unidades en Z_n (números coprimos con **n**), tales que su gaussiano es máximo y coincidente con φ(n). Estas raíces, mediante sus potencias, engendran todo $Z\times_n$, luego un elemento inversible cualquiera coincidirá con una potencia de la raíz primitiva. El exponente comprendido entre 0 y φ(n)-1 que logra esta coincidencia recibe el nombre de **índice del elemento respecto a la raíz primitiva**. También es llamado **logaritmo discreto**.

Es decir; si **a** es una raíz primitiva y **b** un elemento inversible, existe un exponente k en el intervalo (0, φ(n)-1) tal que $\mathbf{a^k \equiv b}$, y a ese exponente le llamaremos índice de **b** respecto a **a**.

Por ejemplo, el módulo 7 posee dos raíces primitivas. La raíz 3 engendra mediante potencias todos los elementos desde 1 a 6 (por ser 7 primo son todos inversibles), $3^0 \equiv 1$, $3^1 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$,$3^4 \equiv 4$, $3^5 \equiv 5$. Cada uno de los exponents es el índice de ese elemento.

La función índice que asigna a cada elemento inversible el exponente de la menor potencia de la raíz primitiva que lo engendra la podemos representar por $ind_a(b)$ o simplemente ind(b) si se conoce la raíz. También podemos representarlo como un logaritmo, que en este caso recibe el nombre de *logaritmo discreto*. En el ejemplo anterior $ind_3(6)=3$, $ind_3(4)=4$,…Si existe una raíz primitiva, todos los elementos inversibles de Z_m tendrán definido el índice.

Al ser un exponente, las propiedades del índice o logaritmo discreto son previsibles (supongamos módulo m):

- $Ind_a(1)=0$
- $Ind_a(a)=1$
- $Ind(a \times b)=ind(a)+ind(b)$
- $Ind(a^k)=k \times ind(a)$
- $Ind_a(x)=ind_a(b) \times ind_b(x)$ (fórmula del cambio de base)
- $Ind_a(x^{-1})= \varphi(m)-Ind_a(x)$

El cálculo de los índices en grupos complejos no es fácil, aunque se han creado muchos algoritmos eficientes, y por eso los índices son usados en algunos sistemas criptográficos.

Ecuaciones potenciales

Las tablas de índices nos pueden servir para resolver la ecuación

$$x^n \equiv a\ (mod\ m$$

El comportamiento de los índices como logaritmos nos permite transformar esta ecuación en otra lineal, eligiendo cualquier raíz primitiva **b** y aplicando índices en ambos miembros respecto a ella.

$$n \times ind_b(x) \equiv ind_b(a)\ (mod\ \varphi(m)$$

Según la teoría de las ecuaciones lineales en Z_m, si llamamos **d** al MCD(n, φ(m)), el índice de **a** ha de ser múltiplo de **d** para que exista solución. En ese caso basta despejar el índice de x y buscar después el valor de x en las tablas. Podíamos haber automatizado todo el proceso, pero parece que se aprende más de esta forma.

Ejemplo: Resolver $x^6 \equiv 37$ (mod 54

En primer lugar encontramos que φ(54)=18 (ver tabla y párrafos anteriores), luego d=MCD(6,18)=6. En la tabla citada buscamos el índice de 37 respecto a la raíz primitiva 5 y encontramos que es 12. Por tanto, como 12 es múltiplo de 6, deberá existir una solución (en realidad, según las propiedades de las ecuaciones lineales, deberían aparecer 6). Tomamos índices respecto al 5:

$6 \times ind_5(x) \equiv ind_5(37)$ (mod 54 ≡12

$ind_5(x) \equiv 12/6=2$.

Buscamos en la tabla qué inversible tiene índice 5 respecto a la raíz primitiva 5, y nos resulta 25. Comprobamos:

$25^1 \equiv 25$; $25^2 \equiv 25 \times 25 \equiv 31$; $25^3 \equiv 25 \times 31 \equiv 19$; $25^4 \equiv 25 \times 19 \equiv 43$; $25^5 \equiv 25 \times 43 \equiv 49$; $25^6 \equiv 25 \times 49 \equiv 37$

Así comprobamos que 25 es una solución de la ecuación propuesta. Pero hemos asegurado que existen otras cinco soluciones, que se pueden leer en la tabla si hubiéramos usado otra raíz primitiva. Son estas: 13, 43, 31, 7 y 49. Esto completa el conjunto de seis soluciones de la ecuación propuesta.

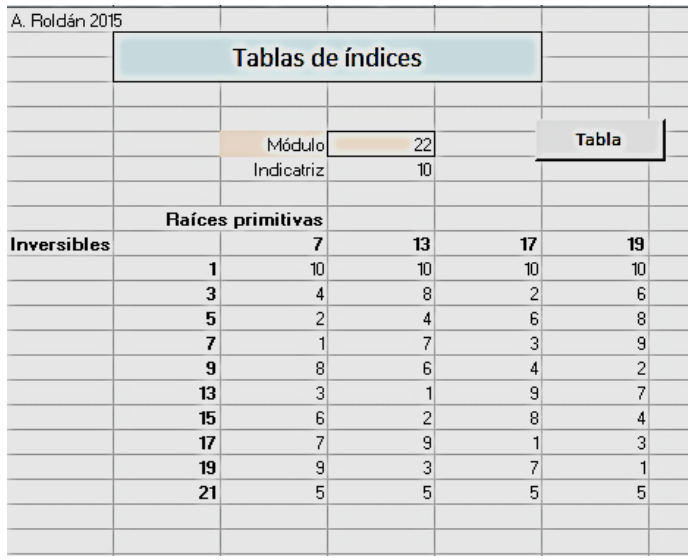
Otras ecuaciones de ese tipo no tienen solución. Por ejemplo:

$X^7 \equiv 12 \pmod{49}$

Formamos la tabla de índices módulo 49 y vemos que $ind_3(12)=11$, que $\varphi(49)=42$ y $MCD(7,42)=7$, pero 11 no es múltiplo de 7, luego no existe solución. Hemos creado una tabla con las séptimas potencias de los inversibles de $Z\times_{49}$ y sólo nos resultan seis resultados posibles: {1, 30, 31, 18, 19, 48}, y el 12 no está entre ellos.

El ejemplo anterior nos da una pista para descubrir si un resto dado es cúbico, bicuadrado o de otro orden en un módulo dado. Por ejemplo, ¿es resto bicuadrado 15 en módulo 22? Planteamos $a^4=15 \pmod{22}$ y analizamos:

Formamos la tabla de índices módulo 22



A. Roldán 2015

Tablas de índices

Módulo 22

Indicatriz 10

Tabla

Inversibles	Raíces primitivas 7	13	17	19
1	10	10	10	10
3	4	8	2	6
5	2	4	6	8
7	1	7	3	9
9	8	6	4	2
13	3	1	9	7
15	6	2	8	4
17	7	9	1	3
19	9	3	7	1
21	5	5	5	5

φ(22)=10 y MCD(4,10)=2, luego ind(15) ha de ser múltiplo de 2. Según la tabla, se cumple para cualquier raíz primitiva, luego sí es un resto bicuadrado. Podemos encontrar su raíz cuarta:

4ind(a)=2, luego ind(a)=2/4 (mod 22 = 6

El 3 posee índice 6, y cumple 3^4=15 (mod 22, luego existe la raíz bicuadrada de 15, y este valor 15 es resto bicuadrado (sólo hemos investigado una posibilidad, pero con una basta)

Las herramientas de cálculo en hojas de cálculo se encuentran actualmente en esta dirección:

http://www.hojamat.es/sindecimales/congruencias/herramientas/calendarios/inicalend.htm

Allí se desarrollan algunos esquemas que incluiremos en este apartado.

Fundamentos

Los calendarios están formados por múltiples congruencias y todos los elementos fundamentales de la hora, día y año pertenecen a las clases Z/mZ. Por ejemplo:

× Los días de la semana pertenecen a Z/7Z (identificamos Domingo=0, Lunes=1, etc.)

× Los meses del año a Z/12Z (Por ejemplo Enero=0, Febrero=1, etc.)

× Los minutos y segundos a Z/60Z

× La aparición o no de años bisiestos forma el conjunto {0,1,2,3} = Z/4Z

E igual con los siglos, los años terminados en 0 no bisiestos y otros.

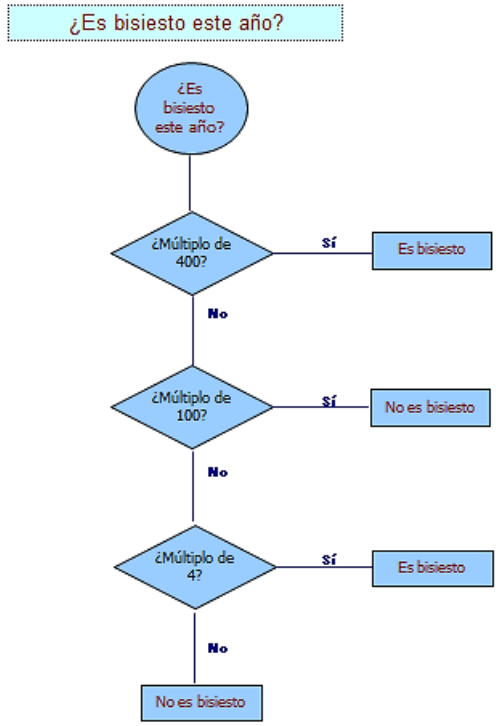
Años bisiestos

Se considera año bisiesto a aquel que contiene 366 días en lugar de 365. Aquí nos interesará la definición y los algoritmos para averiguar si un año es bisiesto. Los temas históricos se pueden consultar en otras publicaciones.

Los algoritmos para averiguar esta cuestión se basan en las tres reglas que se establecieron en el calendario gregorianoen el año 1582:

- Si el número de año es múltiplo de 400, no se considera bisiesto.
- Si es múltiplo de 100, pero no de 400, se considera bisiesto.
- En los demás casos, sólo si es múltiplo de 4 será bisiesto.

Por tanto, basta responder a las tres preguntas y decidir:



Lo podemos plasmar en esta fórmula de hoja de cálculo:

=SI(O(Y(RESIDUO(D5;4)=0;RESIDUO(D5;100)<>0);RESIDUO(D5;400)=0);"SÍ";"NO")

Si el año lo escribimos en la celda D5, esta fórmula nos responderá “SÍ” o “NO”.

Estas preguntas se desprenden del valor del año trópico, (tiempo medio que tarda el Sol, en su movimiento aparente entre dos pasos consecutivos por el equinocio, por ejemplo el de primavera)

El mejor valor que se conoce de este año trópico es el de 365,242199074 días.

El calendario juliano sustituyó este valor por 365 + 1/4 - 1/100 + 1/400, que equivale a 365,2425

¼ Se acumula un día cada 4 años

1/100 Se descuenta un día cada 100

1/400 Se añade otro día cada 400

Sigue habiendo un error, pues hay diferencia entre el verdadero valor de 365,242199074 y 365,2425. El error es

365,2425 – 365,242199074, es decir: 3,01E-004

Si dividimos un día entre la diferencia de ambos nos dan: 3323,076105 años, que es lo que el calendario actual nos garantiza de exactitud en días.

Cálculo del día de la semana

Dada un fecha cualquiera del calendario gregoriano (el vigente en la actualidad), constituye un problema muy interesante el calcular en qué día de la semana cae.

Todos los algoritmos existentes hacen uso de los siguientes hechos:

El día de la semana correspondiente a una fecha siempre proviene de considerar una congruencia respecto al número 7, porque la sucesión de días de la semana siempre es un elemento de Z/7.

Este hecho nos permite representar los días de la semana como los números del 0 al 6 en un “reloj” de siete números.

Como el número de días de un año no bisiesto, 365, es congruente con 1 módulo 7, cada año que transcurra se incrementa en una unidad el día de la semana. Si el año pasado una fiesta cayó en viernes, este año lo hará en sábado.

365 = 52 × 7 + 1365 ≡ 1 (mód 7

Si el año es bisiesto, se incrementará el número en dos días por año. Recordando que son bisiestos los múltiplos de 4 que no lo sean de 100 y los múltiplos de 400, deberemos considerar también las congruencias respecto a 4, 100 y 400

Así, el avance de días que se produce en T años vendrá dado por

A = T + COCIENTE(T;4) – COCIENTE(T;100) + COCIENTE(T;400)

La función COCIENTE se refiere al entero, sin decimales, por lo que equivale a ENTERO(T/4). Por ejemplo.

Los distintos algoritmos que se basan en esta idea difieren de cómo tratar el problema de la fecha inicial a partir de la cual se incrementa el día de la semana. Aquí incluimos el de Zeller, que se basa en la siguiente congruencia (tomada de la Wikipedia)

$$h = \left(q + \left\lfloor \frac{(m+1)26}{10} \right\rfloor + K + \left\lfloor \frac{K}{4} \right\rfloor + \left\lfloor \frac{J}{4} \right\rfloor - 2J \right) \mod 7$$

Si llamamos D al día de la fecha, M al mes, C a la centuria (siglo menos 1) y A al año dentro de la centuria, la congruencia de Zeller es la siguiente:

DIASEM= RESIDUO(D + COCIENTE((M+1)×26;10) + A + COCIENTE(A;4)+COCIENTE(C;4) + 5×C) ; 7)

Si el mes es Enero o Febrero, se les suma 12 y se resta un año.

El esquema para la fecha 19/07/22 sería:

D	19
COCIENTE((M+1)*26;10)	20
A	22
COCIENTE(A;4)	5
COCIENTE(C;4)	5
5C	100
SUMA	171
MÓDULO 7	3
Día de la semana	Martes

Cálculo de la fecha juliana

La fecha juliana o día juliano es una forma de situar cualquier fecha independientemente de que pertenezca a un calendario concreto. Se basa en el cómputo de días transcurridos desde el 1 de Enero del año 4713 aC a las 12h del mediodía.

Así, José Scaliger creó una escala continuada en el tiempo, válida para comparar fechas lejanas o pertenecientes a distintos calendarios.

Existen varios algoritmos para calcular el día juliano de cualquier fecha, sea anterior al 4 de Octubre de 1582 (calendario juliano) o posterior al 15 del mismo mes, día en el que comienza el calendario gregoriano en varios

países. Otros se retrasaron en adoptarlo, como Inglaterra, y otros aún usan el calendario juliano.

Así, el día en el que se escribe este texto, 25 de Noviembre de 2007, posee una fecha juliana equivalente a 2.454.429,5

Esta escala nos proporciona un método fiable para contar el número de días transcurridos entre dos fechas. Basta restar las dos fechas julianas correspondientes.

Incluimos los esquemas del algoritmo para números reales y el correspondiente a enteros, aplicados ambos a la fecha 19/07/22:

Números reales

Llamo A1 al cociente del año entre 100	A1	20
Llamo A2 a A1/4	A2	5
Llamo A3 a 2-A1+A2	A3	-13
Llamamos A4 a 365.25*(año+4716)	A4	2461054
A5 será igual a 30,6001*(mes+1)	A5	244

Día juliano es la suma sde D+A3+A4+A5-1524,5	2459779,5

Números enteros

JD1 es (a1/4000)*1460969	JD1	0
A2 es el módulo de A1 respecto a 4000	A2	2022
JD2 es ((A1/100*146097)/4	JD2	730485
JD3 es ((A1 mod 100)*1461)/4	JD3	8035
JD$ es (153*M1+2)/5	JD4	122

Sumo JD1+JD2+JD3+JD4+D+1721119-0,5	DIAJUL	2459779,5

Fecha de la Pascua

Este cálculo era fundamental en las iglesias cristianas, por lo que se estudió mucho y justificó cargos de astrónomos. Aquí tampoco entraremos en detalles históricos, pues solo copiaremos el esquema del algoritmo de Butcher, aplicado al año 2022:

	Cociente		Resto	
Se divide el año entre 19		106	A	
Se divide el año entre 100	B	20	C	
Se divide B entre 4	D	5	E	
Se divide (B+8) entre 25	F	1		
Se divide (B-F+1) entre 3	G	6		
Dividimos (19A+B-D-G+15) entre 30			H	
Se divide C entre 4	I	5	K	
Dividimos 32+2E+2I-H-K entre 7			L	
Se divide A+11H+22L entre 451	M	0		
Se divide H+L-7M+114 entre 31	N	4	P	

Fecha	17	de	Abril	

Estos temas se desarrollan de forma sucinta, tan sólo para presentarlos. Si deseas adquirir más conocimientos debes acudir a manuales o direcciones de Internet que los tratan.

Números pseudoaleatorios

Las congruencias nos permiten generar números naturales, que aunque procedentes de fórmulas o algoritmos, semejan haber sido generados al azar.

Una técnica muy sencilla para ello es la siguiente:

× Se fija un módulo grande, que se ha estudiado previamente y se ha visto que funciona bien. Por ejemplo 199017 (usado en algunas calculadoras Texas Instrument).

× Un primer número pseudoaleatorio se elige entre 0 y el módulo, por ejemplo el 34900, al que llamaremos semilla.

× Sobre la semilla se aplica reiteradamente una fórmula de recurrencia lineal del tipo $x_{n+1} = a.x_n+c \pmod{199017}$

En este caso se puede elegir a=24298 y como c=99991

En los ordenadores, la semilla se toma del estado actual del reloj interno, lo que aumenta la sensación de aleatoriedad.

Como ejemplos de generadores populares podemos recordar dos:

Si a=75, c=0 y m=231 - 1, resulta el generador usado durante muchos años por IBM y el programa MATLAB

Si a=1103515425, c=12345 y m=232, obtendremos el generador del sistema UNIX

Criterios de divisibilidad

Los criterios que estudiábamos de niños (Un número es divisible entre 9 si la suma de sus cifras...) están basados en los restos potenciales.

Si deseamos ver si el número abcde es divisible entre m, podríamos descomponer ese número en unidades, decenas, centenas, de la forma

abcde = a104 + b103 + c102+d10+e con lo que el resto de dividirlo entre m, según los teoremas de las congruencias, equivale a

Resto: (ar4 + br3 + cr2 + dr1 + er0) (mod m) (1)

siendo r4,r3... los restos potenciales de 10 respecto a m.

Estos restos pueden ser:

Módulo 2: r0=1, r1=0,r2=0, r3=0,... La expresión (1) se reduce a a MOD m

En el criterio sólo habrá que mirar las unidades, que corresponden al único resto no nulo.

Módulo 3: r0=1, r1=1,r2=1, r3=1,... Todos los restos valen 1. En este caso la expresión (1) del resto será a +b +c +d +e MOD m

por lo que habrá que sumar todas las cifras y ver su resto respecto a m

y así con todos.

No es imprescindible usar el número 10. Con el número 1000 se pueden construir criterios para el 13, 11 y 7, porque sus restos potenciales son r0=1, r1=1,r2=1, r3=1,...lo que permite usar sumas alternadas de números de tres cifras.

Cálculo con números grandes

El Teorema Chino nos garantiza que dados A1, A2, …An primos entre sí dos a dos, todo número natural menor que A1× A2× …×An viene determinado por a1, a2, a3,…an, tales que que cumple N=ai (mod Ai) para todo i entre 1 y n. Esto nos permite representar N de forma unívoca por el vector (a1, a2, a3,…an)

Por ejemplo, 9 y 10 son primos entre sí, luego todos los números menores que su producto 90 vendrán

representados de forma unívoca por sus restos respecto a ellos. Así, el número 57 se representaría por el par de coordenadas (3,7), porque 57=3(mod9 y 57=7(mod 10. Recíprocamente, si resolvemos por el teorema chino estas dos condiciones nos daría como solución 9×9×7 + 10×1×3 = 597, que reducido a módulo 90 se convierte en 57.

Como las operaciones de suma y producto son compatibles con la relación de congruencia, a veces nos puede convenir sustituir números grandes por sus coordenadas, operar con ellas y después reconstruir los números. En Informática, si una unidad aritmética posee sus registros limitados, puede ser la única forma de operar.

Dígitos de control

Los dígitos de control se introducen en números grandes para verificar la corrección de su escritura. Los más populares son los de las cuentas bancarias, que tienen la forma EEEE OOOO CD NNNN NNNN, en la que EEEE representa a la entidad, OOOO a la oficina, CD son los dígitos de control y NN... la cuenta de referencia. Tanto C como D se calculan mediante congruencias módulo 11 a partir del resto de dígitos. En concreto, C proviene de una suma ponderada de los EEEE y OOOO y D procede del número de cuenta.

DNI

La letra del NIF se obtiene a partir del número del DNI hallándole su resto módulo 23 y usando después una tabla de equivalencia:

Funciones hash

Están basadas en las congruencias, y se usan para asignar posiciones de memoria de un ordenador a partir del número clave de un registro en una base de datos. Por ejemplo, si un alumno tiene una clave de seis dígitos, como 344 231, y sólo tenemos 512 posiciones de memoria para almacenar las claves, se utiliza la función de tipo hash (direccionamiento calculado)

$$f(344231) = 344231 \bmod 512$$

El problema de esto reside en que dos claves pueden ser asignadas a una misma posición. Diremos que se ha producido una colisión y a las claves se les llama sinónimas. Existen técnicas informáticas para resolverlo.

