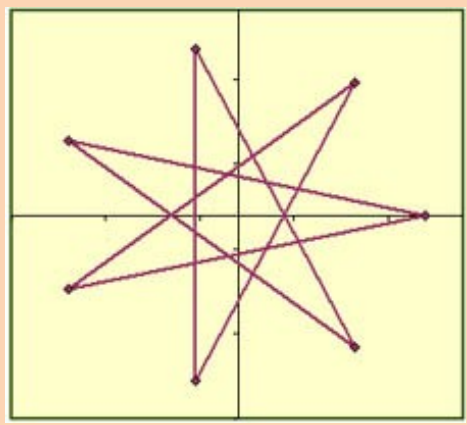
Cuestiones modulares



Edición 2016

Colección Hojamat.es

http://www.hojamat.es

PRESENTACIÓN

Los temas de Aritmética Modular son muy poco conocidos para personas con cultura matemática de tipo medio. Sin embargo, su aparente simplicidad y la elegancia de sus desarrollos los convierten en un pequeño tesoro.

Otra característica es que aparecen por sorpresa en otros planteamientos que se diría ajenos a estas cuestiones. Son pocos conceptos pero muy potentes.

Como advertiremos en todos los documentos de esta colección, el material presentado no contiene desarrollos sistemáticos, ni pretende ser un manual teórico. En cada tema se incluirán cuestiones curiosas o relacionadas con las hojas de cálculo, con la única pretensión de explicar algunos conceptos de forma amena.

A partir de la edición 2016 se han incorporado los temas de orden de un lemento, raíces primitivas y e índices modulares, con lo que ha quedado un documento bastante completo.

TABLA DE CONTENIDO

GENERALIDADES

LA EXPONENCIACIÓN MODULAR

En algunos problemas, como en el criterio de primalidad de Fermat, debemos elevar un elemento de Z_m a un exponente alto. 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.

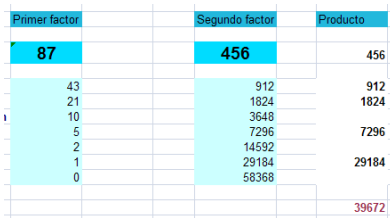
Tenemos implementada, como una curiosidad, esta suma para hojas de cálculo

(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 0. 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 entrada

http://hojaynumeros.blogspot.com.es/2012/03/funciones-recursivas-en-las-hojas-de.html

