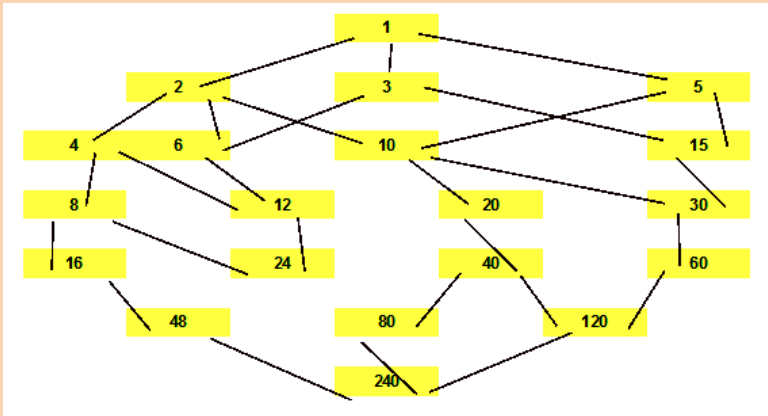
Números y hoja de cálculo IV



Curso 2011-2012

Colección Hojamat.es

http://www.hojamat.es

PRESENTACIÓN

Llegamos al cuarto tomo de la colección y a partir del mismo sólo se ofrecerán este y los siguientes como documentos en PDF descargables. La edición en papel suponía trabajo extra que no compensaba lo suficiente. Para la labor de divulgación que pretendemos basta con el ofrecimiento del documento descargable.

El orden de las entradas recogidas en este tomo es el cronológico dentro de cada capítulo. De esta forma nos garantizamos una revisión realizada cuando han transcurrido unos meses, con lo que se amplían las posibilidades de nuevas ideas complementarias.

Como en ocasiones anteriores, los números primos y los divisores son los conceptos que más nos han inspirado en la confección de las entradas, aunque en este curso se han desarrollado con cierto detalle las funciones multiplicativas y los conceptos derivados del algoritmo extendido de Euclides.

A partir de este curso disponemos ya de suficiente material para iniciar publicaciones temáticas, cuya presentación se iniciará en el otoño de 2012. Mientras se mantenga el blog *Números y hoja de cálculo* estos documentos permanecerán actualizados a través de sucesivas ediciones.

CONTENIDO

PRIMOS INAGOTABLES

LOS HUECOS DE UN PRIMO

Los cinco primos de Fermat conocidos, 3, 5, 17, 257 y 65537, tienen en común que su representación en el sistema de numeración binario está formada por un 1, un conjunto de ceros y al final otro 1. Son números con un gran hueco entre dos unidades. Por ejemplo el 65537 está representado por 10000000000000001. Sólo se conocen esos cinco primos con esa estructura. Es fácil razonar que los de Fermat son los únicos posibles, pues su expresión ha de ser del tipo 2^n+1

¿Habrá primos con otras estructuras posibles en sus huecos entre unos?

Podíamos buscar los que estuvieran formados por dos intervalos iguales, como 100010001. ¿Habrá alguno? Sí, pero sólo se conocen tres: 7, 73 y 262657. Puedes leer algunos detalles en http://oeis.org/A051154. Su expresión sería del tipo $2^{2n}+2^n+1$. Golomb dedujo que para que sean primos n ha de ser potencia de 3. Puedes también consultar

http://www.alpertron.com.ar/MODFERM.HTM

¿Y si buscáramos primos con estructuras similares a 1000100010001?, con cuatro unos? Pues yo no lo

haría. Seguro que son compuestos. En realidad no debes probar con ningún ejemplo que contenga un número par de unos situados de forma equidistante. No hemos encontrado más ejemplos con un número impar de huecos similares.

Podemos renunciar a la periodicidad de los ceros. Pueden existir primos con dos unos iniciales y el resto ceros hasta el último uno. Los hemos buscado con hoja de cálculo y aparecieron 7, 13, 97, 193, 769, 12289, 786433, 3221225473, 206158430209,…El primero, 7, sólo presenta los unos, 111, pero los demás son espectaculares, como 206158430209 con expresión

11000000000000000000000000000000001.

Puedes ver los siguientes en

http://oeis.org/A039687

El problema inverso de encontrar estructuras del tipo 1000000011 ya está también resuelto y publicado en http://oeis.org/A057733

Podíamos buscar otros con dos unos al principio y al final, pero me temo que sería inútil ¿no?. Ahí no hay primos.

Otras estructuras

Los siguientes primos poseen sus huecos en magnitud creciente:

3	11
11	1011
689900432111	1000000010000001000001000010001001011
36064050381096011	1000000000100000000100000001000000100000100001001011

Con la estructura simétrica de conjuntos de ceros de longitud creciente de derecha a izquierda, al menos con hoja de cálculo, sólo he encontrado el 3 y el 13.

A estos otros les llamo “primos piano”:

26417	110011100110001
422657	1100111001100000001
108199937	11001110011000000000000001

Si deseas saber el porqué, mira el teclado de un piano.

Este otro es similar, con otra visión del “teclado”:

989721526273 es un primo con estos huecos: 11100110011100000000000000000000000000001

Y estos otros son más simétricos:

134323393	10000000000110011100110000001
137442334721	100000000000000011001110011000000000001

¿Deseas investigar otras estructuras? Puedes probar con

Números 2-repunits (o repunos o repitunos): No tienen huecos en el sistema binario. Busca por ahí cuáles son primos, y verás qué escasez.¡Son los primos de Mersenne!

Números de Carol: Sólo tienen un hueco, pero bien situado. Tampoco hay muchos primos entre ellos. Los puedes ver en http://oeis.org/A091516

Números de Thabit: Los números del tipo 3.2n-1 se llaman números de Thabit y en el sistema de numeración binario vienen representados por las cifras 1, 0 seguidas de la cifra 1 repetida hasta terminar la expresión. Por ejemplo, el número de Thabit 786431 viene representado por 10111111111111111111. Investiga por ahí cuáles son primos. También existen los de estructura simétrica. Los tienes en http://oeis.org/A050415

La historia se repite

En una entrada anterior “¿Alguien sabe algo de esto?” nos planteábamos si dado un primo p cualquiera, existe otro q tal que la suma de ambos sea una potencia de 2. Después de algo de reflexión y ayudas externas llegamos a la conclusión de que esta posibilidad fallaba, quizás en el número 1871.

Al revisar la entrada para integrarla en una publicación se me ocurrió usar la diferencia entre primos en lugar de la suma: dado un número primo p, ¿existe siempre un exponente k entero tal que $p+2^k$ sea primo? Al mínimo valor posible de este exponente le llamaremos “distancia binaria entre ambos primos” o DISTBIN.

Podíamos interpretar ese número k como el lugar donde podríamos sumar 1 a la expresión binaria de p para que se convirtiera en otro número primo, el menor posible.

Por ejemplo, el número primo 61 tiene como expresión binaria 111101 y su función ***distbin*** vale 8. Esto quiere decir que en el orden 8 de su expresión binaria hay que añadir un 1 (tomamos como 0 la primera posición): 100111101, que equivale al número primo 317.

En los primeros números primos el cálculo de ***distbin*** es sencillo:

Primo P	Distancia binaria	Primo Q
2	0	3
3	1	5
5	1	7
7	2	11
11	1	13
13	2	17
17	1	19
19	2	23
23	3	31
29	1	31
31	4	47
37	2	41
41	1	43
43	2	47
47	5	79
53	3	61
59	1	61
61	8	317

Tienes los datos de **q** en ***http://oeis.org/A139758*** y los de **k** en ***http://oeis.org/A094076***

Como en el caso anterior de p+q=2^n, hay primos en los que el cálculo de esta distancia desborda la capacidad de una hoja de cálculo. Destacan los siguientes:

El 773

Se tiene que distbin(773)=955, con lo que el otro primo presenta 288 dígitos:

304541062856249971261043199621099634714882089299843985214622076787904646586450815702050470808812820600790778632231520880733099058287596688955562103009770419360352428123639782183462176734064176511024987296225574339802674935168589842054573862983405175400866837597008673346307143437247316741

Imagina que su expresión binaria estará formada por un 1, más de novecientos ceros y después la expresión del 773.

El 1627

Distbin: 127 q:

85070591730234615865843651857942054491

El 2131

Bloquea las herramientas que hemos usado.

En http://oeis.org/A094076 se afirma que se ha probado el 2131 para k<30000

Si deseas practicar con el tema, te ofrecemos los códigos de búsqueda que se han usado:

Basic

Definición de DISTBIN

```
Function distbin(a)
Dim c, p, p2, i

c = 0
If a > 2 And esprimo Then
p = 0
p2 = 1
i = 1
Do Until esprimo(p2)
i = i * 2
p2 = a + i
p = p + 1
If esprimo(p2)  Then c = p
Loop
End If
distbin = c
End Function
```

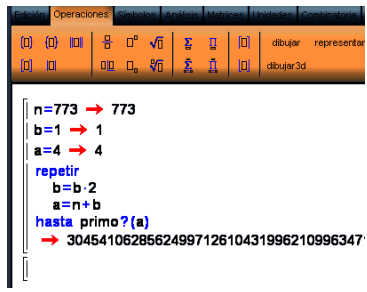
Wxmáxima

Imagen del cálculo de distbin(1627)

```
(%i1) n:1627$
      b:1$
      c:4$
      p:1$
      for i:1 unless primep(c) do (
      b:b*2,
      p:p+1,
      c:b+n
      )$
      display(p);
      display(c);
p=127
 (%o6) done
c=85070591730234615865843651857942054491
 (%o7) done
```

Calculadora Wiris

Imagen del cálculo de distbin(773). En ella no entra todo el resultado.



Con ellas puedes tener una idea de los algoritmos usados.

AL COMPLICAR SE SIMPLIFICA

El uso conjunto de las operaciones de sumar y multiplicar en los temas de Teoría de Números da lugar a resultados aparentemente paradójicos. Los conceptos

de divisor y múltiplo, de número primo, compuesto, abundante o deficiente se basan en la operación de multiplicar, pero nos empeñamos en sumarlos. A veces lo que logramos con esto es que al complicar una situación desembocamos en una estructura menos compleja.

Un ejemplo claro es el de sumar números compuestos de varios divisores y que el resultado resulte ser un número primo. Así, $60=2^2*3*5$ y $931=7^2*19$ y sin embargo su suma 991 es un número primo. La operación de sumar ha significado una pérdida de complejidad.

Otro ejemplo: En una entrada anterior

(http://hojaynumeros.blogspot.com/2011/06/un-par-de-abundantes.html)

vimos que todo número par mayor que 46 es suma de dos abundantes. Esta operación también puede suponer una pérdida de complejidad. Así, 18 y 40, ambos abundantes, con su suma producen el número 58, que es deficiente.

Estudiaremos con detenimiento otro ejemplo: La función ***sigma***

(http://hojaynumeros.blogspot.com/2011/03/la-familia-de-las-sigmas-2.html)

suma todos los divisores de un número. Es una operación que requiere varios pasos y bastantes

operaciones. **¿Podrá producir resultados primos o semiprimos?**

Podríamos intentar una búsqueda simple con hoja de cálculo: recorreríamos todos los números en un cierto rango, calculando su sigma y viendo si es prima o semiprima. El resultado sería el siguiente (para números menores que 1000):

Número N	Sigma	Tipo	Factores de N	Factores de Sigma(N)
3	4	Semiprimo	3	2 2
4	7	Primo	2 2	7
5	6	Semiprimo	5	2 3
8	15	Semiprimo	2 2 2	3 5
9	13	Primo	3 3	13
13	14	Semiprimo	13	2 7
16	31	Primo	2 2 2 2	31
18	39	Semiprimo	2 3 3	3 13
25	31	Primo	5 5	31
36	91	Semiprimo	2 2 3 3	7 13
37	38	Semiprimo	37	2 19
49	57	Semiprimo	7 7	3 19
50	93	Semiprimo	2 5 5	3 31
61	62	Semiprimo	61	2 31
64	127	Primo	2 2 2 2 2 2	127
73	74	Semiprimo	73	2 37
81	121	Semiprimo	3 3 3 3	11 11
100	217	Semiprimo	2 2 5 5	7 31
121	133	Semiprimo	11 11	7 19
144	403	Semiprimo	2 2 2 2 3 3	13 31
157	158	Semiprimo	157	2 79
169	183	Semiprimo	13 13	3 61
193	194	Semiprimo	193	2 97
225	403	Semiprimo	3 3 5 5	13 31

256	511	Semiprimo	2 2 2 2 2 2 2 2	7 73
277	278	Semiprimo	277	2 139
289	307	Primo	17 17	307
313	314	Semiprimo	313	2 157
361	381	Semiprimo	19 19	3 127
397	398	Semiprimo	397	2 199
400	961	Semiprimo	2 2 2 2 5 5	31 31
421	422	Semiprimo	421	2 211
457	458	Semiprimo	457	2 229
529	553	Semiprimo	23 23	7 79
541	542	Semiprimo	541	2 271
576	1651	Semiprimo	2 2 2 2 2 2 3 3	13 127
578	921	Semiprimo	2 17 17	3 307
613	614	Semiprimo	613	2 307
625	781	Semiprimo	5 5 5 5	11 71
661	662	Semiprimo	661	2 331
673	674	Semiprimo	673	2 337
729	1093	Primo	3 3 3 3 3 3	1093
733	734	Semiprimo	733	2 367
757	758	Semiprimo	757	2 379
841	871	Semiprimo	29 29	13 67
877	878	Semiprimo	877	2 439
961	993	Semiprimo	31 31	3 331
997	998	Semiprimo	997	2 499

Se ve que en algunos casos, como el del 576, la pérdida de complejidad es notable.

Concretemos un poco, y supongamos que N es semiprimo: N=p*q con p y q ambos primos. ¿Cuándo su ***sigma*** resultaría ser prima o semiprima?

Podemos razonar que p ha de ser igual a q: si son ambos iguales a 2, se cumple, porque 4=2*2 y

sigma(4)=1+2+4=7 que es primo. En caso contrario, uno de ellos, supongamos que sea p, ha de ser impar, con lo que sigma(N)=(1+p)(1+q)=2h(1+q), con al menos tres factores, por lo que no puede ser primo ni semiprimo. En resumen: **N ha de tener la forma de $N=p^2$ con p primo.** Puedes comprobarlo en la tabla anterior, pues todos los valores de N que presentan dos factores son cuadrados de primos (aunque no están todos)

Número N	Sigma	Factores de sigma
4	7	7
9	13	13
25	31	31
49	57	3 19
121	133	7 19
169	183	3 61
289	307	307
361	381	3 127
529	553	7 79
841	871	13 67
961	993	3 331

En efecto, no están todos los cuadrados de primos, y además, los factores que aparecen en sigma(N) **son el**

3 y números primos del tipo 6m+1. ¿Por qué? Aclararemos algo a continuación. Repasaremos con ello la teoría de los restos cuadráticos:

Para este tipo de números sigma(N)=1+p+p^2. Como el caso de p=2 está resuelto, podemos suponer que p>2 y por tanto impar, N será impar y sigma(N) también. Por tanto, si poseen divisores h, estos serán mayores que 2. Llamemos k a un posible divisor de sigma(N). Al ser primo impar, podremos aplicar la teoría de los restos cuadráticos (ver Parra *Restos cuadráticos y Ley de reciprocidad cuadrática*

http://hojamat.es/parra/restocuad.pdf)

Si k es un divisor, se ha de cumplir que $1+p+p^2\equiv 0 \pmod k$. Si multiplicamos por 4 quedará:

$4+4p+4p^2\equiv(2p+1)^2+3\equiv 0 \pmod k$ (1)

Esta congruencia puede darse en dos situaciones:

(a) Que sea k=3. Con ello se cumpliría (1) siempre que $2p+1\equiv 0 \pmod 3$, $2p\equiv 2 \pmod 3$, $p\equiv 1 \pmod 3$ (se puede dividir entre 2 porque es primo con k), es decir que **p ha de ser de la forma 3m+1**. Esta es condición necesaria para que k=3, pero no suficiente.

(b) Que k no sea 3. En ese caso el número -3 ha de ser resto cuadrático respecto a k

(Ver Parra http://hojamat.es/parra/restocuad.pdf). Para que esto se cumpla, **k ha de tener la forma k=6m+1**.

Esto completa el razonamiento: k ha de ser 3 o del tipo 6m+1, como puedes comprobar en la tabla anterior.

Una vez determinada la naturaleza de los factores (que sean el 3 u otro primo de la forma 6m+1), debemos tener en cuenta que sigma(N) puede tener un sólo factor y por tanto ser primo, o bien dos, pasando a ser semiprimo.

(A) Sigma(N) es primo

Para el caso de sigma prima puedes consultar https://oeis.org/A023194.

Es interesante que leas algunos comentarios, pero ten en cuenta que aquí solo hemos estudiado el caso en el que N era el cuadrado de un primo. Por tanto, nuestra secuencia de estos primos

2, 3, 5, 17, 41, 59, 71, 89, 101, 131, 167, 173, 293, 383, 677, 701, 743, 761, 773, 827, 839, 857, 911, 1091, 1097, 1163, 1181, 1193, 1217…

es una subsecuencia de https://oeis.org/A055638 y coincide con https://oeis.org/A053182 en la que figura un comentario de nuestro amigo Claudio Meller (http://simplementenumeros.blogspot.com/).

Todos sus elementos, salvo los primeros 2 y 3, son números primos de la forma 6m-1.

(B) Sigma(N) es semiprimo

En este caso los resultados son:

Primo	Sigma(p*p)	Factores de Sigma
7	57	3 19
11	133	7 19
13	183	3 61
19	381	3 127
23	553	7 79
29	871	13 67
31	993	3 331
43	1893	3 631
47	2257	37 61
53	2863	7 409
73	5403	3 1801
83	6973	19 367
97	9507	3 3169
103	10713	3 3571
113	12883	13 991
127	16257	3 5419
157	24807	3 8269

179	32221	7 4603
197	39007	19 2053
199	39801	3 13267
223	49953	3 16651
227	51757	73 709

Como se ve, los factores primos de Sigma sólo pueden ser el 3 o los del tipo 6m+1

PASITO A PASITO HACIA LA COMPLEJIDAD

Toma el número 807905281, que es primo. Súmale una unidad y lo habrás convertido en un semiprimo múltiplo de 2:

807905282 = 2*403952641

Una unidad más y ahora será un 3-casiprimo (tres factores primos) múltiplo de 3:

807905283 = 3*15733*17117

Pero sigue de uno en uno. Descubrirás que cada vez tendremos un factor primo más y que será múltiplo de 4, 5, 6, 7,… Observa:

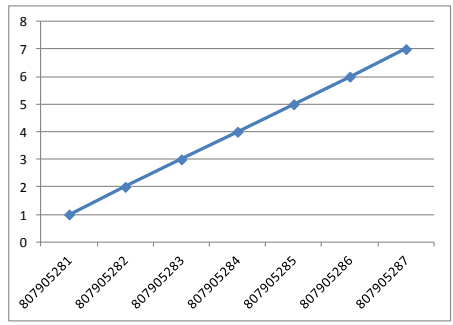
807905284 = 2*2*1871*107951

807905285 = 5*11*43*211*1619

807905286 = 2*3*3*3*37*404357

807905287 = 7*7*7*7*29*41*283

Si recordamos que la función BIGOMEGA cuenta los factores primos de un número teniendo en cuenta los repetidos, la situación anterior se podría representar así:



Pero hasta aquí llegamos, pues con una unidad más se disminuye el número de primos. En efecto, 807905288 = 2*2*2*53*1905437

¿Es frecuente este avanzar de unidad en unidad a estructuras más complejas? Pues sí y no. Muy frecuente no es, pero si nos conformamos con menos pasos, existen muchos ejemplos, ya publicados, y que puedes reproducir fácilmente con un par de funciones. Aprovecharemos estos ejemplos para que razonemos un poco.

Un paso

Es el caso más simple, el de N primo y N+1 semiprimo. Lo cumplen estos primos: 3, 5, 13, 37, 61, 73, 157, 193, 277, 313, 397, 421, 457, 541, 613, 661, 673, 733,… y está publicado en https://oeis.org/A005383

(a) Un razonamiento sencillo: Una condición equivalente para todos los primos N de la lista es que (N+1)/2 sea también primo. ¿Descubres la causa?

(b) Otro más difícil: Estas condiciones también equivalen a que sigma(N)/2 sea un número primo. ¿Por qué?

(c) Salvo el 3, todos los demás son primos del tipo 4k+1. Piensa en resto que debería tener N+1 con módulo 4.

Dos pasos

Existen primos N en los que N+1 es semiprimo y N+2 tiene 3 factores primos. Son estos:

61, 73, 193, 277, 397, 421, 613, 661, 757, 1093, 1237, 1453, 1657, 2137, 2341, 2593,…

https://oeis.org/A112998

Es evidente que forman un subconjunto de los anteriores, y esto nos va ocurrir en cada paso que demos.

Piensa un poco: **(d)** Si N>5 (y todos lo son) N+2 ha de ser múltiplo de 3

Y otro poco más: **(e)** Todos los primos de la sucesión presentan resto 1 al dividirlos entre 12: 61=5*12+1; 73=6*12+1,…Razónalo (lo tienes en inglés en A112998)

Tres pasos

También los conocemos (https://oeis.org/A113000): 193, 421, 661, 1093, 1657, 2137, 2341, 2593, 6217, 7057, 8101, 9817, 12421, 12853,…

Subconjunto de los anteriores y con las mismas propiedades.

En ellos N+1 es par, n+2 múltiplo de 3 y N+3 múltiplo de 4. Si has desarrollado las cuestiones anteriores, no te costará entenderlo.

Más pasos

Para seguir jugando a esto necesitas las funciones ESPRIMO y BIGOMEGA, que es la función que cuenta los factores primos con multiplicidad (Ver su código en

http://hojaynumeros.blogspot.com/2011/01/redondez-de-un-numero.html)

Para crear un código de búsqueda puedes tener en cuenta que para el caso de k pasos, el número primo inicial ha de tener resto 1 tomando como módulo el MCM de los números 1,2,3…k (f) Si has entendido todo lo anterior sabrás la razón.

En Basic puedes intentar algo así:

Input k ‘Escribimos el número de pasos
Input mcm ‘Para dar más velocidad, escribimos ya calculado el MCM

Input n ‘Final de búsqueda. Generalmente un número grande.

For i = 1 To n Step ***‘***mcm los saltos de mcm en mcm ahorran muchos pasos de cálculo

```
a = 0
If esprimo(i)  Then
  For p = 1 To k
  If bigomega(i + p) = p + 1 Then a = a + 1
```

La línea fundamental

```
  Next p
  If a = k Then Msgbox(i)
End If
Next i
End Sub
```

Por ejemplo, para k=4, bastante tiempo y paciencia, llegarías a esta sucesión:

15121, 35521, 52321, 117841, 235441, 313561, 398821, 516421, 520021, 531121, 570601, 623641,… http://oeis.org/A113008

Para comprobar tu código y ahorrar tiempo, aquí tienes el primer número primo de cada caso:

2, 3, 61, 193, 15121, 838561, 807905281, 19896463921, 3059220303001, 3931520917431241,…

https://oeis.org/A072875

Y para ampliar y asombrarte con el trabajo de algunos, estudia esta página:

http://www.primepuzzles.net/puzzles/puzz_425.htm

Pasos hacia atrás

Después de publicar lo anterior, nuestro amigo Claudio Meller nos escribió destacando propiedades muy parecidas. En concreto:

47 primo
46 = 2 x 23
45 = 3 x 3 x 5

107 primo
106 = 2 x 53
105 = 3 x 5 x 7
104 = 2 x 2 x 2 x 13

71999 primo
71998 = 2 x 35999
71997 = 3 x 103 x 233
71996 = 2 x 2 x 41 x 439
71995 = 5 x 7 x 11 x 11 x 17

En este blog si nos dan un empujoncito salimos corriendo a descubrir cosas nuevas. Así que Claudio ha

sido en este caso el motor de arranque de nuevas búsquedas.

En efecto, los pasos no tienen que ser necesariamente hacia un crecimiento. Pueden decrecer, como en los ejemplos propuestos por nuestro amigo. Investigando en OEIS y con nuestros buscadores podemos presentar lo siguiente:

Primos p con p-1 semiprimo

5, 7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, 383, 467,…

https://oeis.org/A005385

Como en la entradas anteriores, p-1 ha de ser múltiplo de 2 y de otro primo q=(p-1)/2 Por tanto ese nuevo primo q sería del tipo de Sofie Germain.

(Ver http://es.wikipedia.org/wiki/N%C3%BAmero_primo_de_Sophie_Germain y http://oeis.org/A005384)

Primos p con p-1 semiprimo y p-2 3-casiprimo .....

47, 107, 167, 263, 347, 359, 467, 479, 563, 863, 887, 983, 1019, 1187, 1283, 1907, 2039, 2063, 2099, 2447, 2819, 2879,…

En ellos p-1 es par, p-2 múltiplo de 3 y p es del tipo 12k-1

Esta sucesión estaba inédita en OEIS y la acabamos de publicar incluyendo a Claudio Meller como “sugeridor”. Está en http://oeis.org/A201147

Con tres pasos

107, 263, 347, 479, 863, 887, 1019, 2063, 2447, 3023, 3167, 3623, 5387, 5399, 5879, 6599, 6983, 7079, 8423, 8699, 9743, 9887,…

En ellos p-1 es par, p-2 múltiplo de 3, p-3 múltiplo de 4 y p es del tipo 12k-1

También la acabamos de publicar con la cita correspondiente a Claudio en

http://oeis.org/A201220

Más pasos

Los primeros números naturales que inician sucesiones similares son

2, 5, 47, 107, 71999, 392279, 4533292679

http://oeis.org/A093552

Por ejemplo, tenemos:

4533292679=4533292679
4533292678=2*2266646339
4533292677=3*251*6020309
4533292676=2*2*11*103029379
4533292675=5*5*17*1871*5701
4533292674=2*3*3*41*661*9293
4533292673=7*7*13*13*29*43*439

Después de publicar lo anterior he seguido descubriendo más cosas:

Saltos de dos unidades

Existen números p primos con p+2 semiprimo

2, 7, 13, 19, 23, 31, 37, 47, 53, 67, 83, 89

Ver http://oeis.org/A063637

Otra forma de definirlos: Son primos de la forma **p*q-2**, con **p** y **q** primos.