COMBINATORIA

FUNDAMENTOS

CONCEPTOS ELEMENTALES

Independientemente de la definición que se elija para la Combinatoria, es evidente que sus fundamentos están en los conjuntos y las correspondencias entre ellos. Después, en la práctica se pueden usar los conceptos de ordenación, permutación o elección, pero todos ellos están relacionados por el término básico de *correspondencia unívoca* o *aplicación* entre conjuntos.

Producto cartesiano, correspondencias y aplicaciones

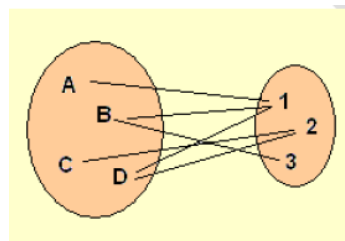
El producto cartesiano de dos conjuntos A y B es otro conjunto cuyos elementos son todos los pares ordenados posibles formados por un elemento de A y otro de B en ese orden. Se representa como A×B

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

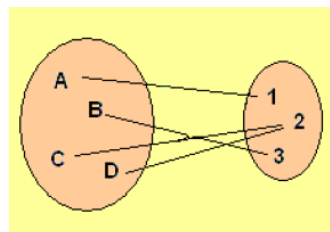
Una **correspondencia** entre dos conjuntos es cualquier subconjunto de su producto cartesiano. En la práctica consiste en asignar **una pareja o varias a todos o algunos elementos del conjunto.**

X	A	B	C	D
1	A1	B1		D1
2			C2	D2
3		B3		

Se puede representar con diagramas de conjuntos



Una **aplicación** es una correspondencia en la que a cada elemento del primer conjunto le corresponde **un elemento del segundo conjunto y solo uno**. También se le llama correspondencia *unívoca*.



Según esta definición podremos asignar un nombre (por ejemplo G) a la aplicación y usar la notación G(A)=B, en la que expresamos que al elemento A del primer conjunto le asignamos el elemento B del segundo. En este caso, a A la llamaremos *origen* o *antecedente*, y al B, *imagen.* Así, en el diagrama de la figura, se puede afirmar que G(A)=1, G(B)=3, G(C)=2, G(D)=2.

Como se ve, la definición permite que dos orígenes compartan la misma imagen. Al conjunto de todas las imágenes le llamaremos **Recorrido, Rango o Conjunto Imagen o final** de la aplicación G. Si el conjunto de orígenes es A, el de imágenes será G(A). Al conjunto de todos los orígenes, que según la definición es todo el primer conjunto, le llamaremos **Dominio o conjunto inicial** de la aplicación.

Una aplicación es *suprayectiva* si su conjunto imagen coincide con todo el segundo conjunto, *inyectiva* si a orígenes distintos les corresponden imágenes distintas, y *biyectiva* si presenta las dos propiedades anteriores.

Si dos conjuntos admiten una correspondencia biyectiva se llamarán *coordinables*, con la propiedad de que tendrán el mismo cardinal. Esta propiedad es básica en combinatoria.

Factoriales

Llamaremos factorial de un número natural n (o el cero) a otro número natural **n!** definido por

a) Si n=0 su factorial se define como 1: 0! = 1
b) Si n=1 definiremos su factorial como 1: 1! = 1
c) Si n>1 su factorial viene dado por la expresión n! = 2.3.4.....(n-1).n

Podemos también definir el factorial por recurrencia:

0! =1 ; n! = n×(n-1)!

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

a(a-d)(a-2d)..... (hasta k factores)

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

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

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

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

En hojas de cálculo el factorial ordinario se representa como FACT(N). Es una notación mucho más cómoda que la clásica n!

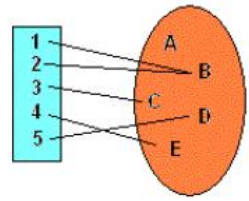
Arreglos

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

En los textos de Combinatoria encontrarás varias formas de nombrar estas sucesiones:

- **Palabras**, en recuerdo de las palabras de un idioma, en las que sí interviene el orden y pueden repetirse elementos
- **n-plas**, que es la notación más usada en textos clásicos.
- **Selecciones ordenadas**: es una denominación muy sugerente, porque describe perfectamente la construcción de cualquier arreglo.

Se puede caracterizar cada arreglo como una aplicación de un conjunto finito de números naturales del tipo {1, 2, 3, 4,... } sobre elementos del conjunto.



El arreglo representado en la imagen se corresponde con la sucesión {B, B, C, E, D}

También se podría representar como u_1=B, u_2=B, u_3=C, u_4=E, u_5=D.

Aquí usaremos preferentemente la notación {B, B, C, E, D}

Este concepto permite desarrollar las definiciones clásicas de variaciones y permutaciones.

Variaciones con repetición

Llamaremos **variaciones con repetición** de **m** elementos tomados de **n** en **n**, (simbolizadas por **VRm,n**) a todos los arreglos de **n** elementos que se pueden formar en un conjunto de **m** elementos, **si se permite la repetición de los mismos**. En términos de aplicaciones de conjuntos, en este caso se trataría de una aplicación **no inyectiva** entre el conjunto {1, 2, 3,…,n) y el conjunto {a_1, a_2, a_3, …, a_m)

Según esta definición, en las variaciones interviene el orden.

El arreglo de la imagen anterior es un ejemplo de variación con repetición de 5 elementos tomados de 5 en 5.

El número total de variaciones de este tipo viene dado por la fórmula $\mathbf{VRm,n = m^n}$

En el ejemplo anterior el número total de variaciones sería $5^5 = 3.125$

Otro ejemplo: el número total de posibles quinielas de 14 partidos será $3^{14} = 4.782.969$

Variaciones sin repetición

Llamaremos **variaciones sin repetición** de **m** elementos tomados de **n** en **n**, (simbolizadas por **Vm,n**) a todos los arreglos de **n** elementos que se pueden formar en un conjunto de **m** elementos, **si no se permite la repetición de los mismos**. Si deseamos usar el concepto de aplicación, se trataría de una aplicación inyectiva entre el conjunto {1, 2, 3,…,n) y el conjunto $\{a_1, a_2, a_3, \ldots, a_m)$

Se pueden considerar otras interpretaciones de las variaciones:

- Formas de elegir ordenadamente **n** elementos distintos de un conjunto de **m** elementos

- Órdenes totales posibles definidos en todos los subconjuntos de orden **n**.

El número total de variaciones de este tipo viene dado por la fórmula

$V_{m,n} = m(m-1)(m-2)...(m-n+1) = m!/(m-n)!$

Según la notación explicada más arriba, esta expresión también se puede escribir como **$m^{(n}$**

Dos variaciones se pueden distinguir entre sí o por los elementos que contienen o por su orden. Esta es la caracterización clásica de las variaciones.

Si en una carrera intervienen 9 atletas, la composición del podio puede presentar $V_{9,3}=9\times8\times7 = 504$ resultados distintos.

Permutaciones ordinarias

Se llaman permutaciones ordinarias o sin repetición (**Pn**) a las variaciones sin repetición en las que **m=n**, es decir, que en cada arreglo entran **todos** los elementos del conjunto.

Dos permutaciones sobre un conjunto se distinguen sólo por el orden de los elementos. Por ello se pueden identificar con los distintos órdenes que se pueden establecer en los elementos de un conjunto.

También se llaman permutaciones a las **aplicaciones biyectivas** de un conjunto en sí mismo. Es el concepto tradicional de **sustitución** en un conjunto. Más adelante trataremos este concepto de permutación como aplicación biyectiva interna en un conjunto.

El número de permutaciones formadas con un conjunto de n elementos coincide con su factorial: **Pn = n!**

Un caso especial de permutaciones es el de las **circulares**, que son las distintas formas de ordenar unos objetos en círculo (por ejemplo, invitados a una cena). Su número es (**n-1)!**

Permutaciones con repetición

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

Para calcular el número de permutaciones de este tipo bastará dividir el factorial del número total de símbolos, contando sus repeticiones, entre el número de veces que se repite cada uno.

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

En el ejemplo, el número de permutaciones de la palabra CATAPULTA sería de 9!/(3!×2!) =30240

Combinaciones

Llamaremos **combinaciones** de **m** elementos tomados de **n** en **n**, (simbolizadas por **Cm,n**) a todos los subconjuntos de **n** elementos que se pueden formar en un conjunto de **m** elementos.

Por su propia definición se deduce que el orden no interviene para distinguir unas combinaciones de otras.

El número total de combinaciones viene dado por la fórmula

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

Combinaciones con repetición

Las combinaciones con repetición ***CRm,n*** de **m** elementos tomados de **n** en **n** admiten varias definiciones. Se usan todas porque es un concepto más difícil que los anteriores y para abrir aplicaciones diversas de este tipo de arreglos.

Podemos elegir las siguientes:

(1) Son los distintos arreglos que se pueden formar en un conjunto de **m** elementos de forma que en cada uno se elijan **n** elementos que pueden ser repetidos y se diferencien unos arreglos de otros sólo en los elementos que los forman y no por el orden elegido.

(2) Son aplicaciones del conjunto (1,2,3...n) en el

conjunto dado con la condición de que sean crecientes en sentido amplio. Esta definición se entenderá bien.

(3) Las ***CRm,n*** equivalen a un reparto de **m** objetos en **n** cajas. Se supone que dentro de las cajas no se tiene en cuenta el orden. Para muchas cuestiones resulta ser la mejor definición.

(4) Las ***CRm,n*** equivalen al conjunto de todas las soluciones enteras positivas de la ecuación

$$x_1 + x_2 + \ldots + x_n = m$$

La fórmula para calcular CRm,n se puede expresar de varias formas:

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

También se interpretan como coeficientes multinomiales, que son los correspondientes a la fórmula de Leibnitz para la potencia de un polinomio. Su desarrollo con notación simplificada es

$$(a+b+c+d+\cdots)^k = \sum_{m+n+p+q+\cdots=k} \binom{k}{m,n,p,q,\ldots} a^m b^n c^p \ldots$$

En cualquier texto de Matemática Discreta puedes leer el desarrollo más detallado. Son muchos exponentes y subíndices.

Más adelante se estudiarán los coeficientes trinomiales.

Casi todos los problemas combinatorios elementales se pueden resolver con las definiciones y fórmulas anteriores, el concepto de producto cartesiano y los principios fundamentales que se explican a continuación.

Representaremos por Card(A) el cardinal de un conjunto A, es decir, su número de elementos si es finito.

Principio de la Adición

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

$$Card(A_1 \cup A_2 \cup ... \cup A_k) = Card(A_1) + Card(A_2) + ... + Card(A_k)$$

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

Consecuencias de este principio (que se puede demostrar rigurosamente) son:

Si A está incluido en B, el cardinal de A será menor o igual que el de B

Si A y B no son disjuntos, el principio de adición se deberá corregir así:

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

Es decir, en la suma se deben restar los elementos repetidos

Esta fórmula se generaliza fácilmente a varios conjuntos, con la particularidad de que las intersecciones aparecerán con signos más o menos según el número de conjuntos que abarquen.

Principio de la Multiplicación

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

$Card(A_1 \times A_2 \times ... \times A_k) = Card(A_1) \times Card(A_2) \times ... \times Card(A_k)$

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

Como consecuencia, el número de aplicaciones que se pueden construir entre un conjunto A de cardinal n y otro B de cardinal m viene dado por

$A^B = m^n$

Este principio también se aplica cuando un arreglo se construye en varias etapas y las posibilidades de cada una son independientes de los resultados anteriores, por ejemplo en una tirada de tres dados.

También es útil al combinar dos conjuntos de arreglos distintos, como en las matrículas de los coches **D - 1234 - AZ**, en las que se combinan tres variaciones distintas.

Principio de Distribución

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

Lo desarrollaremos en dos versiones equivalentes:

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

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

Ambos principios, que resuelven muchas cuestiones combinatorias, los damos sin demostración.

Según ellos, en una clase con 35 alumnos, habrá al menos dos que compartan el mismo número de día del mes como cumpleaños. "Ambos nacieron un 12, pero de distinto mes". Si en un centro de enseñanza hay más de 366 alumnos, habrá al menos dos que compartan la misma fecha de cumpleaños. Lo que no sabemos es qué fecha será esa.

Principio de Inclusión y exclusión

Se llama así a la fórmula obtenida anteriormente

Card(A∪B) =Card(A) + Card(B) - Card(A∩B)

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

Card(A∪B∪C) =Card(A) + Card(B) + Card(C) - Card(A∩B) - Card(A∩C) - Card(B∩C) + Card(A∩B∩C)

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

$Card(\cup S_i) = \sum Card(S_i) - \sum Card(S_i \cap S_j) + \sum Card(S_i \cap S_j \cap S_k) + ... + (-1)^n \sum Card(S_i \cap ... \cap S_n)$

NÚMEROS COMBINATORIOS

Los números combinatorios o binomiales se definen por la fórmula

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

Equivalen al número de **combinaciones sin repetición** de **n** elementos tomados de **r** en **r**. También se llaman coeficientes binomiales, por serlo en el binomio de Newton.

En hoja de cálculo se representan como **COMBINAT(M;N)**.

Sus principales propiedades son:

$\binom{n}{0} = 1 \quad \binom{n}{n} = 1$

$$\binom{n}{r} = \binom{n}{n-r}$$

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$$

que aplicándola reiteradamente nos lleva a esta otra

$$\binom{n}{r} = \sum_{i=1}^{n-p-1} \binom{n-i}{p-i}$$

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots \binom{n}{n} = 2^n$$

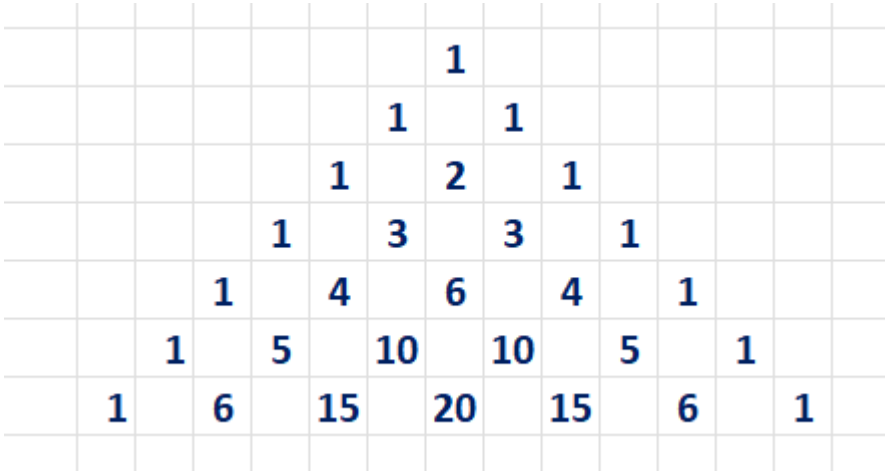
$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots (-1)^n \binom{n}{n} = 0$$

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n-1}{k} + \binom{n-2}{k} + \cdots + \binom{k}{k}$$

$$\binom{n+m}{k} = \binom{n}{0}\binom{m}{k} + \binom{n}{1}\binom{m}{k-1} + \binom{n}{2}\binom{m}{k-2} + \cdots + \binom{n}{k}\binom{m}{0}$$

(Identidad de Vandermonde, que, en realidad es también una convolución. Se puede usar para determinar de cuantas formas se pueden seleccionar **r** objetos de un conjunto que comprende dos tipos de ellos, n de tipo A y m de tipo B. Descompone ese número en los distintos repartos posibles entre los dos tipos)

Su conjunto ordenado en forma de triángulo toma el nombre de ***Triángulo de Pascal, de Tartaglia o Aritmético***



Es clásica la fórmula del Binomio de Newton, que expresa la potencia de un binomio en términos de números combinatorios siguiendo las filas de este triángulo . Su desarrollo es

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-1}$$

Mediante la sustitución de **a** y **b** por valores adecuados (1, -1,...) se pueden demostrar bastantes propiedades, como algunas de las contenidas en párrafos anteriores.

Es fácil demostrar esta colección de propiedades:

La suma de los elementos de la fila n es 2^n.

Basta considerar $(1+1)^n$

Los elementos de cada fila son simétricos, ya que

$$\binom{n}{r} = \binom{n}{n-r}$$

Cada elemento es suma de los dos que están sobre él en la fila anterior (recordando que los elementos exteriores al triángulo valen 0)

Basta acudir a

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$$

Las diagonales del triángulo, por orden, contienen:

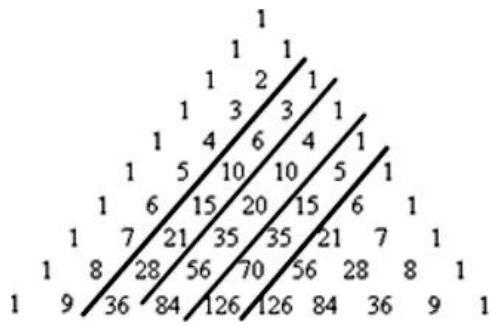
Fila de 1, 1, 1, 1, 1, …

Números naturales: 1, 2, 3, 4, 5, …

Triangulares. 1, 3, 6, 10, …

Tetraédricos: 1, 4, 10, 20, 35, …

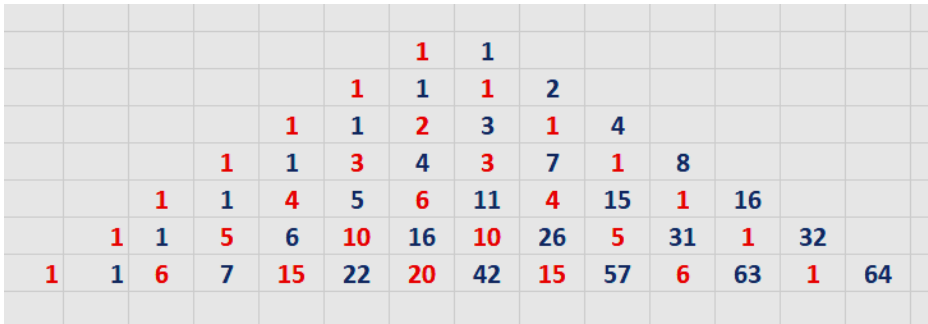
(Ver imagen)



Triángulo de Bernouilli

Si en el triángulo de Pascal volvemos a sumar cada dos elementos consecutivos, o bien, si vamos sumando elementos de una fila de forma acumulada, obtendremos el triángulo de Bernouilli. En la imagen están marcados

en rojo los elementos del triángulo de Pascal, y, en azul. Los de Bernouilli:



						1	1						
					1	1	1	2					
				1	1	2	3	1	4				
			1	1	3	4	3	7	1	8			
		1	1	4	5	6	11	4	15	1	16		
	1	1	5	6	10	16	10	26	5	31	1	32	
1	1	6	7	15	22	20	42	15	57	6	63	1	64

El último elemento de cada fila, al ser suma de toda ella, valdrá 2^k.

En Wikipedia puedes leer qué significado poseen en él las diagonales, y descubrirás la sucesión del “catering perezoso” y la de los “números pastel”.

(https://en.wikipedia.org/wiki/Bernoulli%27s_triangle)

GRUPOS DE PERMUTACIONES – CICLOS

Como una permutación equivale a una aplicación biyectiva de un conjunto en sí mismo, al igual que estas, formará **un grupo** (el grupo **simétrico** del conjunto) para la operación de **componer aplicaciones**. Toda la teoría que sigue es independiente del tipo que tengan los elementos del conjunto, por lo que supondremos en toda la sección que trabajamos con {1, 2, 3, …, n}

Es trivial considerar que se cumple la propiedad asociativa, que existe una permutación identidad (en la que no se altera el orden existente) y una permutación inversa.

Este grupo no posee la propiedad conmutativa. En general S×S' produce un resultado distinto a S'×S, pero sí existirán sustituciones permutables entre sí, como por ejemplo una sustitución y su inversa. Para destacar el carácter de aplicaciones biyectivas, las permutaciones las podemos escribir así:

(1 2 3 4 5 6 7 8)
(2 1 8 4 6 7 5 3)

en las que el conjunto de arriba sería el origen y el de abajo la imagen. Al conjunto de arriba le podemos llamar **numerador** y al de abajo **denominador**. Si aplicamos una misma permutación a ambos no se altera la correspondencia entre orígenes e imágenes, por lo que podemos escribir el numerador siempre en el mismo orden, al que llamaremos **principal**. Así, con números, podemos usar el orden creciente1, 2, 3, 4...

A este grupo le llamaremos **Grupo de Sustituciones** S_n del conjunto. Su número de elementos será **n!**

Descomposición en ciclos

Si en una permutación vamos recorriendo los transformados de cada elemento de forma consecutiva, pudiera ser que uno de ellos coincidiera con el primero, con lo que se habría cerrado un **ciclo o permutación circular**. Así, la permutación

(1 2 3 4 5 6 7 8)
(2 1 8 4 6 7 5 3)

contiene un ciclo que recorre 5 - 6 - 7 - 5, otro formado por el 3 y el 8, otro por el 1 y el 2 y un último que forma 4 consigo mismo.