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
```

¿QUÉ HAY DETRÁS DE LOS DECIMALES PERIÓDICOS?

Hace unos meses comentaba con un amigo el tratamiento que se podía hacer con hoja de cálculo de

los decimales periódicos. Ya en una de las primeras entradas de este blog encontrábamos los decimales de este tipo

(***http://hojaynumeros.blogspot.com.es/2008/10/grandes-periodos.html)***

Lo que no nos planteamos en esa ocasión fue el cálculo del número de decimales del periodo, su longitud, mediante un cálculo directo, ni tampoco la del anteperiodo. Lo abordamos hoy mediante la ayuda de las congruencias y de los restos potenciales.

¿Qué es sacar decimales en una división o en una fracción?

Fundamentalmente se trata de multiplicar los distintos restos por 10 y hallar su nuevo resto respecto al cociente. Al reiterar el proceso, cuando este se repita, ya hay periodo. Lo desarrollamos.

Si tenemos una división entera de dividendo **D**, divisor **d**, cociente **Q** y resto **R**, sabemos que están relacionados por **D=d*Q+R**. Si multiplicamos R por 10 y volvemos a dividir entre Q (sacar el primer decimal) obtendremos $R*10=d*q_1+r_1$, donde q_1 es el primer decimal y r_1 el siguiente resto. Si unimos ambas relaciones se obtendrá

$D*10=(10*Q+q_1)*d+r_1$

El paréntesis representa el nuevo cociente con un decimal, pero sin coma, es decir, multiplicado por 10. Ya hemos sacado un decimal.

Si damos otros pasos obtendremos

$D*10^2=(10^2*Q+10*q_1+q_2)*d+r_2$

$D*10^3=(10^3*Q+10^2*q_1+10*q_2+q_3)*d+r_3$

Y así seguiríamos hasta un resto cero o una repetición de valores que diera lugar a un periodo.

Desarrollo decimal exacto o periódico

Sabemos desde la enseñanza secundaria que si el divisor sólo posee los factores primos 2 y 5 el proceso anterior nos lleva a un resto nulo y al fin del cálculo, lo que llamamos **decimal exacto**. Si existen otros factores aparecerá un anteperiodo si entre ellos figuran el 2 o el 5 y finalmente, el decimal se convertirá en periódico con un periodo inferior o igual a **d-1**.

¿Qué hay detrás de estos hechos? Pues los restos potenciales del 10 respecto al divisor.

Los repasamos.

Restos potenciales

Imaginemos las congruencias definidas respecto a un módulo m ***(http://hojamat.es/sindecimales/congruencias/teoria/teorcong.pdf)*** y sea **n** un número natural. Llamaremos

Restos potenciales de **n** respecto a **m** a **los restos producidos por las distintas potencias naturales de n** respecto al módulo **m**.

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

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

Se puede ver muy fácilmente que si se tiene un resto potencial de **n** respecto a **m**, para conseguir el siguiente basta **multiplicar el actual resto de nuevo por n** y hallarle el resto respecto a **m**. No hay que hallar la potencia completa.

El conjunto de restos potenciales sigue unas pautas muy sencillas:

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

Sería el caso, por ejemplo, de los restos potenciales de 60 respecto al 18, cuyos factores primos 2 y 3 lo son también de 60. La potencia k que consiga que 60^k sea múltiplo de 18 producirá un resto cero y al seguir multiplicando por 60 también serán nulos los restos que aparezcan.

$60^0 \equiv 1 (\text{mod } 18$

$60^1 \equiv 6 \pmod{18}$

$60^2 \equiv 0 \pmod{18}$

$60^3 \equiv 0 \pmod{18}$

$60^4 \equiv 0 \pmod{18}$

…..

Ya todos serían nulos. Hemos tenido que llegar a 60^2 para absorber el 3^2 que figura en el desarrollo de $18=2*3^2$

Este desarrollo y los siguientes los puedes comprobar con la herramienta ***"Restos potenciales"*** que puedes descargar desde

http://hojamat.es/sindecimales/congruencias/inicongruencias.htm

En general, habrá que llegar a la potencia que viene determinada por el mayor de los cocientes (por exceso si no son enteros) entre los exponentes de los factores primos de m y sus homólogos en n.

En efecto, si $\mathbf{n=p^a q^b r^c}$ y $\mathbf{m=p^{a'} q^{b'} r^{c'}}$ supongamos que elevamos n a un exponente k y que con eso conseguimos que n^k sea múltiplo de m. Esto nos llevaría a que

$N^k=(p^a q^b r^c)^k = p^{ak} q^{bk} r^{ck}$ sea múltiplo de $m= p^{a'} q^{b'} r^{c'}$, que a su vez implica que $ak \geq a'$, $bk \geq b'$ y $ck \geq c'$, lo que supone que k sea mayor o igual que los cocientes a'/a, b'/b y

c’/c, tal como hemos afirmado: el mínimo valor de k es el mayor cociente tomado por exceso entre los exponentes en n y sus homólogos en m.

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

Si recorremos los restos potenciales de n respecto a m, si ambos son primos entre sí, por el teorema de Euler se cumplirá que

$$n^{\varphi(m)} \equiv 1 \ (mod\ m$$

Se representa mediante φ(m) la indicatriz de Euler