N primo y N-2 semiprimo

11, 17, 23, 37, 41, 53, 59, 67, 71, 79, 89, 97, 113

http://oeis.org/A063638

Son primos de la forma **p*q + 2**, siendo **p** y **q** primos.

Saltos de tres unidades

Existen números p primos con p+3 semiprimo

3, 7, 11, 19, 23, 31, 43, 59, 71, 79, 83, 103,…

http://oeis.org/A092109

Son del tipo p=4k+3 y cumplen que (p+3)/2 es primo

Existen números p primos con p-3 semiprimo

7, 13, 17, 29, 37, 41, 61, 89, 97, 109, 137

http://oeis.org/A089531

Sus propiedades son simétricas de las de los anteriores

Dejamos el tema para el curso próximo, en el que daremos unas vueltas más a estas propiedades.

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: **$N=a^2b^3$** con a y b naturales. ¿Te atreves a demostrarlo? Antes de que te pongas a ello, recuerda que no hemos dicho que a y b tengan que ser primos.

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

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

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

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

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

Los primeros números de Aquiles son

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

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

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

* Los números de Aquiles consecutivos más pequeños son

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

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

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

500, 864, 1944, 2000, 2592, 3456, 5000, 10125, 10368, 12348, 12500, 16875, 19652, 19773,

(https://oeis.org/A194085)

Damos unas vueltas

Primera vuelta: Jerarquía entre aquileanos

Sabemos ya que los números de Aquiles son números poderosos que no pueden representarse como potencias perfectas. También que se pueden representar como $\mathbf{N=a^2b^3}$ con a y b naturales y mayores que 1.

¿Es posible que algún divisor propio de un número de Aquiles también tenga esa propiedad?

Basta pensar un poco en ello y descubrir que sí es posible: Toma dos números primos entre sí mayores que 1, como el 2 y el 5. Añade a ellos otro que forme un trío de números también primos entre sí (no hace falta que lo sean dos a dos). En nuestro ejemplo podría ser el 6. Con el conjunto 2,5,6 como signatura formamos un número de Aquiles mediante tres primos p,q,r. Así: $N=p^2q^5r^6$, Si ahora dividimos entre r^6, nos quedará p^2q^5, que es divisor propio de N y también es de Aquiles.

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

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

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

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

Según esto, los números de Aquiles minimales son los contenidos en la secuencia

https://oeis.org/A143610

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

Esta secuencia de OEIS no recogía en principio el carácter de número de Aquiles minimal, por lo que hemos propuesto su inclusión mediante este comentario:

Every a(n) is an Achilles number (A052486). They are minimal, meaning no proper divisor is an Achilles number. [Antonio Roldán, Dec 27 2011]

A la inversa ¿Qué múltiplos de un número de Aquiles también lo son? En principio, adivinarás que infinitos. Se pueden ir añadiendo potencias de primos de forma que sus exponentes sean primos entre sí en su conjunto.

Proponemos una demostración sencilla: Todo número de Aquiles posee un divisor (no necesariamente propio) que tiene el carácter de número de Aquiles minimal

Ya tenemos una jerarquía completa de divisores y múltiplos de números de Aquiles, que comienzan en los minimales y no están acotados.

Segunda vuelta: Emparedado de Aquiles

El conjunto de divisores de un número de Aquiles N que también sean aquileanos no es vacío, luego tendrá un máximo, eventualmente el mismo N. El de múltiplos también tendrá un mínimo. Para que sea más útil consideraremos el mínimo múltiplo con la condición de que sea distinto de N, y el máximo divisor, si es posible, que también lo sea. Llegaremos así a “emparedar” N, en el sentido que ya le dimos a los “emparedados de cuadrados”, de encerrarlo entre dos congéneres. He aquí los resultados

Cociente	Máx Div. Aq.	Aquiles	Mín. Múlt. Aq.	Cociente	Holgura	Factores
1	*72*	**72**	288	*4*	4	2 2 2 3 3
1	*108*	**108**	432	*4*	4	2 2 3 3 3
1	*200*	**200**	800	*4*	4	2 2 2 5 5
4	*72*	**288**	864	*3*	12	2 2 2 2 2 3 3
1	*392*	**392**	1568	*4*	4	2 2 2 7 7
4	*108*	**432**	864	*2*	8	2 2 2 2 3 3 3
1	*500*	**500**	2000	*4*	4	2 2 5 5 5
6	*108*	**648**	1944	*3*	18	2 2 2 3 3 3 3
1	*675*	**675**	2700	*4*	4	3 3 3 5 5
4	*200*	**800**	3200	*4*	16	2 2 2 2 2 5 5
2	*432*	**864**	2592	*3*	6	2 2 2 2 2 3 3 3
1	*968*	**968**	3872	*4*	4	2 2 2 11 11
9	*108*	**972**	1944	*2*	18	2 2 3 3 3 3 3
1	*1125*	**1125**	4500	*4*	4	3 3 5 5 5
4	*288*	**1152**	3456	*3*	12	2 2 2 2 2 2 2 3 3
1	*1323*	**1323**	5292	*4*	4	3 3 3 7 7
1	*1352*	**1352**	5408	*4*	4	2 2 2 13 13
1	*1372*	**1372**	5488	*4*	4	2 2 7 7 7
4	*392*	**1568**	6272	*4*	16	2 2 2 2 2 7 7
9	*200*	**1800**	5400	*3*	27	2 2 2 3 3 5 5
2	*972*	**1944**	3888	*2*	4	2 2 2 3 3 3 3 3

En negrita hemos destacado los números de Aquiles N, en cursiva, a izquierda su mayor divisor que también es de Aquiles. Para que no deje de existir hemos permitido que no sea un divisor propio. A su derecha el mínimo múltiplo de N también de Aquiles.

Más a los lados figuran los cocientes entre N y sus “emparedadores”. Si multiplicamos esos cocientes nos dará la “holgura”, el espacio por el que puede mover N antes de llegar al siguiente número de Aquiles.

Finalmente, en la última columna tenemos la explicación de todo, los factores primos de N. Invitamos al cálculo de la holgura manualmente, sin ayuda de hoja de cálculo, para ver cuánto se aprende sobre los números de Aquiles.

Un ejemplo es el número

1800=2*2*2*3*3*5*5=2^3*3^2*5^2.

Es de Aquiles porque sus exponentes son primos entre sí y todos mayores que la unidad. Probemos a ir suprimiendo factores: el 2 no podemos suprimirlo, pues se igualarían los exponentes y obtendríamos una potencia. Un 3 o un 5 tampoco, porque daría exponente 1. Luego habrá que probar a suprimir dos factores. Como 2*2 no se puede (¿por qué?), probamos la solución mínima, 3*3, que si deja un divisor igual a 200=2*2*2*5*5=2^3*5^2, que coincide con la tabla. Otra solución sería suprimir 5*5, pero ya nos daría un divisor más pequeño.

Con el múltiplo nos ocurriría lo mismo. Omitimos los pasos. La solución mejor es aumentar un 3 y llegar al múltiplo 5400=2*2*2*3*3*3*5*5=2^3*3^3*5^2. Queda así comprobado que la holgura de 1800 es 27: dos veces el 3 para conseguir el divisor y una vez para el múltiplo.

Puedes intentar razonar la holgura de otros números de la tabla o fuera de ella. Aprenderás mucho.

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

864 1944, 3888, 4000, 5400, 6912, 9000, 10584, 10800, 10976, 17496, 18000, 21168, 21600, 24696,

25000, 26136, 30375, 31104, 32000, 34992, 36000, 36504, 42336, 42592, 43200, 48600, 49000, 49392, 50000…(los hemos publicado en

http://oeis.org/A203662)

En ellos se cumplen dos propiedades que podrías intentar justificar:

El exponente del menor factor primo de cada uno de ellos es mayor que 2.

Todos tienen los mismos factores primos (salvo los exponentes) que su mayor divisor propio.

Un ejercicio muy interesante es tomar los primeros primos 2, 3, 5, … y combinar sus potencias para formar números de Aquiles, procurando que la primera tenga al menos exponente 3, y que al suprimir el factor más pequeño siga resultando un número de Aquiles. Por ejemplo: 2*2*2*2*3*3*3*3*3 es de Aquiles y si suprimimos un 2, queda 2*2*2*3*3*3*3*3, también de Aquiles. Si calculas descubrirás que se trata de 1944, que ya está en la tabla.

La cuestión inversa es mucho más fácil, porque el mínimo múltiplo de un número es su doble. Así que sólo habrá que buscar números de Aquiles cuyo doble también lo sea. Son estos:

432, 972, 1944, 2000, 2700, 3456, 4500, 5292, 5400, 5488, 8748, 9000, 10584, 10800, 12348, 12500, 13068, 15552, 16000, 17496. 18000, 18252 (http://oeis.org/A2036623)

Otro emparedado

Podemos emparedar un número de Aquiles N mediante potencias, una que sea el mínimo múltiplo de N que sea potencia perfecta y el otro el máximo divisor con ese carácter.

Los resultados serían estos

a/d	Divipot	Aquiles	Multipot	m/a
2	36	72	144	2
3	36	108	216	2
2	100	200	400	2
2	144	288	576	2
2	196	392	784	2
2	216	432	1296	3
4	125	500	1000	2
2	324	648	1296	2
3	225	675	2025	3
2	400	800	1600	2
4	216	864	1728	2
2	484	968	1936	2
3	324	972	2916	3
5	225	1125	3375	3
2	576	1152	2304	2

3	441	1323	3969	3
2	676	1352	2704	2
4	343	1372	2744	2
2	784	1568	3136	2
2	900	1800	3600	2
6	324	1944	5832	3
2	1000	2000	8000	4
2	1156	2312	4624	2
2	1296	2592	5184	2
3	900	2700	8100	3
2	1444	2888	5776	2
7	441	3087	9261	3
2	1600	3200	6400	2
3	1089	3267	9801	3
2	1728	3456	13824	4
2	1764	3528	7056	2
2	1936	3872	7744	2
3	1296	3888	7776	2
4	1000	4000	8000	2

Es interesante la parte derecha, porque el cociente da una pista sobre los números de Aquiles que pueden estar intercalados, como ocurre con el número 10584.

Sólo incluimos la tabla para que puedas analizarla y buscar explicaciones.

	N	Es de Aquiles	
1	10584	VERDADERO	2 2 2 3 3 3 7 7
2	21168	VERDADERO	
3	31752	VERDADERO	
4	42336	VERDADERO	
5	52920	FALSO	
6	63504	FALSO	

PRIMORIAL

La palabra primorial se suele usar con tres significados distintos:

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

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

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

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

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

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

(https://oeis.org/A006862)

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

Como ves, tenemos donde elegir. Nos quedaremos con las dos primeras. Es fácil programar en el Basic de las hojas de cálculo la función primorial de N si posees la

función ESPRIMO, ya explicada en este blog. (Puedes buscarla en el Apéndice de

http://hojamat.es/publicaciones/hojanum1.pdf)

Su código podría ser

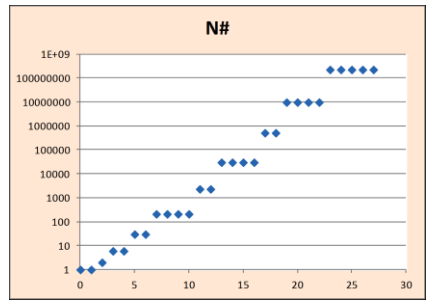
Public Function primorial(n)
Dim k, p

p = 1
For k = 1 To n
If esprimo(k) Then p = p * k
Next k
primorial = p
End Function

No es el más eficiente, pero para explicaciones vale. Con él se puede formar la tabla de la función

N	N#
0	1
1	1
2	2
3	6
4	6
5	30
6	30
7	210
8	210
9	210
10	210
11	2310
12	2310
13	30030
14	30030
15	30030
16	30030
17	510510
18	510510
19	9699690
20	9699690
21	9699690
22	9699690
23	223092870
24	223092870
25	223092870
26	223092870
27	223092870

Como era de esperar, su crecimiento es notable. A partir de la tabla se puede construir el gráfico



Se ha usado una escala logarítmica para ver mejor su estructura escalonada.

¿Dónde tienen lugar los saltos?¿Por qué unos tramos son de dos, otros de cuatro o de cinco? Preguntas con respuesta sencilla que te puedes plantear.

Algunas propiedades

Todos los números primoriales están libres de cuadrados y cada uno de ellos posee más factores primos distintos que los números menores que él. Ambas propiedades son triviales. La segunda se puede expresar de otra forma:

La función omega de un número primorial tiene mayor valor que las correspondientes a los números que le preceden.

Recuerda que la función omega cuenta los factores primos distintos de un número natural. No hay que cavilar mucho para entenderlo. Esta definición nos proporciona otra idea fácil:

Para un valor dado k de la función omega, el primorial k# es el número más pequeño con ese valor de omega.

El primorial y el factorial

La forma de crecer el primorial nos recuerda a la del factorial. ¿Cuál es mayor? Evidentemente, el factorial. ¿Qué números forman el cociente n!/n#?

Pues a ese cociente entenderás que le podamos llamar el "***compositorial de n***". Reflexiona sobre el porqué de ese nombre. ¿Lo has encontrado?, pues demuestra esto:

Dos primoriales consecutivos se corresponden con el mismo compositorial.

Tienes los compositoriales en http://oeis.org/A036691 y la función compositorial de un número en http://oeis.org/A049614

Descomposición factorial de un compositorial

Este es un buen momento para recordar la fórmula de Polignac

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

(Ver http://hojaynumeros.blogspot.com/2009/02/formula-de-polignac.html)

Si descompones cualquier factorial mediante esa fórmula, bastará restarle una unidad a cada factor primo

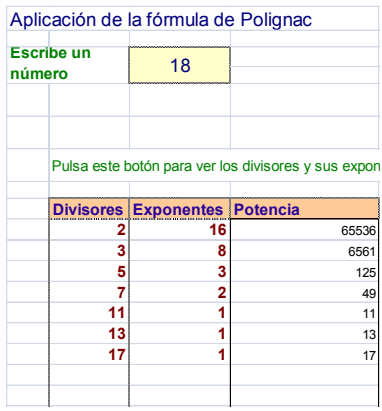
para que resulte la descomposición factorial del compositorial. No es tan complicado como parece.

Lo vemos con un ejemplo: Descomponer en factores primos el compositorial de 18.

Puedes abrir la hoja de cálculo polignac.xls o polignac.ods desde la dirección

http://hojamat.es/sindecimales/divisibilidad/herramientas/herrdiv.htm

Con ella descubrimos que 18! Se descompone tal como se ve en la imagen:



Aplicación de la fórmula de Polignac

Escribe un número: 18

Pulsa este botón para ver los divisores y sus expon

Divisores	Exponentes	Potencia
2	16	65536
3	8	6561
5	3	125
7	2	49
11	1	11
13	1	13
17	1	17

Restamos una unidad a cada exponente y nos resultará comp(18)=$2^{15}*3^{7}*5^{2}*7$=12541132800

Si visitas http://oeis.org/A049614 podrás comprobar este resultado.

En realidad, el primorial de N es el radical de su factorial. Parece un trabalenguas, pero es que se llama radical de un número al mayor divisor libre de

cuadrados que tenga, lo que nos lleva a que el radical es el producto de los factores primos elevados todos a la unidad. Eso es lo que significa el primorial respecto al factorial. Por cierto, es una función multiplicativa, pero esto se alarga y es mejor dejarlo.

SUBIDA A RITMO DE M.C.M

Si te paras unos segundos, ¿sabrías descubrir cómo se ha generado esta sucesión?

1, 2, 6, 12, 60, 60, 420, 840, 2520, 2520, 27720, 27720, 360360, 360360, 360360, 720720, 12252240, 12252240, 232792560, 232792560,

232792560…(http://oeis.org/A003418)

Se parece a la de factoriales, pero crece a menos ritmo.

¿Ya lo sabes? Se trata del M.C.M. de los primeros números naturales: A(n)=MCM(1,2,3,…n). Así el 420=M.C.M(1,2,3,4,5,6,7)

La puedes engendrar con hoja de cálculo, escribiendo los primeros números y abajo encuentras el M.C.M del número de arriba y el número de la izquierda. No damos más detalles.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2	6	12	60	60	420	840	2520	2520	27720	27720	360360	360360

Una bonita pregunta es qué aporta cada número al resultado final del MCM. Observa en la tabla que el

valor A(5)=60 y A(6)=60 también. ¿Por qué el 6 no ha aportado nada al cálculo? Parece ser que sus factores primos estaban ya contabilizados. Entonces, ¿cuáles aportan? Para verlo más claro dividiremos A(n) entre A(n-1)

Si dividimos cada MCM por el anterior nos resulta la sucesión B(n), si definimos B(1)=1

1, 2, 3, 2, 5, 1, 7, 2, 3, 1, 11, 1, 13, 1, 1, 2, 17, 1, 19, 1, 1, 1, 23,…

http://oeis.org/A014963

Con hoja de cálculo se ve mejor:

1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2	6	12	60	60	420	840	2520	2520	27720	27720	360360	360360
	2	**3**	**2**	**5**	**1**	**7**	**2**	**3**	**1**	**11**	**1**	**13**	**1**

Sólo aportan un factor mayor que 1 los números primos y sus potencias. Es claro que es porque sólo ellos suponen algo nuevo. El resto, como el 12, usa factores que ya han aportado el 3 y el 4. ¿Qué ocurre entonces? Que al llegar a cada potencia de primo se habrá acumulado este tantas veces como indique esa potencia. Estudia el 8. Antes de él ha aparecido el 2 como factor de sí mismo y como factor de 4. Con el 2 que aporta el 8 ya tenemos tres, que es precisamente el exponente correspondiente al 8.

En esta sucesión se van acumulando los factores primos de forma que al llegar sus potencias las reproducen exactamente.

Esto tiene una consecuencia muy elegante:

$$n = \prod_{(d|n)} B(n)$$

Si tomas todos los divisores de un número y multiplicas los factores que aportan al MCM (sucesión B(n)) nos resultará de nuevo ese número.

Por ejemplo, en el caso de 24 tendríamos:

Divisores: 1, 2, 3, 4, 6, 8, 12, 24

Valores de B(n): 1, 2, 3, 2, 1, 2, 1, 1

Es evidente que el producto de los valores de B(n) vuelve a dar 24.

¿Conoces la función de Mangoldt? Si has leído a nuestro amigo Rafael Parra te sonará

(http://hojamat.es/parra/funesp.pdf)

Pues bien, nuestra función B(n) es la exponencial de dicha función. Si tomas logaritmos en B(n) obtendrás 0, log(2), log(3), log(2), log(5), 0,… que es la definición de la función de Mahgoldt (tomamos la imagen de http://mathworld.wolfram.com/MangoldtFunction.html)

The Mangoldt function is the function defined by

$$\Lambda(n) \equiv \begin{cases} \ln p & \text{if } n = p^k \text{ for } p \text{ a prime} \\ 0 & \text{otherwise,} \end{cases}$$

Quiere decir que si tomamos logaritmos en la fórmula de arriba nos resultará esta otra:

$$\log(n) = \sum_{(d|n)} \Lambda(d)$$

que podrás encontrar en textos de Teoría de Números. No seguimos por ahí.

Relación con los factoriales

Dijimos en la entrada anterior que la sucesión A(n) subía rápido, pero la de factoriales más. Si dividimos los factoriales entre los MCM que estamos estudiando nos da esta otra sucesión C(n), que basta verla para comprender las distintas "velocidades":

1, 1, 1, 2, 2, 12, 12, 48, 144, 1440, 1440, 17280, 241920, 3626800…

http://oeis.org/A025527

¿Qué números no aportan nada y dejan los valores iguales? Los primos, porque para pasar de (n-1)! a n! hay que multiplicar por n, pero esta operación es la misma que hay que realizar en la sucesión A(n) si n es primo.

Podemos emprender el mismo estudio que para A(n) y es dividir cada término por el anterior.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14
N!	1	2	6	24	120	720	5040	40320	362880	4E+06	4E+07	5E+08	6E+09	9E+10
A(N)	1	2	6	12	60	60	420	840	2520	2520	27720	27720	360360	360360
C(N)=N!/A(N	1	1	1	2	2	12	12	48	144	1440	1440	17280	17280	241920
C(N)/C(N-1)		**1**	**1**	**2**	**1**	**6**	**1**	**4**	**3**	**10**	**1**	**12**	**1**	**14**

Tienes esta sucesión D(n) en http://oeis.org/A048671

En esta tabla vemos que las potencias de primos p^r hacen crecer los términos en p^{r-1} y el resto aporta su propio valor. Para justificarlo volvemos a considerar el paso de (n-1)! a n! y de MCM(1,2,3,…n-1) a MCM(1,2,3,..n):

- Vimos que en los primos en ambos casos se multiplicaba por el mismo número primo y por eso en ellos $C(N)/C(N-1)=1=p^0=p^{1-1}$, luego se cumple.
- En el caso de las potencias de primos el factorial se incrementa multiplicándose por p^r y los MCM s incrementan en p, luego el cociente se incrementará en p^{r-1} , como hemos afirmado.
- En los demás casos el factorial se multiplica por n y el MCM queda igual, luego C(n) quedará también multiplicada por n.

Pero bueno, ¿qué es todo esto? Pues sencillamente, que B(n)*D(n)=n Era de esperar. Una aporta lo que le falta a la otra para ser n. Ahí lo tienes:

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14
B(n)	1	2	3	2	5	1	7	2	3	1	11	1	13	1
D(n)	1	1	1	2	1	6	1	4	3	10	1	12	1	14
B(n)*D(n)	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Los múltiplos y divisores nunca dejan de asombrarnos.

Hace unos días Honorio, un seguidor de este blog, nos envió la siguiente conjetura: “Entre dos números primos consecutivos cuyos dígitos sumen lo mismo, como mínimo hay una diferencia de 18 entre ambos”.

Me causó sorpresa y aunque el tema de primos y cifras no es de los que más me entusiasman me puse a pensar en ella. Pronto descubrí que esta propiedad no la tienen por ser primos, sino por ser impares (el 2 no entra en la conjetura porque no coincide su suma de cifras con el consecutivo). Lo podemos demostrar:

La diferencia entre dos números impares distintos que presenten la misma suma de cifras es siempre un múltiplo (no nulo) de 18.

En efecto, si tienen la misma suma de cifras ambos presentarán el mismo resto módulo 9 (recuerda el criterio de divisibilidad entre 9), luego su diferencia es múltiplo de 9. Pero como ambos son impares, su diferencia es par, luego también es múltiplo de 18, no nulo, porque ambos números son distintos. Luego el valor mínimo de la diferencia es 18, y todas las demás, múltiplos de dicho número.

Esta propiedad abre un abanico de posibilidades: los primos pueden ser consecutivos o no. La diferencia suele ser 18 pero puede ser mayor. Podíamos dar algunas vueltecitas al tema:

V1) Primos consecutivos con la misma suma de cifras y diferencia 18

Si disponemos de las funciones PRIMPROX (próximo primo), ESPRIMO y SUMACIFRAS, ya tenemos las condiciones de búsqueda. Lo hemos realizado con el resultado de

523, 1069, 1259, 1759, 1913, 2503, 3803, 4159, 4373, 4423, 4463, 4603, 4703, 4733, 5059, 5209. 6229. 6529, 6619, 7159, 7433, 7459, 8191, 9109, 9749, 9949, 10691, 10753, 12619, 12763, 12923, 13763, 14033, 14303, 14369, 15859, 15973

(Sólo se escribe el primer número primo de cada par)

Con nuestro Buscador de naturales puedes reproducirla planteando las condiciones

ES PRIMO(N)
ES SUMACIF(N)=SUMACIF(PRIMPROX(N))
ES PRIMPROX(N)=18+N

523
1069
1259
1759
1913
2503
3803
4159
4373
4423
4463
4603
4703
4733
5059
5209

Se exige que N sea primo, que tenga la misma suma de cifras que el siguiente primo y que su diferencia sea 18. Si deseas ver el par completo añade EVALUAR PRIMPROX(N)

Siempre que encontramos una secuencia la comprobamos en OEIS para ver si está publicada, y en este caso no lo está, por lo que la hemos propuesto con

el número A209875 http://oeis.org/A209875 Hoy la nombraré como V1

V2) Primos con la misma suma de cifras que se diferencian en 18

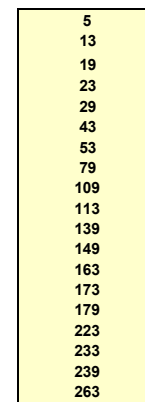
Parece la misma cuestión, pero es que **no exigimos que sean consecutivos**. Por ejemplo, el 2 y el 11 presentan la misma suma y se diferencian en 9. Para buscarlos bastará ver que **p** sea primo y **p+18** también, y que tengan la misma suma de cifras. Como las condiciones son menos restrictivas, es normal que aparezcan muchos más.

El resultado es este:

5, 13, 19, 23, 29, 43, 53, 79, 109, 113, 139, 149, 163, 173, 179, 223, 233, 239, 263, 313, 349, 379, 439, 443, 449, 491, 503, 523, 569, 613, 643, 659,…

Se puede reproducir con el Buscador con las siguientes condiciones:

PRIMO
ES PRIMO(N+18)
ES SUMACIF(N)=SUMACIF(N+18)



En la imagen tienes el resultado. También aquí puedes ver el par completo con **EVALUAR N+18**

Esta sucesión incluye a la V1. No estaba publicada en OEIS, por lo que la hemos

incluido con el número A209663 https://oeis.org/A209663

Si la nombramos como V2, ya tenemos que **V1** $\subset$**V2**.

V3) Primos consecutivos con la misma suma de cifras

En este caso las diferencias entre ellos serán múltiplos de 18.