Al considerar un ciclo se debe recordar que actúa sobre k elementos dejando invariantes los n-k restantes. Otro hecho que se debe tener en cuenta es que dentro del ciclo es indiferente cuál sea el primer elemento que se escriba. Así, (3,4,2), (4,2,3) y (2,3,4) representan el mismo ciclo.

Toda permutación se puede descomponer en ciclos.

Si prescindimos de escribir el conjunto origen, podríamos expresar este hecho de la siguiente forma:

(2 1 8 4 6 7 5 3) = (1 2)(3 8)(4)(5 6 7)

Esta descomposición es única salvo el orden y la forma de escribirla. Para encontrarla podemos usar este procedimiento sistemático:

Elegimos el elemento 1, y aplicamos la permutación de forma reiterada hasta que la imagen vuelva a ser 1. Como el conjunto es finito, esto se acabará logrando, con lo que ya tendremos el primer ciclo de la descomposición. Buscamos después el siguiente elemento que no pertenezca al ciclo conseguido (si hemos acabado es que la permutación estudiada se reduce a un solo ciclo, es cíclica) y efectuamos la misma operación para obtener el segundo ciclo, y así sucesivamente hasta agotar el conjunto.

Como cada ciclo opera sobre elementos distintos, dos ciclos de una misma descomposición serán siempre **permutables**.

La potenciación de sustituciones se define como su composición reiterada: $S^n = S \times S \times S ... \times S$ (n veces). Es también trivial demostrar que el conjunto de potencias de una sustitución S forma un subgrupo, llamado **cíclico** o **monógeno** engendrado por S

Recordamos la definición de **orden** de un elemento **a** en un grupo **G**, como el menor exponente natural (en notación multiplicativa) para el que $\mathbf{a^n = I}$ (identidad). Esto también es válido para sustituciones, y los grupos cíclicos engendrados por S, que tendrá cada uno un **orden**, que coincide con su número de elementos. Según la teoría de grupos, todos los órdenes serán divisores de n!

Es fácil demostrar esta propiedad:

Si una permutación se descompone en ciclos, su orden coincidirá con el M.C.M de los órdenes de dichos ciclos.

Así, la sustitución del ejemplo anterior tendrá orden 6.

CÁLCULOS INTERESANTES

Multiconjuntos

Un ***multiconjunto*** (*multiset* en inglés) es un conjunto en el que se permite la repetición de algunos o todos sus elementos un número determinado de veces, llamado *multiplicidad* del elemento. Al conjunto de elementos tomados sin repetición se le llama conjunto *subyacente*,

Un ejemplo claro son los conjuntos de tiradas en Combinatoria, las extracciones de bolas con repetición o el conjunto de los factores primos de un número. En todos ellos se permite que algunos elementos estén repetidos, Otro ejemplo típico es el las letras de una palabra. Por ejemplo, las letras de la palabra ZARAGOZA. Aquí se permite que la Z se repita dos veces y la A tres. Su conjunto subyacente es ZARGO.

Formalmente, un multiconjunto es un conjunto de elementos que son pares del tipo *(elemento, multiplicidad).* Por ejemplo, las letras de ZARAGOZA forman el multiconjunto

{(A,3),(Z,2),(R,1),(G,1),(O,1)}

Un **submulticonjunto** de un multiconjunto es otro multiconjunto cuyos elementos pertenecen al multiconjunto inicial con multiplicidades **no mayores** que las del mismo.

Así, GOZAR es submulticonjunto de ZARAGOZA, pero no lo es ARROZ, porque la R tiene una multiplicidad mayor.

Combinaciones con repetición

En todas las cuestiones sobre multiconjuntos la base son las combinaciones con repetición. Podremos usar la fórmula para n objetos tomados de k en k, fórmula elemental y conocida:

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

A partir de esta fórmula, los cálculos se basarán en ir rechazando combinaciones según las condiciones a los que se sometan. Por ejemplo, si una multiplicidad es 3, habrá que rechazar las combinaciones en las que aparezca ese elemento más de tres veces. Al final se llegará a expresiones similares a las siguientes:

CR(4,3)-CR(4,1)-CR(4,1)-CR(4,0)-CR(4,0)

Existen fórmulas exactas para los submulticonjuntos (ver https://arxiv.org/abs/2009.01233, ***m-submultisets and m-permutations of multisets elements)***, aunque con procesos guiados por el Principio de inclusión-exclusión se consigue el resultado correcto.

Permutaciones circulares o cíclicas

Puede ocurrir que una permutación sea en sí misma un ciclo. La llamaremos cíclica o circular. Dentro del grupo simétrico S_n el número de permutaciones cíclicas equivale a (n-1)! Es algo muy conocido y se justifica porque para inventarte una permutación de este tipo en primer lugar ordenar todos los elementos, lo que puedes realizar de n! formas diferentes y una vez elegida una, esta representa n circulares idénticas, porque tienes n formas de elegir el primer elemento, luego el número es n!/n=(n-1)!

Permutaciones de n elementos que son ciclos de orden k

Deberemos elegir k elementos para el ciclo y dejar los restantes n-k fijos. El elegirlos nos supone Cn,k formas y dentro de los elegidos, (k-1)! ciclos posibles, luego el número total de ciclos de orden k será

$$\binom{n}{k}(k-1)!$$

Permutaciones reducidas

Son aquellas que no dejan fijo ningún elemento, las que en la descomposición en ciclos ninguno de ellos tiene orden 1. Son las conocidas como desarreglos, que explicaremos más adelante.

Paridad de una permutación

Un caso particular de ciclo es el compuesto sólo por dos elementos. En este caso lo llamaremos **transposición**, y consiste en la permutación entre esos dos elementos, por ejemplo (3 8)

Todo ciclo se descompone en transposiciones, pero no de forma única. Así, tenemos que (1 2 3) = (1 2)(1 3) = (1 3)(2 3).

Lo que sí se conserva la **paridad**: todas las descomposiciones en ciclos de una misma permutación comparten el tener un número par o bien impar de transposiciones. Llamaremos permutación **par** a aquella que se puede descomponer en un número par de transposiciones, e igualmente definiremos la permutación **impar**.

Es fácil ver que transponiendo dos elementos de una permutación se añade o se quita una transposición, con lo que todas las permutaciones pares se pueden convertir de esta forma en pares, y viceversa. Por tanto.

En todo conjunto de n elementos se pueden definir n!/2 permutaciones pares y n!/2 impares

También es fácil demostrar que las pares forman **un semigrupo,** llamado **grupo alternado** del conjunto sobre el que actúan. No así las impares, que al componerse entre sí producen una par.

Se puede definir la **signatura** de una permutación como el número +1 si es par y el -1 si es impar.

Números de Stirling de primera clase.

Dado el grupo de permutaciones $\mathbf{S_n}$ sobre un conjunto de **n** elementos, se podría plantear la cuestión de cuántas permutaciones se pueden descomponer exactamente en k ciclos. A este número **S1(n,k)** así definido lo llamaremos **Número de Stirling de primera clase**.

Por ejemplo, el número S1(4,3) = 6 significa que hay seis permutaciones de 4 elementos (por ejemplo. en el conjunto 1234) que se pueden descomponer en 3 ciclos. Serían estas: (1)(2)(34), (1)(3)(24), (1)(4)(23), (2)(3)(14), (2)(4)(13) y (3)(4)(12).

Se puede definir S1(n,0) con n>0 como 0, y aceptaremos que S1(0,0)=1 y que S1(0,n)=0.

Es claro que se cumple que S1(n,n)=1 pues sólo obtendríamos la permutación identidad, y es fácil demostrar que S1(n,1)=(n-1)!

Los primeros números de Stirling de primera clase son

	0	1	2	3	4	5	6	7	8
0	1								
1	0	1							
2	0	1	1						
3	0	2	3	1					
4	0	6	11	6	1				
5	0	24	50	35	10	1			
6	0	120	274	225	85	15	1		
7	0	720	1764	1624	735	175	21	1	
8	0	5040	13068	13132	6769	1960	322	28	1

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

S1(n,r) = (n-1)×S1(n-1,r)+S1(n-1,r-1)

Se puede comprobar en la tabla.

Desarreglos

Dentro del grupo de permutaciones son interesantes aquellas llamadas ***desarreglos,*** en las que la imagen de cada elemento es distinta del mismo. Por ejemplo, S=3412, es un desarreglo, pues S(1)=2, S(2)=4, S(3)=1, S(4)=2. Un ejemplo clásico es el de las cartas a las que se asignan sobres con la dirección ya escrita, y si se emparejan al azar, los desarreglos se producirían

cuando todas las cartas se metieran en un sobre inadecuado (Problema de los sobres o de Montmort)

Si llamamos S a un desarreglo, se deberá cumplir que S(i) sea distinta de i para todo i del conjunto.

Para conseguir su fórmula es mejor contar las permutaciones contrarias F, es decir, en la que existe algún elemento fijo S(i)=i. Basta considerar que las que dejan fijo un sólo elemento son en total (n-1)!, las que dejan 2, (n-2)!... pero cada una deberá ser multiplicada por las formas de elegir un elemento, o dos, o tres, etc., es decir las combinaciones de los elementos que son fijos. Por el principio de inclusión-exclusión quedará:

$$F = \binom{n}{1}(n-1)! - \binom{n}{2}(n-2)! + \binom{n}{3}(n-3)! \dots - (-1)^n \binom{n}{n}$$

El número de desarreglos D equivaldrá a la diferencia de F con el número total de permutaciones, luego quedará:

$$D_n = n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! \dots + (-1)^n \binom{n}{n}$$

que se suele escribir más bien de esta forma:

$$D = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots (-1)^n \frac{1}{n!}\right)$$

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

El paréntesis es el desarrollo del número **1/e** truncado por los términos que dan cocientes enteros con n! Por ello podemos interpretar esta fórmula como "el número entero más cercano a n!/e"

Una propiedad importante de D_n, derivada de la fórmula anterior, es que tiende al límite (1/e)n! = 0,36787944n! cuando n tiende a infinito. Por tanto, para valores grandes de **n** podemos suponer que un 37% de las permutaciones de un conjunto de n elementos son desarreglos.

D_n también se calcula mediante recurrencias. Se puede demostrar que $D_n = nD_{n-1}+(-1)^n$, lo que unido a que $D_1=0$ y $D_2=1$ nos da la lista de los primeros subfactoriales: 0, 1, 2, 9, 44, 265, 1854...

Curiosidad:

El numero 148,349 es el único numero en que es igual a la suma de los subfactoriales de sus dígitos:

148,349 = !1 + !4 + !8 + !3 + !4 + !9

PARTICIONES DE UN CONJUNTO

Una partición de un conjunto C es una familia X de subconjuntos, disjuntos dos a dos, cuya unión coincide con el conjunto total. Es decir:

$$\cup X_i = C \;\; ; \;\; X_i \cap X_j = \varphi \quad \text{para todo par i, j}$$

Es interesante preguntarse cuántas particiones distintas de k conjuntos se pueden definir en un conjunto de n elementos. El resultado se denomina como **número de Stirling de segunda clase** y lo representaremos por S2(n,k). Así, el número S2(5,4) representará el número de particiones distintas en cuatro conjuntos disjuntos que se pueden definir en un conjunto de 5 elementos. Por ejemplo, en el conjunto {1,2,3,4,5} se pueden definir estas particiones de 4:

{1}{2}{3}{45}, {1}{2}{4}{35}, {1}{2}{5}{34}, {1}{3}{4}{25}, {1}{3}{5}{24}, {1}{4}{5}{23}, {2}{3}{4}{15}, {2}{3}{5}{14}, {2}{4}{5}{13}, {3}{4}{5}{12}.

En total 10, como se puede comprobar en la tabla de abajo.

Es claro que S2(n,0)=0 y que S2(n,1)=S2(n,n)=1 porque sólo hay una forma de partir un conjunto de n elementos en conjuntos de n elementos (él mismo) y también una sola forma de partirlo en n subconjuntos (los de un solo elemento).

La propiedad que permite generar estos números es:

S2(n,r) = r×S1(n-1,r)+S1(n-1,r-1)

Puedes comprobar esta propiedad en la siguiente tabla de números de Stirling de segunda clase:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	1									
1	0	1								
2	0	1	1							
3	0	1	3	1						
4	0	1	7	6	1					
5	0	1	15	25	10	1				
6	0	1	31	90	65	15	1			
7	0	1	63	301	350	140	21	1		
8	0	1	127	966	1701	1050	266	28	1	
9	0	1	255	3025	7770	6951	2646	462	36	1

El número total de particiones que admite un conjunto, independientemente de su estructura, se llama **número de Bell** del conjunto y se representa por B(n). Es evidente que se pueden deducir de los anteriores sumando toda una fila. Los primeros números de Bell son, por tanto:

0	1	2	3	4	5	6	7	8	9	10
1	1	2	5	15	52	203	877	4140	21147	115975

Particiones de un número

En toda esta sección nos referiremos a la descomposición de un número en sumandos.

Se llaman **particiones de un número natural N** a las distintas formas de descomponerlo en sumandos enteros positivos sin tener en cuenta el orden y admitiendo repetición de sumandos. Para no tener en cuenta el orden se puede exigir que los sumandos sean decrecientes en sentido amplio. Así es más fácil representarlos.

Al número total de particiones de N lo representaremos por la función P(N). Por tanto la afirmación anterior se puede representar como P(9)=30.

En efecto, el 9 se puede descomponer en estas sumas:

9, 8+1, 7+2, 7+1+1, 6+3, 6+2+1, 6+1+1+1, 5+4, 5+3+1, 5+2+2, 5+2+1+1, 5+1+1+1+1, 4+4+1, 4+3+2, 4+3+1+1, 4+2+2+1, 4+2+1+1+1,

4+1+1+1+1+1, 3+3+3, 3+3+2+1, 3+3+1+1+1, 3+2+2+2, 3+2+2+1+1, 3+2+1+1+1+1

3+1+1+1+1+1+1, 2+2+2+2+1, 2+2+2+1+1+1, 2+2+1+1+1+1+1, 2+1+1+1+1+1+1+1

1+1+1+1+1+1+1+1+1

Son 30 en total

Cada posible suma se puede representar mediante los llamados diagramas de Ferrer, en los que los sumandos se dibujan como conjuntos en filas.

Por ejemplo, 3+2+2+1+1 se puede representar así:

OOO
OO
OO
O
O

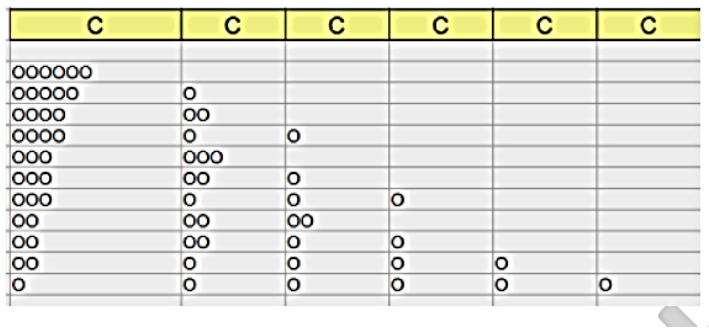
Puedes investigar en la Red las propiedades de estos diagramas.

El número de particiones se corresponde con el de soluciones no negativas de la ecuación diofántica $1x_1+2x_2+3x_3+\ldots nx_n = N$, como es fácil demostrar.

También coincide con el de soluciones no negativas de la ecuación diofántica $x_1+x_2+x_3+\ldots x_n = N$ si se exige que las soluciones formen una sucesión no creciente:

$$x_1>=x_2>=x_3>=...x_n$$

Igualmente, representa también las formas de repartir N objetos indistinguibles en cajas indistinguibles. En la imagen, extraída de una hoja de cálculo, puedes observar la distribución de seis bolas (11 particiones del número 6)



C	C	C	C	C	C
oooooo					
ooooo	o				
oooo	oo				
oooo	o	o			
ooo	ooo				
ooo	oo	o			
ooo	o	o	o		
oo	oo	oo			
oo	oo	o	o		
oo	o	o	o	o	
o	o	o	o	o	o

Más adelante estudiaremos otras funciones de partición condicionada de un número y su cálculo. Mientras tanto te puedes dedicar a comprobar (con piezas, bolitas o lápiz) estos resultados:

N	P(N)
1	1
2	2
3	3
4	5
5	7
6	11
7	15
8	22
9	30

10	42
11	56
12	77

No perderás el tiempo, porque es divertido encontrar estrategias para no olvidar ninguna suma.

Funciones de partición de un número

Hemos llamado P(N) al número de particiones en sumandos decrecientes del número N, pero se pueden definir otras:

Esta definición básica de número de particiones P(N) se puede someter a condicionamientos de los que surgirán nuevas definiciones. Las expresaremos así:

P(N / condicionamiento)

Vemos algunos ejemplos y sus propiedades

Función de partición Pk(N)

Es la misma función P(N) condicionada a que sólo intervenga un número K de sumandos:

$P_k(N)$= P(N / k sumandos): Particiones con un número k de sumandos fijado.

Su interés radica en que permite una fórmula de recurrencia para el cálculo de P(N). La demostración se puede consultar en manuales especializados.

$$p_k(n) = \sum_{i=1}^{k} p_i(n-k)$$

Se parte de $P_1(k)=1$ y de $P_k(k)=1$ y se van calculando todos los $P_k(N)$ por recurrencia.

Es claro que después de encontrar los valores de $P_k(N)$ bastará sumarlos todos para k menor o igual a N a fin de obtener P(N), pues la suma abarcaría todas las posibilidades.

El siguiente esquema está copiado de una hoja de cálculo programada para encontrar P(7)

		K	1	2	3	4	5	6	7
N									
1	1		1						
2	2		1	1					
3	3		1	1	1				
4	5		1	2	1	1			
5	7		1	2	2	1	1		
6	11		1	3	3	2	1	1	
7	15		1	3	4	3	2	1	1

Función de partición Q(N)

Como la anterior, cuenta el número de particiones, pero en este caso se exige que los sumandos sean todos distintos. Por ejemplo, el entero 7 admite las siguientes particiones como números distintos: 7 = 6+1 = 5+2 = 4+3 = 4+2+1, luego Q(7)=5

Euler demostró que esta función coincide con el número de particiones de n en partes impares.

FUNCIONES GENERATRICES

Un ejemplo introductorio

Antes de iniciar cualquier planteamiento teórico sobre las funciones generadoras (o generatrices), muy usadas en Combinatoria y en el estudio de las sucesiones de números, las introduciremos mediante un ejemplo.

Problema

Deseamos elegir nueve cuentas de colores. Disponemos de cantidad suficiente de cuentas rojas, amarillas y verdes, pero queremos elegir entre 2 y 5 rojas, menos de 4 amarillas y al menos 3 verdes. ¿De cuántas formas podemos efectuar la elección?

Este problema nos plantea el desarrollo de **particiones condicionadas** de un número. Independientemente de que se trate de particiones, intentaremos resolver el

problema con varias técnicas, y entre ellas la del uso de una función generatriz.

Con un producto cartesiano

Como de las rojas hemos de elegir entre 2 y 5, de las amarillas de 0 a 3 y de las verdes un mínimo de 3 y un máximo de 7 (¿por qué 7?), bastará formar el producto cartesiano {2,3,4,5}{0,1,2,3}{3,4,5,6,7} e ir eligiendo las ternas que sumen 9. Un problema totalmente elemental que se puede resolver en enseñanzas medias.

A poco que nos pongamos obtendremos: 9= 2+0+7 = 2+1+6 = 2+2+5 = 2+3+4 = 3+0+6 = 3+1+5 = 3+2+4 = 3+3+3 =4+0+5 = 4+1+4 = 4+2+3 = 5+0+4 = 5+1+3.

En total 13 particiones. Para este problema no se necesitarían más técnicas, pero lo estamos tomando como modelo sencillo de introducción.

Función generatriz

La idea revolucionaria de la función generatriz consiste en sustituir los distintos elementos numéricos por potencias de una indeterminada, **y los conjuntos convertirlos en polinomios**. Así el producto cartesiano {2,3,4,5}{0,1,2,3}{3,4,5,6,7} se puede escribir en forma de producto de polinomios:

$(x^2+ x^3+ x^4+ x^5)(1+x+ x^2+ x^3)(x^3+ x^4+ x^5+ x^6+ x^7)$

Es fácil darse cuenta de que si multiplicamos algebraicamente estos polinomios, el término de grado 9 tendrá como coeficiente el número de particiones pedido, en este caso 13.

Hemos sustituido una técnica de conteo por otra de tipo algebraico o analítico (esto último lo veremos más adelante)

En este caso tan sencillo parece que esto es una complicación, pero en casos generales veremos que puede resultar muy útil. Por dos motivos:

- Las técnicas algebraicas y analíticas permiten simplificar estos productos y encontrar directamente el coeficiente deseado.
- Al desarrollar estos polinomios no sólo resolvemos el problema para 9 cuentas, sino para cualquier otro total posible.

Disponemos en este caso de una ayuda, y es que sabemos sumar muy bien las progresiones geométricas. Así, el producto de polinomios dado se puede expresar como

$$P(x) = \frac{x^2(x^4-1)(x^4-1)x^3(x^5-1)}{(x-1)^3}$$

Este a su vez se puede simplificar

$$P(x) = \frac{x^{18} - 2x^{14} - x^{13} + x^{10} + 2x^9 - x^5}{(x-1)^3}$$

Con tres pasadas del algoritmo de Ruffini encontraremos todos los coeficientes (omitimos los que no influyen en el problema)

Grado	18	17	16	15	14	13	12	11	10	9	8
	1	0	0	0	-2	-1	0	0	1	2	0
1											
	1	1	1	1	-1	-2	-2	-2	-1	1	1
1											
	1	2	3	4	3	1	-1	-3	-4	-3	-2
1											
A	1	3	6	10	13	14	13	10	6	3	1
Grado	15	14	13	12	11	10	9	8	7		

Hemos destacado el que nos interesa: con grado 9 aparece el coeficiente 13, que es la solución, pero este procedimiento **nos devuelve mucho más**. Por ejemplo, con suma 7 sólo son posibles estas elecciones: 7=2+0+5=2+1+4=2+2+3=3+0+4=3+1+3=4+0+3, **seis en total**, como marca el esquema, y con suma 14 sólo deberán aparecer 3. Son estas: 4+3+7 = 5+3+6 = 5+2+7

Hemos resuelto varios problemas en uno

La teoría

En el apartado anterior presentábamos como un artificio sustituir los elementos de un producto cartesiano

condicionado de conjuntos numéricos por polinomios en una indeterminada con exponentes idénticos a los números a combinar.

Ahora lo convertiremos en un desarrollo teórico.

Función generatriz de un conjunto numérico

Dado un conjunto ordenado de números reales o complejos (aquí usaremos casi exclusivamente los enteros positivos) $\{a_0, a_1, a_2, a_3, \ldots a_n\}$ llamaremos función generatriz (ordinaria) o generadora del mismo al polinomio de la forma

$$P(x) = a_0 + a_1 x^1 + a_2 x^2 + a_3 x^3 + \cdots a_4 x^n = \sum_{i=0}^{n} a_i x^i$$

Si el conjunto tiene infinitos términos sustituiremos el polinomio por una serie de potencias, pero en este caso la igualdad

$$P(x) = a_0 + a_1 x^1 + a_2 x^2 + a_3 x^3 + \cdots = \sum_{i=0}^{\infty} a_i x^i$$

sólo tendrá sentido si dicha serie posee un radio de convergencia no nulo y la función está definida dentro de ese radio. No obstante, aquí no trataremos la convergencia, sino las relaciones entre coeficientes. Si

no converge, P(x) no será una función, pero las técnicas siguen valiendo.

Casos sencillos

El caso más sencillo de función generatriz es la que corresponde al conjunto {1, 1, 1, 1,…1}

Si este es finito con **n** elementos, sabemos que su función generatriz se puede obtener mediante la fórmula de la suma de una progresión geométrica

$$1 + x + x^2 + x^3 + ... + x^n = \frac{1 - x^{n+1}}{1 - x}$$

Ya usamos esta fórmula anteriormente.

Si el conjunto es infinito {1, 1, 1, 1,…}también es sencillo verificar que

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1 - x}$$

Aquí nos encontramos con la potencia que tiene este método. Si derivamos miembro a miembro (omitimos detalles y también la cuestión de la convergencia) nos encontraremos con que

$$1 + 2x + 3x^2 + 4x^3 + \cdots = \frac{1}{(1 - x)^2}$$

Por tanto esta es la función generatriz del conjunto {1, 2, 3, 4,….}

La fórmula del binomio de Newton nos proporciona otro ejemplo de función generatriz. Los números combinatorios para un n dado tienen por función generatriz **$(1+x)^n$** ya que

$$(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$$

Podíamos seguir dando ejemplos hasta llenar páginas enteras, pero destacaremos especialmente dos técnicas

Manipulación algebraica

Con las técnicas algebraicas y sin plantearnos ahora el problema de la convergencia podemos encontrar la función generatriz de muchos conjuntos de coeficientes.

Por ejemplo, es fácil encontrarla para los números de Fibonacci F_0, F_1, F_2, F_3, F_4…, de los que suponemos se conocen sus valores y propiedades. Observa estas manipulaciones:

$F(x)=F_0+F_1x+F_2x^2+ F_3x^3+ F_4x^4+\ldots=$

$F_0+F_1x+(F_0+F_1)x^2+(F_1+F_2)x^3+(F_2+F_3)x^4+\ldots =$

$F_0+F_1x+(F_0 x^2+ F_1 x^3+ F_2 x^4+\ldots) + (F_1 x^2+ F_2 x^3+ F_3 x^4+\ldots)$

Pero en los paréntesis se está reconstruyendo F(x) de alguna forma, por lo que podemos escribir (pon tú los detalles)

$F(x)= F_0+F_1x+F(x) x^2+(F(x)- F_0)x$

Despejamos F(x), sustituimos F_0 por su valor 0 (a veces se toma 1) y F_1 por 1 y ya la tenemos:

$$F(x) = \frac{x}{1 - x - x^2}$$

Sólo hemos usado técnicas algebraicas sencillas. Más adelante comprobaremos este resultado.

Manipulación analítica

Si consideramos la derivación e integración formales podemos encontrar fácilmente funciones generatrices. Ya hemos considerado un ejemplo de derivación.

De la misma forma podemos usar la integración. Por ejemplo en la geométrica podemos integrar

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1 - x}$$

Nos resultaría entonces

$$o + x + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \frac{1}{4}x^4 + \cdots = ln\frac{1}{1 - x}$$

En cualquier manual puedes encontrar muchos ejemplos similares de este tipo de manipulación. No olvides que podemos mezclar las dos técnicas, analítica y algebraica, así como sumar, multiplicar y otras.

Problema inverso

Si la serie que define la función generatriz converge y conocemos esta, encontrar los coeficientes de la misma siempre es posible por la fórmula de McLaurin

$$P(x) = \sum_{n=0}^{\infty} \frac{P^{(n)}(0)}{n!} x^n$$

Es un camino muy pesado, pero seguro. Sin embargo el problema contrario de dar los coeficientes y encontrar la expresión de P(x) quizás no lo puedas resolver. Es el clásico problema de la suma de series.

Con la ayuda de un ordenador se puede simplificar el proceso. Damos un ejemplo:

Antes vimos que los números de Fibonacci tenían como función generatriz (si se toma F_0=0. A veces se toma F_0=1 y entonces tiene una expresión ligeramente distinta)

$$F(x) = \frac{x}{1 - x - x^2}$$

Si tuviéramos posibilidad de desarrollar por McLaurin en algún lenguaje o programa, nos ahorraríamos mucho trabajo. Nosotros lo hemos hecho con el lenguaje PARI. Se entiende fácilmente aunque no se haya usado nunca:

{write("final.txt",taylor(x/(1-x-x^2), x,12))}

Ordenamos que escriba en el archivo "***final.txt***" 12 términos del desarrollo de Taylor (es en x=0) de la función dada. El resultado es:

0+x + x^2 + 2×x^3 + 3×x^4 + 5×x^5 + 8×x^6 + 13×x^7 + 21×x^8 + 34×x^9 + 55×x^10 + 89×x^11 + O(x^12)

Como vemos, los coeficientes son los números de Fibonacci. Si quisiéramos hacer F_0=1 nos daría otro resultado, pues la función generatriz seria $1/(1-x-x^2)$ (intenta demostrarlo)

Programaríamos en PARI esta variante:

{write("final.txt",taylor(1/(1-x-x^2), x,12))}

Obtendríamos la sucesión comenzando en 1:

1 + x + 2×x^2 + 3×x^3 + 5×x^4 + 8×x^5 + 13×x^6 + 21×x^7 + 34×x^8 + 55×x^9 + 89×x^10 + 144×x^11 + O(x^12)

Lo podemos intentar con el ejemplo del aparatado anterior, el de las bolas de colores, cuya función generatriz sin desarrollar era

$$P(x) = \frac{x^2(x^4-1)(x^4-1)x^3(x^5-1)}{(x-1)^3}$$

Deberíamos escribir en PARI

{write("final.txt",taylor(x^5×(x^4-1)^2×(x^5-1)/(x-1)^3, x,20))}

Obtendríamos

x^5 + 3×x^6 + 6×x^7 + 10×x^8 + 13×x^9 + 14×x^10 + 13×x^11 + 10×x^12 + 6×x^13 + 3×x^14 + x^15 + O(x^20)

Identificamos los resultados anteriores: Con grado 9 el coeficiente es el esperado, 13. Para el grado 14 sólo 3 y para el grado 7 los 6 que ya se obtuvieron.

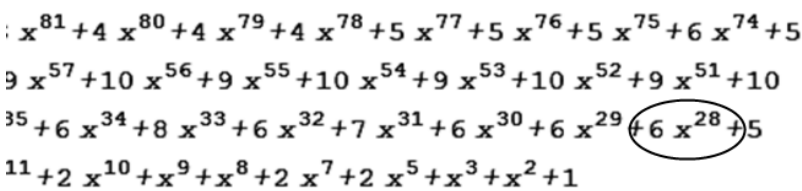
Más adelante veremos las funciones generatrices de combinaciones, variaciones y demás. Ahora seguiremos con ejemplos:

¿De cuántas formas se puede descomponer el número 28 como suma de primos distintos?

Los primos inferiores a 28 son 2, 3, 5, 7, 11, 13, 17, 19, 23. Cada uno de ellos o está en la suma una vez o no está. Entonces podemos usar términos del tipo $(1+x^7)$ o $(1+x^{11})$ para combinarlos en la función generatriz:

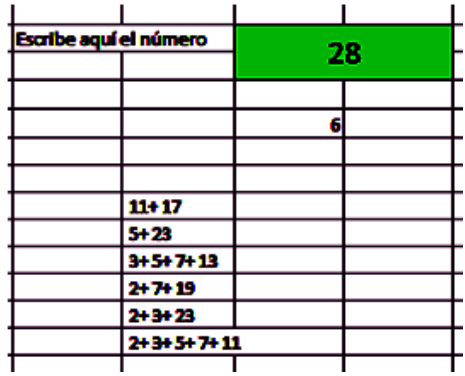
$F(x)= (1+x^2)\ (1+x^3)\ (1+x^5)\ (1+x^7)\ (1+x^{11})\ (1+x^{13})\ (1+x^{17})\ (1+x^{19})\ (1+x^{23})$

Desarrollamos con wxMmaxima y nos da (hemos recortado la imagen):



Vemos que para el exponente 28 el coeficiente es 6, luego existen 6 formas distintas de expresar 28 como suma de primos distintos

Lo comprobamos con nuestra herramienta PARTLISTA (http://hojamat.es/sindecimales/aritmetica/herramientas/herrarit.htm#reprenum)



Con ella vemos las seis sumas:

28=11+17=5+23=3+5+7+13=2+7+19=2+3+23=2+3+5+7+11

Con la función generatriz hemos conseguido también otros muchos coeficientes, pero cuidado con la lista de primos 2, 3, 5, 7, 11, 13, 17, 19, 23. Este desarrollo sólo valdría hasta el 28. Para números mayores deberíamos añadir $(1+x^{29})(1+x^{31})$…

Con la función generatriz podemos resolver varios problemas a la vez.

Estos desarrollos algebraicos son pesados incluso con ayuda de los CAS. Sería bueno elegir un solo coeficiente en ellos. El lenguaje PARI que estamos usando últimamente (es gratuito aunque de gestión poco amigable) posee la función POLCOEFF(P(x),E) en la

que P(x) es un polinomio y E un exponente dado, y nos devuelve el coeficiente de ese polinomio correspondiente al grado E. Nuestro problema del 28 se calcularía así:

print(polcoeff((x^2+1)×(x^3+1)×(x^5+1)×(x^7+1)×(x^11+1)×(x^13+1)×(x^17+1)×(x^19+1)×(x^23+1),28))

Daría un resultado de 6. Si cambiamos 28 por un número inferior obtendremos más resultados. Para números superiores deberíamos incrementar los primos.

Combinaciones y variaciones

Ya vimos esta relación

$$(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$$

Es el clásico Binomio de Newton y nos da de forma inmediata la función generatriz de las **combinaciones de n elementos sin repetición**.

Esta forma de expresar los números combinatorios da lugar a demostraciones muy sencillas de algunas de sus propiedades. Observa esta identidad

$$(1+x)^m \cdot (1+x)^n = (1+x)^{m+n}$$

Si la desarrollas da lugar a la identidad de Vandermonde

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}$$

Basta imaginarse cómo sería el producto de las dos potencias

De igual forma, de esta otra identidad

$$(1+x)^{n+1} = (1+x)^n + x(1+x)^n$$

Nos resultaría

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

Basta con igualar términos con el exponente k

Así se podría demostrar otras similares.

Combinaciones con repetición

La fórmula del binomio de Newton es válida también para exponente negativo, pero en ese caso los números combinatorios tendrían la forma

$$\binom{-n}{r} = \frac{(-n)(-n-1)(-n-2)\ldots}{r!} = (-1)^r \frac{(n)(n+1)(n+2)\ldots(n+r-1)}{r!}$$

Pero la última expresión coincide con las combinaciones con repetición, luego

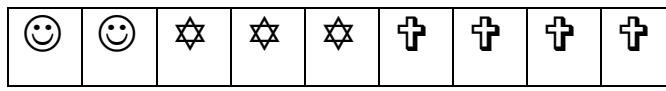
$$(1+x)^{-n} = \sum_{r=0}^{n} (-1)^r \binom{n+r-1}{r}$$

Sería, teniendo en cuenta los signos, la F.G. de las combinaciones con repetición.

Caso de elementos con repetición prefijada

Este es el caso con el que comenzamos a estudiar las F.G. Si deseamos combinaciones con repetición, pero en las que algunos elementos tienen un máximo en su repetición (no se suele estudiar este caso en los niveles elementales), debemos usar otra técnica. Por ejemplo:

Disponemos de varias fichas en cada una de las cuales se ha dibujado una forma distinta. Por ejemplo esta distribución:



¿De cuántas formas distintas se puede tomar un conjunto de cinco símbolos? Al hablar de conjunto, no tendremos en cuenta el orden.

Basta usar, como ya vimos, un producto de polinomios en los que los exponentes representan las repeticiones posibles de cada símbolo:

$$\mathbf{F(x)=(1+x+x^2)(1+x+x^2+x^3)(1+x+x^2+x^3+x^4)}$$

Buscamos con PARI su coeficiente de grado 5, que representa los elementos seleccionados:

print(polcoeff((x^2+x+1)×(x^3+x^2+x+1)×(x^4+x^3+x^2+x+1),5))

con un resultado de 11 posibilidades

Son estas:

X1	X2	X3	X4
0	1	4	
0	2	3	
0	3	2	
1	0	4	
1	1	3	
1	2	2	
1	3	1	
2	0	3	
2	1	2	
2	2	1	
2	3	0	

Podemos interpretarlas así:

✞✞✞✞✡ ✞✞✞✡✡ ✞✞✡✡✡ ✞✞✞✞☺ ✞✞✞✡☺ ✞✞✡✡☺

✞✡✡✡☺ ✞✞✞☺☺ ✞✞✡☺☺ ✞✡✡☺☺ ✡✡✡☺☺

Este método es general: para crear la F.G, en un caso de combinaciones con repeticiones prefijadas **basta con formar polinomios de potencias para cada uno de los elementos** y después multiplicarlos todos.

Funciones generatrices exponenciales

Hasta ahora hemos manejado combinaciones, no hemos tenido en cuenta el orden. Cuando éste interviene, para abordar las variaciones y permutaciones, necesitamos otro tipo de funciones generatrices, las exponenciales:

Dada una sucesión de números (en general complejos) $\{a_0, a_1, a_2, a_3, \ldots a_{n,\ldots}\}$ llamaremos **función generatriz exponencial** de esa sucesión a la formada por

$$E(x) = a_0 + \frac{a_1 x}{1!} + \frac{a_2 x^2}{2!} + \frac{a_3 x^3}{3!} + \frac{a_4 x^4}{4!} + \cdots$$

Es idéntica a la definición general, pero en cada término de la suma dividimos entre el factorial del exponente. La raíz de esta técnica está en el desarrollo del binomio de Newton, en el que podemos sustituir Cm,n por Vm,n/n!

De esta forma, si $(1+x)^m$ era la F.G. de las combinaciones, también será ahora la **F.G exponencial de las variaciones**. Esta idea no es de mucha utilidad así en general, pero nos será muy útil en lo que sigue.

Variaciones con elementos repetidos

Un caso que no se suele estudiar en las enseñanzas medias es el las variaciones en las que se permite un máximo de repeticiones para cada elemento. Por ejemplo, tomar variaciones de 4 elementos en este conjunto de elementos con repetición: AAABBCDD.

Efectuamos previamente un acercamiento sin F.G.

En la imagen hemos obtenido todas las posibles combinaciones, escribiendo en cada columna el número de veces que se toman A,B,C y D, contando después las distintas ordenaciones de cada una. La suma obtenida fue de 162 variaciones.

X1	X2	X3	X4	X5	X6
0	1	1	2		12
0	2	0	2		6
0	2	1	1		12
1	0	1	2		12
1	1	0	2		12
1	1	1	1		24
1	2	0	1		12
1	2	1	0		12
2	0	0	2		6
2	0	1	1		12
2	1	0	1		12
2	1	1	0		12
2	2	0	0		6
3	0	0	1		4
3	0	1	0		4
3	1	0	0		4
					162

Probamos ahora con una F.G. exponencial para cada elemento, hasta 3 para A, 2 para B y D y una para C. Observa que los términos de los polinomios están divididos entre factoriales.

FG=(1+x+x^2/2+x^3/6)(1+x+x^2/2)(1+x)(1+ x+x^2/2)

Desarrollamos esta función con wMaxima

```
(%i1) p:(1+x+x^2/2+x^3/6)*(1+x+x^2/2)*(1+x)*(1+ x+x^2/2);
      ratexpand(p);
```

$$(\%o1)\quad (x+1)\left(\frac{x^2}{2}+x+1\right)^2\left(\frac{x^3}{6}+\frac{x^2}{2}+x+1\right)$$

$$(\%o2)\quad \frac{x^8}{24}+\frac{x^7}{3}+\frac{11\,x^6}{8}+\frac{11\,x^5}{3}+\frac{27\,x^4}{4}+\frac{26\,x^3}{3}+\frac{15\,x^2}{2}+4\,x+1$$

Nos resulta para el exponente 4 un coeficiente de 27/4, pero recordemos que es una F.G. exponencial, luego hay que multiplicar por 4! para encontrar el verdadero coeficiente, el número de variaciones:

27/4×4!=27×6=162, que confirma el resultado previo.

Lo que hemos aprovechado en realidad es que al escribir estos paréntesis **cada elemento está representado por**

los órdenes que puede presentar. Si usamos este factor (1+x+x^2/2+x^3/6) lo que estamos comunicando es que x^2 presenta dos posibles órdenes (que al repetir el símbolo se han perdido) y que x^3 proviene de 6 órdenes (permutaciones con tres elementos)

Quiere decir lo anterior que las contribuciones al coeficiente final de x^4, 27/4, ya vienen descontados los órdenes que se han perdido al repetir. Al final, al multiplicar por el factorial de 4, nos quedamos con los órdenes verdaderos. Es un poco complicado de entender, pero estúdialo, que funciona.

Lo comprobamos para el variaciones de 3 elementos: el coeficiente es 26/3 y si multiplicamos por 3! nos queda 26×2=52

Lo generalizamos sin demostración:

Para encontrar el número de variaciones con repetición en el que conocemos el número máximo de repeticiones de un elemento, sean por ejemplo k, aportaremos a la F.G. un factor del tipo $1+x+x^2/2!+x^3/3!+\ldots+x^k/k!$ por cada elemento.

Permutaciones con repetición

La función generatriz que hemos empleado para variaciones coincide con la de permutaciones si el coeficiente que buscamos coincide con el total de las repeticiones de símbolos. En el ejemplo que estamos usando, AAABBCDD, el total de elementos es 8. Busca

en el desarrollo mediante wMaxima de arriba el exponente 8 de la F.G. y verás que es 1/24. Como estamos usando funciones exponenciales, el verdadero valor será (1/24)×8! = 1680.

En este caso no es necesaria la F.G., pues ya sabemos que el número de permutaciones de AAABBCDD se calcula mediante 8!/(3!2!1!2!) =8!/24 = 1680, pero es conveniente comprobar que en este caso también funciona la técnica de las F.G.