El resultado es muy parecido al de V1 y está publicado en OEIS hace tiempo

523, 1069, 1259, 1759, 1913, 2503, 3803, 4159, 4373, 4423, 4463, 4603, 4703, 4733, 5059, 5209, 6229, 6529, 6619, 7159, 7433, 7459, 8191, 9109, 9749, 9949, 10691, 10753, 12619, 12763, 12923, 13763, 14033, 14107, 14303,… https://oeis.org/A066540

Puedes reproducirla en el Buscador de Naturales con

PRIMO
ES SUMACIF(N)=SUMACIF(PRIMPROX(N))

El primer par con diferencia 36 es (14107,14143). El primero con diferencia 54 es (35617, 35671) y el primero con 72 (31397, 31469)

Es claro que V1 es un subconjunto de V3, porque 14107 o 35617 pertenecen a V3 y no a V1

Estos pares de consecutivos se pueden ampliar a tripletes: tres números primos consecutivos con la misma suma de dígitos

Los primeros que hemos encontrado son:

22193	22229	22247
25373	25391	25409
69539	69557	69593
107509	107563	107581
111373	111409	111427
167917	167953	167971
200807	200843	200861
202291	202309	202327
208591	208609	208627
217253	217271	217307
221873	221891	221909
236573	236609	236627
238573	238591	238627
250073	250091	250109
250307	250343	250361
274591	274609	274627
290539	290557	290593

Estos tripletes tampoco figuraban en OEIS. Ya es de prever que los hemos incorporado (ver A209396)

Me he puesto a buscar conjuntos de primos consecutivos con la misma suma de cifras. Después de encontrar este me he cansado. Si alguien quiere seguir…

1442173, 1442191, 1442209, 1442227

(Claudio Meller, en la entrada que enlazamos al final, presenta estos cuatro, aunque referidos a igual promedio: ***8508473, 8508491, 8508509, 8508527***. También nos ha indicado dónde se pueden consultar los primeros elementos de los pares, tripletes y demás conjuntos de primos consecutivos con la misma suma. Los puedes encontrar en https://oeis.org/A071613. Gracias, Claudio)

V4) Otra vuelta más.

Si dos números presentan la misma suma de cifras también coinciden en el valor de su **raíz digital**, que es el número entre 0 y 8 que resulta si sumamos sus cifras, y después volvemos a sumar las cifras de esa suma y reiteramos hasta obtener un número menor que 9. Es fácil razonar que ese número es el resto de dividir el número primitivo entre 9.

El inverso no es cierto: si se da la misma raíz digital las sumas de cifras no han de ser iguales, sino congruentes módulo 9.

Pues bien, si sólo exigimos que dos números primos consecutivos tengan la misma raíz digital nos resulta otra sucesión más amplia que la V1 y la V3, que también se ha publicado en OEIS

523, 1069, 1259, 1381, 1759, 1913, 2161, 2503, 2861, 3803, 3889, 4159, 4373, 4423, 4463, 4603, 4703, 4733, 5059, 5209, 5483, 6011, 6229, 6451, 6529, 6581, 6619, 7159, 7351, 7393, 7433, 7459, 7621, 7883, 8191, 8761, 9109, 9293, 9551, 9749, 9949,…

(https://oeis.org/A117838)

Aquí se puede razonar también que las diferencias han de ser múltiplos de 18. Inténtalo.

V5) Aún quedan vueltas que dar, pero lejos de mí producir mareos irreversibles. Las presento con breves referencias:

V51) Tener la misma suma de dígitos es una condición fuerte, pero es más exigente pedir que sean los mismos dígitos, aunque en distinto orden, los que tengan dos primos consecutivos. Puedes verlos en https://oeis.org/A069567 y se llaman pares de Ormiston. Los tienes completos en https://oeis.org/A072274 También existen tripletes de Ormiston.

V52) Y otra vuelta: Claudio Meller, de forma casi simultánea a nosotros ha tratado el tema, pero con promedios

(verhttp://simplementenumeros.blogspot.com/2012/03/889-primos-consecutivos-con-igual.html)

Bueno, bueno, ya vale de dar vueltas. Si encontráis temas similares los incorporo como extensión.

VA A RESULTAR QUE ERES PRIMO

Hoy vamos de pseudoprimos. Si recordáis, 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. Es recomendable igualmente visitar las páginas

http://mathworld.wolfram.com/FermatsLittleTheorem.html
http://hojamat.es/parra/modular.pdf
http://hojamat.es/sindecimales/congruencias/teoria/teorcong.pdf

El recíproco no es cierto. Si para un a primo con m se cumple $a^{m-1} \equiv 1 \pmod{m}$, entonces m no tiene que ser necesariamente primo. A estos números compuestos

que cumplen el teorema les llamaremos pseudoprimos de Fermat para ese número a (hay otros, como los de Euler y los de Poulet, pero los dejamos para otra ocasión)

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

Vemos algún ejemplo de lo explicado:

91 pasa la prueba con 3 pero no es primo Es pseudoprimo para el 3. En efecto, lo vemos por duplicación de exponentes: $3 \equiv 3 \pmod{91}$, luego $32 \equiv 9 \pmod{91}$; $34 \equiv 81 \pmod{91}$; $38 \equiv 9 \pmod{91}$; $316 \equiv 81 \pmod{91}$; $332 \equiv 9 \pmod{91}$; $364 \equiv 81 \pmod{91}$ y queda $390 = 364+16+8+2 \equiv 81*81*9*9 \equiv 1 \pmod{91}$;

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

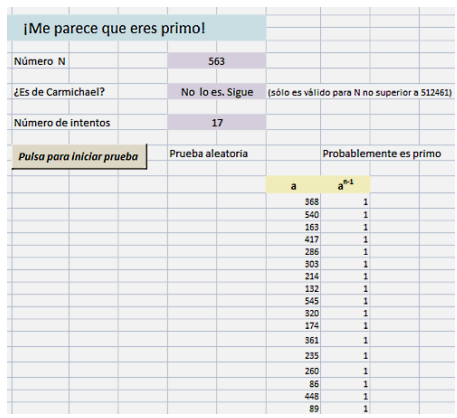
Hemos presentado los números de Carmichael o primos absolutos. Son estos:

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

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

Experimentación con hoja de cálculo

Los algoritmos aleatorios para intentar descubrir si N es primo, se basan en someterlo a la prueba del Pequeño Teorema con varios números aleatorios menores que N y primos con él. Si la prueba da positiva para todo ellos, le daremos a N el calificativo de “primo probable”, y si falla una vez, será con seguridad compuesto. Hemos construido un modelo con hoja de cálculo con objetivos puramente didácticos, sin ninguna otra pretensión. Confiamos que sirva de estímulo a quienes deseen profundizar más en el tema.



Como vemos en la imagen, se admite un número candidato a primo. Si resulta que es de Carmichael, se aconseja no seguir, aunque puedes hacerlo. Fijas el número de intentos aleatorios (en la imagen 17) y si en

todos ellos se cumple $a^{m-1} \equiv 1 \pmod{m}$, se califica como primo posible. Si falla uno de ellos, con seguridad es compuesto.

El proceso es muy rápido porque hemos usado la exponenciación modular explicada en una entrada anterior.

Se ha añadido un botón para descomponer el número en factores primos y así tener la seguridad de que hemos acertado. Si el número es grande puede tardar mucho la comprobación, pero se puede abortar con la tecla ESC.

Puedes experimentar con él descargándolo desde la dirección

http://hojamat.es/blog/pseudoprimos.xslm

Nuestro deseo es que te aficiones a estos temas de los criterios de primalidad. Hay mucho escrito sobre eso y puede hasta ser divertido.

CUESTIONES MODULARES

LA EXPONENCIACIÓN MODULAR

En algunos problemas, como en el criterio de primalidad de Fermat, debemos elevar un elemento de Z_m a un exponente grande. Son frecuentes los problemas del tipo "¿en qué cifra termina 263^{721}?" o "¿es cierta la congruencia $2^{34125} \equiv 1 \pmod{23}$?"

Si el exponente es grande pueden desembocar en cálculos muy complicados, por lo que se acude a la exponenciación **por duplicación**. Estas técnicas que se basan en duplicar son muy antiguas. Ya conocemos el método usado en Egipto

(ver http://hojamat.es/parra/mat_antig.pdf) y posteriormente la llamada multiplicación a la rusa.

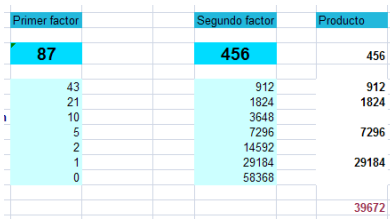
Tenemos implementada, como una curiosidad, esta suma para hojas de cálculo

(ver http://hojamat.es/sindecimales/aritmetica/herramientas/herrarit.htm#peque) y también tienes una exposición teórica en

http://tiopetrus.blogia.com/2005/042501-multiplicacion-a-la-rusa-1-.php

Aquí nos va a interesar la parte común de los algoritmos de duplicación.

Recordemos el algoritmo de la multiplicación rusa:



Primer factor	Segundo factor	Producto
87	456	456
43	912	912
21	1824	1824
10	3648	
5	7296	7296
2	14592	
1	29184	29184
0	58368	
		39672

Si multiplicamos, por ejemplo, 87 por 456, vamos dividiendo 87 entre dos de forma entera, sin decimales, hasta llegar al 1. Simultáneamente duplicamos el otro factor 456 cada vez que dividamos el otro. Después sumamos los múltiplos de este número que se correspondan con los cocientes impares del otro, en el ejemplo

456+912+1824+7296+29184=39672

que coincide con el producto de 87*456.

Esto funciona porque los cocientes impares producen un 1 en la representación binaria de 87 y los pares un cero, por lo que tiene sentido sumar sólo los primeros, y como estamos duplicando en cada proceso, lo que hemos conseguido es lo siguiente:

87*456=(1+2+4+16+64)*456=456+912+1824+7296+29184=39672

En forma de algoritmo podría expresarse así:

```
Public Function rusa(a,b)
Dim  s

s = 0      'Se inicia la suma a cero
While a > 0   'Mientras a no llegue a cero, se divide entre 2
If (a / 2) <> Int(a / 2) Then s = s + b  'Si es impar se suma
b = 2 * b   'Se duplica b
a = Int(a / 2)  ' Se divide a
Wend
rusa = s  ' La función recoge el valor de s
End Function
```

Si copias este listado, lo puedes trasladar al módulo Basic de una hoja de cálculo para comprobarlo. Los parámetros **a** y **b** son los factores.

Podíamos intentar un proceso similar con la potenciación. Por ejemplo, para calcular 7^{13} podríamos proceder así:

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

En lugar de duplicar, elevamos al cuadrado, y al final multiplicamos en vez de sumar.

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): $7 \equiv 2$ (mod 5); $7^2 \equiv 4$ (mod 5); $7^4 \equiv 1$ (mod 5); $7^8 \equiv 1$ (mod 5) y ya todos valen 1, luego

$7^{63}=7^{32+16+8+4+2+1} \equiv 2*4*1*1*1*1 \equiv 8 \equiv 3$, luego $7^{63} \equiv 3$ (mod 5)

El algoritmo de la multiplicación rusa se puede adaptar fácilmente a esta exponenciación

Public Function expo(a, e, m) 'Los parámetros son base, exponente y módulo

Dim p
p = 1 'inicia el producto final
While e > 0
If (e / 2) <> Int(e / 2) Then p = p * a: p = p - m * Int(p / m) 'si es impar multiplica y reduce a resto módulo m
a = a ^ 2: a = a - Int(a / m) * m 'se eleva al cuadrado reduciendo a módulo m
e = Int(e / 2) 'se divide el exponente
Wend
expo = p
End Function

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.

No resisto incluir la versión recursiva que aparece en Wikipedia (para Z)

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

Si has leído nuestra anterior entrada, sabrás que, con limitaciones, el Basic de las hojas admite recursividad. En efecto, hemos probado esta definición para módulo m y funciona:

```
Public Function expo2(a, e, m)
Dim ep

If e = 1 Then
ep = a  'Definición de parada de la recursión
ElseIf e = Int(e / 2) * 2 Then 'Caso par
ep = (expo2(a, e / 2, m)) ^ 2: ep = ep - m * Int(ep / m)
'Elevación al cuadrado
Else
ep = a * expo2(a, e - 1, m): ep = ep - m * Int(ep / m)
'Caso impar
End If
expo2 = ep
End Function
```

EL ALGORITMO EXTENDIDO DE EUCLIDES

No vamos aquí a explicar el algoritmo de Euclides. Mucho mejor lo desarrollan estas páginas y documentos:

http://es.wikipedia.org/wiki/Algoritmo_de_Euclides

http://mathworld.wolfram.com/EuclideanAlgorithm.html

http://hojamat.es/parra/divisibilidad.pdf

Así que supondremos que nuestros lectores conocen el algoritmo y poseen alguna noción de su variante extendida, que viene a reducirse al 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. Si no te suena esto mucho puedes profundizar en las páginas anteriormente citadas y en estas:

http://hojaynumeros.blogspot.com/2009/09/fracciones-continuas-1-definicion.html

http://hojaynumeros.blogspot.com/2009/10/fracciones-continuas-2-reducidas.html

y mejor todavía

http://www.hojamat.es/parra/fraccioncont.pdf

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: **MCD=m*D+n*d**

Este proceso puede complicarse algebraicamente, por lo que se sustituye por cálculos más automáticos, como el algoritmo de las reducidas, que explicamos en

http://hojaynumeros.blogspot.com/2009/10/fracciones-continuas-2-reducidas.html

Aquí nuestro objetivo es recorrer con una hoja de cálculo la técnica del algoritmo de Euclides extendido y su aplicación a la resolución de **ecuaciones lineales** en Z_n, del **teorema chino**, los **elementos inversibles** de ese anillo Z_n y su aplicación a las propiedades de la

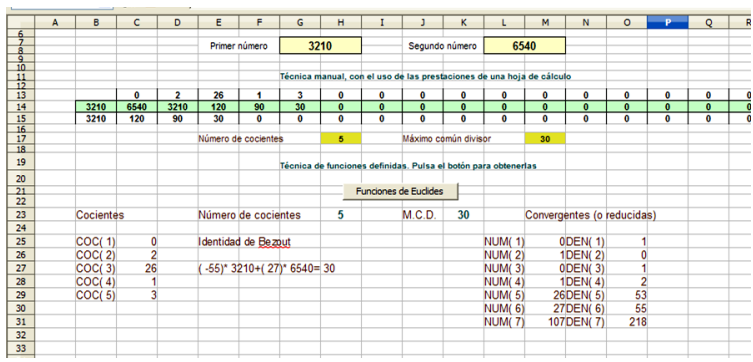
indicatriz de Euler. Todo un programa de trabajo que nos ocupará algunas entradas.

Rutinas y funciones

Para este estudio hemos confeccionado una hoja de cálculo en la que todo el algoritmo extendido se puede expresar mediante funciones. Así, el segundo cociente puede escribirse, según veremos, como COC(2), una convergente en el desarrollo mediante fracciones continuas como NUM(4) y DEN(4), y así con otras. Esto se ha concebido así porque existen varios cálculos que usan el algoritmo extendido, y es preferible, en lugar de usar varias celdas cada vez, efectuar una llamada a la rutina **Euclides(x;y)** que nos devuelve los resultados en forma de función.

Para entenderlo es mejor estudiar la primera hoja de la herramienta que hemos confeccionado (Euclides.ods o Euclides.xlsx) y que puedes descargar en esta dirección

http://hojamat.es/sindecimales/divisibilidad/herramientas/herrdiv.htm



Se observa que en la parte superior se desarrolla el algoritmo de Euclides sin uso de macros. El M.C.D(3210,6540) se obtiene por las clásicas divisiones enteras en las que los restos pasan a ser divisores. Aprenderás mucho de hoja de cálculo si la analizas.

La segunda parte se activa con un botón. Esto significa que hay una macro detrás. En efecto, es la subrutina ***Euclides(X;Y)***, donde X e Y son los números a los que se les calcula el M.C.D. Estas son explicaciones sobre la programación de la hoja, pero puedes prescindir de ellas. Toma esto como una herramienta que sistematiza los cálculos. Lo importante es que según ves en la imagen, aparecen todos los datos en forma de función.

COC: Son los cocientes que aparecen en el algoritmo aplicado a 3210 y 6540 (ver imagen), 0, 2, 26, 1, 3. Estos serían también los cocientes de la fracción continua que desarrolla 3210/6540. Así que esta hoja te permite efectuar esos desarrollos. Puedes comprobar los ejemplos que da Rafael Parra en su documento para entender esto mejor.

Reducidas: También las reducidas de la fracción las tienes en la parte derecha en forma de funciones. Las rotuladas como NUM son los numeradores y DEN los denominadores.

Por curiosidad, efectúa productos cruzados entre ellos y verás que siempre obtienes +1 o -1. Por ejemplo, 26*55-53*27=-1. Esto se puede demostrar que es así. Consulta las páginas recomendadas. El más interesante es el que se forma con las dos últimas: 27*218-55*107=1, por varias razones:

- La última reducida coincide con la fracción primitiva simplificada 3210/6540=218/107, luego esta hoja también te sirve para simplificar fracciones dividiéndolas entre el M.C.D. del numerador y el denominador, que por cierto **en la hoja no se llega a efectuar esa división nunca**. El algoritmo extendido simplifica los datos originales sin dividir.
- La igualdad 27*218-55*107=1 multiplicada por el MCD 30 y quizás con un cambio de signo (que no es el caso en este ejemplo) se convierte en la **Identidad de Bezout**, que la tienes también reflejada en la hoja: El MCD 30 expresado como combinación lineal entera de 3210 y 6540: **(-55)* 3210+(27)* 6540= 30.** Además, 30 es el mínimo número entero positivo que satisface una relación lineal de este tipo. Siempre me ha encantado esta propiedad, que algunos autores toman como definición del MCD. Y como señalábamos más arriba, sin usar el concepto de divisor.
- Adelantando el contenido de la siguiente hoja, la igualdad 27*218-55*107=1 permite reconocer 27 como

el inverso de 218 en el anillo Z_{107}, pero esto es correr mucho por ahora. Lo abordaremos en otra entrada.

Con esta hoja no se pretende sustituir los cálculos manuales. En este blog siempre insistiremos en su necesidad. Sólo se pretendía el poder resumir en una sola página todas las consecuencias inmediatas del algoritmo de Euclides extendido.

LA ECUACIÓN AX=B (MOD M)

También aquí remitimos a otras páginas para entender las condiciones de esta ecuación. En primer lugar has de conocer la teoría elemental de las congruencias o Aritmética modular. Si no es así, puedes visitar

http://hojamat.es/parra/modular.pdf

http://hojamat.es/sindecimales/congruencias/teoria/teorcong.htm

http://mathworld.wolfram.com/ModularArithmetic.html

Dentro de esta teoría uno de los primeros temas importantes es el de la resolución de la ecuación lineal $Ax \equiv B \pmod m$ y lo traemos aquí por su relación con el algoritmo de Euclides. En efecto, la ecuación dada equivale a exigir que Ax y B se diferencien en un múltiplo de m, es decir, que Ax+Cm=B. Si leíste la

entrada anterior, esto te recordará la Identidad de Bezout.

¿Qué sabes de la estructura de anillo? La repasaremos en la siguiente entrada de esta serie. Por ahora sólo tienes que recordar que en el Álgebra Elemental la ecuación Ax=B para números reales se resuelve multiplicando por el inverso de A, si es que lo posee (siendo distinto de cero en este caso), con lo que tendremos $A^{-1}Ax=1x=x=A^{-1}B$, que es una solución para x.

En los anillos en general no todo elemento posee un inverso, es decir, otro elemento que multiplicado por él lo convierta en la unidad (si esa unidad existe – ver http://es.wikipedia.org/wiki/Anillo_unitario-).

En el caso de las congruencias, el anillo Z_m de las clases de restos módulo m está formado por las clases {0,1,2,3,…m-1} a las que llamaremos restos, y en ellos existen algunos que pueden no tener inverso. Por ejemplo, si m=9 los elementos de Z_9 son los restos {0,1,2,3,…8} y si elegimos el 6, ningún múltiplo de 6 produce un 1 como resto módulo 9. Veamos (haz tú los cálculos mentalmente para practicar):

$6*1\equiv6 \pmod 9$; $6*2\equiv3 \pmod 9$; $6*3\equiv0 \pmod 9$; $6*4\equiv6 \pmod 9$; $6*5\equiv3 \pmod 9$; $6*6\equiv0 \pmod 9$; $6*7\equiv6 \pmod 9$; $6*8\equiv3 \pmod 9$

Nunca resulta un producto congruente con 1, **luego el 6 carece de inverso**.

Si repasas la teoría del anillo Z_m (lo haremos también en la siguiente entrada) descubrirás que los elementos inversibles son los números primos con m. Como estamos hablando del conjunto de restos {0,1,2,3,…m-1}, el número de inversibles coincidirá con la indicatriz de Euler, como también veremos más adelante. Ya ves, todo se relaciona.

En la resolución de $A*x \equiv B \pmod m$ se presentan estos tipos:

1. Si A es primo con m, existe una sola solución $x \equiv A\text{-}1*B \pmod m$, por ser A inversible.
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 $x_0 \equiv A^{-1}*B \pmod m$ y existirán en total d soluciones, que vienen dadas por la fórmula $x_r = x_0+r*m/d$ (ver las páginas recomendadas)

   En la segunda hoja de la herramienta que estamos usando (Euclides.ods o Euclides.xlsx en

   http://hojamat.es/sindecimales/divisibilidad/herramientas/herrdiv.htm)

   se sigue este procedimiento. Escribimos los tres datos A,B y m. Sin usar macros, la hoja determina si tiene solución o no y si en caso de tenerla es única o múltiple. Si existe, simplifica los datos.

Ecuación lineal $Ax=B_{(m}$	

Datos	
A	6
B	4
m	10

Reducidos
3
2
5

Tipo de ecuación
Tiene varias soluciones

En la imagen se intenta resolver 6X≡4 (mod 10), que tomaremos como ejemplo. La hoja detecta que existen varias soluciones y simplifica 6, 4, 10 a 3, 2 y 5.

El truco está en las celdas I9, I10 y J10. Investiga y aprenderás.

Abajo figura la resolución, que se basa en la rutina Euclides(X,Y) ya explicada en la entrada anterior y en ella se dan estos pasos:

Reducidas					
				Producto cruzado	1
NUM(1)	0	DEN(1)	1	Penúltimo DEN	2
NUM(2)	1	DEN(2)	0		
NUM(3)	0	DEN(3)	1	INV(A) mod m	2
NUM(4)	1	DEN(4)	1		
NUM(5)	1	DEN(5)	2	INV(A)*B	4
NUM(6)	3	DEN(6)	5		
				Soluciones	4
					9

- Se calculan las reducidas y se toma el penúltimo denominador DEN(5)=2, que es un buen candidato a inverso de A (ver la identidad de Bezout en la entrada anterior).

- Se comprueba el último producto cruzado NUM(6)*DEN(5)-DEN(6)*NUM(5)=3*2-1*5=1 y como vale 1, DEN(5)=2 es el inverso por ser 3*2≡1 (mod 5. Si el producto cruzado hubiera valido -1 deberíamos haber cambiado de signo.

- Según hemos explicado, la solución será igual a INV(A)*B=2*2=4. En efecto, 6*4≡4 (mod 10)

- El MCD(6,4)=2, luego existirán dos soluciones a la ecuación (hablamos en Z_{10}, porque en Z existirían infinitas). Según la teoría, bastará ir sumando el cociente 10/2=5 a las soluciones, lo que nos da (lo ves en la imagen) las soluciones 4 y 9.

Caso homogéneo

Si B es cero, esta ecuación queda como A*x ≡ 0 (mod 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, resuelve con la hoja 6*x ≡ 0 (mod 9) y obtendrás las soluciones 0, 3 y 6, ya que M.C.D(6,9)=3>1. Sin embargo, resuelve 6*x ≡ 0 (mod 7) y sólo obtendrás x=0, ya que en este caso 6 es inversible.

Te proponemos una demostración o comprobación, según te atrevas.

Las diferencias existentes entre las soluciones de la ecuación A*x ≡ B (mod m) son soluciones de la homogénea A*x ≡ 0 (mod m). Inversamente: dada una solución de A*x ≡ B (mod m), si le vamos sumando por separado las soluciones de la homogénea, resulta el conjunto de todas las soluciones de A*x ≡ B (mod m)

Nuestro único objetivo ha sido el que veas la relación de la resolución de esta ecuación con el algoritmo de Euclides y que recorras toda la resolución efectuada por la hoja para comprender mejor los detalles de la misma. Cualquier otro aspecto lo podrás ver en las páginas recomendadas, aunque tampoco se puede decir mucho más.

EL ANILLO Z_M

Recordábamos en la entrada anterior la formación del anillo Z_m mediante clases de restos hasta formar el conjunto {0, 1, 2, … m-1}. Repasa estas páginas si lo deseas:

http://es.wikipedia.org/wiki/Aritm%C3%A9tica_modular

http://hojamat.es/sindecimales/congruencias/teoria/teorcong.htm

http://mathworld.wolfram.com/ModularArithmetic.html

A este conjunto Z_m se le puede dotar de la suma y el producto módulo m que lo convierten en un anillo conmutativo con unidad, que es el resto 1. Esto lo tienes en

http://personales.unican.es/ruizvc/algebra/anillos1.pdf

http://en.wikipedia.org/wiki/Ring_(mathematics)

http://hojamat.es/sindecimales/congruencias/teoria/teorcong.htm#residuales

En realidad, bastaría afirmar que **Z_m es el anillo cíclico de m elementos**. Busca en la Red ese concepto, que es muy sencillo. Por esta estructura cíclica se pensó en llamarles ***anillos*** por primera vez.

En los anillos con unidad son importantes los elementos inversibles. De ellos trataremos aquí.

Un elemento A de Z_m es inversible si existe otro elemento X de Z_m tal que $A*X \equiv 1 \pmod m$ Según vimos en la entrada anterior, esta ecuación 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. 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' (que es no nulo) resulta Am'=A'D*m/D=A'm, que es congruente con cero, luego $A*m' \equiv 0 \pmod m$ 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. En entradas anteriores vimos cómo encontrarlo mediante el algoritmo extendido de Euclides.
- 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 $B^{-1}*A^{-1}$, ya que

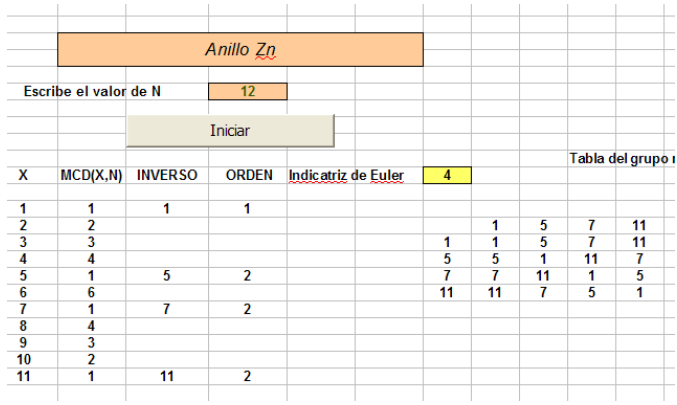
$(B^{-1}*A^{-1})*A*B=B^{-1}*(A^{-1}*A)*B=B^{-1}*1*B=1$

Como el 1 es inversible trivialmente y el inverso también, tenemos que los inversibles forman grupo abeliano, llamado grupo de las unidades Z^*_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^*_m coincide con la indicatriz o función φ(x) de Euler**.

Si m es primo, todos los elementos son inversibles y Z_m se convierte en un cuerpo, pero yo creo que eso ya lo sabías.

La hoja que estamos usando en esta serie de entradas también nos da el grupo Z^*_m de unidades de Z_m. Nos seguimos basando en el algoritmo de Euclides extendido.



Para cada elemento de Z_m se va llamando a la rutina ***euclides(X,m***)(de ahí la ventaja de tenerla implementada como una rutina en Basic), mediante la cual se encuentra el MCD(X,m). Si es igual a 1, se escribe el inverso junto al elemento. En la imagen puedes ver el desarrollo para m=12, y nos da como elementos inversibles 1, 5, 7 y 11.

Contando los inversibles se encuentra la indicatriz de Euler, a la que volveremos próximamente. Finalmente, a la derecha del esquema se construye el grupo multiplicativo de unidades. Observa que, como era de esperar, todos los productos pertenecen al conjunto {1, 5, 7, 11}

Con esta hoja es fácil comprender el teorema de Euler. Observa, por ejemplo, la fila que corresponde al valor 7:{7, 11, 1, 5} Esto quiere decir que 7*1≡7, 7*5≡11,

$7*7 \equiv 1$ y $7*11 \equiv 5$. Imagina que multiplicamos las cuatro congruencias miembro a miembro:

$7*1*7*5*7*7*7*11 \equiv 7*11*1*5$ Simplificamos entre $7*11*1*5$ (porque son inversibles, si no, no se podría) y queda

$7*7*7*7 \equiv 1$, es decir $7^4 \equiv 1$. Pero 4 es la función de Euler de 12 y de ahí la comprobación del teorema:

$7^{\varphi(12)} \equiv 1 \pmod{12}$

Esto no es una demostración, pero si repites lo mismo con valores generales **p** y **m** con **p** inversible, es fácil demostrar que $\mathbf{p^{\varphi(m)} \equiv 1 \pmod{m}}$

Orden de un elemento

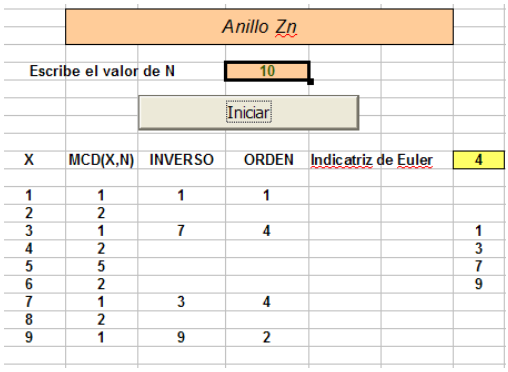
Dado un elemento inversible **a**, llamaremos ***orden*** de ese elemento al mínimo número entero tal que $\mathbf{a^r \equiv 1}$. Según el teorema citado, ese valor existe y puede ser φ(m). Si es menor, ha de ser un divisor suyo. En efecto, supongamos que φ(m) no fuera múltiplo del orden r. Entonces efectuando la división entera entre ambos quedaría φ(m)=qr+s, con s<r. Aplicamos esa potencia al elemento **a** y obtendríamos

$1 \equiv a^{\varphi(m)} \equiv a^{qr+s} \equiv a^{qr} * a^s \equiv a^s$, 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)

Hemos incorporado a la hoja el cálculo del orden de los elementos inversibles, pero sería un buen ejercicio que

los comprobaras usando la tabla de multiplicar. En la imagen puedes consultar el orden de los elementos en el caso de m=10. Observa que los cuatro son divisores de la indicatriz φ(m)



Anillo Zn

Escribe el valor de N 10

Iniciar

X	MCD(X,N)	INVERSO	ORDEN	Indicatriz de Euler	4
1	1	1	1		
2	2				
3	1	7	4		1
4	2				3
5	5				7
6	2				9
7	1	3	4		
8	2				
9	1	9	2		

EL TEOREMA CHINO DE LOS RESTOS

Este teorema lo conocemos todos, pero quizás no hayamos pensado que es la garantía de algún isomorfismo de anillos. Lo iremos viendo.

Se enuncia así:

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 $N \equiv B_i \pmod{M_i}$ 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.

La demostración la puedes consultar en cualquier manual. A nosotros nos va interesar especialmente **la unicidad de la solución** respecto al módulo H. Su fundamento está en que si dos números son congruentes respecto a módulos primos entre sí, también 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, $M_3 \ldots M_n$ y por tanto congruentes respecto a H, que es lo que garantiza su unicidad.

La resolución más popular de este sistema de ecuaciones es la que ideó Gauss:

Algoritmo de Gauss

Para calcular el número N se sigue el proceso:

- Llamemos H al producto de todos los módulos M_i y sea $M'_i = H/M_i$.
- Se buscan unas m_i tales que $m_i.M'_i \equiv 1 \pmod{M_i}$ es decir, sus inversos, y entonces la solución será:
- $N = \sum_{i=0}^{n} M_i \, m_i B_i = \sum_{i=0}^{n} E_i \, B_i$

  donde hemos llamado E_i al producto $M_i * m_i$

- Se puede demostrar que las demás soluciones son congruentes con N módulo H

  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.

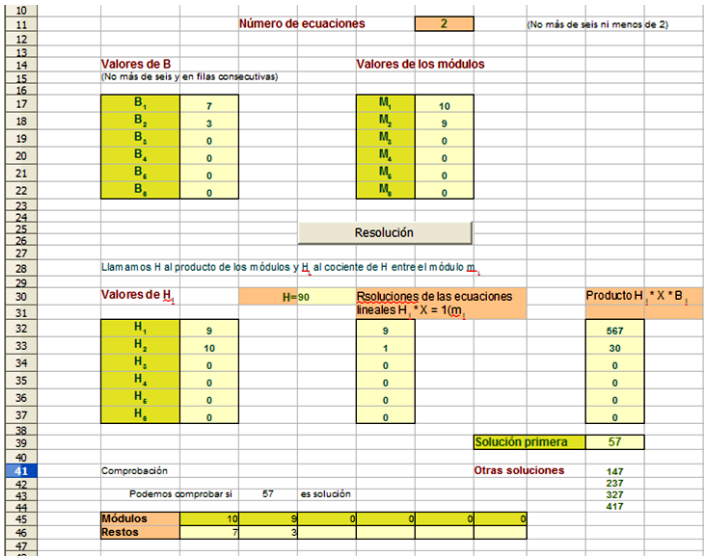
  H=9.10 = 90 ; M'_1=9 ; M'_2=10 ; m_1=9 (porque 9*9=81≡1 (mod 10)); m_2=1 (porque 1*10=10≡1 (mod 9)). Así tenemos que E_1=9*9=81 y E_2=10*1=10 y por último:

  N=81.7+10.3= 597. Lo reducimos a módulo 90 y queda 57. En efecto, 57≡7 (mod 10) y 57≡3 (mod 9)

  Para encontrar las demás soluciones bastará con ir sumando H=90: 57, 147, 237, 327,…

  Estos coeficientes E_i tienen la ventaja de que sólo dependen de los módulos, por lo que se pueden tener almacenados si se van a usar varias veces. Por ejemplo, si el resto deseado para módulo 10 hubiese sido el 2 y para módulo 9 el 6, la solución hubiera sido N=81.2+10.6=162+60=222≡42 (mod 90) y se cumple que el resto de 42 respecto a 10 es 2 y respecto a 9 es 6, como deseábamos.

  Ya te habrás imaginado que vendría la hoja de cálculo en nuestro auxilio para librarnos de algunos cálculos si el número de ecuaciones aumenta. En la imagen tienes el desarrollo del ejemplo anterior:



En la región superior escribimos los módulos M_i, los valores de B_i y el número de ecuaciones. En el central se calcula H, las H_i y sus inversos (mediante el algoritmo de Euclides interno que estamos usando en esta serie). Por último, se efectúa la suma de los productos triples y se reduce a módulo H, se escriben varias soluciones y se comprueba la primera.

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≡a (mod m) y N≡b (mod 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)

Esta biyección la hemos representado en la hoja de cálculo que nos sirve de herramienta en esta serie. En una hoja dedicada a la misma puedes consultar las distintas correspondencias. En la imagen tienes la existente entre $\mathbf{Z_8 \times Z_9}$ y el conjunto $\mathbf{Z_{72}}$.

	0	1	2	3	4	5	6	7
0	0	9	18	27	36	45	54	63
1	64	1	10	19	28	37	46	55
2	56	65	2	11	20	29	38	47
3	48	57	66	3	12	21	30	39
4	40	49	58	67	4	13	22	31
5	32	41	50	59	68	5	14	23
6	24	33	42	51	60	69	6	15
7	16	25	34	43	52	61	70	7
8	8	17	26	35	44	53	62	71

Pero esta correspondencia es más fuerte, porque constituye un isomomorfismo de anillos para la suma y el producto. En efecto, sabemos que para cada resto **N** de $\mathbf{Z_{mn}}$, según el teorema chino, corresponde un resto **p** en $\mathbf{Z_m}$ y otro **q** en **Zn** y que esa correspondencia es biunívoca. Supongamos otro N' que se corresponda con p' y q' respectivamente. Así, si N'≡p' (mod m) y N'≡q' (mod n), podemos sumar y multiplicar miembro a miembro ambas congruencias y quedará: N+N'≡p+p' (mod m) y de igual forma N+N'≡q+q' (mod n). Por tanto, a la suma (p,q)+(p'+q') en $\mathbf{Z_m \times Z_n}$ le corresponde la suma N+N' en $\mathbf{Z_{mn}}$. Esto nos demuestra que la

correspondencia es un homomorfismo para la suma. Igual razonaríamos para el producto.

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 $\Psi(a*a', b*b') = \Psi(a, b) * \Psi(a', b')$

Compruébalo en la tabla de más arriba m=8 y n=9:$\Psi(4,7)=52$, :$\Psi(2,4)=58$ y si sumamos modularmente, $\Psi(6,2)=38$, que es congruente con 52+58=110, módulo 72. Si multiplicamos modularmente ocurre lo mismo: $\Psi(0,1)=64$ y $52*58=3016 \equiv 64 \pmod{72}$

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.

Volvemos a la tabla ejemplo: 5 es inversible en Z_8, 4 es inversible en Z_9. Les aplicamos la función Ψ y según la tabla queda $\Psi(5,3)=13$, que es inversible módulo 72.

LA FUNCIÓN INDICATRIZ DE EULER $\varphi(N)$

Terminamos esta serie sobre las aplicaciones encadenadas del algoritmo extendido de Euclides con la presentación de la función $\varphi(n)$ (indicatriz o indicador de Euler) como **el cardinal del conjunto de elementos inversibles en Z_n**

Sólo nos interesará por ahora este aspecto de la función $\varphi(n)$

Todas las propiedades de $\varphi(n)$ las tienes en multitud de libros y páginas web. Entre ellas puedes consultar

http://gaussianos.com/la-funcion-phi-de-euler-otra-genialidad-del-maestro/

http://hojamat.es/sindecimales/divisibilidad/teoria/teordivi.pdf

http://hojamat.es/parra/funesp.pdf

http://mathworld.wolfram.com/TotientFunction.html

Aquí sólo destacaremos que **$\varphi(n)$ es el cardinal del grupo de inversibles Z^*_n**, (ver nuestra anterior entrada) es decir, el conjunto de números menores que **n** y primos con él, **contando el 1**. Esta definición nos desemboca inmediatamente en su carácter multiplicativo.

En efecto, en la entrada anterior explicábamos que el Teorema Chino de los Restos nos garantizaba que

existía un isomorfismo entre el anillo $\mathbf{Z_m \times Z_n}$ y el anillo $\mathbf{Z_{mn}}$ cuando **m y n son coprimos**. También vimos que este isomorfismo se podía restringir a los grupos de inversibles, es decir, que el grupo $\mathbf{Z^*_m \times Z^*_n}$ es isomorfo a $\mathbf{Z^*_{mn}}$**.** Pues ya lo puedes tener claro…el cardinal del primero es $\varphi(m).\ \varphi(n)$ y el cardinal del segundo $\varphi(m.n)$, luego…

¡Ya hemos llegado a donde queríamos después de más de un mes!

La función indicatriz de Euler es multiplicativa, porque si m y n son coprimos, se cumple que

$\varphi(m).\ \varphi(n) = \varphi(m.n)$

No estaría mal que buscaras otra demostración de esta importante propiedad.

En la hoja euclides.xlsm o en la euclides.ods (http://hojamat.es/sindecimales/congruencias/herramientas/herrcong.htm), en el apartado del isomorfismo, puedes comprobar esta propiedad en casos concretos.

Es curioso que sea multiplicativa una función que cuenta “huecos” (los que no tienen factores comunes con n), que proceden de un cribado, pero si los cuentas como los elementos inversibles de un anillo, los que sobran son los otros, los divisores de cero.

Si has leído las páginas recomendadas o si nos sigues con atención no tendrás problemas en entender que

Si p es primo, $\varphi(p)=p-1$

¡Pues claro! ¿Qué número va a tener divisores con p, salvo él mismo?

Si $n=p^k$ con p primo(es decir, es un número *primario*), $\varphi(n)=p^k(1-1/p)$

Aquí nos detenemos algo más: Los números menores que p^k que tienen divisores comunes con él sólo pueden ser p, p^2, p^3,…p^k, es decir, son en total p^{k-1} números, luego

$\varphi(n)=p^k - p^{k-1} = p^k(1-1/p)$

¿Y si n no es primo ni primario?

En ese caso viene en nuestra ayuda **la propiedad multiplicativa**:

Si $N=p^aq^br^cs^d$, siendo p,q,r,s divisores primos de N, entonces se tendrá $\varphi(N)=N(1-1/p)\ (1-1/q)\ (1-1/r)\ (1-1/s)$

Lo ponemos en limpio:

$$Si\ N = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$$

es la descomposición en factores primos de N, entonces

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

Implementación de la función en hoja de cálculo

Podemos definir la función de dos formas, por su definición o mediante la fórmula anterior. En el primer caso nos resultará un código sencillo y fácil de entender, pero que se vuelve insoportablemente largo para números grandes. Sería este:

Mediante su definición

Definimos en primer lugar el MCD mediante el algoritmo de Euclides

```
Public Function mcd(a1, b1)
Dim a, b, r
r = 1
a = a1
b = b1
If b = 0 Then b = 1
If a = 0 Then a = 1
While r <> 0
r = a - b * Int(a / b)
If r <> 0 Then a = b: b = r
Wend
mcd = b
End Function
```

Después vamos contando los números menores que N coprimos con él

```
Public Function euler(a)
Dim  n, eu, s
If a = 0 Then a = 1
n = 1: s = 0
If a = 1 Then
s = 0
Else
```

While n < a
If mcd(a, n) = 1 Then s = s + 1
n = n + 1
Wend
End If
euler = s
End Function

Esta función no va mal para números pequeños, pero es más rápida en general esta otra:

Public Function euler(n)

Dim f, a, e

Dim recoge As Boolean

'Calcula la indicatriz de Euler de un número

a = n ‘se copia porque se va a alterar su valor en el algoritmo
f = 3 ‘variable de búsqueda de factores primos
e = n ‘valor inicial de la indicatriz
If n / 2 = Int(n / 2) Then e = e / 2 ‘si es par, la indicatriz se divide entre 2
While f <= a ‘se van buscando los factores primos
If esprimo(f) Then
recoge = True
While esmultiplo(a, f)
a = a / f ‘se divide para ahorrar tiempo (algoritmo voraz)

If recoge Then e = e * (f - 1) / f: recoge = False ’sólo se recoge el factor una vez
Wend
End If
f = f + 2 ‘recorre los impares
Wend
euler = e
End Function

El código está basado en la fórmula que hemos obtenido: por cada factor primo **p** se multiplica por **p-1** y se divide entre **p**.

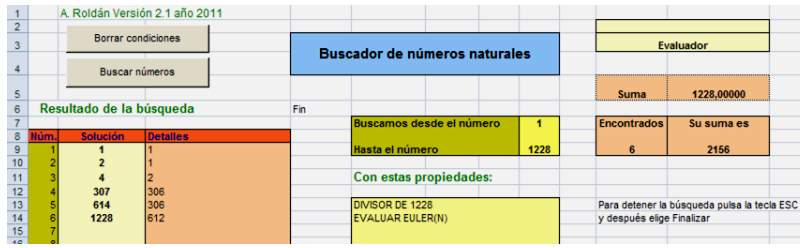
Hemos efectuado pruebas, y para números del orden de 10^5 el tiempo de cálculo se reduce en más de una quinta parte respecto a la primera versión de la función. Así que adoptaremos esta.

También la tenemos implementada en el Buscador de Naturales con el nombre de EULER(N), pero por ahora en la versión lenta.

Te proponemos una búsqueda: Elige un número cualquiera y busca todos sus divisores con el Buscador

(http://hojamat.es/sindecimales/divisibilidad/herramientas/herrdiv.htm)

y evalúa **φ(N)** en cada uno de ellos. Observa la suma: ¿qué obtienes?



Hemos buscado los divisores de 1228, le hemos sumado los valores de la indicatriz y hemos obtenido como suma en el Evaluador otra vez el número 1228.

SUMA DE ELEMENTOS DE 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 $n*2^{n-1}$. Luego será $S_{n-1}+ n*2^{n-1}$.

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 $S_{n-1}=(n-1)*n*2^{n-3}$.

Aplicamos la fórmula de recurrencia presentada más arriba y nos queda:

$S_n=2*(n-1)*n*2^{n-3}+n*2^{n-1}=(n^2-n)*\ 2^{n-2}+2*n*2^{n-2}=(\ n^2-n+2n)*\ 2^{n-2}=n(n+1)2^{n-2}$ 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*Cn-1,0+T* Cn-1,1+ T* Cn-1,2+ T* Cn-1,3+…+ T* Cn-1,n-1 = $T*2^{n-1}$ = $n(n+1)/2*2^{n-1}$ = $n(n+1)*2^{n-2}$, que es la fórmula propuesta.

¿Se te escapó algún detalle? Repasa, repasa…

Quienes acostumbráis a visitar OEIS habréis descubierto que estas sumas forman la secuencia http://oeis.org/A001788. Si la estudiáis podréis descubrir la gran cantidad de interpretaciones que tiene.

LO TENGO REPE

Mi nieta y sus amigas ya tienen edad para coleccionar cromos. Así que las hemos visto repetidamente pasar del entusiasmo de los primeros días -“No lo tengo, no lo tengo, este tampoco”-, a las medias desilusiones de los últimos –“Repe, otro repe, este lo tengo, pero no pasa nada, me pondré a cambiar…, o lo regalo”-. Al final, los padres se van al Rastro o piden a las distribuidoras los cromos que faltan. Siempre ha sido así, al menos desde que éramos niños los que ahora somos abuelos.

Este proceso de evolución de la esperanza en obtener un nuevo cromo ha interesado a especialistas y divulgadores, especialmente al explicar las simulaciones. Recuerdo con mucha nostalgia un artículo de Ricardo Aguado, Agustín Blanco y Ricardo Zamarreño, compañeros en los tiempos heroicos (años 80) de introducción de los ordenadores en la enseñanza.

http://www.doredin.mec.es/documentos/00820073007308.pdf

Ellos simularon la evolución de la colección de cromo en cromo, y con una ampliación para el caso de dos coleccionistas que intercambian.

He visto también alguna simulación sobre cromos con MINITAB, pero ninguna con hoja de cálculo. Quien siga este blog sabrá ya que eso es motivo suficiente para que se emprenda en él otra nueva tarea.

Aquí estudiaremos la evolución de sobre en sobre, que es como verdaderamente se compran los cromos y consideraremos una sola colección sin intercambio con otras.

Primera aproximación

Si se tienen ya **K** cromos y la colección consta de **N**, la probabilidad de que obtengas **h** cromos nuevos en un sobre que trae **m** es, **en primera aproximación**, de tipo binomial. En efecto, se trata de obtener **h** éxitos en **m** intentos dentro de una variable dicotómica (REPE-NO REPE). Pero de esta forma hemos hecho una pequeña trampa, que es suponer que la probabilidad **permanece constante** mientras sacas cromos del sobre, y eso no es así, pues cualquier cromo no repetido altera la situación, pero ya hemos advertido que es una

aproximación para abrir camino. Después pasaremos a una simulación exacta.

Con esta idea, si la probabilidad de que no tengamos un cromo que saquemos del sobre es **p=(N-K)/N**, la esperanza matemática de obtener **m** cromos nuevos será, según la teoría de las distribuciones binomiales, **E=mp**. En cada sobre esperamos obtener E cromos.

(ver
http://hojamat.es/estadistica/tema6/teoria/teoria6.pdf)

En esa idea nos basaremos para construir con la hoja de cálculo un modelo aproximado: para cada sobre hallaremos las probabilidades de que salga repetido o no, calculamos E y vamos acumulando. El gran problema de este estudio es que cada cromo nuevo que incorporemos a la colección hace variar la probabilidad **p**, por lo que tendremos que ir calculando de sobre en sobre. De ahí la utilidad de una hoja de cálculo, aunque, al ser las operaciones bastante simples, se puede usar una calculadora.

Una forma de abordar el tema es construyendo una función de cuatro variables:

Public Function paso_med(total, tengo, sobre, compra)
Dim i, salen
For i = 1 To compra

salen = sobre * (total - tengo) / total
tengo = tengo + salen
Next i
paso_med = Int(tengo)
End Function

Los parámetros son TOTAL, que es el número de cromos de la colección completa, TENGO, los que ya tengo, SOBRE, los que vienen en cada sobre y COMPRA, los sobres que compro. Para llegar al resultado (insistimos, aproximado y estimativo), se recorren los sobres uno a uno, se le estima la media de no repetidos (variable SALEN) y se acumula a los que tengo. Todo el cálculo se recoge en el resultado PASO_MED.

Con esta función puedes construir una tabla de evolución de la colección. Parte de un inicio, que puede ser de 0 cromos, y vas usando de forma recurrente la función anterior hacia abajo, saltando cada vez el número de sobres que desees. Así lo hemos hecho en esta tabla, contando también los cromos comprados y los que salen repetidos:

Sobre	Total	Sobres en cada compra
5	250	10

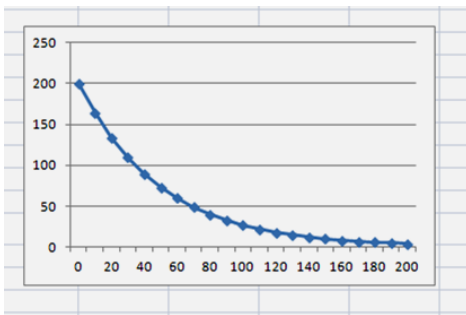
Sobres	Salen	Compro	Repes	Faltan
0	0	0	0	250
10	45	50	5	205
20	82	100	18	168
30	112	150	38	138
40	137	200	63	113
50	157	250	93	93
60	174	300	126	76
70	187	350	163	63
80	198	400	202	52
90	207	450	243	43
100	214	500	286	36
110	220	550	330	30
120	225	600	375	25
130	229	650	421	21
140	232	700	468	18
150	235	750	515	15
160	237	800	563	13
170	239	850	611	11
180	241	900	659	9

Si consideramos terminada una colección cuando faltan por tener menos de 10 cromos (en ese momento suele aparecer la decisión paterna de comprar los que quedan), según este ejemplo, que no anda muy descaminado, hay que comprar unos 180 sobres en lugar de los 50 que en este caso constituirían el número mínimo, es decir un 360% sin contar los últimos. Si quisiéramos aproximarnos al último cromo sería necesario comprar más del 500%

De todas las columnas nos fijaremos en primer lugar en la última

Evolución de los cromos que faltan por tener

Si representamos gráficamente el número de cromos que van faltando en cada compra, obtenemos una gráfica de siguiente tipo

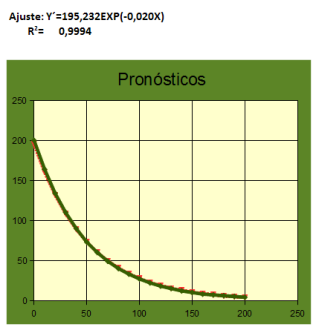


No constituye ninguna sorpresa. Sabemos que el incremento (negativo) del número de los que nos faltan

va decreciendo alarmantemente con cada compra. Tampoco nos asombrará el que se ajuste bien a una función exponencial, ya que la probabilidad de disminuir el número de cromos que nos faltan es aproximadamente proporcional a dicho número, en virtud de la probabilidad **p=(N-K)/N.**

Hemos ido cambiando los parámetros TOTAL y SOBRE, comprobando que una función del tipo

$$FALTAN(X) = TOTAL \cdot e^{(-SOBRE/TOTAL)X}$$



donde X es el número de sobres comprados, se ajusta bastante bien al proceso, como puedes observar en el siguiente ajuste realizado con un total de 200 cromos cuando entran 4 en cada sobre.

Acumulación de repetidos

Si tienes el dato de los que te faltan, también sabes los repetidos que te han salido. Su fórmula aproximada sería:

$$REPES(X) = SOBRE \cdot X - TOTAL \cdot \left(1 - e^{(-SOBRE/TOTAL)X}\right)$$

Te dejamos que razones este resultado. La gráfica de los repes tiene como asíntota y=SOBRE.X-TOTAL. Es fácil de ver: los cromos que ya tengo se acercan poco a poco al TOTAL y SOBRE.X representa los que ya he comprado, luego es lógico que los repetidos se acerquen a su diferencia.

¿Y si quisiéramos llegar a los últimos cromos?