PARTICIONES Y FUNCIONES GENERATRICES

Al unir los conceptos de partición y función generatriz nos dan resultados mucho más potentes.

Particiones ordinarias P(n)

En un apartado anterior las estudiamos desde un punto de vista general. Aplicaremos ahora el concepto de función generatriz.

Supongamos que deseamos encontrar todas las particiones ordinarias del número 6 (formas de representar 6 como suma con posible repetición de sumandos). Para ello no necesitamos ni funciones ni técnicas informáticas. Con un poco de atención

llegaremos a que el 6 se descompone en suma de las siguientes formas:

6 = 5+1 = 4+2 = 4+1+1 = 3+3 = 3+2+1 = 3+1+1+1 = 2+2+2 = 2+2+1+1 = 2+1+1+1+1 = 1+1+1+1+1+1

Son once en total. Se supone que no se tiene en cuenta el orden.

Si queremos expresar este proceso mediante funciones generatrices hay que recordar que sus sumandos provenían de exponentes en un polinomio. En efecto, en este caso del 6 podemos considerar la función

$F(x) = (1+x+x^2+x^3+\ldots)(1+x^2+x^4+x^6\ldots)(1+x^3+x^6+x^9\ldots)\ldots(1+x^6+x^{12}+x^{18}\ldots)$

Si multiplicamos todo, el término de grado 6 se compondrá de todos los productos en los que el primer paréntesis aporta los sumandos iguales a 1, el segundo los que valen 2, el tercero, 3, y así hasta llegar al 6. Hemos tomado infinitas potencias en cada uno porque las mayores que 6 no van a influir, pero gracias a ello la expresión se simplifica como una progresión geométrica:

$$F(x) = \frac{1}{1-x}\frac{1}{1-x^2}\frac{1}{1--x^3}\cdots\frac{1}{1-x^6}$$

O expresado de forma sintética y generalizando hasta n:

$$F(n) = \prod_{j=1}^{n} \frac{1}{1 - x^j}$$

Después volveremos a esta función generatriz para adaptarla a casos particulares. La comprobamos para n=6. Vimos en anteriormente que con PARI se pueden desarrollar fácilmente.

print(taylor(1/(1-x)/(1-x^2)/(1-x^3)/(1-x^4)/(1-x^5)/(1-x^6),x,7))

Resultado:

1+x+2x^2+3x^3+5x^4+7x^5+**11x^6**+O(x^7) con el coeficiente 11 para x^6, como era de esperar.

Serían las once particiones esperadas. Como en ocasiones anteriores, este método nos da más, pues podemos leer otros coeficientes: con el 5 tendríamos 7 particiones, con el 4, 5, y así…A la inversa, si en lugar de pararnos en el 6 hubiéramos seguido escribiendo factores, obtendríamos más particiones, para 7, 8,… Así que recordemos la función generatriz (F.G.) para las particiones ordinarias del número n:

$$F(n) = \prod_{j=1}^{n} \frac{1}{1 - x^j}$$

Intenta obtener otros resultados similares al planteado en este ejemplo. Lo importante es que recuerdes la definición de partición de un número y su F.G.

Particiones en sumandos distintos Q(N)

Si al descomponer un número en sumandos no permitimos que figuren repetidos, obtendríamos resultados muy distintos, recogidos como la función de partición Q(n)

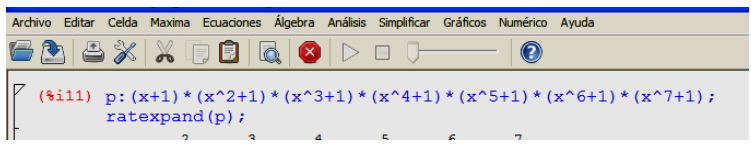
En este caso la función generatriz se simplifica mucho, pues en los paréntesis no han de figurar todas las potencias sino una sola por cada sumando. Así, para n=7 la F.G. sería

$F(x) = (1+x)(1+x^2)\,(1+x^3)\ldots\,(1+x^7)$

y generalizando para n

$$F(x) = \prod_{j=1}^{n}\left(1 + x^{j}\right)$$

Para el caso de 7 podemos expandir la F.G. mediante wxMaxima



Obtendremos un desarrollo en forma de polinomio, pero sólo serán útiles los coeficientes menores o iguales a 7:

$5x^7+4x^6+3x^5+2x^4+2x^3+x^2+x+1$

Ya tenemos la solución, el 7 se puede descomponer en 5 formas diferentes como suma de números naturales distintos:

7=6+1=5+2=4+3=4+2+1

Además, hemos obtenido que el 6 tiene 4 descomposiciones, el 5, 3 y así hasta el 1. Recuerda: estos son los únicos fiables en el desarrollo.

Particiones en partes impares P(N/Impar)

Aquí vemos rápidamente la utilidad de la función generatriz. Si en la fórmula general de las particiones eliminamos los pares de los paréntesis quedaría

$F(x) = (1+x+x^2+\ldots)(1+x^3+x^6+x^9\ldots)(1+x^5+x^{10}+x^{20}\ldots)\ldots(1+x^{2k+1}+x^{4k+2}+x^{6k+3}\ldots)$

que fácilmente se traduce, al igual que en las particiones ordinarias, a cocientes:

$$F(x) = \frac{1}{1-x}\frac{1}{1-x^3}\frac{1}{1-x^5}\frac{1}{1-x^7}\cdots$$

O bien

$$F(n) = \prod_{j=1}^{n}\frac{1}{1-x^{2j-1}}$$

Por ejemplo, para n=7, usando PARI, nos resultaría

print(taylor(1/(1-x)/(1-x^3)/(1-x^5)/(1-x^7),x,8))

1+x+x^2+2×x^3+2×x^4+3×x^5+4×x^6+5×x^7+O(x^8)

Como el coeficiente de x^7 es 5, ese será el número de particiones en impares. Como son tan pocas, las podemos escribir directamente: 7 = 5+1+1 = 3+3+1 = 3+1+1+1+1 = 1+1+1+1+1+1+1

Intenta comprobar, como en los casos anteriores, que con 6 resultarían 4, con 5, 3, y así con todos los coeficientes resultantes.

.En realidad siempre es así, como demostró Euler usando funciones generatrices:

El número de particiones de un número en sumandos distintos coincide con el de particiones en sumandos impares

Con el uso de las F.G. todo se reduce a un artificio algebraico:

Demostración

Todo se basa en que

$$1 + x^k = \frac{1-x^{2k}}{1-x^k}$$

Así que partiendo de la F.G. de la partición en elementos distintos, representamos cada factor de esta forma, se

simplificarán los factores de exponente par y sólo quedarán los impares en el denominador

$$Q(x) = \prod_{j=1}^{n}\left(1 + x^{j}\right) = \prod_{j=1}^{n}\frac{1 - x^{2j}}{1 - x^{j}} = \prod_{j=1}^{n}\frac{1}{1 - x^{2j-1}} = P(n/impar)$$

En el caso de n=7 te proponemos una correspondencia biyectiva por el método de Sylvester. Para que pienses un poco más sólo daremos el proceso y tú sacas tus consecuencias:

7=6+1=5+2=4+3=4+2+1 = 2×3+1 = 5+2×1=4×1+3=4×1+2×1+1 y ahora sustituimos cada producto por la suma correspondiente: 7 = 3+3+1 = 5+1+1 = 1+1+1+1+3 = 1+1+1+1+1+1+1

Para el camino inverso deberíamos expresar cada suma de repetidos como suma respecto a potencias de 2 distintas que se sacan como factor común.

7 = 3+3+1 = 5+1+1 = 1+1+1+1+3 = 1+1+1+1+1+1+1 = ×2+1=5+2×1=4×1+3=4×1+2×1+1

Serían siempre todos distintos, porque o se diferencian en el números sacado factor común o en las distintas potencias de 2.

Particiones con sumandos restringidos

En el anterior apartado hemos supuesto que el número de sumandos en una partición era libre, hasta el mayor

posible. Puede ocurrir, sin embargo, que sólo deseemos usar un máximo de hasta tres sumandos, o exactamente cuatro o cualquier otra posibilidad. Por otra parte, los sumandos pueden estar restringidos en magnitud dentro de un rango. Esto complica un poco las cuestiones.

Veremos con algunos ejemplos la utilidad de las funciones generatrices y la posibilidad de comprobar resultados con la hoja Cartesius.

¿De cuántas formas se puede descomponer el número 8 en sumandos no mayores que 4?

Si has entendido de qué van las funciones generatrices comprobarás que la siguiente es la adecuada para este caso

$F(x)=(1+x+x^2+x^3+x^4+\ldots)(1+x^2+x^4+x^6+\ldots)(1+x^3+x^6+x^9+\ldots)(1+x^4+x^8+x^{12}+\ldots)$

Como en casos anteriores podemos expresarlo como sumas de sucesiones geométricas

$$P_{x\leq 4}(n) = \frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)}$$

Y en general

$$P_{x\leq k}(n) = \prod_{j=1}^{k} \frac{1}{(1-x^j)}$$

Para aplicarlo al caso de 8 bastará buscar su coeficiente en la F.G. aplicada al caso en el que k=4. Lo escribimos en PARI

print(taylor(1/(1-x)/(1-x^2)/(1-x^3)/(1-x^4),x,9))

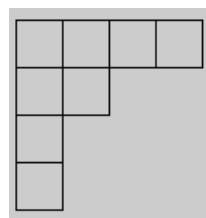
Y obtenemos

F.G.=1+x+2x^2+3×x^3+5×x^4+6×x^5+9×x^6+11×x^7 +15×x^8+O(x^9)

Luego la solución del problema es P(8/sumandos no mayores que 4)=15

Particiones conjugadas

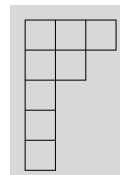
Ahora usaremos una técnica muy simple, pero que da buenos resultados. Como veíamos anteriormente, cada una de las particiones se puede representar mediante un diagrama de Ferrer, en el que se adosan tantas filas como sumandos entran en la partición, siendo la longitud de cada columna el valor del sumando. Así, la partición 8=4+2+1+1 se puede representar como



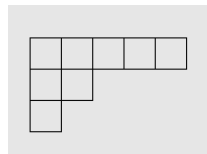
Cada fila representa un sumando: 4, 2, 1 y 1. Todos los diagramas que formemos con estas 15 particiones tendrán como máxima anchura cuatro cuadrados.

Lo bueno de estos diagramas, entre otras ventajas, es que si los giramos convirtiendo las filas en columnas y las columnas por filas seguirán siendo particiones, llamadas ***particiones conjugadas***.

Así, la partición 3+2+1+1+1



Se puede convertir en 5+2+1



Esta correspondencia es biyectiva. Si en las 15 particiones consideradas ninguna podía sobrepasar la anchura de 4, sus conjugadas no podrán tener más de cuatro filas, es decir, **más de cuatro sumandos**.

Esto es muy interesante: **Las particiones en sumandos no mayores que k coinciden en número con las particiones en no más de k sumandos**.

En nuestro ejemplo: si existen 15 particiones de 8 en sumandos no mayores que 4, también serán 15 las que se obtengan con no más de cuatro sumandos libres.

Así que si alguna vez no puedes construir la F.G. de un tipo de particiones, puedes acudir a las conjugadas por si resulta más sencillo. El siguiente ejemplo lo aclara.

¿De cuántas formas distintas podemos descomponer el número 12 en exactamente cuatro sumandos?

Acudimos a la conjugada: Este problema es el mismo que descomponer 12 en sumas de las cuales el mayor sumando sea 4. De otra forma: debe figurar al menos un 4 y el resto ser 1,2 o 3.

De esa forma la F.G. es fácil de obtener:

$F(x)=(1+x+x^2+x^3+\ldots)(1+x^2+x^4+x^6+\ldots)(1+x^3+x^6+x^9+\ldots)(x^4+x^8+x^{12}+\ldots)$

(hemos suprimido el 1 en el mayor sumando)

Generalizando

$$P_k(x) = x^k \prod_{j=1}^{k} \frac{1}{1-x^j}$$

Efectuamos las comprobaciones en nuestro ejemplo

Con la función generatriz y PARI

print(taylor(x^4/(1-x)/(1-x^2)/(1-x^3)/(1-x^4),x,9))

Desarrollo:

x^4+x^5+2×x^6+3×x^7+5×x^8+6×x^9+9×x^10+11×x^11+15×x^12+O(x^13)

Solución: el coeficiente de 12, que es 15.

Problema conjugado

Ahora, en lugar de cuatro sumandos, el máximo ha de ser siempre 4, pero eso no es operativo, pues podemos eliminar siempre ese 4 y en lugar de formar una suma 12 pedimos que la suma sea 8. Este problema lo tenemos resuelto más arriba y nos resultó 15, como era de esperar.

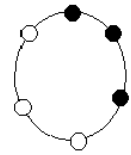
COLLARES BICOLORES

En esta sección se usan los collares como objetos matemáticos que nos permiten aclarar los conceptos de **órbita y estabilizador**.

Introducción

Supongamos que en un hilo cerrado ensartamos **n** cuentas para formar un collar, **r** de ellas de color negro y **s** de color blanco, con **r+s=n**. Lo dejamos sobre una mesa y permitimos todos los giros posibles, lo que evidentemente deja invariante la estructura de las posiciones mutuas de las blancas y las negras. Por razones de simplicidad (aunque de hecho se hace y está

estudiado) prohibiremos cualquier movimiento del collar fuera de la mesa (en el espacio tridimensional)



¿Cómo se estudiarían matemáticamente estas estructuras en forma de collar?

La primera idea es la de que se trata de permutaciones circulares, pero el problema es algo más complicado. Lo abordamos.

Consideremos todas las permutaciones posibles de r negras y s blancas. Sabemos que su número es $C_{n,r}=C_{n,s}$. =n!/(r!.s!) Así, si usamos 3 negras y 3 blancas obtendríamos $C_{6,3}=C_{6,2}$= 6!/(3!×3!)= 20 permutaciones. Si representamos las blancas con una O y las negras con X, resultarían las siguientes (se puede ignorar por ahora la última columna):

O O O X X X C1

O O X O X X C2

O O X X O X C3

O O X X X O C1

O X O O X X C3

O X O X O X C4

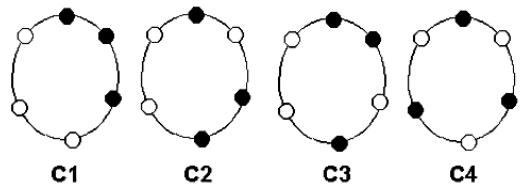
O X O X X O C2

O	X	X	O	O	X	C2
O	X	X	O	X	O	C3
O	X	X	X	O	O	C1
X	O	O	O	X	X	C1
X	O	O	X	O	X	C2
X	O	O	X	X	O	C3
X	O	X	O	O	X	C3
X	O	X	O	X	O	C4
X	O	X	X	O	O	C2
X	X	O	O	O	X	C1
X	X	O	O	X	O	C2
X	X	O	X	O	O	C3
X	X	X	O	O	O	C1

Intenta imaginar cada permutación como circular y agrupa aquellas que representen el mismo collar. Puedes imaginarlas situadas sobre la esfera de un reloj con la primera cuenta en “las doce” y avanzando en el sentido de las agujas. Así lo haremos a partir de ahora.

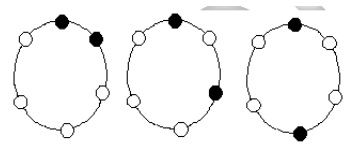
Es un ejercicio muy bueno para dominar el tema. En la última columna de la tabla se han destacado con los símbolos C1, C2,… los distintos collares que se pueden considerar.

Han resultado tres tipos de collares C1, C2 y C3 representados cada uno por 6 permutaciones y luego otro tipo, el C4, representado por dos. Los dibujamos:



Si analizas un poco este conjunto adivinarás por qué el cuarto tipo contiene sólo 2 permutaciones y los otros 6. Por ahora lo dejamos aquí y lo interpretaremos en términos de órbitas en un conjunto sobre el que actúa un grupo.

Mientras tanto, intenta estudiar el mismo tipo de collar pero con sólo dos cuentas negras y cuatro blancas.



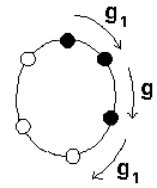
¿Cuántas permutaciones forman cada uno de los tres tipos de collar? ¿Por qué sólo existen tres tipos?

Órbitas y estabilizadores

Llamemos **C** al conjunto de permutaciones de **n** cuentas, **r** de ellas de color negro y **s** de color blanco, con **r+s=n.** En total existirán **Cn,r=Cn,s** elementos**.** Con las condiciones que se impusieron en la anteriormente en la definición de un collar se advierte que vamos a someter

a ese conjunto C a una serie de giros, y que consideraremos pertenecientes a un mismo collar a las permutaciones que se pueden convertir una en la otra mediante un giro.

Concretamos:



Llamemos **g_1** al giro que traslada cada cuenta al lugar de su siguiente en el sentido de las agujas del reloj. En términos de permutaciones equivaldría a mover cada elemento un lugar y al último convertirlo en primero. Así, en la permutación XOXXO el efecto de g_1 sería OXXOX. Se puede formalizar más, pero así se entiende bien. Esta definición es independiente del número de cuentas.

Igualmente, llamaremos g_2 a la composición de g_1 consigo mismo, es decir $g_2(x)= (g_1.g_1)(x)=g_1(g_1(x))$. En la práctica equivaldría a un giro doble. De igual forma podemos definir el giro triple $g_3(x)= (g_1.g_2)(x)=g_1(g_2(x))$ y así sucesivamente hasta llegar a g_n que equivaldría a la transformación identidad e.

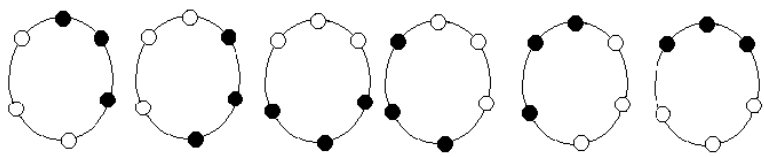
Hemos definido en realidad un grupo G (puedes demostrarlo), el de los giros en C, subgrupo del de sustituciones de C. Formalizamos la idea.

Diremos que un grupo G actúa sobre un conjunto C cuando para cada elemento g de G se define una operación externa g(x)=y, donde x e y son elementos del conjunto C, tal que cumpla e(x)=x y además (g.f)(x)=g(f(x)), ambas para todo x de C. En nuestro caso de giros sobre permutaciones se cumplen ambas, luego diremos que G actúa sobre C. La imagen intuitiva es que se hacen girar las cuentas de todas las formas posibles.

Dos conceptos importantes se desprenden de esa definición

Órbita

Llamaremos **órbita o trayectoria** de un elemento x del conjunto C sobre el que actúa G, al conjunto **orb(x)** formado por todas las imágenes posibles de x mediante los elementos de G. En la imagen tienes un ejemplo de órbita según los giros en un conjunto de seis cuentas.



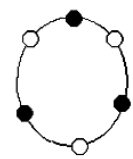
Las órbitas no son subgrupos, sino subconjuntos de C. Si vuelves a leer desde el principio, entenderás que la definición de “collar” coincide con la de “órbita”

Los collares que hemos definido coinciden con las órbitas de las permutaciones si sobre ellas actúan los giros.

Hay otra definición de collar en la que entran las simetrías, pero lo dejamos por si deseas ampliar el tema.

Estabilizador

Para una permutación cualquiera x, llamaremos estabilizador de x **est(x)** al subgrupo de giros que lo dejan invariante, es decir, todos los g tales que g(x)=x. Es fácil demostrar que est(x) constituye un subgrupo.



C4

Así, el estabilizador de la permutación de la imagen está formado por el subgrupo {e, g_2, g_4}. Si no ves simetrías aparentes en una permutación, es fácil que su estabilizador sea {e}, sólo la identidad. Repasa algunos ejemplos y verás que es fácil encontrar su estabilizador.

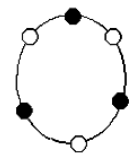
¿Por qué hablamos de estabilizadores? Porque nos sirven para contar órbitas o, lo que es lo mismo, collares.

Conteo de collares

Los conceptos de órbita (collares en nuestro caso) y de estabilizadores está relacionados por un cálculo. Si representamos como |C| al cardinal de un conjunto C, tendremos que

Si G actúa sobre un conjunto C, para cada elemento x de C se cumple que

|Orb(xI|=|G|/|est(x) |



C4

Es decir, el cardinal de la órbita de x equivale al cociente del cardinal del grupo que actúa sobre él y el de su estabilizador. Así, en el ejemplo de la imagen, el grupo de giros tiene cardinal 6 y en párrafos anteriores vimos que su estabilizador tiene 3, luego su órbita contendrá 6/3=2 elementos, el de la imagen y su simétrico intercambiando negras y blancas.

En los collares con **n** primo no existen subgrupos propios, luego todos los collares tendrán n elementos equivalentes. Estudia los collares de siete elementos y lo comprobarás.