Sin cambiar ni comprar podríamos llegar a un proceso infinito de compra. Por eso, lo lógico es detenerse cuando ya faltan diez o doce cromos y acudir a la compra directa.

Hemos introducido la función inversa (también aproximada), por la que sabiendo los cromos que ya tengo y los que quiero, te devuelve el número de sobres que necesitas comprar por término medio.

Su código es

```
Public Function compra_med(total, tengo, sobre, quiero)
Dim i, salen, t
i = 1
t = 0
While tengo < quiero
salen = sobre * (total - tengo) / total
tengo = tengo + salen
```

```
i = i + 1
Wend
compra_med = i
End Function
```

Con ella se llega a resultados muy interesantes. En la siguiente tabla se recogen los sobres de cinco cromos que se tendrían que comprar en una colección de 250, partiendo de cero, para llegar a 240, 245 o incluso 249 (con 250 podría llegar a un bucle sin salida). En teoría, si no salieran repetidos, serían 50 sobres, pero en la realidad, observa…

Colección de 250 cromos en sobres de 5

Paro de comprar en	Sobres que he de comprar	Porcentaje respecto al mínimo
240	161	322%
245	195	390%
247	220	440%
248	240	480%
249	275	550%

Al último resultado ya llegaron los autores citados arriba: necesitas comprar más de cinco veces el número mínimo de sobres necesario. También llama la

atención que para que sólo te falten 10 debas comprar el 322%. Es todo un aviso a los papás.

¿Qué exactitud tendrá todo esto? Pues ahora efectuaremos una simulación cromo a cromo y realizaremos series para ver si se confirman estos resultados.

Simulación de una colección de cromos

En esta segunda parte intentaremos acercarnos algo más al problema mediante una simulación cromo a cromo. Seguiremos pensando en términos de sobres completos, pero simularemos la aparición de cada cromo individualmente.

Una de las ventajas que tiene la hoja de cálculo es que toda ella es una matriz de datos, con lo que nos ahorramos dimensionar variables tipo array, ya que las tenemos delante de nuestra vista.

15	*Simulación*	
16	Cromos que ya tengo	
17	1	4
18	2	10
19	3	4
20	4	4
21	5	3
22	6	1
23	7	1
24	8	3
25	9	5
26	10	2
27	11	2
28	12	2

Para simular una colección de cromos, lo primero que confeccionaremos es una lista de ellos numerados del 1 al total de la colección. Posteriormente figurarán junto a ellos el total de repetidos que nos han salido.

En la imagen se ha elegido la columna A para la lista de cromos y la B para sus frecuencias de aparición.

Una vez preparada la lista, procederemos a simular la apertura de un sobre. No cansaremos a los lectores con códigos, pero sí señalaremos que los pasos de simulación necesarios son:

- Se simula la aparición de cada cromo nuevo. Suponemos que no hay malicia en la distribuidora y que todos van saliendo de forma equiprobable.
- Una vez tengamos el sobre simulado, desecharemos aquellos conjuntos en los que hay cromos repetidos, porque parece ser que esto no suele ocurrir.
- Admitida la composición del sobre, recorreremos la lista de los cromos que ya tenemos. Si su frecuencia es cero, los consideramos nuevos y se incorporan a la lista de los que tenemos y en caso contrario se consideran repetidos. En ambos casos se incrementa la frecuencia.

Este proceso va bastante rápido, y se puede observar la composición de cada sobre nuevo y la evolución de la lista.

Simulación

Cromos que ya tengo		Sobre	Tengo	Me faltan	Repes	Máximo repe
1	3	60	238	12	662	9
2	2	57				
3	4	158				
4	3	196				
5	2	230				

Como observarás en la imagen, se pueden crear contadores para ver los cromos que vamos teniendo, los que nos faltan y los repetidos. También, aunque después no lo hemos visto muy interesante, la máxima

frecuencia de repetición que se observa en la simulación. En la imagen vemos que un cromo al menos ha aparecido 9 veces.

En la dirección hojamat.es/blog/cromos.xlsm tienes la hoja de Excel que contiene esta simulación. En la parte superior se puede realizar el estudio por medias de la primera parte y en la inferior, además de simular la compra de X cromos, es posible planificar una serie de simulaciones para equilibrar los resultados. Si la descargas, recuerda que los datos para la simulación son los de la parte superior.

Aquí nos limitaremos a presentar los resultados.

¿Confirma la simulación los resultados aproximados del estudio por medias?

Pues en gran parte sí. En la siguiente tabla comparamos los datos obtenidos por medias binomiales en la entrada anterior y los procedentes de series de 50 simulaciones cada una.

Sobre	Total	Sobres en cada compra
5	250	10

Sobres	Medias	Simulación	Diferencia
0	0	0	0
10	45	45,74	0,74

20	82	83,64	1,64
30	112	114,52	2,52
40	137	137,96	0,96
50	157	159,16	2,16
60	174	176,78	2,78
70	187	190,56	3,56
80	198	201,82	3,82
90	207	208,96	1,96
100	214	216,38	2,38
110	220	223,22	3,22
120	225	227,82	2,82
130	229	232,22	3,22
140	232	235,26	3,26
150	235	238,18	3,18
160	237	239,82	2,82
170	239	242,38	3,38
180	241	243,54	2,54

Las diferencias son muy pequeñas, nunca superiores a 4 cromos, lo que da validez a la aproximación por medias, teniendo en cuenta que tampoco la simulación tiene carácter exacto (aquí todo es azar).

También aquí son bastante aproximadas las funciones exponenciales que creamos para explicar la evolución de la colección.

Hay un punto interesante: La esperanza de obtener cromos nuevos en cada sobre es ligeramente superior a la que nos daría la fórmula **E=mp** de la media binomial con probabilidad constante. Esto es debido a que cada cromo que aparece, si no lo tenemos, disminuye la probabilidad del siguiente y aumenta la de obtener el siguiente repetido. Si nos sale repetido, no altera las probabilidades, porque lo guardamos en otra parte. Hemos usado este hecho para estudiar todos los casos que se pueden dar en la apertura de un sobre de 4 cromos en una colección de 200 si ya tenemos 72. Si lees la tabla es natural que te “marees”, porque no es fácil seguir cada caso, pero al final resulta que la media bien calculada es un 1,3% superior a la obtenida sin cambiar las probabilidades:

Colección	128	127	126	125	256032000	0,16002	4	0,64008
200	128	127	126	75	153619200	0,096012	3	0,288036
Sobre	128	127	74	126	151570944	0,0947318	3	0,2841955
4	128	127	74	74	89017856	0,0556362	2	0,1112723
Tengo	128	73	127	126	149522688	0,0934517	3	0,280355
72	128	73	127	74	87814912	0,0548843	3	0,164653
Faltan	128	73	73	127	86628224	0,0541426	2	0,1082853
128	128	73	73	73	49794176	0,0311214	1	0,0311214
	72	128	127	126	147474432	0,0921715	3	0,2765146
	72	128	127	73	85441536	0,053401	2	0,1068019
	72	128	73	127	85441536	0,053401	2	0,1068019
	72	128	73	73	49112064	0,030695	1	0,030695
	72	72	128	127	84271104	0,0526694	2	0,1053389
	72	72	128	73	48439296	0,0302746	1	0,0302746
	72	72	72	128	47775744	0,0298598	1	0,0298598
	72	72	72	72	26873856	0,0167962	0	0
					1598829568	0,9992685		**2,5942852**
						E=n*p		**2,56**
						Incremento		**1,3%**

De este orden son las diferencias entre las dos tablas que hemos confeccionado, por lo que una valida a la otra.

¿Se atreve alguien a sacar una fórmula algebraica que resuma esta tabla? Yo no, pero parece que alguien ha obtenido algo similar.

Resumen de hechos notables

Destacamos algunos hechos observados con ambos métodos (media binomial y simulación) y dejamos que los lectores intenten justificarlos con los medios que les hemos propuesto.

(1) Si compras el mínimo de sobres de una colección (cociente entre el TOTAL y el SOBRE) sólo conseguirás completar un 63% de la misma (en realidad, unas décimas más, entre 63,2% y 63,8% aproximadamente según los casos. Cerca del valor de 1-1/e ¿por qué?)

(2) El momento de compra en el que se igualan el número de cromos que tienes con los que te faltan (mitad de la colección) es cuando has adquirido el 69% de los cromos. (cerca del valor de 100*LN(2) ¿de dónde sale esa estimación?). Los papás se han gastado un 19% más de lo previsto. A partir de ahora saldrán más repetidos que nuevos.

(3) Un momento crítico ocurre cuando al abrir sobres nuevos hay una gran posibilidad de que todos sus cromos estén ya repetidos. Esto se dará cuando la

esperanza E en un sobre no llegue a la unidad. Una fórmula aproximada para encontrar ese punto crítico es

$$X = TOTAL \cdot \frac{Ln(SOBRE)}{SOBRE}$$

Por ejemplo, en una colección de 240 cromos que vienen en sobres de 6, cuando lleves comprados 71 sobres comenzarán los problemas.

(4) Por último, una fórmula medio empírica para relacionar el porcentaje de la colección **P** que deseas alcanzar y los sobres comprados:

$$X = -\frac{TOTAL}{SOBRE} Ln(1 - P)$$

Si la aplicas, no te asustes, y piensa en ir cambiando cromos.

Estos cálculos los hemos comprobado con la simulación y en realidad son algo más favorables, por ese 1,3% de diferencia que existía entre calcular por medias y simular.

OBTENCIÓN DE LA LISTA DE DIVISORES

Algoritmo con hoja de cálculo

Para encontrar los divisores de un número N la búsqueda más simple consiste (salvo alguna pequeña modificación que la acelere) en recorrer todos los números menores o iguales a N y tomar nota de los que son divisores suyos. Es muy sencilla de programar y sólo ocupa unas pocas líneas de código. Tiene el inconveniente de que para números de más de cuatro o cinco cifras decimales resulta muy lenta en hoja de cálculo, que es la herramienta que usamos en este blog.

Un algoritmo más rápido consiste en reproducir en la hoja el esquema que siempre se ha usado en las clases de Matemáticas, el que desarrolla las distintas potencias del primer divisor primo y después las combina con las de los demás en una tabla bidimensional como la siguiente, que se corresponde con los divisores del número 33075=33*52*72

3	1	3	9	27
5	5	15	45	135
	25	75	225	675
7	7	21	63	189
	35	105	315	945
	175	525	1575	4725
	49	147	441	1323
	245	735	2205	6615
	1225	3675	11025	33075

En ella se han situado en la primera columna los factores primos, en la primera fila las potencias del 3 y en las demás filas los distintos productos que se pueden formar entre las potencias, sumandos formados en la fórmula

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

de la obtención de sigma(N).

Para poder construir este esquema en la hoja necesitamos saber qué factores primos posee el número y con qué exponentes. La siguiente subrutina en Basic nos los proporciona:

Global p(50) as long Se definen las variables p para los factores, e los exponentes y np el número total

```
Global e(50) as integer
Global np%

Sub sacaprimos(a)
Dim f,i
dim vale as boolean

f=2:i=1:e(i)=0:vale=false:np=0
while f<=a  'El bucle while_wend divide el número entre el factor todas las veces posibles
if esprimo(f) then
while a/f=int(a/f)  'es divisor primo
vale=true
p(i)=f
e(i)=e(i)+1  'aumenta el exponente
a=a/f
wend
if vale then
np=np+1  'aumenta el número de factores
i=i+1:e(i)=0  'se inicia un nuevo exponente
end if
vale=false
end if
f=f+1 'buscamos otro factor primo
wend
End sub
```

Con este código obtenemos la lista de factores primos p(i), la de exponentes e(i) y el número total de factores primos np.

Al usar estos datos la búsqueda de divisores se simplifica mucho, pues todo el trabajo consistirá ahora en construir la tabla que estudiamos en nuestros años escolares:

(a) Formamos una fila con las potencias posibles del primer factor primo. Tomamos nota de que la altura de la tabla es de 1. También recogeremos el dato de la variable fila en la que se han escrito.

(b) Vamos multiplicando esas potencias de la primera fila por todas las de los otros primos, pero teniendo cuidado de:

- En cada nuevo primo la altura queda multiplicada por e(i)+1, que es el número de sus potencias posibles.
- En cada nuevo producto deberemos incrementar la variable fila en una unidad, para que se vaya formando la tabla hacia abajo.
- Deberemos usar muchos bucles anidados, porque intervienen as variables del número de potencias de la primera fila, el de las del resto de primos y las del número de primos diferentes.

Un posible código en OpenOffice sería:

sub todosdivisores

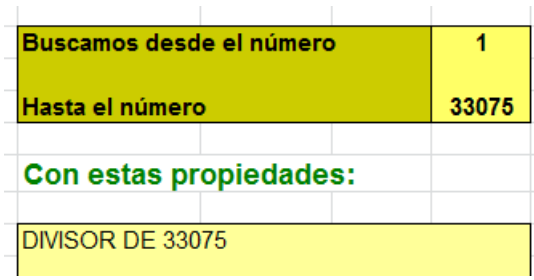
dim i,j,k,l, altura,fila
dim divi as long

Rellena la primera fila con las potencias del primer primo
if np>=1 then
StarDesktop.CurrentComponent.sheets(1).GetCellByPosition(2,11).value=p(1)
for k=0 to e(1)
StarDesktop.CurrentComponent.sheets(1).GetCellByPosition(3+k,11).value=p(1)^k
next k
end if

Va multiplicando las potencias de los demás primos
if np>=2 then
altura=1:fila=12
for k=2 to np Este bucle recorre los primos
StarDesktop.CurrentComponent.sheets(1).GetCellByPosition(2,fila).value=p(k)
for j=1 to e(k) Recorre las potencias del primo actual
for i=1 to altura Recorre todos los divisores anteriores
for l=0 to e(1) Ídem los elementos de cada fila

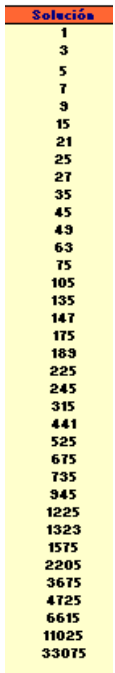
divi=StarDesktop.CurrentComponent.sheets(1).GetCellByPosition(3+l,10+i).value
divi=divi*p(k)^j Efectúa el producto y lo escribe
StarDesktop.CurrentComponent.sheets(1).GetCellByPosition(3+l,fila).value=divi
next l
fila=fila+1 Una vez escritos, aumenta la fila
next i
next j
altura=altura*(e(k)+1) La altura se amplía
next k
end if
end sub

Otra posibilidad fácil, pero algo lenta, de encontrar la lista de divisores es con nuestro Buscador. Basta una condición para lograrlo.



Recorremos los números del 1 al 33075 (por conservar el ejmplo) y exigimos que sean divisores de ese número.

El resultado es



Si observas la parte deracha de la hoja, allí verás que han resltado 36 divisores, y que suman 70680, que es la función SIGMA de 33075.

Pues ya tienes una idea. El resto es cosa tuya. Seguro que la mejoras.

EL ALGORITMO DE MOESSNER

Presentamos en este apartado una curiosidad matemática a base de cribados: toma la lista de los primeros números naturales. Tacha después uno de cada cuatro, comenzando con el mismo 4:

1 2 3 5 6 7 9 10 11 13 14

Después escribe la lista de sus sumas parciales.

1 3 6 11 17 24 33 43 54 67 81

Y ahora tachas de tres en tres, sumando después de nuevo.

1 3 11 17 33 43 67 81

1 4 15 32 65 108 175 256

Después tachas de dos en dos

1 15 65 175

Y sumas

1 16 81 256

El resultado es la serie de las potencias cuartas de los naturales. Recuerda que hemos comenzando tachando de cuatro en cuatro. ¿Funcionará con el tres?

Lo escribimos sin explicaciones:

1 2 4 5 7 8 10 11 13 14 16 17

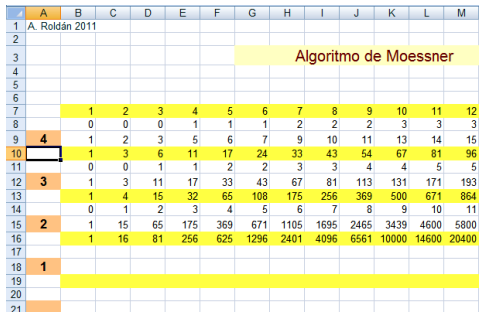
1 3 7 12 19 27 37 48 61 75 91 108

1 7 19 37 61 91

1 8 27 64 125 216

Resultan los cubos. Prueba de dos en dos y obtendrás los cuadrados. ¿Funcionará esto siempre? Este algoritmo lo propuso Alfred Moessner y fue demostrada su validez para cualquier valor natural por Oskar Perron en 1951 usando la inducción matemática.

Nuestro objetivo hoy es reproducir este algoritmo con hoja de cálculo, que por cierto no es nada fácil. Contiene una verdadera trampa, que es la posible confusión entre valores y posiciones. Lo vemos:



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	A. Roldán 2011												
2													
3							Algoritmo de Moessner						
4													
5													
6													
7		1	2	3	4	5	6	7	8	9	10	11	12
8		0	0	0	1	1	1	2	2	2	3	3	3
9	4	1	2	3	5	6	7	9	10	11	13	14	15
10	1	1	3	6	11	17	24	33	43	54	67	81	96
11		0	0	1	1	2	2	3	3	4	4	5	5
12	3	1	3	11	17	33	43	67	81	113	131	171	193
13		1	4	15	32	65	108	175	256	369	500	671	864
14		0	1	2	3	4	5	6	7	8	9	10	11
15	2	1	15	65	175	369	671	1105	1695	2465	3439	4600	5800
16		1	16	81	256	625	1296	2401	4096	6561	10000	14600	20400
17													
18	1												
19													
20													
21													

En la celda A9 escribimos la amplitud de los saltos. En la imagen está preparado para que resulten las cuartas potencias. La hoja se encarga de ir restando una unidad hacia abajo y dejar de escribir cuando se llegue a 1. El modelo está preparado para llegar a 5, pero si lo descargas puedes ampliarlo a tu gusto.

La fila 7 contiene la serie de números naturales. Después se van repitiendo hacia abajo tres filas:

Primera: Es un artificio, pues la hoja debe buscar el elemento a tachar cada vez más lejos, y dependiendo del valor de A9. Esto lo hemos resuelto con la fórmula (usamos la contenida en C8)

=SI(ESNUMERO($A12);SI(RESIDUO(C$7-1;$A12)=0;B8+1;B8);"")

En primer lugar verifica si aún quedan saltos por dar con **ESNUMERO($A12**). Después encuentra el residuo del número de arriba respecto al salto y hace avanzar el contador (B8) si ese número es múltiplo del salto. Así medimos el alejamiento del elemento que debemos tachar. Observa que van aumentando los valores cada

tres (representan los tres supervivientes después de tachar)

Segunda: Aquí se eligen los números entre los de arriba, saltando los que ocupan un lugar múltiplo de 3. Después, con la función DESREF se dirigen a la celda adecuada para copiar el número:

=SI(ESNUMERO($A12);DESREF(C9;-2;C8);"")

DESREF se dirige a dos filas más arriba (-2) y salta según indica el valor de arriba (C8). Como esta contiene los saltos adecuados, cada vez que cambie su valor se tacha un número. Es lo que queríamos. No es fácil de entender y cuesta encontrar el procedimiento.

Tercera: Se limita a acumular sumas, y al llegar al nivel 1 produce las potencias deseadas.

Aunque esto no pasa de una curiosidad, la construcción del algoritmo es apasionante. Este que ofrecemos no usa macros, y lo puedes descargar en dos versiones desde

hojamat.es/blog/moessner.zip

SIMULACIÓN PARA VAGOS

El otro día, buscando temas por ahí, me topé con la secuencia http://oeis.org/A051293
1, 2, 5, 8, 15, 26, 45, 76, 135, 238, 425, 768, 1399, 2570, 4761, 8856, 16567, 31138… que representa el

número de subconjuntos de {1,2,3,...,n} cuya media aritmética es entera.

Por ejemplo, en el caso de 4, los subconjuntos con media entera son {1}, {2},{3},{4},{1,3},{2,4},{1,2,3} y {2,3,4}, en total 8.

Me pareció un tema interesante e intenté abordarlo usando congruencias y después particiones, pero la cosa se complicó y me sentí *vago*. Quien tenga más disposición que yo puede seguir con ello. Además, el autor de esta secuencia en OEIS se vio obligado a conjeturar cosas. Malo.

¿Y si lo simulara? Yo nunca lo había intentado con conjuntos de este tipo y quizás podría reproducir la secuencia, al menos con algún pequeño error. Me puse a ello:

(a) Simulación de subconjuntos

Se puede usar la técnica de tirar una moneda: recorremos los elementos de {1,2,3,...,n} y para cada uno de ellos tiramos una moneda. Si sale *cara*, lo incluimos en el subconjunto, y si sale *cruz*, no lo incluimos. En los lenguajes de programación disponemos de la función ALEATORIO(), que en Basic es RND. Así que el algoritmo de formación de un subconjunto de {1,2,3,...,n} podría ser similar a este esquema:

Randomize

For i=1 to n

If rnd(1)>1/2 then … se incluye en el subconjunto

Next i

Para quienes no lo sepan, ***randomize*** hace que cada vez que usemos el algoritmo se forme una secuencia distinta de números aleatorios (en realidad, seudoaleatorios)

(b) Identificación de las medias aritméticas enteras

Como en nuestro caso nos interesa la media en cada subconjunto, las sentencias presentadas en Basic se podrían concretar en el sentido de que para cada subconjunto tomemos nota del número de elementos y de su suma, para luego dividir y hallar la media.

Podemos definir la variable n para recoger el número de elementos y la variable s para formar la suma. En ese caso las sentencias anteriores se podían modificar así:

Randomize
n=0:s=0
For i=1 to n
If rnd(1)>1/2 then n=n+1:s=s+i
Next i
media=s/n

De esta forma obtendríamos la media de los elementos de cada subconjunto.

Ahora sólo nos quedaría comprobar si la media es entera. Esta prueba consistirá en ver si media=INT(media). Podemos generar muchos conjuntos aleatorios, por ejemplo 10000 y contar aquellos en los que la media es entera. En caso afirmativo incrementamos un contador.

Por último. Lo que marque el contador lo convertimos en proporción dividiendo entre 10000 y multiplicamos después por 2^n para que cuente subconjuntos. Después presentamos resultados. Aquí tienes un listado aproximado en Basic de Excel:

Randomize
a = 0 Contador de exitos
Input n o cualquier otra forma de capturar n
For i = 1 To 10000
ActiveWorkbook.Sheets(1).Cells(3, 3).Value = i esto sólo sirve para saber por dónde va la simulación
c = 0 cuenta elementos del conjunto aleatorio
s = 0 suma elementos del conjunto aleatorio
b = 1 / 2 es la media, que la declaramos al principio no entera.
For k = 1 To n se genera el conjunto aleatorio
m = Rnd(1)
If m < 1 / 2 Then c = c + 1: s = s + k: b = s / c
Next k
If b = Int(b) Then si es entero se incrementa el contador

a = a + 1
ActiveWorkbook.Sheets(1).Cells(fila, 6).Value = a / i * 2 ^ n Valor adaptado a 2^n
End If
Next i

Los resultados obtenidos han sido bastante acertados. Transcribimos los correspondientes a una sola pasada del algoritmo:

N	S(N)	Simulació	Errores relativos
3	5	5,0576	0,01152
4	8	8,03121	0,00390117
5	15	14,8704	-0,00864
6	26	25,5872	-0,015876923
7	45	44,6464	-0,007857778
8	76	76,3468	0,004563614
9	135	133,971	-0,00762392
10	238	236,032	-0,008268908

Como era de esperar, al aumentar N se presentan desviaciones mayores. Los errores relativos son más estables.

Pues hemos hecho el vago, pero con diversión.

Cuando yo programaba hace años en Pascal se nos vendía su posibilidad de usar la recursión, es decir, que una función se llamara a sí misma, en declaraciones del tipo

Factorial(n)=n*factorial(n-1)

Esta y otras características nos hizo abandonar el Basic como un lenguaje más primitivo y que no admitía funciones recursivas ni por asomo. Pasados bastantes años dejé la confección de programas ejecutables y consiguientemente el Pascal. Ahora que mis trabajos, por voluntad propia, los restrinjo a las hojas de cálculo y a su Basic, no uso la recursión…hasta hoy.

Preparando una próxima entrada se me ocurrió usar funciones recursivas en Excel, OpenOffice y LibreOffice (en Google Docs no funcionan las macros en Basic) con la sorpresa de que sí funcionaban bastante bien.

Toda función recursiva contiene una llamada a sí misma, directa o indirectamente a través de otra función. Como esto nos puede llevar a un proceso sin fin, debe contener también un código de parada, que suele ser una definición en un caso concreto, como veremos en los ejemplos.

La recursividad no se resuelve hasta que no desemboca en ese caso de parada. Mientras tanto hay que guardar los datos pendientes situándolos en una

pila. Por tanto, ahí está el único problema de usar la recursividad en las hojas, y es que se puede agotar la pila si se alargan mucho los cálculos, con el consiguiente mensaje de error. Un fallo de principiante es programar una función recursiva sin facilitar su salida. En ese caso el error será más grave aún: un cálculo sin fin.

Explicamos a continuación algunas funciones recursivas, comenzando con el factorial, que es la más popular y que nos servirá para explicar algunos detalles:

```
Public Function factorial(n)
Dim f
If n = 0 Then f = 1 Else f = factorial(n - 1) * n
factorial = f
End Function
```

Es fácil entender el código: Para evitar confusiones, comenzamos almacenando el factorial en la variable f, para al final recoger su valor en factorial. El cálculo de f es el clásico de la función n!: si n es cero, definimos el factorial como 1 y en caso contrario multiplicamos por n el factorial de n-1.