Hay una forma de contar todos los collares mediante órbitas y estabilizadores. Se trata del lema o teorema de Burnside:

Sea G un grupo que actúa sobre un conjunto C, y llamemos r(g) al número de elementos de C que quedan invariantes respecto a g (x=g(x)). En ese caso el número de órbitas en C viene dado por

$$O_G = \frac{1}{|G|}\sum_{g \in G} r(g)$$

Puedes consultar la demostración en textos adecuados.

Lo aplicamos al caso de collares de 6 cuentas, 3 negras y 3 blancas. Contamos los puntos fijos de cada giro:

e: Todos los elementos son fijos, contamos 20 elementos

g_1, g_3, g_5: No tienen elementos fijos

g_2, g_4: Cada uno presenta 2 elementos fijos. Contamos 4

Aplicamos el teorema de Burnside: O=(20+0+4)/6 = 4 órbitas, tal como sabíamos desde el principio. Encontramos cuatro collares distintos.

En el caso que propusimos de 2 cuentas negras y 4 blancas tendríamos:

Número total de elementos: 6!/(2!.4!)= 15 permutaciones

e: Todos los elementos son fijos, contamos 15 elementos

g_1, g_2, g_3, g_5: No tienen elementos fijos

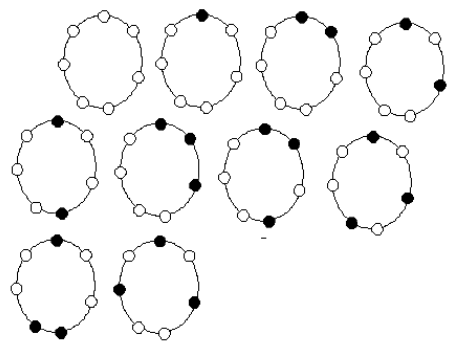
g_3: Presenta 3 elementos fijos.

Luego O=(15+0+3)/6 = 3 órbitas, que se corresponden con los propuestos anteriormente.

Puedes estudiar el caso sencillo de collares de 4 cuentas. Desarrolla por separado los casos de 3 de un color y 1 del otro o el de 2 colores de cada clase. Te deben resultar un collar del primer tipo y dos del segundo. Dibújalos si quieres.

En el caso de 7, al ser primo, no hay puntos fijos y el cálculo se reduce a dividir entre 7 el número de permutaciones. Por ejemplo, si $C_{7,4}=C_{7,3}=35$, el número de collares será igual a 35/7 = 5. En el caso de 5 y 2 serían 3=21/7

Ahí los tienes todos



Son 10 en total, y si le añadimos los que resultan de intercambiar negras y blancas, se convierten en 20. Este resultado y otros similares los puedes encontrar en http://oeis.org/A000031

Conteo total

Seguimos con el tema de collares, pero sólo aquellos que están sometidos a giros planos, sin tener en cuenta

simetrías. Hemos indicado que este otro caso, algo más complejo, lo dejamos como complemento.

Descubrimos anteriormente que para n=7 existían 20 collares distintos, e igualmente se podría haber razonado que para n=6, caso que hemos estudiado exhaustivamente, serían 14.

Si consultas http://oeis.org/A000031 verás que los resultados son

N	0	1	2	3	4	5	6	7	8	9	10	11
C	1	2	3	4	6	8	14	20	36	60	108	188

Existe una fórmula, que puedes consultar en http://mathworld.wolfram.com/Necklace.html

Para calcular esos números sin acudir a un análisis individual de cada collar. Es esta, adaptada al caso de 2 colores:

$$C(n) = \frac{1}{n}\sum_{d:n} \varphi(d) 2^{n/d}$$

La variable **d** recorre todos los divisores de n desde 1 hasta n, y **φ(d)** es la función indicatriz de Euler que indica el total de números menores que d y primos con él incluido el 1.

Apliquemos la fórmula al caso 6:

Divisores: 1,2,3,6

Indicadores: φ(1)=1, φ(2)=1, φ(3)=2, φ(6)=2

Total:
$C=(1\times2^6+1\times2^3+2\times2^2+2\times2^1)/6=(64+8+8+4)/6=84/6=14$, como ya sabíamos.

En el caso de 7:

Divisores:1,7

Indicadores: $\varphi(1)=1$, $\varphi(7)=6$

Total: $C=(1\times2^7+6\times2^1)/7 = (128+12)/7 = 140/7 = 20$, que también coincide.

NÚMEROS EULERIANOS

Los números eulerianos (o de Euler), representados, por ejemplo, mediante A(n,k), equivalen al número de permutaciones sin repetición del número N en las que se producen *k ascensos*, es decir, pares de elementos consecutivos en los que el primero es menor que el segundo.

Por ejemplo, A(4,2)=11, porque según el listado siguiente, existen 11 permutaciones del conjunto (1,2,3,4) que presentan dos ascensos:

X1	X2	X3	X4
1	2	4	3
1	3	2	4
1	3	4	2
1	4	2	3
2	1	3	4
2	3	1	4
2	3	4	1
2	4	1	3
3	1	2	4
3	4	1	2
4	1	2	3

Si poseen dos ascensos, sus permutaciones simétricas poseerán uno, luego A(4,1)=11 también.

Si escribimos los números eulerianos en una matriz triangular, los elementos de cada fila serán simétricos, y su suma coincidirá con el factorial de N.

Puedes darte una idea con los datos de esta tabla (elaboración propia):

N	0	1	2	3	4	5	6	7	8	9
0	1									
1	1									
2	1	1								
3	1	4	1							
4	1	11	11	1						
5	1	26	66	26	1					
6	1	57	302	302	57	1				
7	1	120	1191	2416	1191	120	1			
8	1	247	4293	15619	15619	4293	247	1		
9	1	502	14608	88234	156190	88234	14608	502	1	
10	1	1013	47840	455192	1310354	1310354	455192	47840	1013	1

Los datos son simétricos y su suma por filas es el factorial de N.

Estos números obedecen a esta relación de recurrencia:

A(N,k) = (k+1)A(N-1,k) + (n-k)A(n-1,k-1)

El primer sumando representa las permutaciones de N elementos que mantienen los mismos ascensos existentes en N-1. La idea es sencilla, ya que N es mayor que los elementos de las permutaciones de N-1, y para que no cambie el número de ascensos, o bien N es el primer elemento, o bien, se ha intercalado en un ascenso, con lo que se gana uno, pero se pierde otro.

Por ejemplo, si en el ascenso 2, 4 intercalamos un 5, quedará 2, 5, 4. Se gana el ascenso 2,5 pero se pierde el 2,4. Queda igual el número de ascensos, pero ha habido k+1 inclusiones. De ahí (k+1)A(N-1,k).

El otro sumando representa los ascensos que se crean nuevos, al intercalar N entre dos elementos que no presentaban ascenso, que son N-k en total. En ellos se crea un ascenso nuevo, por lo que es necesario que la permutación primitiva tenga un ascenso menos, es decir, (n-k)A(n-1,k-1).

Fórmula explícita

Se demuestra que un número euleriano se calcula mediante la fórmula

$$A(n,k) = \sum_{i=0}^{k} (-1)^i \binom{n+1}{i} (k+1-i)^n$$

Se puede traducir a PARI. Por ejemplo, estas líneas reproducen los valores para N=8:

T(n, k) = sum(j=0, k, (-1)^j * (k+1-j)^n * binomial(n+1, j))
for(i=0,7,print1(T(8,i),", "))

```
? T(n, k) = sum( j=0, k, (-1)^j * (k+1-j)^n * binomial( n+1, j))
for(i=0,7,print1(T(8,i),", "))
%7 = (n,k)->sum(j=0,k,(-1)^j*(k+1-j)^n*binomial(n+1,j))
1, 247, 4293, 15619, 15619, 4293, 247, 1,
```

Con esta fórmula se pueden construir las columnas de la matriz. Por ejemplo, la columna de k=1, 1, 4, 11, 26, … sigue la expresión $\mathbf{2^m-(m+1)}$, y la de k=2, sigue la expresión $\mathbf{3^m - (m+1)*2^m + (1/2)*m*(m+1)}$

Podemos generalizar a todas las columnas si usamos una suma y sustituimos k por un valor concreto. Por ejemplo, para k=4 obtendríamos:

T(n) = sum(j=0, 4, (-1)^j * (5-j)^n * binomial(n+1, j))
for(i=5,10,print1(T(i),", "))

El resultado concuerda con la matriz triangular obtenida:

```
? T(n) = sum( j=0, 4, (-1)^j * (5-j)^n * binomial( n+1, j))
for(i=5,10,print1(T(i),", "))
%3 = (n)->sum(j=0,4,(-1)^j*(5-j)^n*binomial(n+1,j))
1, 57, 1191, 15619, 156190, 1310354,
```

COEFICIENTES TRINOMIALES

Los coeficientes trinomiales son una extensión de los binomiales, definidos estos como

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

Y que son los coeficientes del binomio de Newton:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-1}$$

De forma análoga se pueden definir los coeficientes trinomiales, propios de un trinomio similar al anterior.

En realidad, los binomiales se podrían expresar de otra forma:

$$\binom{m}{n_1, n_2} = \frac{m!}{n_1!\,n_2!}, con\ n_1 + n_2 = m$$

A partir de aquí podemos explicar mejor la definición de coeficientes trinomiales:

$$\binom{m}{n_1, n_2, n_3} = \frac{m!}{n_1!\,n_2!\,n_3!}, con\ n_1 + n_2 + n_3 = m$$

También, al igual que con los binomiales, los podemos identificar con los coeficientes de la potencia de un trinomio:

$$(a+b+c)^n = \sum_{i+j+k=n} \binom{n}{i,j,k} a^i\, b^j c^k$$

Las demostraciones son similares a las del caso binomial. Es un caso particular de la fórmula de Leibnitz.

Esta fórmula produce siempre resultados enteros positivos, debido al teorema de que un producto de k números consecutivos decrecientes es siempre múltiplo de los k primeros números enteros positivos. Es fácil recordar que coincide con el número de permutaciones con repetición en las que se fija el número de cada una.

Para entender esto mejor podemos descomponer la definición en tres bloques. Lo vemos con un ejemplo:

$$\binom{8}{3,2,3} = \frac{8!}{3!\,2!\,3!} = \frac{8\times 7\times 6}{3\times 2\times 1} \times \frac{5\times 4}{2\times 1} \times \frac{3\times 2\times 1}{3\times 2\times 1}$$
$$= 8\times 7\times 10\times 1 = 560$$

A la vista de este esquema de tres cocientes, observamos que el tercer número de la definición no influye en el resultado, luego podemos usar sólo n_1 y n_2. Incluso estos son intercambiables, los que nos lleva a qu e el coeficiente trinomial se puede expresar como

$$\binom{m}{n_1, n_2, n_3} = \binom{m}{n_1}\binom{m-n_1}{n_2} = \binom{m}{n_2}\binom{m-n_2}{n_1}$$

En nuestro ejemplo, usando la función COMBINAT de Excel y Calc, nos quedaría:

COMBINAT(8;2)×COMBINAT(6;3)=560

COMBINAT(8;3)×COMBINAT(5;2)=560

Cálculo de un coeficiente trinomial en la práctica

Si no se desea depender de la función COMBINAT, se puede calcular directamente. El problema con el cálculo práctico de un coeficiente de este tipo es que los factoriales alcanzan números muy grandes. Si usamos calculadora o bien hoja de cálculo, los resultados pasan a coma flotante y se pierde el carácter entero de estos coeficientes. Por ello, es conveniente usar el desarrollo del párrafo anterior: dividir los números consecutivos a partir de **m** entre el primer factorial, los siguientes entre el segundo, y parar el cálculo, porque el tercer factorial produce un uno. En VBasic y otros lenguajes se puede construir una función similar a la siguiente:

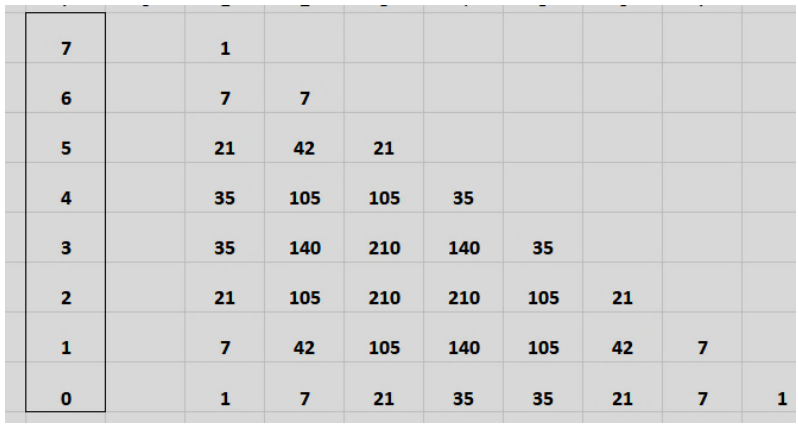
Function trinomial(m, x, y, z)
Dim t, k, v
If x + y + z <> m Then trinomial = 0: Exit Function' Datos no válidos
t = m: k = x: v = 1
While k > 0
v = v × t / k: t = t - 1: k = k – 1 'Divide factores consecutivos entre el primer coeficiente. Es el primer combinatorio de la fórmula.
Wend
k = y
While k > 0
v = v × t / k: t = t - 1: k = k – 1' Igual, en el segundo coeficiente para calcular el segundo combinatorio.

Wend
trinomial = v
End Function

Presenta un pequeño riesgo de redondeo inadecuado, pero suele funcionar bastante bien. Devuelve un cero si los coeficientes de abajo no suman el de arriba. No analiza si los datos son enteros.

Tetraedro de Pascal

Con la expresión **COMBINAT(m;n_1)×COMBINAT(m-n_1;n_2)** se puede construir un triángulo de coeficientes para un m dado. En una hoja de cálculo se puede visualizar bien. En la imagen figuran los correspondientes a m=7, vistos anteriormente:

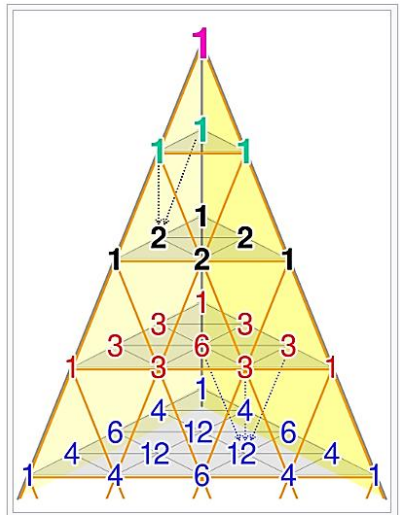


7		1						
6		7	7					
5		21	42	21				
4		35	105	105	35			
3		35	140	210	140	35		
2		21	105	210	210	105	21	
1		7	42	105	140	105	42	7
0		1	7	21	35	35	21	7	1

Observamos que los lados del triángulo son filas del triángulo de Pascal. Si ahora apilamos triángulos según los valores de m, nos resultará un tetraedro, al que también se le llama de Pascal. En la siguiente página de Wikipedia se explica el proceso:

https://en.wikipedia.org/wiki/Pascal%27s_pyramid

La siguiente imagen pertenece a dicha página:



(Fuente: Wikipedia https://en.wikipedia.org/wiki/Pascal%27s_pyramid)

Para quienes deseéis profundizar en el tema. La lectura de esta página es recomendable.

Recurrencia

Es fácil la comprobación de esta recurrencia para calcular coeficientes trinomiales:

$$\binom{n}{n,0,0} = \binom{n}{0,n,0} = \binom{n}{0,0,n} = 1$$

$$\binom{n}{n_1,n_2,n_3} = \binom{n-1}{n_1-1,n_2,n_3} + \binom{n-1}{n_1,n_2-1,n_3} + \binom{n-1}{n_1,n_2,n_3-1}$$

En realidad, este es el fundamento del tetraedro de Pascal.

TRIÁNGULO TRINOMIAL

Al igual que construíamos el triángulo de Pascal para binomiales sumando cada dos consecutivos, podemos definir el triángulo trinomial si cada coeficiente es la suma de los tres situados en la fila anterior y sobre él. Los coeficientes de los extremos serán suma de dos o de uno, como si a izquierda y derecha del triángulo existieran ceros. Así quedaría con una hoja de cálculo.

				1				
			1	1	1			
		1	2	3	2	1		
	1	3	6	7	6	3	1	
1	4	10	16	19	16	10	4	1

A diferencia de los binomiales, estos coeficientes del triángulo forman filas de longitud impar, 2n+1, por lo que se puede hablar siempre de términos centrales, que en la imagen son 1, 1, 3, 7 y 19.

Este proceso equivale a la siguiente recurrencia:

$$\binom{0}{0} = 1$$

$$\binom{n}{k}$$
$$= \binom{n-1}{k-1} + \binom{n-1}{k}$$
$$+ \binom{n-1}{k} \; si\ están\ definidos, si\ no, ceros$$

Como curiosidad, John D. Cook relaciona estos números con los pasos del rey en el ajedrez para llegar a las distintas posiciones (ver https://www.johndcook.com/blog/2025/05/16/trinomial-coefficients-and-kings/)

Este triángulo posee diversas propiedades, tal como ocurría con el binomial. Por ejemplo, la primera diagonal de la izquierda contiene los números naturales, 1, 2, 3, 4, … y la segunda los triangulares, 1, 3, 6, 10, 15, …Igualmente, si en los binomiales la suma por filas era 2^n, aquí es 3^n. Por ejemplo, $1+3+6+7+6+3+1=27=3^3$

Estos números se pueden interpretar también como los coeficientes de la potencia $(1+x+x^2)^n$

Por ejemplo, para n=4 nos queda, en wxMaxima:

```
(%i1) ratexpand((1+x+x^2)^4);
                  8      7      6      5      4      3      2
(%o1)            x  + 4 x  + 10 x  + 16 x  + 19 x  + 16 x  + 10 x  + 4 x + 1
```

Los coeficientes coinciden con los de la fila 4 del triángulo.

Para distinguir estos coeficientes de los binomiales, se suele añadir un 2 a la derecha de su símbolo. El resto queda igual porque vemos que dependen de solo dos parámetros. Así que, a partir de ahora, los representaremos así:

$$\binom{n}{k}_2$$

En ese símbolo k es un entero que cumple -n ≤ k ≤ n, por lo que puede tomar valores negativos. Lo podemos interpretar como la diferencia entre el lugar central de la fila y el del término definido.

Cálculo directo

Según la Wikipedia, existe una fórmula para el cálculo directo:

$$\binom{n}{k}_2 = \sum_{i=0}^{n} (-1)^i \binom{n}{i} \binom{2(n-i)}{n-k-i}^2$$

Usa un sumatorio algo complicado, por lo que es más directo y formativo el seguir la recurrencia definida.

Por recurrencia

El esquema de recurrencia ya presentado se puede traducir a una función directa, en la que dados n y k nos devuelva el coeficiente correspondiente en el triángulo trinomial. Para ello, traducimos las filas de hoja de cálculo a dos vectores u(i) y v(i) que comiencen y

terminen con ceros, y con ellos ir construyendo la recurrencia hasta llegar al coeficiente deseado:

```
Function trinomial2(n, k)
Dim u(50), v(50), i, j, h, t


For i = 1 To 2 × n + 3: u(i) = 0: v(i) = 0:  Next I ‘Se rellenan los vectores con ceros
u(n + 3) = 1 ‘Primer coeficiente
For i = 1 To n ‘Se trabaja hasta la fila n
For j = 3 To 2 × n + 3 ‘Longitud de la fila contando con ceros iniciales
v(j) = u(j - 1) + u(j) + u(j + 1) ‘Recurrencia
Next j
For h = 3 To 2 × n + 3: u(h) = v(h: Next h ‘Se copia v(i) en u(i)
For h = 1 To 2 × n + 1: v(h) = 0: Next h ‘Y se rellena con ceros
Next i
t = u(n + k + 3) ‘Se localiza el coeficiente pedido
trinomial2 = t
End Function
```

Aunque parece algo complejo, funciona con rapidez. En la imagen se recogen los coeficientes correspondientes a n=5 y n=6:

	5	6
-6	0	1
-5	1	6
-4	5	21
-3	15	50
-2	30	90
-1	45	126
0	51	141
1	45	126
2	30	90
3	15	50
4	5	21
5	1	6
6	0	1

Coeficientes centrales

Los números centrales de cada fila poseen importancia propia. Por eso, en OEIS, se les dedican muchas referencias y descripciones de propiedades. Aquí sólo se darán algunos detalles, remitiendo para un estudio completo a la página https://oeis.org/A002426.

Su cálculo no es difícil. En la página mencionada se usa la definición como coeficientes de $(1+x+x^2)^n$, pero eligiendo el coeficiente número n. Se propone este código PARI de fácil comprensión, extendido aquí con un bucle FOR:

a(n) = if(n<0, 0, polcoeff((1 + x + x^2)^n, n))
for(k=0,20,print1(a(k),", "))

Su resultado, en la página oficial de PARI es:

```
? a(n) = if( n<0, 0, polcoeff( (1 + x + x^2)^n, n))
for(k=0,20,print1(a(k),", "))
%2 = (n)->if(n<0,0,polcoeff((1+x+x^2)^n,n))
1, 1, 3, 7, 19, 51, 141, 393, 1107, 3139, 8953, 25653, 73789, 212941, 616227, 178760
7, 5196627, 15134931, 44152809, 128996853, 377379369,
```

Coincide con lo publicado.

Con nuestra función trinomial2(n,k) basta dar a k el valor 0. Así se ha efectuado para crear esta columna de Excel:

	Coeficiente central
1	1
2	3
3	7
4	19
5	51
6	141
7	393
8	1107
9	3139
10	8953
11	25653
12	73789
13	212941

Una interpretación interesante de estos números es la de David Callan, que los identifica con el número de sucesiones de n elementos tomados del conjunto (1, 2, 3, … n), crecientes en sentido amplio, en las que ningún elemento se repite más de dos veces. Propone como ejemplo si n = 3, las sucesiones son 112, 113, 122, 123, 133, 223, 233, es decir, son siete como indica su coeficiente central.

He añadido la condición FMAX a mi herramienta Cartesius (https://www.hojamat.es/sindecimales/combinatoria/herramientas/herrcomb.htm#cartesius) y, aunque aún no está publicada, la he usado para comprobar esta propiedad. He concretado las condiciones siguientes:

xtotal=5
xt=1..5
FMAX<3
Creciente

Con ellas se combinan en arreglos crecientes los números del 1 al 5, con la condición de que la frecuencia máxima sea 2, tal como plantea David Callan, y se han obtenido 51 posibilidades, como corresponde al coeficiente central de orden 5. Este recorte contiene los primeros y su total:

Total
51
11223
11224
11225
11233
11234
11235
11244
11245
11255
11334
11335
11344
11345
11355
11445
11455
12233
12234
12235
12244

El título es la traducción literal de la sucesión “Lazy Caterer's Sequence” publicada en

https://oeis.org/A000124

con el título *Central polygonal numbers*, que se refiere al máximo número de porciones que se puede obtener en una tarta si la sometemos a **n** cortes. Su referencia a los números de Hogben, ya tratados en mi blog

(https://hojaynumeros.blogspot.com/2021/11/numeros-de-hogben.html)

me ha llevado a estudiarla, sólo en los aspectos que trata normalmente mi blog.

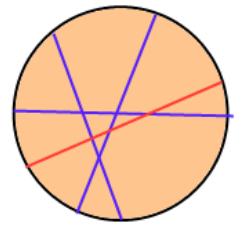
Fórmula de la sucesión

Si solo nos interesan los números máximos de piezas resultantes, deberemos suponer que cada corte posee intersección con todos los anteriores, evitando paralelismos, por lo que se cumplirá que **c(n+1)=c(n)+n**. Como c(1)=2, ya que el primer corte produce dos piezas, es fácil ver que la sucesión será: 2, 2+2,2+2+3, 2+2+3+4 ,… pero en OEIS se considera siempre c(0), que aquí sería 1 (ningún corte), por lo que resultaría al final 1, 2, 4, 7, 11, 16, …, que es la publicada.

El hecho de que la suma de los primeros números naturales sea un número triangular, n(n+1)/2, nos da directamente la fórmula de estos números:

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

En la imagen vemos la generación de c(4), porque de los tres cortes existentes, el cuarto produce 4 nuevos, y el resultado es 4×5/2+1=11



Si la fórmula de c(n) es n(n+1)/2+1, la de c(n-1) será, desarrollando (n^2-n+2)/2, y podemos identificar el numerador con un número de Hogben aumentado en una unidad. Esto relaciona las dos sucesiones, pues si añadimos una unidad a la Hogben y dividimos entre 2 nos resulta la que estamos estudiando.

$$c(n) = \frac{h(n+1)+1}{2}$$

Si emparejamos índices, se comprueba esta relación:

Hogben: 1, 1, 3, 7, 13, 21, 31, 43, 57, 73, 91

Lazy Caterer's: 1, 2, 4, 7, 11, 16, 22, 29, 37, 46

(13+1)/2=7, (21+1)/2=11, (31+1)/2=16, …

Los números de Hogben, según es fácil de demostrar, se generan con la recurrencia **h(n+1)=h(n)+2n**, ajustando bien el índice inicial. Es otra forma de razonar la relación entre las dos sucesiones.

Si repasamos mi estudio de estos números, podemos descubrir que los **c(n)** son la cuarta parte de la suma de dos de **h(n)** diferenciados en dos órdenes:

2=(1+7)/4, 4=(13+3)/4, 7=(21+7)/4, 11=(31+13)/4, …

Los primeros términos de la sucesión **c(n)** son:

1, 2, 4, 7, 11, 16, 22, 29, 37, 46, 56, 67, 79, 92, 106, 121, 137, 154, 172, 191, 211, 232, 254, 277, 301, 326, 352, 379, …

https://oeis.org/A000124

Basta aplicar la formula a los primeros números naturales para conseguirla.

Algunas curiosidades

En la página citada se proponen varias propiedades y curiosidades, pero sin desarrollar. Estudiaremos algunas.

Todo proceso en el que el término enésimo produzca el siguiente al sumarle **n** puede interpretarse como número del tipo **C(n).**

Un ejemplo que se propone que el de contar los términos de la expresión $(x+y)\times(x^2+y^2)\times(x^3+y^3)\times...\times(x^n+y^n)$.

For n >= 1 a(n) is the number of terms in the expansion of (x+y)×(x^2+y^2)×(x^3+y^3)×...×(x^n+y^n). - Yuval Dekel (dekelyuval(AT)hotmail.com), Jul 28 2003

La justificación es la siguiente: Los primeros términos la cumplen, porque c(0)=1, c(1)=2 y c(2)=4, como fácilmente se comprueba. Los siguientes deberán incrementar los términos en **n** elementos, porque, por ejemplo, la expresión segunda $x^3+x^2y+xy^2+y^3$ se convertiría en $x^3\times(x^3+x^2y+xy^2+y^3)+y^3\times(x^3+x^2y+xy^2+y^3)$, aparentemente ocho términos, pero se pierde uno al sumar los dos términos del tipo x^3y^3, con lo que se suman sólo tres términos, quedando 7, que es c(3). Lo vemos con wxMaxima:

ratsimp((x+y)×(x^2+y^2)×(x^3+y^3));

y^6+x×y^5+x^2×y^4+2×x^3×y^3+x^4×y^2+x^5×y+x^6

Siete términos, c(3)=7

Se razonaría de igual forma para grado 4. Lo comprobamos:

ratsimp((x+y)×(x^2+y^2)×(x^3+y^3)×(x^4+y^4));

y^10+x×y^9+x^2×y^8+2×x^3×y^7+2×x^4×y^6+2×x^5×y^5+2×x^6×y^4+2×x^7×y^3+x^8×y^2+x^9×y+x^10

Once términos, c(4)=11

Otra forma de ver las curiosidades es la relación con técnicas de elegir dos elementos en un conjunto. La propuesta de nuestro compatriota Arregui aprovecha ese detalle:

Number of interval subsets of {1, 2, 3, ..., n} (cf. A002662). - Jose Luis Arregui (arregui(AT)unizar.es), Jun 27 2006

Para fijar un intervalo en el conjunto {1, 2, 3, ..., n} bastará elegir un inicio y un final, pero existen n(n-1)/2 formas de efectuar la elección, y añadimos el intervalo vacío, obtendremos los términos C(n). Por ejemplo, {1} sólo posee el intervalo vacío (), {1, 2} los intervalos (), (1,2), (2,3), (1,3), que son c(2)=4, {1, 2, 3} tendría estos: intervalos (), (1,2), (2,3), (1,3) (1,4), (2,4), (3,4), en total c(3)=7.

Cualquier otro proceso de este tipo, ajustando los índices, se puede representar con los números c(n)

Termino con dos propiedades triviales:

Numbers m such that 8m - 7 is a square. - Bruce J. Nicholson, Jul 24 2017

En efecto, si T(n) es triangular, 8T(n)+1 es un cuadrado, según una popular propiedad, luego 8C(n)-7=8T(n)+8-7=8T(n)+1, que es un cuadrado.

a(n) is the sum of the first three entries of row n of Pascal's triangle. - Daniel T. Martin, Apr 13 2022

En efecto, los tres primeros términos son 1, n y n(n-1)/2 y su suma $1+(n^2-n+2n)/2=1+n(n+1)/2=c(n)$. Por ejemplo, para n=4 queda 1+4+6=11=c(4)

Recurrencia lineal

Las sucesiones dependientes de cuadrados suelen presentar esta recurrencia: a(n+3) = 3×a(n+2) - 3×a(n+1) + a(n). En nuestro caso los términos iniciales son 1, 2, 4. Con mi herramienta de recurrencias se puede comprobar.

(https://www.hojamat.es/sindecimales/aritmetica/herramientas/herrarit.htm#recurre2)

Rellenamos las condiciones iniciales:

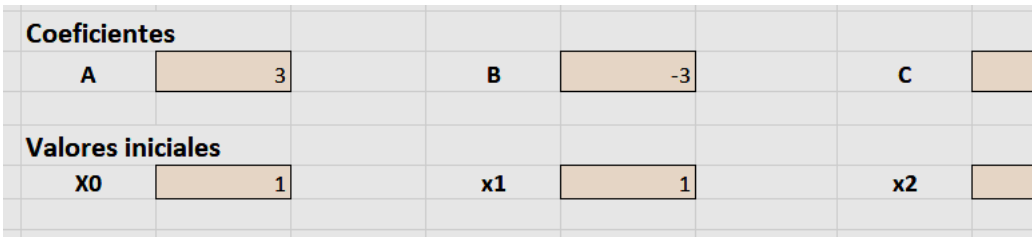
Coeficientes					
A	3	**B**	-3	**C**	
Valores iniciales					
X0	1	**x1**	2	**x2**	

Pedimos ver la sucesión:

1
2
4
7
11
16
22
29
37
46
56
67
79
92
106
121

Como era de esperar, obtenemos C(n)

Como los números de Hogben también dependen de un cuadrado, se obtendrán con una recurrencia idéntica, pero iniciando en 1, 1, 3:



Coeficientes					
A	3	B	-3	C	
Valores iniciales					
X0	1	x1	1	x2	

Pedimos ver la sucesión y obtenemos H(n):

1
1
3
7
13
21
31
43
57
73
91
111
133
157
183

En nuestra entrada de blog sobre estos números se explica el fundamento de que esta recurrencia sea válida para expresiones de segundo grado.

NÚMEROS DE PASTEL

Estos números constituyen una extensión natural de los traducidos como “Catering perezoso” (o también como “Cortador perezoso”), que ya se han estudiado en esta publicación. Si aquellos contaban el máximo de cortes rectilíneos sobre una tarta o pizza, considerados en dos dimensiones (todos frontales a la superficie mayor de la tarta), aquí se trata de cortar un cubo o una tarta mediante cortes planos que actúan sobre tres dimensiones. Buscaremos siempre el número máximo de partes, por lo que no se consideran planos paralelos, ni cortes paralelos, ni varios planos incidentes en el mismo punto.

Siguiendo las ideas de Peter C. Heinig en https://oeis.org/A000125, podemos contemplar tres escalas de complejidad en estos cortes:

Una dimensión, cortes sobre una recta. Es evidente que el número máximo de regiones para n cortes es

$C_1(n)=\text{binomial}(n,0)+\text{binomial}(n,1)=1+n$

En el caso de un plano, vimos, en la sucesión de catering perezoso, https://hojaynumeros.blogspot.com/2026/02/el-catering-perezoso.html, que el número era: n(n+1)/2+1, que también se puede escribir como

$C_2(n)$= binomial(n,0)+binomial(n,1)+binomial(n,2)

En nuestro caso actual, sobre tres dimensiones, es fácil razonar que su expresión es C(n+1,3)+n+1=(n+1)n(n-1)/6+n+1, lo que nos llevaría a

$C_3(n)$ = binomial(n,0) + binomial(n,1) + binomial(n,2) + binomial(n,3)

Lo vemos:

Una tarta, con el corte mediante un solo plano se divide en dos partes, y se cumple C(1)=0+1+1=2

Para dos cortes obtenemos cuatro partes como máximo, y se cumple:

C(2)=3×2×1/6+2+1=4

Aquí podemos seguir por inducción: Supongamos efectuados los n-1 cortes primeros. Al cortarlos con un nuevo plano, si ese número es máximo, se formarán en el nuevo plano el máximo de cortes posible, que sabemos que es $C_2(n-1)$, y serían elementos de la sucesión del catering perezoso, luego $C_3(n)= C_3(n-1)+C_2(n-1)$, y quedaría:

$C_3(n)= C_3(n-1)+(n-1)n/2+1=n(n-1)(n-2)/6+n+(n-1)n/2+1$

Mediante el programa wxMaxima comprobamos la identidad entre este resultado y el propuesto. En el recorte de pantalla observamos además que las expresiones se pueden simplificar bastante:

```
(%i1) ratexpand(x·(x−1)·(x−2)/6+x+(x−1)·x/2+1);
```

$$(\%o1)\ \frac{x^3}{6}+\frac{5x}{6}+1$$

```
(%i2) ratexpand((x+1)·x·(x−1)/6+x+1);
```

$$(\%o2)\ \frac{x^3}{6}+\frac{5x}{6}+1$$

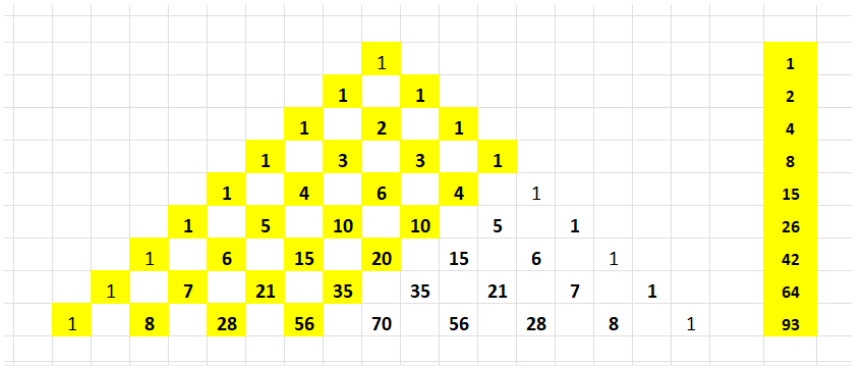
Por una parte, hemos obtenido una fórmula manejable:

$$C_3(n) = \frac{n^3 + 5n + 6}{6}$$

Por otra, se ha comprobado en el razonamiento que $C_3(n)= C_3(n-1)+C_2(n-1)$ y, por tanto, que es válida la sugerencia de:

$C_3(n)$ = binomial(n,0) + binomial(n,1) + binomial(n,2) + binomial(n,3)

Con esta comprobación se ha descubierto también que estos números son la suma de los cuatro primeros elementos de la fila n del triángulo de Pascal:



Esta propiedad nos permite identificar los números de pastel con el número de subconjuntos de un conjunto de

n elementos cuyo cardinal **no supere los tres elementos**. Expresado de otra forma, la suma del número de combinaciones de n elementos tomados de 0, 1, 2 o 3 elementos.

Al igual que ocurría con la sucesión del catering perezoso, la existencia de una fórmula tan directa hace inútil la búsqueda de otro algoritmo o función. Basta organizar una tabla con esa fórmula:

N		C(N)
0		1
1		2
2		4
3		8
4		15
5		26
6		42
7		64
8		93
9		130
10		176
11		232

Coinciden los valores extraídos del triángulo de Pascal y con los publicados en https://oeis.org/A000125,

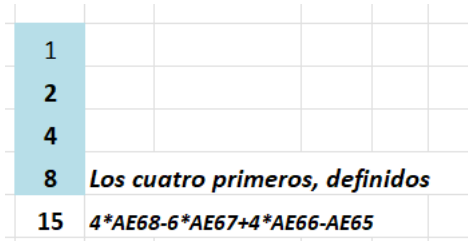
Recurrencia

Con la fórmula básica se puede llegar a números de orden grande, pero quizás se prefiera una recurrencia por la rapidez de cálculo. En la página de OEIS citada se propone la siguiente:

a(n) = 4×a(n-1) - 6×a(n-2) + 4×a(n-3) - a(n-4).

Bastará, pues, crear una columna con los cuatro primeros en una hoja de cálculo y después aplicar la fórmula a esos cuatro y rellenar hacia abajo hasta el punto que deseemos.

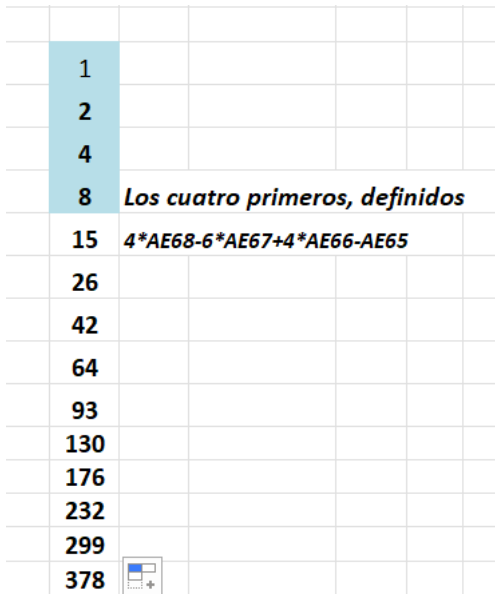
Comienzo:



Escribimos los cuatro primeros, y al quinto le aplicamos la fórmula de recurrencia.

Segundo paso

Rellenamos hacia bajo la fórmula:



De esta forma, en segundos, llegamos al orden que deseemos:

2325
2626
2952
3304
3683
4090
4526
4992
5489
6018
6580
7176
7807

Las recurrencias lineales son muy útiles para construir tablas de forma casi instantánea.

CURIOSIDADES

SUMAS EN TODOS LOS SUBCONJUNTOS

Tomemos el conjunto formado por los n primeros números naturales {1, 2, 3, …, n}. Imagina que formamos todos los subconjuntos posibles y que en cada uno sumamos los elementos, acumulando después todas las sumas en un total general ¿Cuánto valdrá esa suma S(n) de todos los elementos de todos los subconjuntos? Al conjunto vacío le asignamos suma 0.

Te damos un ejemplo:

S(4)=80, porque tendríamos que sumar (escribimos entre paréntesis la suma parcial de cada subconjunto) lo siguiente. Sería así:

(0)+(1)+(2)+(3)+(4)+(1+2)+(1+3)+(1+4)+(2+3)+(2+4)+(3+4)+(1+2+3)+(1+2+4)+(1+3+4)+(2+3+4)+(1+2+3+4)=10+3+4+5+5+6+7+6+7+8+9+10=27+26+27=80

Los primeros resultados para la función S son S(1)=1; S(2)=6; S(3)=24; S(4)=80; S(5)= 240; S(6)=672, formando la sucesión 1, 6, 24, 80, 240, 672, 1792, 4608, 11520, 28160, 67584, 159744…

¿Sabrías justificar este resultado?

Podemos encontrar una definición por recurrencia. Que S(1)=1 y S(2)=6 es fácil de justificar. A partir de ahí razonamos de una forma muy común en Combinatoria:

Sea S_{n-1} la suma de los subconjuntos de {1, 2, 3, …, n-1}. Para formar la suma S_n deberemos añadir el elemento n a los subconjuntos. Entonces estos serán de dos formas:

(a) Subconjuntos que no contienen al elemento n. Su suma será la misma S_{n-1}

(b) Subconjuntos que contienen al elemento n. Estarán formados por los subconjuntos de 1, 2, 3, …, n-1} a los que añadimos a cada uno el elemento nuevo n. El número de tales subconjuntos equivale a 2^{n-1}. Como cada uno se ha incrementado en el elemento n, la suma se habrá incrementado en $n\times2^{n-1}$. Luego será $S_{n-1}+ n\times2^{n-1}$.

Si reunimos las sumas (a) y (b) nos resulta la fórmula de recurrencia:

$$S_n = 2S_{n-1} + n2^{n-1}$$

En efecto: S(3)=2×6+3×4=12+12=24;
S(4)=2×24+4×8=48+32=80;
S(5)=2×80+5×16=160+80=240.

Es fácil programarlo en hoja de cálculo. Sólo incluimos una tabla creada así sin dar más detalles:

1	1	1
6	2	2
24	4	3
80	8	4
240	16	5
672	32	6
1792	64	7
4608	128	8
11520	256	9
28160	512	10
67584	1024	11
159744	2048	12
372736	4096	13

Generalmente nos sentimos más a gusto con una fórmula algebraica. Ahí va:

$$S_n = n(n+1)2^{n-2}$$

S(1)=1×2×(1/2)=1; S(2)=2×3×1=6; S(3)=3×4×2=24; S(4)=4×5×4=80…

Se puede demostrar por inducción. Vemos que se cumple para los primeros casos, luego podemos

suponer que se cumple para n-1, es decir, que $S_{n-1}=(n-1)\times n\times 2^{n-3}$.