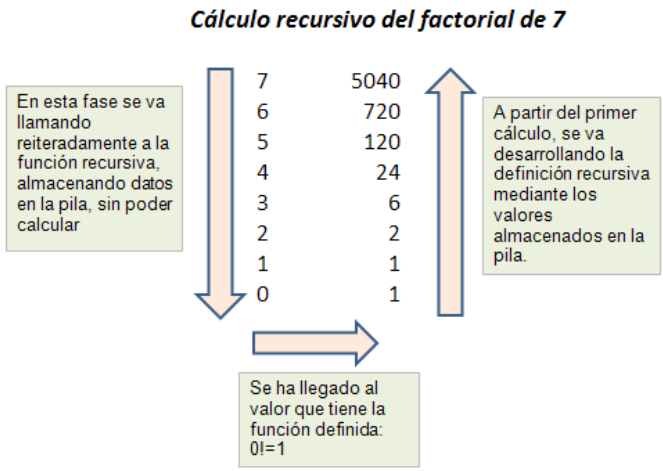
Prueba esta función en cualquiera de las tres hojas propuestas más arriba.

Este primer ejemplo contiene las dos partes imprescindibles en una función de este tipo:

- Alguna asignación de un valor concreto, que servirá para detener la primera fase de lectura de datos y comenzar los cálculos hacia atrás. Aquí es la asignación 0!=1

- La definición recursiva propiamente dicha, que, como es conocido, consiste en exigir que n!=n*(n-1)!

Lo explicamos con un esquema:



Al intentar calcular el factorial de 7, el programa se encuentra con una referencia al factorial de 6, guarda el 7 en la pila y se dedica a calcular el nuevo factorial. Como no puede, almacena el 6 encima del 7 (es una pila) y lo intenta con el 5, y así va de fracaso en fracaso (flecha descendente) hasta llegar al 0.

El valor 0 admite el cálculo, porque está definido como 1. Resuelto esto, es como si el programa se preguntara: ¿por dónde iba? Acude a la pila y ve un 1, con lo que ya puede calcular 1!=1*0!=1 y así sigue (flecha ascendente) buscando datos en la pila y resolviendo los cálculos según la definición recursiva.

Es evidente que para números grandes la pila se puede agotar por falta de memoria asignada.

Con esta función recursiva (la más inútil que me he inventado nunca) puedes tener una idea de la amplitud de la pila de tu hoja de cálculo.

```
Public Function identidad(n)
Dim i
If n = 1 Then i = 1 Else i = identidad(n - 1) + 1
identidad = i
End Function
```

La he elegido para que no influya la magnitud de los números, sino la cantidad de ellos que permanecen en la pila. Con ella he llegado la valor n=3270 como el último que no me da error. En los siguientes no consigo realizar el cálculo.

¿Qué margen tendrá tu hoja de cálculo? Prueba a ver.

Ejemplos varios

Si deseas el enésimo número triangular, sólo tienes que usar este código:

```
Public Function triang(a)
Dim p
If a = 1 Then p = 1 Else p = triang(a - 1) + a
triang = p
End Function
```

También se entiende bien: en los números triangulares vamos añadiendo en cada paso una base del triángulo nueva con a elementos. Prueba esta función y si quieres compara los resultados con la clásica fórmula Tn=n(n+1)/2.

¿Puedes analizar esta función?

```
Public Function cuad(a)
Dim p
If a = 1 Then p = 1 Else p = cuad(a - 1) + 2 * a - 1
cuad = p
End Function
```

¿Por qué produce como resultado el cuadrado de a? Este es un bonito ejemplo de elevar un número al cuadrado sin multiplicar en ningún momento.

Y ya que estamos con números poligonales, podríamos generarlos todos con una función recursiva única que

dependiera de a y también del número de lados del polígono. ¿Te atreves con ella?

¿Y qué opinas de esta, con dos variables?¿Qué ***resultado produce?***

```
Public Function combi(m, n)
Dim c
If n = 0 Then c = 1 Else c = combi(m, n - 1) * (m - n + 1) / n
combi = c
End Function
```

Ahora un ejemplo más serio:

En una entrada anterior

(http://hojaynumeros.blogspot.com/2012/02/suma-de-los-elementos-de-todos-los.html)

descubrimos que la suma de todos los elementos de los subconjuntos de un conjunto de n elementos venía dada por la fórmula de recurrencia

$$Sn=2Sn-1+ n*2n-1$$

y que da lugar a esta sucesión de valores en función de n

0, 1, 6, 24, 80, 240, 672, 1792, 4608, 11520, 28160, 67584, 159744, 372736, 860160, 1966080,… (http://oeis.org/A001788)

Si definimos una función según esta recurrencia podremos reproducir esta lista en nuestra hoja de cálculo. Podría ser esta:

```
Public Function sumaelem(n)
Dim s
If n = 1 Then s = 1 Else s = 2 * sumaelem(n - 1) + n * 2 ^ (n - 1)
sumaelem = s
End Function
```

Con ella hemos construido esta tabla que coincide con la de OEIS

1	2	3	4	5	6	7	8
1	6	24	80	240	672	1792	4608

Un ejemplo elegante

Define esta función de texto

```
Public Function simetrico$(a$)
Dim s$
If a$ = "" Then s$ = "" Else s$ = simetrico(Right$(a$, Len(a$) - 1)) + Mid$(a$, 1, 1)
simetrico = s$
End Function
```

Escribe una palabra en una celda y aplícale esta función desde otra celda ¿Cuál es el resultado?

Como ves, todo esto es bastante divertido, pero no muy útil a causa del agotamiento del espacio de memoria asignado a la pila de datos.

Y ahora tú. ¿Cómo hallarías, mediante una función recursiva, el término general en estas sucesiones?

Progresiones aritméticas y geométricas.

La sucesión de Fibonacci (¡cómo no!)

La enésima potencia de un número dado.

A PROPÓSITO DE ORMISTON

Un algoritmo de comparación de cifras

En la entrada anterior señalábamos, un poco de pasada, que los pares de Ormiston están formados por dos números primos consecutivos que presentan las mismas cifras, aunque en distinto orden. El primer par está formado por 1913 y 1931. Todo esto está estudiado y puedes consultar estas secuencias en OEIS:

Pares de Ormiston: https://oeis.org/A072274

Tripletes: https://oeis.org/A075093

Conjuntos de cuatro primos consecutivos:

https://oeis.org/A161160

Pares que sólo se diferencian en las dos últimas cifras: https://oeis.org/A162765

No vamos a seguir la teoría de estos números, no muy interesante, sino las posibles búsquedas de los mismos con hoja de cálculo. Como de hecho ya están encontrados, nuestro interés se dirigirá **al procedimiento de búsqueda**.

Si se piensa un poco en la misma se pueden distinguir tres fases:

Identificar los números primos

Para cada uno de ellos encontrar el siguiente primo

Comparar las cifras de ambos para ver si son las mismas.

Como los dos primeros presentan menos novedad, los abordaremos al final. Comenzaremos con la detección de igualdad en el conjunto de cifras.

1) Las mismas cifras en distinto orden

Aquí tenemos el problema que deseábamos resolver hoy:

¿Qué algoritmo podemos usar para saber si dos números enteros tienen las mismas cifras, con el mismo número de repeticiones, y posiblemente en distinto orden?

El problema está en las repeticiones, porque saber si un número contiene a las cifras del otro es fácil, pero el que el número de repeticiones coincida, ya es más

difícil de averiguar (para la máquina). Por ejemplo, 51613 y 51631 forman un par de Ormiston y el algoritmo ha de detectar que el 1 aparece dos veces en ambos números. Si no, no serían de Ormiston. ¿Cómo hacerlo?

Se nos ha ocurrido ir tachando una cifra cada vez que comprobemos que también está en el otro par. Leemos la primera cifra del primer número y la buscamos en el otro, y si la encontramos se tacha. Así seguimos hasta que exista una discrepancia o el agotamiento de las cifras. En el caso del ejemplo:

51613 **1**613 **6**13 **1**3 **3**

51631 **1**631 **6**31 3**1** **3**

Expresado en pseudocódigo:

Se leen los números m y n

Se convierten en texto (para que el manejo de las cifras sea más rápido)

* Mientras no se agoten las cifras de m se hace lo siguiente:

Buscamos una coincidencia de la primera cifra de m con cualquiera de n

Si se da la coincidencia, se tacha esa cifra tanto en m como en n

Si no hay coincidencia se para el bucle y se avisa

* Fin del mientras

Se lee si hay coincidencia plena o hubo un fallo

En atención a quienes no tienen interés por el código en Basic lo situamos al final.

2) Identificar un número como primo

Aprovechamos este tema para introducir una mejora en el algoritmo de averiguar si un número es primo o no, sugerida por nuestro amigo Goyo Lekuona. En este blog, por simplicidad, buscábamos los divisores de un número entre los pares y los impares, pero una vez descartado el 2, se puede seguir con los impares. Con ello el tiempo se reduce casi a la mitad. Gracias, Goyo.

El nuevo código puede ser (hay alguna otra variante posible):

```
Public Function esprimo(a) As Boolean
Dim n, r
Dim es As Boolean

'Devuelve true si es primo. No analiza el que sea entero, por lo que en un decimal puede dar respuesta ilógica

If a = 1 Then es = False 'El 1 no es primo
If a = 2 Then es = True 'El 2 sí lo es
If a > 2 Then
If a / 2 = Int(a / 2) Then
es = False  'Si el número es par lo descartamos
Else
```

n = 3: es = True: r = Sqr(a)
While n <= r And es = True
If a / n = Int(a / n) Then es = False ‘probamos con todo los impares hasta la raíz cuadrada
n = n + 2
Wend
End If
End If
esprimo = es
End Function

Una pequeña cuestión: ¿funciona para N=3? ¿Por qué?

3) Buscar el próximo primo

Es muy simple y no necesita explicación:

Function primprox(a) As Long
Dim p, prim As Long
Dim sale As Boolean

'Encuentra el menor número primo mayor o igual al dado

p = a + 1: sale = False: prim = 0
While Not sale
If esprimo(p) Then prim = p: sale = True
p = p + 1
Wend
primprox = prim
End Function

Con estas herramientas hemos reproducido fácilmente los primeros pares de Ormiston, y te invitamos a intentarlo

1913	1931
18379	18397
19013	19031
25013	25031
34613	34631
35617	35671
35879	35897
36979	36997
37379	37397
37813	37831

Para probar las funciones y aunque bastaba con una inspección visual, hemos pedido a la hoja un listado de pares de Ormiston en los que no haya cifras repetidas. Aquí tienes los primeros:

18379	18397
25013	25031
35617	35671
35879	35897
40213	40231
40639	40693
45613	45631
48091	48109
56179	56197
56713	56731
58613	58631

Anexo

Código de la función cifras_identicas

```
Public Function cifras_identicas(m, n) As Boolean
Dim i
Dim vale, esta As Boolean
Dim nn$, mm$, c$
```

nn$ = haztexto(n) ‘Convierte los números en textos
mm$ = haztexto(m)

vale = True
While Len(mm$) > 0 And vale
c$ = Mid$(mm$, 1, 1) ‘toma la primera cifra
esta = False
i = 1
While i <= Len(nn$) And Not esta
If c$ = Mid$(nn$, i, 1) Then
esta = True
mm$ = borracar(mm$, 1) ‘si ha coincidencia, borra la cifra
nn$ = borracar(nn$, i)
End If
i = i + 1
Wend
If Not esta Then vale = False ‘si no hay coincidencia, sale del bucle con el valor “false”
Wend
cifras_identicas = vale
End Function

Reciben el nombre de números regulares o 5-lisos aquellos números naturales que son divisibles entre 2,3 o 5 y ningún otro factor primo. Presentan una factorización prima del tipo $2^n3^m5^p$. También puedes identificarlos como aquellos que son divisores de una potencia de 60 (¿por qué?)

Los tienes presentados en estas páginas

http://en.wikipedia.org/wiki/Regular_number

https://oeis.org/A051037

En esta última puedes consultar cuáles son

1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25, 27, 30, 32, 36, 40, 45, 48,…

Si se les añade el número 1 como primer elemento, forman la llamada sucesión de Hamming.

El mayor interés que presentan estos números es el estudio de la formación ordenada de la sucesión, formándola **a partir de los elementos ya descubiertos**. Esto último es importante, pues si no, bastaría con ir recorriendo los números naturales para quedarnos sólo con los del tipo $2^n3^m5^p$.

Los posibles algoritmos, como el de Dijkstra, se estudian frecuentemente en programación funcional, como puedes ver en esta página de José_A_Alonso.

Nosotros, como siempre en este blog, optaremos por un enfoque elemental, didáctico y ¡cómo no!, usando una hoja de cálculo.

Generación del siguiente número de Hamming

Una vez que tienes escritos los primeros números de la sucesión 1,2,3,4,5,6,8,…(veremos que en realidad sólo hay que escribir 1), para obtener el siguiente bastará multiplicar uno de ellos por 2,3 o 5, pero, ¿cuál? En la sucesión 1,2,3,4,5,6,8,… no me sirve multiplicar por 2 el número 3, porque me daría 6 que ya lo tengo. Sí me convendría multiplicar por 2 el 5, con lo que obtendría el 10, o al revés, multiplicar 5 por 2. Esto no tiene nada de sistemático, por lo que deberemos ordenarlo un poco:

Dada una sucesión de Hamming con varios elementos, para formar el siguiente nos basaremos en estos criterios:

(1) Multiplicamos por 2, 3 o 5 todos los elementos que ya tenemos, y nos quedamos con el resultado menor que aún no esté incorporado a la sucesión. En el caso del ejemplo, el 9.

(2) Para guiarnos en este proceso, escribimos todos los números del tipo 2H, 3H y 5H, (representando H los números de Hamming que ya tenemos) en tres columnas.

H	2H	3H	5H

1	2	3	5
2	4	6	10
3	6	9	15
4	8	12	20
5	10	15	25
6	12	18	30
8	16	24	40

(3) En cada columna señalamos aquel número que cumple que todos los de arriba no superan el número que ya tenemos (8) y él es el primero que sí lo sobrepasaría.

En la siguiente tabla los tienes señalados en este caso.

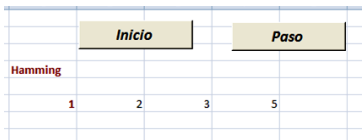
H	2H	3H	5H
1	2	3	5
2	4	6	10
3	6	9	15
4	8	12	20
5	10	15	25
6	12	18	30
8	16	24	40

(4) Por último, de los tres candidatos elegimos el menor, 9, y ese será el siguiente elemento de la sucesión de Hamming.

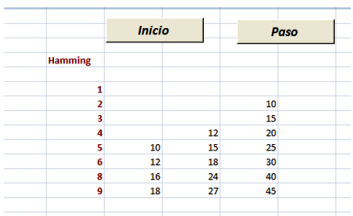
Reiteramos estas operaciones y los obtendremos todos de forma ordenada. Este procedimiento tiene la ventaja de que una vez elegido un número de la columna quedan desechados los anteriores, por lo que es posible mantener unos punteros que nos indiquen por dónde vamos.

El algoritmo con hoja de cálculo

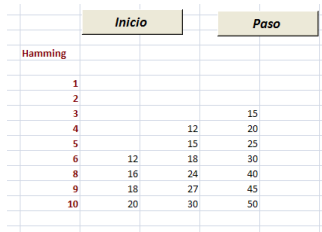
Podemos traducirlo a hoja de cálculo. Lo hemos intentado sin usar macros, pero aparecían referencias circulares muy molestas, por lo que hemos acudido al uso de rutinas y botones. Se inicia el proceso con el botón Inicio, que escribe el primer término 1 y sus tres múltiplos 2,3 y 5.



Después, cada vez que pulsemos sobre el botón Paso se irán eligiendo los múltiplos adecuados desechando los anteriores y los iguales. En la imagen puedes ver el estado del proceso después de obtener el 9:



Se han dejado en blanco los múltiplos usados. La hoja elige después el mínimo (sería 10), elimina sus iguales, lo incorpora a la lista, crea sus múltiplos y borra los innecesarios.



	Inicio		Paso
Hamming			
1			
2			
3			15
4		12	20
5		15	25
6	12	18	30
8	16	24	40
9	18	27	45
10	20	30	50

El cómo lo consigue lo podrás estudiar descargando la hoja en Excel desde

http://hojamat.es/blog/hamming.xlsm

(A OpenOffice lo tenemos en la nevera hasta ver qué pasa con él, y de LibreOffice estamos esperando la nueva versión)

Estudio mediante funciones

Para ver si un número es regular o 5-liso bastaría con esta definición de función:

```
Public Function es_regular(n) As Boolean
Dim nn
nn = n
While nn = 2 * Int(nn / 2): nn = nn / 2: Wend
While nn = 3 * Int(nn / 3): nn = nn / 3: Wend
While nn = 5 * Int(nn / 5): nn = nn / 5: Wend
If nn = 1 Then es_regular = True Else es_regular = False
End Function
```

Observa cómo lo detecta: mientras el número sea par, lo va dividiendo entre 2, con lo que al final deja de serlo. Mientras sea múltiplo de 3 y de 5 también va dividiendo. Si el número es regular se agotarán todos los factores y quedará sólo un 1 y el valor de la función será VERDADERO. Si no es regular es porque o no se puede dividir entre 2,3 o 5, o al final del proceso queda un factor mayor que 1, y la función devuelve FALSO.

Con esta función puedes iniciar la sucesión de Hamming en el punto que desees. Basta ir recorriendo números y eligiendo los que sean regulares. También es muy sencillo usar la función ***proximo_regular***:

```
Public Function proximo_regular(n)
Dim p
p = n + 1
While Not es_regular(p): p = p + 1: Wend
proximo_regular = p
End Function
```

Con esta función puedes descubrir, por ejemplo, que el primer regular de siete cifras es 1012500.

FUNCIONES MULTIPLICATIVAS

DEFINICIONES

Coincidiendo con la publicación en Hojamat.es del documento Funciones especiales y carácter de Dirichlet de Rafael Parra Machío, y como producto de una feliz casualidad, pues no ha habido acuerdo previo con dicho autor, iniciamos hoy una serie de entradas que de forma espaciada y algo periódica tratarán el tema de las funciones multiplicativas a lo largo de este curso.

Este tema está muy bien tratado en muchos manuales y páginas web, entre ellas la referida más arriba. Por eso, en estas entradas no nos limitaremos a repetir el tratamiento teórico, sino que abordaremos los temas mediante esquemas, cálculos, búsquedas o curiosidades. Los lectores no deben buscar en ellas los fundamentos teóricos, porque sólo aparecerán sintetizados. Así constituyen una invitación a la profundización teórica.

Comenzamos con unas definiciones:

Funciones aritméticas

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

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

Por ejemplo, la sucesión siguiente (representada como una correspondencia con los naturales) representa a la función “mayor divisor propio”. En efecto, repasa la tabla y observarás que los números de abajo son los máximos divisores propios de los de arriba.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	1	2	1	3	1	4	3	5	1	6	1	7	5	8	1	9	1	10

Con frecuencia usaremos esta notación u otra similar para representar funciones aritméticas.

Funciones multiplicativas

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

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

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

Hoy lo explicaremos con un ejemplo sencillo: la función Tau, que es la que cuenta los divisores de un número, y que por comodidad tipográfica designaremos por D(n),

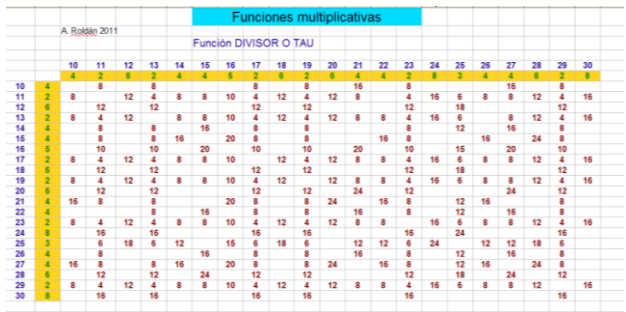
ya que es parte de la familia de las funciones divisor o sigmas

(ver http://hojaynumeros.blogspot.com/2011/02/la-familia-de-las-sigmas-1.html)

Así, D(15)=4, porque admite los divisores 1, 3, 5 y 15. De igual forma, D(28)=6, ya que dividen a 28 los números 1, 2, 4, 7, 14 y 28

Pues bien, como 15 y 28 son coprimos, resulta que D(15*28)=24, como puedes comprobar. Más tarde lo razonaremos en general.

A partir de esta entrada podremos publicar tablas de doble entrada en las que puedas practicar y hacer comprobaciones con las funciones multiplicativas. Aquí tienes la primera, dedicada a la función Tau:



En la tabla sólo aparecen los valores de los productos cuando los dos factores son primos entre sí. Se ha elegido el rango de 20 a 30 porque en el mismo disponemos de gran variedad de números: primos, semiprimos, cuadrados…

Repasa algunos valores, calcúlalos si lo deseas y comprueba el carácter multiplicativo de Tau.

Propiedades de las funciones multiplicativas

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

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

En nuestro ejemplo D(1)=1 porque 1 sólo tiene un divisor.

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

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

Por su carácter multiplicativo se tendrá

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

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

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

Si recuerdas la Teoría de la Divisibilidad, la función Tau tiene un desarrollo muy sencillo, que es el producto de los exponentes en la factorización aumentados en una unidad:

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

Sólo por este desarrollo ya se habría adivinado que es multiplicativa.

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

Consúltalo, pero con un poquito de Álgebra comprenderás esta propiedad.

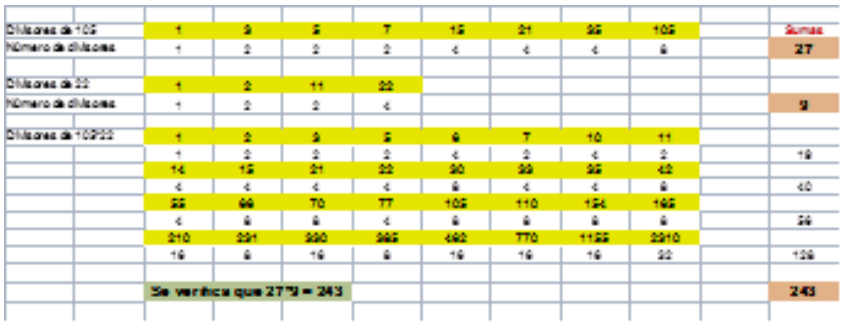
(4) En esta propiedad hay que detenerse un poco, aunque no la demostraremos (busca, busca…): Si g(x) es una función multiplicativa, entonces, la función f(n) definida por

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

En la que el sumatorio recorre todos los divisores de n, también es multiplicativa. Omitiendo detalles, la base de esta propiedad está en que los divisores de un producto de dos números coprimos M y N son productos de dos divisores, uno de M y otro de N, y al final la suma de productos coincidirá con el producto de sumas. ¿Es

difícil de entender? Pues busca el desarrollo en cualquier manual o página que lo explique.

Nosotros lo comprobaremos en el caso de la tau para dos números concretos. Esto no demuestra nada, pero te ayudará a crearte una idea del proceso.



Divisores de 105	1	3	5	7	15	21	35	105		Sumas
Número de divisores	1	2	2	2	4	4	4	8		27
Divisores de 22	1	2	11	22						
Número de divisores	1	2	2	4						9
Divisores de 105*22	1	2	3	5	6	7	10	11		
	1	2	2	2	4	2	4	2		19
	14	15	21	22	30	33	35	42		
	4	4	4	4	8	4	4	8		40
	55	66	70	77	105	110	154	165		
	4	8	8	4	8	8	8	8		56
	210	231	330	385	462	770	1155	2310		
	16	8	16	8	16	16	16	32		128
	Se verifica que 27*9 = 243									243

Ves que arriba hemos escrito los divisores de 105 y debajo de cada uno su número de divisores. Nos dan una suma de 27. Hemos efectuado la misma operación con 22 y nos suman 9. El producto de ambos (nótese que son coprimos) es 2310, que tiene 32 divisores (era de esperar ¿no?) y sus divisores suman 243, que es precisamente el producto de 27 por 9, luego en este caso el proceso ha sido multiplicativo. Pero no generalices. Hay que demostrar las cosas.

Lo dejamos por hoy. Otros días veremos algunos ejemplos de funciones multiplicativas interesantes.

Aunque el conjunto de los divisores de un número aparece en muchas cuestiones y ya hemos hecho bastantes referencias a él, conviene, para entender algunas cuestiones sobre funciones multiplicativas, que le demos un repaso.

Consideremos, por ejemplo, el conjunto de todos los divisores de $240=2^4*3*5$:

1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 20, 24, 30, 40, 48, 60, 80, 120, 240

Lo primero que hay que considerar es que es un conjunto finito. Eso parece una trivialidad, pero nos evita preocuparnos por sumas o productos infinitos.

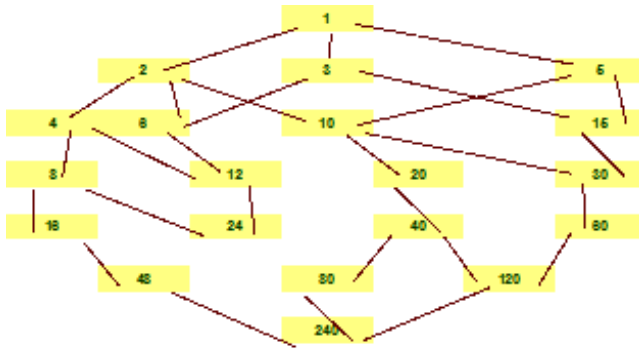
Orden

Los divisores presentan **un orden total** respecto a su valor absoluto, y además, cada divisor **d** está asociado a **N/d** mediante una correspondencia biunívoca que invierte ese orden. Si multiplicamos en la tabla siguiente dos divisores en columna siempre nos resulta 240:

240	120	80	60	48	40	30	24	20	16	15	12	10	8	6	5	4	3	2	1
1	2	3	4	5	6	8	10	12	15	16	20	24	30	40	48	60	80	120	240

Por tanto, d y N/d recorren el mismo conjunto con órdenes opuestos.

Como todo tipo de divisores, los de N presentan también **un orden parcial** respecto a la relación divisor-múltiplo. En el siguiente esquema representamos el retículo correspondiente a los divisores de 240:



No se han representado todas las relaciones, para no complicar el esquema, pero cada dos divisores tiene un elemento minimal que es su MCD y otro maximal, su MCM. Obsérvese que al recorrer el esquema de arriba abajo va aumentando el número de divisores primos de las descomposiciones factoriales.