Aplicamos la fórmula de recurrencia presentada más arriba y nos queda:

$S_n=2\times(n-1)\times n\times 2^{n-3}+n\times 2^{n-1}=(n^2-n)\times 2^{n-2}+2\times n\times 2^{n-2}=(n^2-n+2n)\times 2^{n-2}=n(n+1)2^{n-2}$ lo que completa la demostración.

Otra demostración

La suma T=1+2+3+4+…+n equivale al número triangular n(n+1)/2. Esta suma se repite en S(n) varias veces. Por ejemplo, la suma de todos los elementos unitarios es T. También vale T la suma de elementos del conjunto total. Veamos los demás conjuntos:

Clasifiquemos los subconjuntos por su número de elementos. El número de los que tienen r elementos es Cn,r. Por razones de simetría, los elementos 1,2,3,…n se repiten en total, para un mismo r, igual número de veces, luego la suma de los elementos de estos subconjuntos es múltiplo de T.

Cada elemento se repite en los conjuntos de r elementos tantas veces como indique Cn-1,r-1, luego la suma de todos equivaldrá a Cn-1,r-1×T. Si sumamos todos nos dará:

$T \times C_{n-1,0} + T \times C_{n-1,1} + T \times C_{n-1,2} + T \times C_{n-1,3} + \ldots + T \times C_{n-1,n-1} = T \times 2^{n-1} = n(n+1)/2 \times 2^{n-1} = n(n+1) \times 2^{n-2}$, que es la fórmula propuesta.

Estas sumas forman la secuencia http://oeis.org/A001788. Si la estudiáis podréis descubrir la gran cantidad de interpretaciones que tiene.

RACHAS DE DÍGITOS

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

Aquí estudiaremos algunas rachas de dígitos que puede presentar un número entero. Distinguiremos tres tipos con sus estadísticas correspondientes y después particularizaremos en algunos casos, como primos, cuadrados o triangulares.

Tipos de racheado

Un número puede presentar los dígitos agrupados, es decir, con rachas todas de longitud mayor que 1, como pueden ser 3366677 o 112222. Le llamaremos número de tipo 1, o con “dígitos agrupados”.

Puede ocurrir que ningún dígito se agrupe con el siguiente, que equivale a afirmar que todas las rachas tienen longitud 1, como en 345643. Obsérvese que no se prohíbe que los dígitos se repitan, siempre que no sean consecutivos. Serán estos números los del tipo 2, o de “dígitos aislados”

Los restantes números presentarán rachas de longitud 1 y otras mayores, como en el caso de 1442 o 54322111. Les asignaremos el tipo 3, que es el menos interesante.

Independientemente de consideraciones combinatorias, podemos evaluar de forma aproximada la frecuencia que presenta cada uno de los casos. Usaremos una función en Visual Basic de hoja de cálculo, que, por su relativa complejidad, explicamos al final del tema.

El algoritmo que usa funciona en dos fases:

(1) Búsqueda de las rachas existentes entre los dígitos del número entero. En el listado del final puedes ver que se almacenan en una matriz r.

(2) Estudio de la longitud mínima y máxima de racha existente en el número.

Si la mínima longitud no es 1, los dígitos se presentan agrupados, y el entero será de tipo 1. Si la máxima es 1, no habrá agrupamientos, y el tipo será 2. Los restantes ejemplos serán de tipo 3.

Si te apetece, sigue estas fases en el listado VBA del final.

Frecuencias de los tipos

Mediante la función citada y un contador adecuado, hemos observado que las frecuencias en los distintos intervalos son bastante parecidas a las de la tabla, obtenida en el intervalo (10000, 100000)

A	10000	
B	100000	
Tipo 1	171	0,19%
Tipo 2	59049	65,61%
Tipo 3	30781	34,20%
	90001	100,00%

Se observa que son muy escasos los de tipo 1, con todos los dígitos agrupados, un 0,19%, los más frecuentes los del tipo 2, con dígitos aislados, con un 65,61%, quedando los del tipo mixto en una frecuencia intermedia del 34,20%. En otros intervalos las frecuencias son semejantes, ya que están basadas en propiedades combinatorias.

Justificar estas frecuencias puede resultar complejo, pero en el caso del tipo 1 no es difícil. Son 171 porque de dos cifras los únicos agrupados son 11, 22, 33,…99. Si le añadimos una cifra más, deberá ser idéntica a la

última, luego, seguirán siendo 9: 111,222,…,999. Al llegar a cuatro cifras disponemos de dos caminos para construir los números de tipo 1: O bien añadimos dos cifras iguales por la derecha a los de dos cifras (incluido el cero), con lo que tendríamos 9×10=90 casos, como 1199, 2200,… o bien las añadimos por la izquierda (sin el cero), lo que daría 9×9=81 casos. Sumamos y obtenemos 90+81=171, que es lo que nos da la estadística.

En general, para una racha existen 9 posibilidades si ignoramos el 0. Para dos, 9×9, ya que ambas han de contener dígitos distintos, y para tres rachas, 9×9×9=729. Con una hoja nuestra sobre Combinatoria hemos calculado el número de rachas de cada tipo hasta 7 cifras, quedando esta tabla:

	Número de cifras						
Posibles rachas	1	2	3	4	5	6	7
1	0	1	1	1	1	1	1
2	0	0	0	1	2	3	4
3	0	0	0	0	0	1	3
4	0	0	0	0	0	0	0
Total	0	9	9	90	171	981	2520

Todas las cantidades están comprobadas: 9 números de tipo 1 de dos cifras, 9 de tres, 90 de cuatro, 171 de cinco, 981 de seis y 2520 de siete.

¿Presentarán los distintos tipos de números frecuencias parecidas? Por ejemplo, ¿existirán más

rachas con longitud superior a 1 en los cuadrados?¿y en los primos?...Nos dedicaremos, en plan lúdico, a estudiar diversos casos y observar, si existen, variaciones apreciables en las frecuencias.

Los cuadrados

Por este carácter informal que queremos darle a este estudio, nos limitaremos en todos los casos al intervalo (1, 100000), ya que con él basta para detectar curiosidades.

En ese intervalo sólo aparece el cuadrado 7744=88^2, y las frecuencias son

Cuadrados	
1	0%
208	66%
107	34%
316	100%

Prácticamente coinciden con el caso general. No aparece ningún otro cuadrado de ese tipo entre 1 y 500000. Estás invitado a buscar uno. Por cierto, si lo encuentras, deberá terminar en 00 o 44. Razónalo si te apetece.

Los primos

Establecemos el mismo intervalo, para ver si tampoco en este caso se aprecian diferencias importantes. Y no, resultan casi iguales a las anteriores:

Primos	
15	0%
6387	66%
3190	33%
9592	100%

Los 15 primos encontrados son: 11, 11177, 11777, 22111, 22277, 22777, 33311, 33377, 44111, 44777, 55333, 55511, 77711, 77999 y 88811. Como ves, son muy atractivos. Puedes ver más en

http://oeis.org/A034873

Como en el caso de los cuadrados, sólo unas terminaciones son válidas: 11, 33, 77, 99, como es fácil entender.

Otros casos

Ya vamos sospechando que las frecuencias variarán poco. Lo vemos:

Triangulares

En este caso aumentan algo las frecuencias de tipo 1 y 2 en detrimento del 3:

Triangulares	
4	1%
321	72%
121	27%
446	100%

Los cuatro triangulares de tipo 1 son muy sugestivos: 55, 66, 666, 2211, Tienes más en

http://oeis.org/A116055

Oblongos

Como estos números son los dobles de los triangulares, presentan frecuencias similares, también con ligero predominio de los tipos 1 y 2 respecto al conjunto de todos los números.

En el intervalo (1,100000) sólo aparecen tres de tipo 1: 1122=33×34, 4422=66×67 y 9900=99×100. No están publicados los siguientes. Si te atreves…

Pentagonales

Aparecen tres de tipo 1:22, 8855 y 55777.

Pitagóricos

¿Qué longitudes de hipotenusas de triángulos de lados enteros aparecerán de tipo 1?

De este tipo aparecen muchos más, pues estarían entre ellos algunos múltiplos adecuados de 55, 111 y 100, que presentan rachas de al menos dos elementos. Estos son los primeros, con sus correspondientes catetos:

55	33 , 44
111	36 , 105
222	72 , 210
333	108 , 315
444	144 , 420
555	171 , 528
666	216 , 630
777	252 , 735
888	288 , 840
999	324 , 945
1100	308 , 1056
1111	220 , 1089

Aquí lo dejamos. Podemos analizar algunos más, pero vemos que las proporciones no cambian mucho. Es tan imprevisible la aparición de las cifras en los cálculos previos, que al reunir las frecuencias se llega a resultados muy similares.

Aquí tienes una tabla resumen:

	Frecuencias de agrupamiento							
	Todos los números		Cuadrados		Primos		Triangulares	
Tipo 1	279	0%	1	0%	15	0%	4	1%
Tipo 2	66429	66%	208	66%	6387	66%	321	72%
Tipo 3	33292	33%	107	34%	3190	33%	121	27%
Total	100000	100%	316	100%	9592	100%	446	100%

ANEXO

Función para encontrar el tipo de agrupamiento de dígitos

Public Function tipoagrupa(n)
Dim i, t, nr, l, maxr, minr
Dim r(20) ‘Esta variable contendrá las rachas
Dim sr$, c$, d$

sr$ = Str$(n)
sr$ = Right$(sr$, Len(sr$) - 1) + "$" ‘Convierte el número en un *string* adecuado
nr = 0
maxr = 1: minr = 1000 ‘Máxima y mínima longitud de racha
For i = 1 To 20: r(i) = 0: Next i
i = 1
l = Len(sr$)
While i < l ‘La variable ***i*** recorre los dígitos
nr = nr + 1
r(nr) = 1
c$ = Mid$(sr$, i, 1)
d$ = Mid$(sr$, i + 1, 1)
While c$ = d$ ‘Un dígito es igual al siguiente. Hay racha mayor que 1
r(nr) = r(nr) + 1
i = i + 1
c$ = Mid$(sr$, i, 1)

d$ = Mid$(sr$, i + 1, 1)
Wend
If r(nr) > maxr Then maxr = r(nr) ‘Toma nota de la racha máxima
If r(nr) < minr Then minr = r(nr) ‘Toma nota de la racha mínima
i = i + 1
Wend

t = 3 'En principio suponemos que el tipo es 3, caso mixto
If minr > 1 Then t = 1 'Tipo 1. Todos agrupados, porque las rachas son mayores que 1
If maxr = 1 Then t = 2 'Tipo 2. Todos aislados y rachas unitarias
tipoagrupa = t
End Function

MÁXIMO PRODUCTO EN UNA PARTICIÓN

Ya sabemos que una partición de un número entero positivo N es una suma de números también enteros positivos cuyo resultado es ese número. Si no tienes claro el concepto puedes acudir a las direcciones

http://hojaynumeros.blogspot.com.es/2011/02/particiones-de-un-numero.html

https://es.wikipedia.org/wiki/Partici%C3%B3n_(teor%C3%ADa_de_n%C3%BAmeros)

Está muy estudiado el tema del desarrollo de las particiones y el del cálculo de su número. Aquí nos **interesará el máximo producto que se puede lograr multiplicando los sumandos de cada partición**. Lo introducimos con ejemplos:

Máximo producto logrado con particiones

Tomemos el número 6. Mentalmente se pueden escribir sus particiones (no se tiene en cuenta el orden):

6=5+1=4+2=3+3=4+1+1=…

En cada partición calculamos el producto entre sumandos: 6, 5, 8, 9, 4,… y nos quedamos con el máximo. En el esquema lo verás mejor:

6						6
1	5					5
2	4					8
3	3					9
1	1	4				4
1	2	3				6
2	2	2				8
1	1	1	3			3
1	1	2	2			4
1	1	1	1	2		2
1	1	1	1	1	1	1

Figuran las once particiones del 6 y en la columna de la derecha los productos de sumandos. En la partición de sumando único lo elegimos como producto. Se observa que el máximo producto es 9.

Otro ejemplo: En PARI las particiones se obtienen con la función *partitions*. Si pedimos las particiones del número 8 las obtenemos como vectores independientes:

```
parisize = 4000000, primelimit = 500000
? print(partitions(8))
[Vecsmall([8]), Vecsmall([1, 7]), Vecsmall([2, 6]), Vecsmall([3, 5]), Vecsmall([
4, 4]), Vecsmall([1, 1, 6]), Vecsmall([1, 2, 5]), Vecsmall([1, 3, 4]), Vecsmall(
[2, 2, 4]), Vecsmall([2, 3, 3]), Vecsmall([1, 1, 1, 5]), Vecsmall([1, 1, 2, 4]),
 Vecsmall([1, 1, 3, 3]), Vecsmall([1, 2, 2, 3]), Vecsmall([2, 2, 2, 2]), Vecsmal
l([1, 1, 1, 1, 4]), Vecsmall([1, 1, 1, 2, 3]), Vecsmall([1, 1, 2, 2, 2]), Vecsma
ll([1, 1, 1, 1, 1, 3]), Vecsmall([1, 1, 1, 1, 2, 2]), Vecsmall([1, 1, 1, 1, 1, 1
, 2]), Vecsmall([1, 1, 1, 1, 1, 1, 1, 1])]
?
```

Si multiplicas los sumandos dentro de cada vector descubrirás que el máximo producto es 18=2×3×3, luego MPP(8)=18

Estos resultados figuran en la página de OEIS http://oeis.org/A000792 con una definición recursiva:

1, 1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 81, 108, 162, 243, 324, 486, 729, 972, 1458, 2187, 2916, 4374, 6561, 8748, 13122, 19683, 26244, 39366, 59049, 78732, 118098,

177147, 236196, 354294, 531441, 708588, 1062882, 1594323, 2125764, 3188646, 4782969, …

Como era de esperar, los valores son crecientes (cada uno es un máximo que se apoya en los anteriores) y pronto adquieren una buena tasa de crecimiento. La página citada contiene una fórmula recursiva que es fácil de entender.

a(n) = max{ (n-i)×a(i) : i<n}; a(0) = 1

Se define a(0) como 1, y también es fácil entender las siguientes: a(1)=1, a(2)=2, a(3)=3, … La recursividad tampoco es difícil de captar. Se trata de multiplicar cada valor menor que **n** por el máximo correspondiente a su diferencia con **n**. En efecto, las particiones de **n** se forman eligiendo esos valores i:1…n-1 para luego unirlos con las particiones de **n-i**. Por ejemplo, en las particiones del 7, si elegimos el valor 4, se deberá combinar con las particiones del 3 para formar las particiones del 7 que contengan un 4. Igual ocurre con todos los valores: 5 se añadirá a las particiones del 2 y 3 se unirá a las particiones de 4.

Si conservamos los valores máximos de cada partición de n-i, al multiplicarlos por i resultarán productos de la partición superior, candidatos a ser máximos. Al recorrer todos los valores menores que **n** dispondremos de **n-1** posibles máximos, y uno de ellos será el MPP.

Puedes ampliar este estudio en

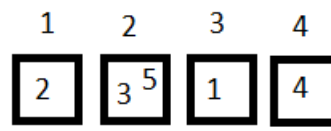
http://hojaynumeros.blogspot.com/2016/11/maximo-producto-en-la-particion-de-un.html

http://hojaynumeros.blogspot.com/2016/11/maximo-producto-en-la-particion-de-un_23.html

UNOS NÚMEROS DE LAH

Si deseamos construir una aplicación sobreyectiva de un conjunto de **n** elementos sobre otro de **n-1**, debemos buscar un origen para cada elemento del segundo conjunto, pero siempre nos sobrará uno del primero, que habrá que asignarlo a un elemento imagen ya elegido, con lo que este poseerá dos orígenes.

Esta situación se entiende bien con el símil de cajas y bolas. Deseamos meter **n** bolas en **n-1** cajas, de forma que todas las cajas tengan al menos una bola y que todas las bolas estén asignadas a alguna caja. Esto nos obliga a meter dos bolas en una caja concreta.



En la imagen observamos una aplicación sobreyectiva de los números {1, 2, 3, 4, 5} sobre las cajas {1, 2, 3, 4} En ella hemos tenido que hacer convivir el 3 y el 5 en una misma caja.

¿Cuántas formas existen de construir este tipo de aplicaciones? Con esta pregunta llegaremos a un caso particular de los llamados números de Lah, cuando el parámetro k es igual a 2

$$L(n,k) = \binom{n-1}{k-1}\frac{n!}{k!}.$$

(Imagen tomada de

https://en.wikipedia.org/wiki/Lah_number)

Deducción de la fórmula

Observemos lo que hemos hecho:

En primer lugar debemos llenar las cajas con una bola. Como tenemos 5 bolas para 4 cajas, las posibles elecciones serán *variaciones sin repetición de 5 sobre 4*, es decir, 5×4×3×2. Esas serían las formas de completar las cajas. Siempre nos sobrará una bola, que podemos asignar a una de las 4 cajas posibles, luego debemos multiplicar por 4 y quedaría 5×4×3×2×4. Si razonamos así, estaríamos contando estos casos como dobles. Por ejemplo, en la imagen, repetiríamos el razonamiento con el 3 y con el 5, con lo que habríamos contado 5×4×3×2×4=480, en lugar de los 240 que efectivamente existen, es decir, 5×4×3×2×4/2=4×5!/2

Generalizando: El número de aplicaciones sobreyectivas de {1,2…n} sobre {1, 2,…n-1} equivale a

un caso concreto de números de Lah (cuando k=2) dado por la expresión

$$N = \frac{(n-1)n!}{2}$$

Estos números están publicados en

http://oeis.org/A001286

1, 6, 36, 240, 1800, 15120, 141120, 1451520, 16329600, 199584000, 2634508800, 37362124800, 566658892800, 9153720576000, 156920924160000, 2845499424768000, 54420176498688000, 1094805903679488000, …

Entre ellos figura el 240 que hemos deducido para n=5: 4×5!/2=2×120=240

Para el caso de n=3 el número de aplicaciones sería 6. Representamos las cajas mediante paréntesis: (12)(3), (13)(2), (23)(1), (1)(23), (2)(13), (3)(12)

Hay que advertir que dentro de cada paréntesis no influye el orden.

La fórmula para Excel sería (N-1)×FACT(N)/2

Podemos deducir la fórmula con otro razonamiento: Se puede decidir antes de nada qué dos bolas comparten caja. Esta elección se hace mediante *combinaciones sin repetición de n elementos tomados de 2 en 2*, es decir **n(n-1)/2**. Una vez elegido el par, hay que asignarle una caja, y esto supone **n-1** posibilidades, con lo que quedaría un total de **n(n-1)/2×(n-1)** casos. Así nos

quedarán libres **n-2** bolas y **n-2** cajas. Entre ellas se pueden formar **(n-2)!** aplicaciones biyectivas, que completarían el proceso. En resumen, tendríamos **n(n-1)/2×(n-1)×(n-2)!=(n-1)×n!/2**, como ya sabíamos.

Una propiedad derivada

En el razonamiento anterior usamos la expresión **n(n-1)/2** como número de combinaciones, pero también es un número triangular de orden n-1, que equivale a la suma de consecutivos 1+2+3+…+n-1, luego estos números también se pueden expresar como

$$L(n) = \sum_{i=1}^{n-1} (n-1)!$$

Lo puedes ver en esta tabla de Excel:

			Factores k*m!					
n	n!	1	2	3	4	5	6	Suma
1	1	1						**1**
2	2	2	4					**6**
3	6	6	12	18				**36**
4	24	24	48	72	96			**240**
5	120	120	240	360	480	600		**1800**
6	720	720	1440	2160	2880	3600	4320	**15120**

La parte central coloreada representa el conjunto de términos del sumatorio. A la derecha figuran en negrita

los números de Lah para k=2, suma de los anteriores, y a la izquierda los factoriales. De esta tabla se pueden extraer unas representaciones interesantes para los números de Lah que estamos estudiando. Te dejamos que lo deduzcas:

6=(1+2)×1×2

36=(1+2+3)×1×2×3

240=(1+2+3+4)×1×2×3×4

1800=(1+2+3+4+5)×1×2×3×4×5

15120=(1+2+3+4+5+6)×1×2×3×4×5×6

Queda atractivo.

Recurrencia

Finalizamos este estudio con una breve referencia a la generación de cada número respecto al anterior y al número de orden. No hay que razonar mucho para comprender que

$$L(n+1) = L(n) \cdot n(n+1)/(n-1)$$

Se puede reproducir esta generación escribiendo una columna de índices y aplicar esta fórmula en una segunda columna a partir del 1:

n	L(n)	Factor multiplicador
1	**1**	
2	6	6
3	36	6
4	240	6,66667
5	1800	7,5
6	15120	8,4
7	141120	9,33333
8	1451520	10,2857

No importa que el factor multiplicador no sea entero, porque se compensa con los factores del anterior número de Lah (sabemos que el resultado ha de ser entero).