Número

Desde las enseñanzas secundarias sabemos que si un número N se descompone como

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

El número de divisores, o función Tau, viene dado por

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

Y el conjunto de divisores coincide con los términos del producto

$$(1 + p_1 + {p_1}^2 + \cdots {p_1}^{a_1})(1 + p_2 + {p_2}^2 + \cdots {p_2}^{a_2}) \ldots (1 + p_k + {p_k}^2 + \cdots {p_k}^{a_k}) \quad \textbf{(1)}$$

Esto ya es algo sabido. Sólo hay que destacar que el número de divisores depende de la **signatura prima**, que es el conjunto de exponentes, y no de los factores primos.

La fórmula anterior se traduce en un producto cartesiano formado eligiendo una potencia de un factor primo cada vez. Este producto cartesiano que forman los términos de la expresión (1) es fundamental para entender más tarde cómo se comportan las funciones multiplicativas sobre el conjunto de divisores.

El conjunto de divisores de un número es uno de los mejores ejemplos que existen de concurrencia entre cuestiones combinatorias y de divisibilidad.

Divisores libres de cuadrados

Si sólo consideramos los factores libres de cuadrados obtendremos un esquema similar al del Binomio de Newton. Esto nos será muy útil para algunas funciones multiplicativas.

Los divisores libres de cuadrados poseen factores primos distintos. De esta forma, para engendrar uno de estos divisores bastará elegir algunos de los factores primos, **pero una sola vez cada uno**. Así

desembocamos en un problema de combinaciones. Lo vemos para el caso del 240, para el que el número de factores primos distintos es 3:

Divisores sin ningún factor primo: El 1. Hay en total $C_{3,0}$

Divisores con un factor: 2, 3, 5. En total $C_{3,1}$

Con dos factores distintos: 6, 10 y 15: $C_{3,2}$

Con tres factores: 30, es decir $C_{3,3}$

Así que en total hay 8. Si recuerdas el desarrollo del binomio, esto ocurre porque $C_{3,0}+ C_{3,1}+ C_{3,2}+ C_{3,3} = 2^3 = 8$

Generalizando:

El número de divisores libres de cuadrados en un número que posee k factores primos distintos es 2^k

Esta clasificación la usaremos en una próxima entrada. Hemos recorrido los ocho números libres de cuadrados 1, 2, 3, 5, 6, 10, 15 y 30.

Por tanto, el número de divisores no libres de cuadrados será:

$$\boldsymbol{D(N) = (1 + a_1) * (1 + a_2) \dots (1 + a_k) - 2^k}$$

En el caso de 240 sería: 5*2*2-8=12, que son estos: 4, 8, 12, 16, 20, 24, 40, 48, 60, 80, 120, 240

Divisores del producto

Si tomamos dos números A y B primos entre sí y los multiplicamos, sus conjuntos de divisores quedarán multiplicados término a término, todos los de A con cada uno de B.

Por ejemplo, si 240, con 20 divisores, lo multiplicamos por 119=7*17, que posee 4 divisores, 1, 7, 17 y 119, resultará 28540, con estos 80 divisores:

1	2	4	8	16
3	6	12	24	48
5	10	20	40	80
15	30	60	120	240
7	14	28	56	112
21	42	84	168	336
35	70	140	280	560
105	210	420	840	1680
17	34	68	136	272
51	102	204	408	816
85	170	340	680	1360
255	510	1020	2040	4080
119	238	476	952	1904
357	714	1428	2856	5712
595	1190	2380	4760	9520
1785	3570	7140	14280	28560

No sólo eso, sino que cada divisor de 28540 será el producto de uno de 240 por otro de 119, como puedes ver en esta otra forma de presentar los divisores:

	1	7	17	119
1	1	7	17	119
2	2	14	34	238
3	3	21	51	357
4	4	28	68	476
5	5	35	85	595
6	6	42	102	714
8	8	56	136	952
10	10	70	170	1190
12	12	84	204	1428
15	15	105	255	1785
16	16	112	272	1904
20	20	140	340	2380
24	24	168	408	2856
30	30	210	510	3570
40	40	280	680	4760
48	48	336	816	5712
60	60	420	1020	7140
80	80	560	1360	9520
120	120	840	2040	14280
240	240	1680	4080	28560

Esto es así porque al ser primos entre sí A y B aportan factores primos distintos sin que se mezclen los de uno con los del otro.

Por tanto, los divisores de un producto AB en el que A y B son coprimos, están formados por todos los productos posibles dd' en los que d divide a A y d' a B

Y con esto llegamos a donde queríamos. Es fácil ya ver lo siguiente:

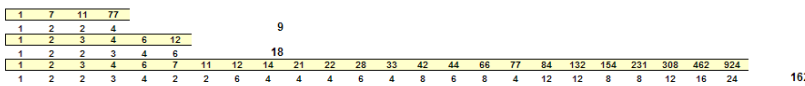
Si f es multiplicativa y se define F como

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

Entonces F es también multiplicativa

Ya que las multiplicativas actúan por separado sobre los factores primos y hemos visto que estos se combinan totalmente en el producto.

Este teorema hace que las funciones sigma y tau sean multiplicativas, pero ya volveremos sobre ello. Por ahora lo comprobaremos para la tau mediante un ejemplo:



La suma de la función Tau para el número 77 recorriendo todos sus divisores es 9, la correspondiente a 12, coprimo con 77, es 18. Si los multiplicamos resulta 77*12=924, cuya suma de Tau es 162, producto de 9 con 18.

Primeras definiciones

Para el estudio que vamos a emprender necesitamos repasar algunas definiciones:

Parte cuadrada PC(N): Es el mayor divisor cuadrado de N (Ver http://oeis.org/A008833)

Parte libre PL(N): Equivale al cociente entre N y su parte cuadrada (http://oeis.org/A007913)

Radical RAD(N): Es el mayor divisor de N que está libre de cuadrados (http://oeis.org/A007947)

Y añadimos otra

Menor múltiplo cuadrado MMC(N): Como indica su nombre, es el menor cuadrado divisible entre N (http://oeis.org/A053143)

Así que el número N está *emparedado* entre dos cuadrados. Uno es el mayor divisor cuadrado PC(N) y el otro es el menor múltiplo de esa clase MMC(N).

Lo aclaramos con un ejemplo

Si consideramos el número 126, sus factores primos son 2*3*3*7, luego

PC(126)=9 porque es el único cuadrado que podemos formar con 2,3,3,7. El exponente de 3 es par, como cabía esperar.

PL(126)=126/9=14, que equivale al producto de 2*7, ambos elevados a 1

RAD(126)=2*3*7=42 Está formado por todos los factores primos elevados a 1.

MMC(126)=2^2*3^2*7^2=1764. Se consigue este número completando los exponentes de sus factores primos a un número par.

Así que, como veremos, cualquier número está comprendido entre dos cuadrados de este tipo. A continuación estudiaremos su cálculo y carácter multiplicativo, dejando para la siguiente entrada sus relaciones.

Parte cuadrada PC

Es evidente que para calcularlo bastará sustituir cada exponente de los factores primos **por el mayor número par contenido en cada uno de ellos**. Por ejemplo, si N=2^3*7^2*11=4312, su parte cuadrada se obtendrá **truncando cada exponente** al máximo número par que contiene, es decir: PC(N)= 2^2*7^2*11^0=196

Vimos que las funciones multiplicativas quedaban caracterizadas por su acción sobre los factores primarios de N. De esta forma, la definición de parte cuadrada podía quedar como

$$PC(p^r) = p^{r-r\,MOD\,2}$$

Es decir, que a cada exponente se le resta su resto al dividirlo entre 2. Por este tipo de actuación sobre factores primarios de forma independiente, multiplicando después los resultados, ya sabemos que la parte cuadrada **es multiplicativa**.

Intenta reproducir esta comprobación:

	1617		49	
	2000		400	
MCD(1617;2000)	1		Producto	19600
Producto	3234000		19600	

En ella vemos que 1617 y 2000 son coprimos y que el producto de sus partes cuadradas 49 y 400 coincide con la parte cuadrada del producto 3234000=1617*2000. Tendrás que trabajar un poquito, pero aprenderás mucho.

Parte libre

Para no alargar el tema, tan sólo destacaremos que su definición para factores primarios puede ser:

$$PL(p^r) = p^{r \ MOD \ 2}$$

Esto quiere decir que los factores pares desaparecerán en la parte libre y que los impares se convertirán en 1. Al actuar sobre los factores primarios de forma independiente, esta función es también multiplicativa.

Te proponemos una comprobación de su carácter multiplicativo:

	1617		33	
	1625		65	
MCD(1617;2000)	1		Producto	2145
Producto	2627625		2145	

Repasa los cálculos y recuerda que ahora se trata de la parte libre.

Mínimo múltiplo cuadrado

Con todo lo que ya llevamos, su definición te vendrá a la mente al momento. Es esta:

$$MMC(p^r) = p^{r+r\ MOD\ 2}$$

Era de esperar. El número N está "emparedado" entre dos cuadrados: el que resulta de restar un 1 o un 0 a los exponentes y el que se calcula sumando ese 1 a los impares y un 0 a los pares. Por ejemplo:

PC(2400)= $=2^4*5^2=400$; 2400= $=2^5*5^2*3$;
MMC(2400)=14400= $=2^6*5^2*3^2$

Esta función es multiplicativa por la misma razón que las anteriores.

Relaciones entre los cuadrados

Según lo definido en la entrada anterior, para conseguir el mínimo múltiplo cuadrado de N sólo tendremos que multiplicar N por su parte libre. En efecto, esa parte libre contiene los factores primos de N elevados al residuo

de cada exponente módulo 2. Más claramente: contiene los números primos elevados a 1 si su exponente era impar. Pero si los multiplicamos por N todos esos exponentes se harán pares, con lo que hemos conseguido el MMC(N). Lo repasamos con un ejemplo:

Sea $11400=5^2*2^3*3*19$. Su parte cuadrada contendrá los factores con exponente truncado a par: $PC(1140)= 5^2*2^2 = 100$. Su parte libre estará formada por el resto de factores, es decir, $PL(1140)=2*3*19=114$. Es evidente pues que:

$PC(N)*PL(N)=N$ (1)

Pero si ahora volvemos a multiplicar por PL(N), todos los exponentes se harán pares y el producto se habrá convertido en MMC(N):

$1140*PL(1140)= 5^2*2^3*3*19*2*3*19=5^2*2^4*3^2*19^2=1299600=MMC(11400)$

Hemos razonado que

$N*PL(N)=MMC(N)$ (2)

Uniendo (1) con (2) llegamos a una conclusión muy elegante: N es la media geométrica entre el mayor cuadrado que lo divide y su menor múltiplo cuadrado.

Es así porque $N^2=PC(N)*MMC(N)$, según (1) y (2)

En nuestro ejemplo $11400^2=100*1299600$.

Como los factores del segundo miembro son cuadrados, podemos considerar sus raíces cuadradas. Así definiremos:

(a) **Raíz interna de N** es la raíz cuadrada de su parte cuadrada. En el ejemplo sería 10. La representaremos como RI(N). En este caso RI(11400)=10

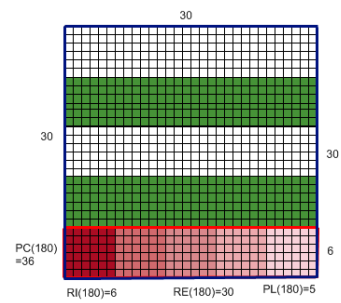
(b) **Raíz externa de N** es la raíz cuadrada de su menor múltiplo cuadrado. En el caso de 11400 podríamos escribir RE(11400)=1140, que es la raíz cuadrada de MMC(11400)

Un resumen también muy elegante:

Todo número natural equivale al producto de sus dos raíces enteras, interna y externa

En efecto: 11400=10*1140

Podemos representar todo lo anterior gráficamente. Observa esta imagen:



Representa los cuadrados correspondientes al número $180=2^2*3^2*5$.

El cuadrado rojo de la esquina es su parte cuadrada $PC(180)= 2^2*3^2=36$, que son los cuadritos que contiene. Su raíz cuadrada es RI(180)=6, que se representa por el lado del cuadrado.

La parte libre de 180 es 5. Si copiamos el cuadrado rojo cinco veces a la derecha nos resultará un rectángulo (el separado por la línea gruesa roja) de 180 cuadros, o sea, el número considerado. Esto es así porque N=PC(N)*PL(N).

Si ese rectángulo que contiene 180 cuadros lo trasladamos cinco veces hacia arriba nos resultan 900 cuadros, que es precisamente el menor múltiplo cuadrado. Esto funciona porque N*PL(N) =MMC(N). El lado de ese cuadrado, 30, será la raíz cuadrada externa de 180.

¿Qué hemos visualizado?: que todo número se puede representar por un rectángulo de base su raíz externa y de altura la interna.

Si el interior de ese rectángulo lo descomponemos en tantos trozos iguales como indique la parte libre obtendremos la parte cuadrada.

Si ese rectángulo lo adosamos consigo mismo por su base tantas veces como indique la parte libre, formaremos un cuadrado que será su menor múltiplo de ese tipo.

¡Se completó el emparedado!

Y lo mejor, como todas las funciones que hemos usado son multiplicativas, dados dos números coprimos, sus esquemas de este tipo se pueden fundir en uno solo

multiplicando uno a uno los datos que han intervenido: PC, PL, RI,…

Todo esto no pasa de ser un divertimento, pero te ayuda a aprender conceptos.

Sumas de funciones

En esta entrada comprobaremos la potencia del concepto de función multiplicativa. Usaremos fundamentalmente dos propiedades:

(1) Según vimos en otro apartado, si g(x) es una función multiplicativa, entonces, la función f(n) definida por

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

En la que el sumatorio **recorre todos los divisores de n**, también es multiplicativa.

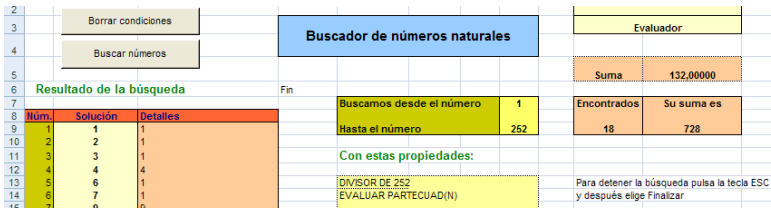
(2) Debemos recordar también que la definición de una función multiplicativa basta hacerla para los factores primarios $\mathbf{p^e}$ de un número, siendo **p** un factor primo y **e** su exponente.

Estudiaremos esas sumas que recorren todos los divisores en las funciones estudiadas en la sección anterior

Suma de las partes cuadradas SPC(N)

Es una función multiplicativa

Si la parte cuadrada de un número es multiplicativa, **su suma a lo largo de los divisores de un número también lo será**. Una forma rápida de encontrar esa suma se consigue con el Buscador de Naturales, usando estas condiciones y consultando después la suma en el evaluador. Observa cómo lo hemos conseguido para el número 252= 2*2*3*3*7



Se ha definido una búsqueda entre 1 y 252, con las condiciones DIVISOR DE 252 y EVALUAR PARTECUAD(N) y nos da un resultado de 132.

Así que la suma de esas partes cuadradas (SPC(N)) para 252 es 132.

Esta función está publicada en http://oeis.org/A068976 y ahí se dan fórmulas y desarrollos para el cálculo de la misma. Es claro que es multiplicativa y por eso la fórmula de Vladeta Jovovic que se propone en esa página sólo define la función para un factor primario p^e.

La escribimos de forma algebraica aplicada a p^e:

Si **e** es par:

$$SPC(p^e) = \frac{p^{e+2}-1}{p^2-1} + \frac{p^e-1}{p^2-1}$$

Si **e** es impar:

$$SPC(p^e) = 2\frac{p^{e+1}-1}{p^2-1}$$

¿Cómo demostrarlo? Te damos una idea.

Considera todos los divisores del número p^e:

1 p p^2 p^3 p^4 p^5 p^6 … p^{e-1} p^e

Si les aplicamos la función "parte cuadrada" PC deberemos truncar los exponentes al máximo número par que contienen.

Si **e** es par quedaría:

1 1 p^2 p^2 p^4 p^4 p^6 … p^{e-2} p^e que se puede descomponer en dos sumas:

$SPC(p^e)=(1 + p^2 + p^4 + p^6 \dots p^e)+(1 + p^2 + p^4 + p^6 \dots p^{e-2})$ que al final desembocan en la suma propuesta

Si es impar las dos sumas serían iguales, luego

$SPC(p^e)=2(1 + p^2 + p^4 + p^6 \dots p^{e-1})$ que también nos lleva a la fórmula propuesta arriba.

Aplicamos estas fórmulas a $252= 2^2*3^2*7$, en el que aplicaría el caso par para el 2 y el 3 y el impar para el 7:

SPC(252)=(15/3+3/3)(80/8+8/8)(2*48/48)=6*11*2=132, como era de esperar.

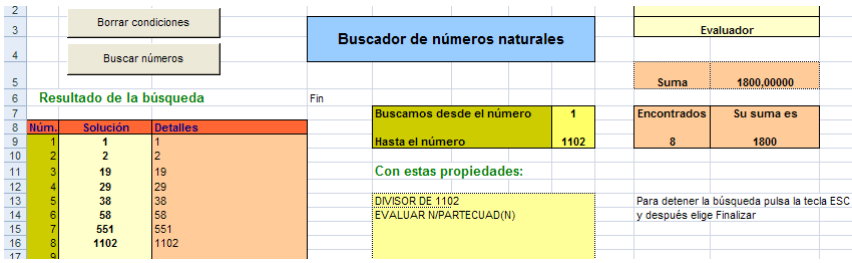
Si practicas estos cálculos con otros números, tanto manualmente como con el Buscador o las fórmulas aprenderás mucho.

Suma de partes libres SPL(N)

Es también multiplicativa

Con los mismos procedimientos y propiedades podemos intentar sumar las partes libres de los divisores de un número.

Con el Buscador podemos encontrar esa suma para 1102, por ejemplo:



Las condiciones usadas son DIVISOR DE 1102 y EVALUAR N/PARTECUAD(N), ya que esa es una definición de parte libre. Recorremos los números del 1 al 1102 y el evaluador nos da una solución de 180.

En la página http://oeis.org/A069088 puedes ver la lista de los primeros valores de esta función (1, 3, 4, 4, 6, 12, 8, 6, 5, 18, 12, 16, 14, 24…) y la definición ligeramente distinta a la nuestra. Lo que no ofrece es una fórmula

para la evaluación directa. La ofrecemos nosotros para p^e, como en los casos anteriores:

Si **e** es par:

$$SPL(p^e) = (p+1)\frac{e}{2} + 1$$

Si **e** es impar

$$SPL(p^e) = (p+1)\frac{e+1}{2}$$

La demostración también se basa en el conjunto

1 p p^2 p^3 p^4 p^5 p^6 … p^{e-1} p^e

Al aplicarle la función “parte libre” PL las potencias pares se convertirán en 1 y las impares en p, por lo que la suma de las partes libres será

1+p+1+p+1+p+1+p+…. Que terminará en 1 o en p según el exponente sea par o impar. El resto de la demostración es trivial, sacando factor común el factor (1+p) hasta donde se pueda.

Aplicamos la fórmula a

$2200=2^3*5^2*11$:

SPL(2200)=(2+1)*4/2*((5+1)*2/2+1)(11+1)*2/2=3*2*7*12=504

Lo hemos comprobado con el Buscador y coincide.

Suma de los mínimos múltiplos cuadrados SMMC(N)

Otra multiplicativa

Si ahora, en lugar de N/PARTECUAD(N) usamos N*N/PARTECUAD(N) en el Buscador (¿por qué? Revisa la propiedades vistas anteriormente) obtendremos la suma de MMC(N)

Esta función multiplicativa la hemos publicado en OEIS, pues en la fecha de su creación permanecía inédita. Sus primeros valores son

1, 5, 10, 9, 26, 50, 50, 25, 19, 130, 122, 90, 170, 250, 260…

(https://oeis.org/A198286)

Podemos usar una fórmula similar a las anteriores. No es difícil que la puedas justificar si entendiste las primeras.

Si **e** es par

$$SMMC(N) = 1 + 2\frac{P^{e+2} - p^2}{p^2 - 1}$$

Si **e** es impar

$$SMMC(N) = (1 + p^2)\frac{P^{e+1} - 1}{p^2 - 1}$$

Lo vemos con un número compuesto, el $12=2^2*3$

En primer lugar aplicamos la definición de SMMC y para cada primo sumamos el mínimo múltiplo cuadrado de cada una de sus potencias:

SMMC(12)=(1+4+4)(1+9)=9*10=90, como puedes ver en la lista general.

Ahora aplicamos la fórmula:

SMMC(2^2) (caso par) = 1+2((16-4)/(4-1))=1+2*4=9, que era lo esperado

SMMC(3) (caso impar) = (1+9)((9-1)/(9-1))=10*1=10, que con el 9 anterior da 90.

Cuestiones

Proponemos unas cuestiones:

(a) La suma de las partes cuadradas de los divisores de un número coincide con esta suma:

$$SPC(N) = \sum_{(d|N)} \left(MCD(d, \frac{N}{d}) \right)^2$$

¿Sabrías demostrarlo? Se consigue como en las anteriores, comenzando a considerar el conjunto 1 p p^2 p^3 p^4 p^5 p^6 … p^{e-1} p^e

(b) Si A divide a B, ¿crees que la parte cuadrada de A dividirá a la de B?

(c) ¿Ocurrirá lo mismo con los menores múltiplos cuadrados?

(d) Si A divide a B y son distintos, ¿cuándo se dará que PC(A)=PC(B)?

(e) ¿Podemos relacionar de igual forma la parte libre de A con la de B?

(f) Considera el máximo común divisor de la parte cuadrada y la libre de un número natural N ¿qué podremos afirmar de él? ¿Se comportará como una función multiplicativa?

CUADRADOS DIVISORES DE N

Como otro ejemplo de función multiplicativa, veremos hoy una muy simple: a cada número natural le hacemos corresponder la suma de todos los divisores cuadrados (SDC) que posea. Por ejemplo. SDC(28)=1+4=5, SDC(1000)=1+4+25+100 = 130. También es multiplicativa la cuenta de esos divisores (NDC)

Es evidente que para algunos, como 15 o 33, el resultado es 1.

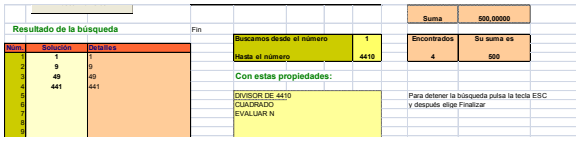
No se debe confundir con la suma **de las partes cuadradas** vista en la entrada

http://hojaynumeros.blogspot.com/2011/12/emparedado-de-cuadrados-3.html

Esta de hoy presenta valores menores, pues solo entran los divisores con parte libre igual a 1 es decir, cuadrados perfectos. En la anterior algunos cuadrados se repetían, por ejemplo en 4*3 y 4*7 como divisores de 4*3*7.

Además del muy conveniente método de calcular manualmente, con hoja de cálculo puedes evaluar fácilmente esta función

Con el Buscador de Naturales



El Buscador te resuelve el problema con las condiciones DIVISOR DE…, CUADRADO y EVALUAR N y después se cuentan y se suman los divisores en el evaluador. En la parte superior de la imagen leemos que 4410 tiene 4 divisores cuadrados que suman 500. Luego NDC(4410)=4 y SDC(4410)=500

Como función en Basic

Se supone que ya poseemos las funciones ESMULTIPLO y ESCUAD, que ya se han usado varias veces en este blog.

```
Public Function sumadivcuad(n)
Dim i, s
s = 0
For i = 1 To n
If esmultiplo(n, i) And escuad(i) = 1 Then s = s + i
Next i
sumadivcuad = s
End Function
```

Con esta función se puede descubrir qué valores presenta la suma de divisores cuadrados para los primeros números naturales:

1, 1, 1, 5, 1, 1, 1, 5, 10, 1, 1, 5, 1, 1, 1, 21, 1, 10, 1, 5, 1, 1, 1, 5, 26, 1, 10…,

La tienes publicada en http://oeis.org/A035316

Si sustituyes la orden ***s=s+i*** por la de ***s=s+***1, en lugar de sumar contará los divisores cuadrados con lo que generará la unción NDC. Los resultados son:

1, 1, 1, 2, 1, 1, 1, 2, 2, 1, 1, 2, 1, 1, 1, 3, 1, 2, 1, 2, 1, 1, 1, 2, 2, 1, 2, 2

http://oeis.org/A046951

En ambas páginas, la A035316 y la A046951 puedes aprender detalles teóricos muy interesantes. Aquí nos detendremos sólo en algunos aspectos.

Son multiplicativas

Basta considerar que ambas provienen de productos de este tipo

$$(\mathbf{1}+\boldsymbol{p^2}+\boldsymbol{p^4}+\boldsymbol{p^6}+\cdots)(\mathbf{1}+\boldsymbol{q^2}+\boldsymbol{q^4}+\boldsymbol{q^6}+\cdots)(\mathbf{1}+\boldsymbol{r^2}+\boldsymbol{r^4}+\boldsymbol{r}+\cdots)$$

siendo p,q y r divisores primos del número.

En un producto de dos números coprimos lo que ocurrirá es que se unirán paréntesis de este tipo pero con primos distintos, con lo que tanto la cuenta de divisores como la suma se convertirán en producto de esas mismas funciones en los factores.

En algún momento de este año relacionaremos estas y otras multiplicativas similares con la función de Moebius, pero hay que ir paso a paso. Si te quieres adelantar, investiga.

Como en todas las multiplicativas, basta dar la operación que efectúan sobre los factores primarios $\mathbf{p^e}$ con **p** factor primo del número y **e** su exponente. Se ve a la primera reflexión.

Los divisores de $\mathbf{p^e}$ forman el conocido conjunto 1 p p^2 p^3 p^4 p^5 p^6 … p^{e-1} p^e

De ellos sólo nos servirán los pares: 1 p^2 p^4 p^6 … p^c, siendo c el máximo par contenido en e, es decir **e – e MOD 2**. Así que el **número de divisores cuadrados NDC(p^e)** será:

$$NDC(p^e) = 1 + \left[\frac{e}{2}\right]$$

El corchete representa la parte entera. En el caso del ejemplo del primer párrafo, el número $4410=2*3^2*5*7^2$ tendrá tantos divisores cuadrados como indica el cálculo

NDC(N)=(1+0)(1+1)(1+0)(1+1)= 4

En efecto, en la imagen del Buscador correspondiente hemos visto sólo cuatro divisores: 1, 9, 49 y 441.

Es interesante destacar que, como ocurre en casos similares, el valor de esta fución no depende de los

divisores primos, sino tan sólo de sus exponentes (su *signatura prima*)

La suma tampoco requiere mucho estudio. Sabemos sumar potencias mediante un cociente de diferencias. Así, si usamos **c**, **el máximo número par contenido en e, es decir e – e MOD 2**, nos resultará la fórmula para SDC(p^e)

$$SDC(p^e) = \frac{p^{c+2} - 1}{p^2 - 1}$$

La aplicamos $4410=2*3^2*5*7^2$

SDC(4410)=((2^2-1)/(2^2-1))*((3^4-1)/(3^2-1))*(5^2-1)/(5^2-1))*(7^4-1)/(7^2-1))=

1*10*1*50=500, que fue el resultado obtenido con el Buscador.

Ya conoces otras dos funciones multiplicativas, pero esto no ha acabado. Nos quedan al menos dos muy interesantes ¿Cuáles?

BALDOSAS, PASOS Y FAROLAS

Como casi todos los profesores de Matemáticas de mi generación he intentado en clase la estimación de distancias, alturas o tiempos, a veces terminada con un aleccionador fracaso. Lo sabréis si habéis intentado medir alturas con medidores de ángulos o sombras. Creo que es una actividad muy educativa, especialmente si no se usan instrumentos de precisión, sino medidas de nuestro propio cuerpo (pasos, pies, manos,..), elementos repetidos (baldosas, vagones de un tren, farolas,…) o representaciones a escala, como los mapas de Google.

Para garantizarnos un resultado honorable y una buena práctica de medición creo que tenemos que contar con al menos estos elementos:

- Repetición de elementos razonablemente iguales (como medir por pies) y, a ser posible, pertenecientes a conjuntos distintos. Así se realizan varias mediciones.
- Un elemento al menos cuya medida real sea fiable: longitud de una baldosa, distancia entre dos bancos de un paseo, altura de un piso…

- Uso de fracciones comparativas entre medidas. Lo que desde la antigüedad hemos llamado “razón entre dos magnitudes”.
- Uso, si es posible, de la media aritmética entre estimaciones.

Ilustro estas ideas con un ejemplo que me sirvió de ejercicio y entretenimiento en mis últimas vacaciones.

Pasé unos días junto a las Salinas de San Pedro del Pinatar (Murcia, España). Un paseo muy popular es el que une dos molinos salineros abandonados, que tiene una longitud aproximada de tres kilómetros. Comienza siendo un paseo urbano (tramo A), frecuentado por quienes se aplican la terapia de los barros de las salinas, y termina como una senda ecológica (tramo B) que va a desembocar al mar abierto.

Como lo recorría con frecuencia, me planteé efectuar una estimación de la distancia total entre los dos molinos usando sólo los elementos propios de un paseo y los de la misma ruta. Para ello contaba con lo siguiente:

Pasos

La parte urbanizada del camino, quizás para estimular a las personas de cierta edad que lo usan, contiene en el pavimento la referencia a la distancia recorrida de 50 en 50 metros. Al final de esta primera parte A figura la distancia de 1182 m. Esa era la parte “fiable” de mi estimación.

Medí los pasos que tenía que dar para recorrer 50 m. Repetí varias veces esa medida contando mentalmente y me resultó una media aproximada de 60 pasos por cada 50 metros. Ya tenía un primer elemento repetitivo razonablemente conocido. Conté los pasos del segundo tramo, con la idea de multiplicarlos por la razón 50/60=5/6. No es fácil contar tantos pasos (intentadlo y veréis) y al final sólo sabía que serían unos 1850, pero con poca seguridad. Esto me daba una primera estimación: 1850*5/6= 1542 metros.

Postes

Al segundo día me di cuenta de que existían unos pequeños postes, de unos 40 cm. de altura, aparentemente equidistantes. Los medí por pasos varias veces y así confirmé que lo eran. Los conté y la parte A contenía 76 y la parte B, cuya distancia deseaba estimar, 102. Ya tenía mi segunda razón fiable: 102/76 = 51/38

Mi siguiente estimación sería 1182*51/38 = 1586 metros. Me quedaba la sospecha de que en el tramo B la distancia entre postes fuera algo menor, porque el número de pasos se acercaba en él a 19 y en el A a 20, pero no estaba seguro.

Minutos

Como sospechaba que los postes podían presentar diferencias en sus distancias mutuas, cronometré varias veces mi paseo por los dos tramos, obteniendo 17 minutos para el tramo B y 13 para la distancia conocida 1182 m., o algo más conservando la proporción. Fue una buena noticia para mí, pues confirmó mi buen estado de forma en esos días. Así que mi segunda razón podía ser 17/13 y la estimación 1182*17/13 = 1545.

Google

Sólo me quedaba acudir a un mapa en Internet. Me costó trabajo, pues no se veía bien la transición entre los dos tramos. Imprimí el mapa, pero la diferencia con las otras estimaciones era demasiado grande. Recordé entonces que el paseo urbanizado terminaba en una especie de semicírculo. Amplié la visión lo más posible hasta que apareció, cuidando después de identificar los accidentes del terreno cuando alejé el zoom para imprimir. Medí con una regla de dibujo en el mapa impreso y me resultó la razón 103/82 estimando con ella una distancia de 1182*103/82=1484

Resumiendo, la distancia total podría ser:

Pasos: 1182+1542 = 2724 m.

Postes: 1182+1586 = 2768 m.

Minutos: 1182+1545=2727 m.

Google: 1182+1484=2666 m.

Antes de encontrar la media quise criticar cada método:

* Contar pasos es cansado y desalentador, sujeto por tanto a olvidos y saltos en la cuenta.

* Los postes parecían estar más cercanos en el segundo tramo.

* Conté minutos, y no segundos, lo que disminuye la precisión.

* En el mapa no se veía bien la transición y tampoco el final de los postes respecto al segundo molino. Me pareció la menos fiable.

Así que mi estimación media fue de 2721 m. Unos días después de este juego, vi un cartel no muy visible al principio del paseo y en él se afirmaba que la distancia entre los dos molinos era de 2,7 km. ¡Pues no estuvo mal!

Ideas para el aula

Se pueden efectuar mediciones semejantes combinando varios conjuntos repetitivos:

- Ancho de un andén de ferrocarril contando baldosas, pasos, vagones o carteles publicitarios. Como elemento

fiable se puede usar una baldosa medida con una regla de dibujo.

- Tramo de una calle mediante pasos, farolas, coches aparcados (asignando unos cuatro o cinco metros por coche). El elemento fiable podrá ser la distancia entre dos farolas medida con una cinta métrica.
- Avenida de un paseo, usando pasos, bancos, distancia entre árboles, etc. Aquí el único elemento fiable sería el de los pasos.

Pues nada, a intentarlo y divertirse con ello. No todo van a ser fórmulas y ecuaciones. Y siempre por equipos.

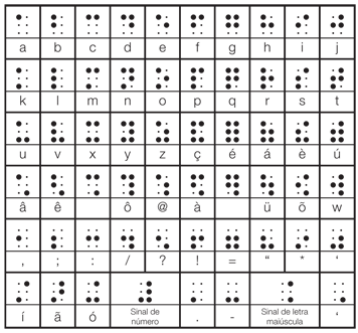
ALFABETO BRAILLE

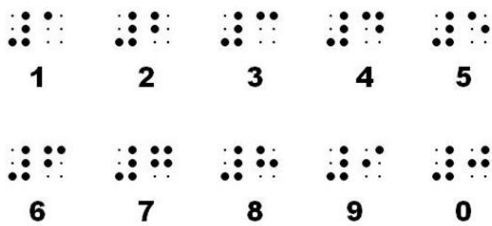
Ideas para un estudio en clase:

Es difícil motivar los temas de Combinatoria en clase, salvo los de conteos triviales. Los ejemplos usados no siempre son cercanos a la realidad de nuestros alumnos. El estudio del alfabeto Braille puede servir para lograr esa motivación si se le da un enfoque lo más interdisciplinar posible. Enunciamos a continuación algunas ideas aisladas sobre objetivos que se pueden lograr con este alfabeto. Se recomienda el trabajo por grupos.

(1) Búsquedas en Internet:

- Qué es el alfabeto Braille. Cómo se lee: Tras una breve introducción se inicia una búsqueda libre en Internet con la obligación de recopilar información. Es imprescindible obtener una imagen o varias con letras y números:





  Esas imágenes se deben almacenar e imprimir para su posterior estudio.
- Escribir un resumen histórico del alfabeto en no más de 15 ó 20 líneas: Con el material almacenado, y pata evitar el uso de un simple copiar y pegar, se exigirá un resumen escrito del nacimiento y utilidad del alfabeto, de no más de 20 líneas. Si algún equipo lo desea puede ampliar el texto con otro documento complementario.
- Completar las búsquedas en la Red con otras en el entorno más próximo, como las teclas de los

ascensores, una visita a la delegación de la Organización Nacional de Ciegos o cualquier otra cercana al alumnado.

- Sería conveniente que alguna frase de los documentos producidos se escribiera en Braille

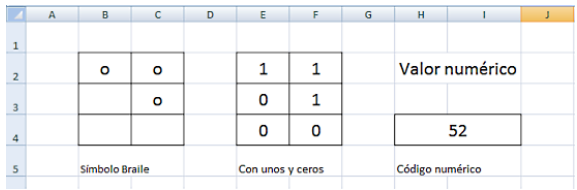
(2) Para repasar Combinatoria:

- Conteo en la celda básica de 2 por 3. Por los procedimientos que cada grupo elija, se debe llegar al total de 2^6=64 símbolos posibles. Si se ve conveniente, se puede interpretar el resultado como total de conjuntos, o variaciones de (0,1) o combinaciones de seis casillas tomadas de uno en uno, de dos en dos,…
- Repaso del producto cartesiano: Investigación de los prefijos, Número total de símbolos usando prefijos: 64*64=4096. Estudio especial de los números del 0 al 9. ¿Siguen alguna pauta de orden? Investigar.

(3) Para trabajar con Hoja de Cálculo:

Se puede confeccionar un traductor de símbolos Braille a letras. Para no complicar el trabajo se puede restringir el estudio a la célula básica sin prefijos. Se podría dividir el diseño en tres etapas:

(a) Traducir el esquema de seis puntos a un número binario



En la imagen se ha preparado, ajustando altura y anchura de las celdas, la célula básica del alfabeto en el rango B2:C4. Como punto se ha usado la letra “o”, pero puede servir cualquier otro.

La traducción a binario se consigue con la función SI. Copiamos a continuación la fórmula implementada en E2, que se ha extendido después al rango E2:F4:

=SI(B2="o";1;0)

Por último, se han asignado los valores 32, 16, 8, 4, 2 y 1 a cada una de las seis celdas. En el ejemplo se ha seguido el orden E2, F2, E3, F3, E4 y F4, para llegar a la fórmula

=E2*32+F2*16+E3*8+F3*4+E4*2+F4

Con ella conseguimos la traducción del símbolo Braille a un código comprendido entre 0 y 63 (64 posibilidades)

(b) Traducir el binario a símbolo Braille

Esta es la parte más pesada del trabajo, y por eso se aconseja el trabajo en equipo. Ahora, para cada letra se generará el código numérico correspondiente y se confeccionará una tabla de traducción. Mientras unos escriben los símbolos Braille en el primer rango otros toman nota del código generado y unos terceros van confeccionando la tabla traductora. Si se ve que falta

tiempo, se pueden considerar sólo las diez o quince primeras letras.

Se pueden organizar en una tabla de dos columnas. Por dar comodidad al resto del diseño, situaremos a la izquierda el código y a su derecha la letra correspondiente:

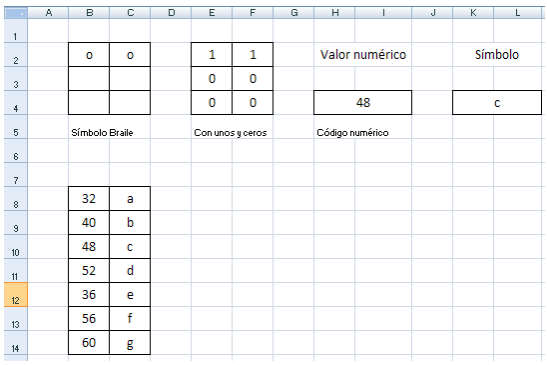
32	a
40	b
48	c
52	d
36	e
56	f
60	g

(c) Traducción de código numérico a símbolo

Una vez confeccionada la tabla, que la suponemos situada en el rango B8:C24, por ejemplo, bastaría con usar la función BUSCARV para que consiguiéramos la escritura del símbolo a la derecha del código en la celda K4:

=BUSCARV(H4;B8:C14;2)

En la imagen puedes ver completa la traducción de la letra c:



1												
2		o	o		1	1		Valor numérico			Símbolo	
3					0	0						
4					0	0		48			c	
5		Símbolo Braille			Con unos y ceros			Código numérico				
6												
7												
8		32	a									
9		40	b									
10		48	c									
11		52	d									
12		36	e									
13		56	f									
14		60	g									

(4) Trabajos complementarios

Para atender a la diversidad y al trabajo voluntario individual, se pueden proponer también:

- Traductor para números
- Estudio e interpretación de los prefijos
- Búsqueda de información sobre el Braille Unicode
- Concurso de microrelatos en Braille.
- Cualquier otro trabajo propuesto por el alumnado

Ayer compré un envase de terrones de azúcar y me llamó la atención la información que daba sobre el contenido: 126 terrones.

Después de pensar un poco creí estar en disposición de adivinar las dimensiones de cada terrón. Medí el envase y resultó tener las dimensiones 8,8, 11,2 y 5,5 respectivamente, de forma aproximada. En contra de lo que creía, aún tenía dudas después de la medida, pero me acordé de que los terrones tienen una cara casi cuadrada.

¿Cuál fue mi solución?

Este tipo de actividad es la que yo habría desarrollado en un taller de Matemáticas si estuviera en activo, pero ahora sólo puedo proponerlo. Creo que daría lugar a una interesante discusión en grupo.

MI PEQUEÑO HOMENAJE AL 11/11/11

111111 se descompone en los factores primos 3, 7, 11, 13, 37. Si los concatenamos resulta otro bonito número primo: 37111337

(Ver http://oeis.org/A046411) Si los sumamos, también: el 71

Y si expresamos 111111 en base 8: 331007(8, usa todas las cifras de la descomposición anterior.

656^2-565^2=111111 El curioso efecto de sustituir entre sí 6 y 5.

NO HAY QUE DEJARSE LLEVAR POR LA ADMIRACIÓN

El otro día “retwiteé” esta igualdad. Me gustó, la enlacé y no le di más importancia.

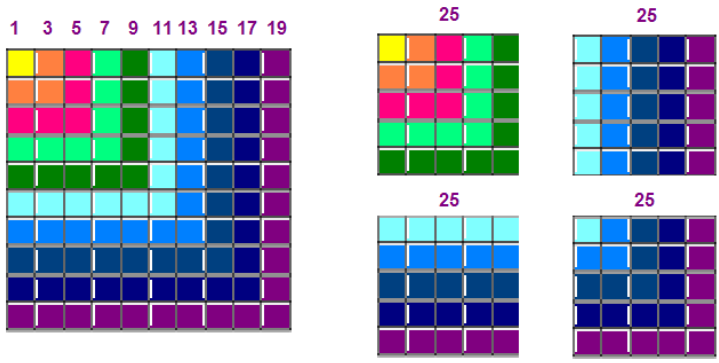
(1+3)/(5+7) = (1+3+5)/(7+9+11)=
(1+3+5+7)/(9+11+13+15)= ... = 1/3

Al día siguiente volví a verla y esta vez sí la analicé y me di cuenta de que era algo trivial:

Los numeradores son sumas de impares, y por tanto equivalen a n^2. Los denominadores equivalen a duplicar el número de elementos de arriba y después

restárselos, es decir $(2n)^2$-n^2 = $3n^2$. Simplificamos y nos da un tercio. Se acabó el misterio y la admiración. Tenía que dar 1/3 tomes los elementos que tomes.

¿Lo quieres más fácil? Estudia estas dos imágenes



En la primera figura el numerador 1+3+5+7+9 como un cuadrado en el que cada número impar viene representado por el mismo color (un gnomon), adosado a la suma 11+13+15+17+19, también formado por gnomones de distinto color hasta completar un cuadrado de 100.

En la segunda hemos separados los cuatro cuadrados, con lo que se percibe que 1+3+5+7+9 sólo ocupa un cuadrado y 11+13+15+17+19 tres, luego su cociente es 1/3

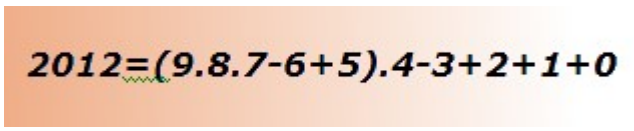
$$2011 = (1+1)^{11} - \frac{111}{(1+1+1)}$$

Un asombro parecido y creo que injustificado produjeron entre algunos amigos mis dos desarrollos sobre los años 2011 y 2012. En el primero la clave estuvo en que por aquellos días yo había estado experimentando con diferencias entre potencias de 2 y números primos.

Vi que 2011=2^11-37. Como recordé que 37=111/3, mi cerebro se llenó de unos, y me vino a la imaginación el desarrollo de la imagen.

Fue una feliz intersección de caminos. Este tipo de curiosidades surge por encuentros entre dos líneas matemáticas.

Con el 2012 me ocurrió algo similar. No era posible buscar unos de la misma forma, pero al factorizar 2012 apareció el número 503, que por proximidad me hizo pensar en el 504, que a su vez recordaba al factorial de 7. De ahí vino la idea de que 9*8*7=504 y que había que seguir las cifras hasta el cero.



Otro caso de feliz intersección de dos caminos. No hay nada admirable en este desarrollo.

En una entrada anterior de este blog comentábamos la casualidad de que la expresión $M=3*5^{2n+1}+2^{3n+1}$ sea siempre múltiplo de 17, pero con algún truco afortunado no sólo se podía demostrar, sino que era fácil inventarse casos parecidos.

Así que antes de admirarnos debemos analizar las cosas.

¿Qué opinas de esta serie de igualdades?

$$\frac{1+5}{1+7}=\frac{1+3+9+11}{1+3+13+15}=\frac{1+3+5+13+15+17}{1+3+5+19+21+23}=\cdots$$

¿Son verdaderas? ¿Se pueden prolongar indefinidamente?¿Cuál es su valor común?

Intenta responder usando técnicas algebraicas y gráficas.

SOLUCIONES

PRIMOS INAGOTABLES

Los huecos de un primo

(1) No es primo porque es múltiplo de 1001. En general, si $P=2^{3n}+2^{2n}+2^n+1$ resultará $P=2^{3n}+2^{2n}+2^n+1=(2^n+1)(2^{2n}+1)$. Puedes generalizarlo a más sumandos si su número es par.

(2) El 6597069766657 es

11000000000000000000000000000000000000001

(ver http://oeis.org/A039687)

(3) Serían múltiplos de 3

Pasito a pasito hacia la complejidad

Soluciones:

(a) Si N es primo y N+1 semiprimo, como N+1 es par, ha de ser múltiplo de 2, luego (N+1)/2 ha de ser primo para que se cumpla que N+1 sea semiprimo. Recíprocamente: si (N+1)/2 es primo, N+1 es semiprimo, pues N+1=2p con p primo.

(b) El directo es muy sencillo, pues sigma(N)=1+N por ser primo, luego sigma(N)/2 es primo. El recíproco hay que verlo con más cuidado: si sigma(N)/2 es primo, sigma(N)=2p con p primo. Pero la fórmula de sigma(N) se compone de varios factores del tipo $1+q+q^2+q^3+\ldots$

con q factor primo de N. En este caso sólo puede haber un factor primo, ya que 1+q>2, luego el 2 se ha producido como factor de $1+q+q^2+q^3+\ldots$Para que $1+q+q^2+q^3+\ldots=2p$ ha de reducirse a 1+q. En efecto, si la potencia mayor es impar, la suma de potencias $1+q+q^2+\ldots$sería impar y no podría ser múltiplo de 2. Si la mayor es par, se puede descomponer en

$(1+q)+q(1+q)+q^2(1+q)+\ldots=(1+q)(1+q+q^2+\ldots)$ y ambos factores serían mayores que 2, lo que no es lo supuesto.

(c) Si N=4k+3 entonces N+1=4(k+1) con lo que no podría ser semiprimo.

(d) N es primo, luego no será múltiplo de 3. N+1 es del tipo 2p con p primo. Ese primo no puede ser 3, porque entonces N+1=6 y N=5 y hemos afirmado que es mayor. Si no es 3, no será tampoco múltiplo de 3, pues entonces N+1 no sería semiprimo. Por tanto, N+1 no es múltiplo de 3, Como los múltiplos de 3 aparecen de 3 en 3 números, N+2 sí tendrá que serlo.

(e) Si N es primo, su resto módulo 12 sólo puede ser **1, 5, 7 u 11**. Por tanto los restos que producirá N+1 serán **2, 6, 8 o 0** y los de N+2 **3, 7, 9 y 1**. Hay que desechar estos:

11- Si el resto es 11, N+1 sería múltiplo de 12, y no podría ser semiprimo.

5- N+2 sería del tipo 12k+7, lo que impediría que fuera múltiplo de 3.

7- N+1 sería del tipo 12k+8=2*2*(3k+1) y no sería semiprimo

Luego sólo nos queda que el resto sea 1.

En la cuestión de si p es primo y p+3 semiprimo, podemos razonar que p es del tipo 4k+3, pues si fuera un primo de Gauss con p=4k+1, p+3 no sería semiprimo, porque sería múltiplo de 4. El que (p+3)/2 sea primo es porque p+3 es par (en el p=2 no se cumple la propiedad) y por tanto p+3=2q siendo q primo.

Números de Aquiles

(a) El número N se descompondrá en varios factores primos, cuyos exponentes podrán ser pares o impares mayores que 2. Si el exponente es par, expresamos p^{2k} como $(p^k)^2$. Si el exponente es impar mayor que 2 podemos escribir p^{2k+1} (con k no nulo) como $(p^{k-1})^2*p^3$. Una vez realizados esos cambios de representación, multiplicaremos entre sí todos los cuadrados y resultará a^2, al multiplicar los cubos, b^3.

(b) Todo número de Aquiles N tiene la forma a^2b^3 por ser poderoso. Si **a** y **b** fueran ambos primos, sería minimal y por tanto se cumpliría lo propuesto. Si uno de ellos no lo es bastará extraer una vez uno de sus factores primos elevado a la misma potencia, e igual haríamos si ninguno fuera primo. Al final se extraería un divisor que fuera de Aquiles y minimal.

Funciones recursivas en las hojas de cálculo

```
Public Function poligon(a, n)
Dim p

If a = 1 Then p = 1 Else p = poligon(a - 1, n) + a * (n - 2) + 3 - n
poligon = p
End Function
```

FUNCIONES MULTIPLICATIVAS

Emparedado de cuadrados

(a) La fórmula

$$SPC(N) = \sum_{(d|N)} \left(MCD(d, \frac{N}{d}) \right)^2$$

Funciona porque en

1 p p^2 p^3 p^4 p^5 p^6 … p^{e-1} p^e

Los MCD entre d y N/d son:

1 p p^2 p^3 p^4 p^5 p^6 … p^{e-1} p^e

(b) Sí, porque B contendrá a todos los factores de A y quizás alguno más. En el caso de los factores primos de A, sus exponentes en B serán iguales o mayores que los de A, luego al truncarlos a un número par darán resultados también iguales o mayores, luego PC(A) divide a PC(B)

(c) Sí, por la misma razón

(d) Llamemos Q al cociente entre B y A. Si sus factores primos son todos distintos de los de la parte cuadrada de A, esta no se incrementará al pasar de A a B. Si algún factor primo coincide, sólo serán iguales si ese factor está elevado a un número par en A y una unidad más en B.

Ejemplo: La parte cuadrada de 72 es 36. Si multiplicamos 72 por factores primos distintos de 2 y 3, como 72*7=504, la parte cuadrada seguirá siendo 36. Si lo multiplicamos por 3 también, porque su exponente pasa de par a impar, pero al truncar coinciden: 72*3=216 y su parte cuadrada sigue siendo 36. Si lo multiplicamos por 2 sí cambiará, porque su exponente 3 pasa a 4 y eso altera la parte cuadrada.

(e) La parte libre sólo quedará inalterada si B aporta como nuevos factores los mismos de la parte cuadrada elevados a un número par, porque así se integrarán en una nueva parte cuadrada dejando inalterada la libre.

(f) Ese MCD sólo podrá contener los factores de N que estén elevados a un exponente impar, pues así PC(N)

se llevará su truncamiento a par y PL(N) se llevará la unidad. Así que esta función no se comporta igual con los exponentes pares que con los impares, luego no ha de ser multiplicativa. Basta un contraejemplo: PC(9)=9, PL(9)=1, MCD(9,1)=1. Por otra parte PC(12)=4; PL(12)=3, MCD(4,3)=1. Sin embargo, si multiplicamos 9*12=108 tenemos que PC(108)=36, PL(108)=3 MCD(36,3)=3 y no 1 como sería de esperar si fuera multiplicativa.

PC*PL^2=MMC

N es la media geométrica entre PC y MMC

N*PL(N)=MMC(N)

Raíz cuadrada interna es la raíz cuadrada de PC(N). En el caso de 126 sería 3

Raíz cuadrada externa es similar con MMC. Así en 126 sería 42

Se comprende que su producto es N, por ser este media geométrica de los dos cuadrados.

Terrones de azúcar

Solución: 126=2*3*3*7, luego la única descomposición parecida a la forma del envase es de 3*6*7, pero no sabía si los terrones se apilaban en 6 capas de abajo a arriba o de 7. Había entonces que basarse en la cara casi cuadrada.

Si divido 8,8/6=1,47 11,2/7=1,6 5,5/3=1,83 lo que me daría una cara no muy cuadrada. Cambié los cocientes: 8,8/7=1,26, 11,2/6=1,87, 5,5/3=1,83, que sí tiene dos lados casi iguales. Así que la solución en mm. Sería 13, 19 y 18.

Abría el envase, medí los terrones y, en efecto, había acertado.