(ver http://hojaynumeros.blogspot.com.es/2012/07/la-herencia-de-euclides-5-la-funcion.html)

Así que a partir de una de las potencias aparece el resto 1 y al seguir multiplicando por **n** irán apareciendo los demás de forma periódica.

Otra forma de verlo es que en este caso **n** es inversible en $\mathbf{Z_m}$, no divisor de cero, por lo que sus potencias producirán todas restos no nulos ***(ver http://hojaynumeros.blogspot.com.es/2012/06/la-herencia-de-euclides-3-el-anillo-zm.html)*** y esto nos llevará a que se repita alguno, porque su máximo número es **m-1**.

Sean dos potencias de n que producen el mismo resto: $\mathbf{n^r \equiv n^{r+h}}$ **(mod m**. En ese caso se cumplirá que $n^{r+h}-n^r=n^r(n^h-1)$ será múltiplo de m. Pero este es primo con **n**, luego no puede dividir a n^r y lo hará a n^h-1. Esto quiere decir que $\mathbf{n^h \equiv 1}$ **(mod m** y podemos afirmar que:

En general, no hay que llegar hasta el exponente φ(m) para conseguir un resto igual a 1. Llamaremos gaussiano, orden o índice de n respecto a m al menor exponente k al que hay que elevar n para producir resto 1 respecto al módulo m.

Por tanto, cuando n y m son primos entre sí, los restos potenciales forman una sucesión periódica a partir del primero con periodo igual al gaussiano de n respecto a m.

3. Por último, si **m** posee **los mismos factores** primos de **n** y **alguno más**, la sucesión comenzará con unos restos no periódicos, tantos como el mayor cociente entre los factores comunes de uno y otro (ver primer caso), a los que seguirán otros periódicos.

Si **m** contiene factores comunes con **n** y otros no comunes, lo podemos descomponer así: $\mathbf{m=m_1*m_2}$, donde $\mathbf{m_1}$ contiene los comunes y $\mathbf{m_2}$ los no comunes. Si volvemos a repetir el análisis anterior sobre potencias cuyos restos se repiten, llegaremos a esto:

$n^r(n^h-1)$ será múltiplo de $m=m_1*m_2$ con la suposición de que $\mathbf{n^r}$ produce el primer resto que se repite.

Pero $\mathbf{m_2}$ es primo con $\mathbf{n^r}$, luego dividirá a (n^h-1). Con un razonamiento similar al del caso 1, llegaremos a que el menor valor de h **es el gaussiano de n respecto a $\mathbf{m_2}$**.

De igual forma, si $\mathbf{m_1}$ sólo contiene factores primos comunes con **n**, no podrá dividir a n^h-1, **luego lo hará a $\mathbf{n^r}$**. Hemos indicado que $\mathbf{n^r}$ produce el primer resto que se repite, luego todos los anteriores no pertenecerán a la parte periódica, y formarán el anteperiodo, ya que la condición de que m_1 divida a n^r garantiza que r es mayor que 0. Para que $\mathbf{n^r}$ sea múltiplo de m_1 sólo tendremos que usar el criterio del mayor cociente de factores comunes, como en el primer caso.

Aplicación a los decimales periódicos

Todo lo que hemos aprendido se aplica a la generación de decimales. Aquí **n=10**, luego los factores comunes sólo serán el 2 y el 5. El divisor **d** equivale a la **m** que hemos usado en los razonamientos.

Antes de generarlos, la fracción **D/d** se habrá convertido en irreducible, luego **D** y **d** son primos entre sí. Esto es muy importante, porque según una conocida propiedad de la aritmética modular, si la sucesión 10, 10^2, 10^3, 10^4,…la multiplicamos por D, coprimo con el módulo d, la sucesión resultante D*10, D*10^2, D*10^3, D*10^4,…forma un sistema de restos con las mismas propiedades, salvo quizás los valores de los mismos.

Resumiendo:

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

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

Si **d** contiene además del 2 o 5 otros factores, el desarrollo comenzará con k decimales no periódicos (el anteperiodo), siendo k el mayor exponente tomado entre los del 2 y el 5 que figuran en la factorización prima de **d**, seguidos de un periodo con tantas cifras como indique el gaussiano de 10 respecto a la parte de **d** que no contiene 2 ni 5. Se formaría un **decimal periódico mixto**

Herramienta con hoja de cálculo

Con el apoyo de la teoría explicada describiremos a continuación una sencilla herramienta para hojas de cálculo que encuentra el anteperiodo y el periodo de un desarrollo decimal.

Necesitaremos las siguientes operaciones:

(1) Simplificar la fracción cuyo desarrollo decimal deseamos conocer. Esto se consigue en las hojas de

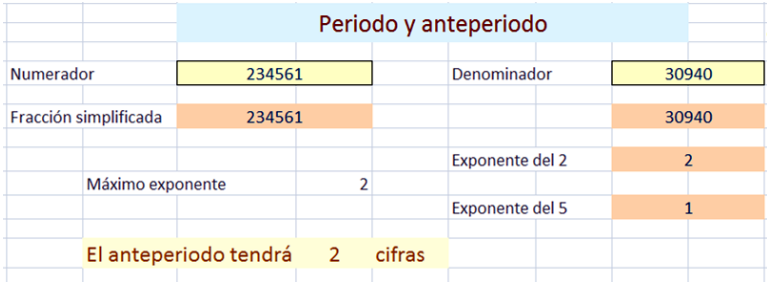
cálculo dividiendo las celdas del numerador y del denominador por su MCD mediante la función M.C.D(A;B)

(2) Extraer del denominador los factores 2 y 5 tomando nota de sus exponentes (cero si no figuran) y quedándonos con el máximo, que será el número de cifras del anteperiodo

Un código posible para la extracción del 2 (igual se procede para el 5) puede ser este:

```
Public Function expo2(n)
Dim e, m
m = n
e = 0
While m / 2 = m \ 2
e = e + 1
m = m / 2
Wend
expo2 = e
End Function
```

Nos devuelve cero si el 2 no es divisor del denominador y el exponente en caso afirmativo. En la imagen puedes ver la disposición de cálculo que hemos elegido. El máximo se consigue con la función MAX(A;B) aplicada a los dos exponentes (del 2 y del 5)



(3) Obtener la parte del denominador coprima con 10. Para ello basta dividir el denominador entre las dos potencias de 2 y 5 obtenidas.

(4) Obtener el gaussiano de 10 respecto a esa parte coprima. Podríamos usar exponenciación modular

(ver http://hojaynumeros.blogspot.com.es/2012/03/de-la-multiplicacion-rusa-la.html),

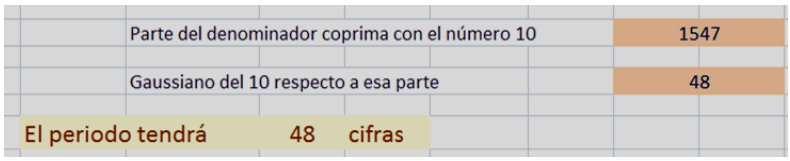
pero en este caso, como la generación de restos se realiza mediante mltiplicaciones por 10, hemos elegido el método directo, que no es demasiado lento en el rango de números que manejan las hojas.

Añadimos comentarios al código:

```
Public Function gauss10(m)
Dim r, g, i

g = 1
r = 10 - m * (10 \ m) 'Obtenemos el primer resto
```

While r <> 1 ‘Mientras no encontremos un resto igual a uno, seguimos
r = r * 10 ‘Cada resto es igual al anterior multiplicado por 10
r = r - m * (r \ m) ‘y convertido en resto módulo m
g = g + 1 ‘En cada ciclo aumenta el gaussiano
Wend
gauss10 = g
End Function



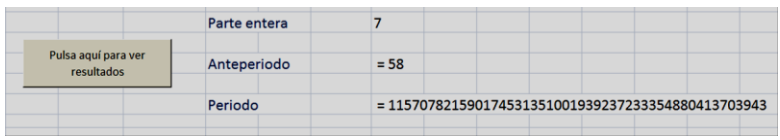
En el caso de la primera imagen el denominador era 30940, que contenía como factor 2^2*5. Eliminado este, quedó reducido a 1547, y aplicando el cálculo del gaussiano resulta nada menos que un periodo de 48 cifras, fuera del alcance ordinario de una hoja de cálculo.

(5) Expresión del anteperiodo y el periodo. Cuando ambos presentan muchas cifras, como en el caso del ejemplo, es mejor expresarlas en forma de texto, y no de número. El procedimiento consiste básicamente en el mismo usado para encontrar el gaussiano, multiplicar cada resto por 10 y reducirlo a resto módulo el denominador. Sirve igual para las cifras periódicas que para las no periódicas. La diferencia ahora es que los

restos los convertimos en texto y los vamos incorporando a una cadena del mismo tipo.

El procedimiento completo puede resultar aburrido y dejamos su estudio a quien descargue la herramienta e inspeccione su código. Para el resto de lectores resultará una buena forma de comprobar los cálculos manuales.

Al necesitar calcular por separado la parte entera, el anteperiodo y el periodo, hemos preferido usar un botón y una macro para mayor comodidad:



Tienes esta herramienta en la dirección

http://hojamat.es/sindecimales/aritmetica/herramientas/herrarit.htm#periodo

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.

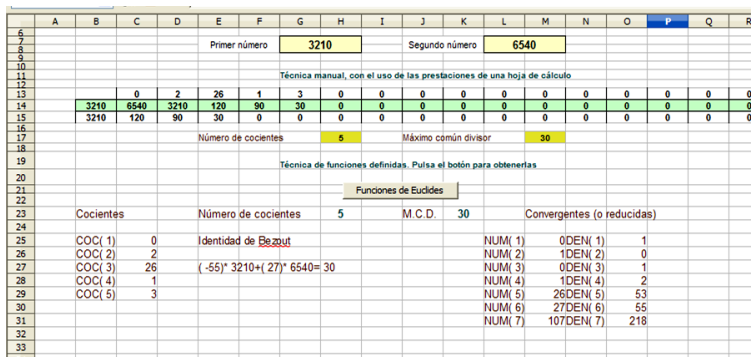
Rutinas y funciones

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.

  En otra entrada posterior lo aplicaremos a la resolución de la ecuación lineal en congruencias. Puedes ir consultando la teoría mientras tanto.

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):

$6*1\equiv 6 \pmod 9$; $6*2\equiv 3 \pmod 9$; $6*3\equiv 0 \pmod 9$; $6*4\equiv 6 \pmod 9$; $6*5\equiv 3 \pmod 9$; $6*6\equiv 0 \pmod 9$; $6*7\equiv 6 \pmod 9$; $6*8\equiv 3 \pmod 9$

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:

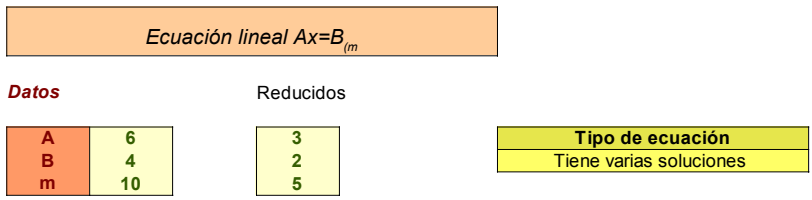
1. Si A es primo con m, existe una sola solución $x \equiv A^{-1}*B \pmod m$, por ser A inversible.
2. Si MCD(A,m)=d, con d mayor que 1, para que exista solución ha de ser B múltiplo de d. En ese caso se simplifican los tres números A, B y m con lo que se

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.



En la imagen se intenta resolver $6X \equiv 4 \pmod{10}$, 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 $3*2 \equiv 1 \pmod 5$. 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, $6*4 \equiv 4 \pmod{10}$

- 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 $A*x \equiv 0 \pmod m$ por lo que además de la solución trivial x=0 existirán otras si M.C.D(A,m)>1, y entonces A se confirmará

como divisor de cero. Por ejemplo, resuelve con la hoja $6*x \equiv 0 \pmod 9$ y obtendrás las soluciones 0, 3 y 6, ya que M.C.D(6,9)=3>1. Sin embargo, resuelve $6*x \equiv 0 \pmod 7$ 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 $A*x \equiv B \pmod m$ son soluciones de la homogénea $A*x \equiv 0 \pmod m$. Inversamente: dada una solución de $A*x \equiv B \pmod m$, si le vamos sumando por separado las soluciones de la homogénea, resulta el conjunto de todas las soluciones de $A*x \equiv B \pmod m$

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'≡0 (mod m) y por tanto divisor de cero.

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

Así que:

- **Si el elemento A es primo con el módulo m, entonces es inversible**, es decir, que existe algún otro elemento B tal que A*B=B*A=1. 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.

Anillo Zn

Escribe el valor de N: 12

Iniciar

X	MCD(X,N)	INVERSO	ORDEN	Indicatriz de Euler	4
1	1	1	1		
2	2				
3	3				
4	4				
5	1	5	2		
6	6				
7	1	7	2		
8	4				
9	3				
10	2				
11	1	11	2		

Tabla del grupo

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

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 $7*1\equiv7$, $7*5\equiv11$, $7*7\equiv1$ y $7*11\equiv5$. Imagina que multiplicamos las cuatro congruencias miembro a miembro:

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

7*7*7*7 ≡1, es decir 7^4≡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 **$p^{\varphi(m)} \equiv 1 \pmod{m}$**

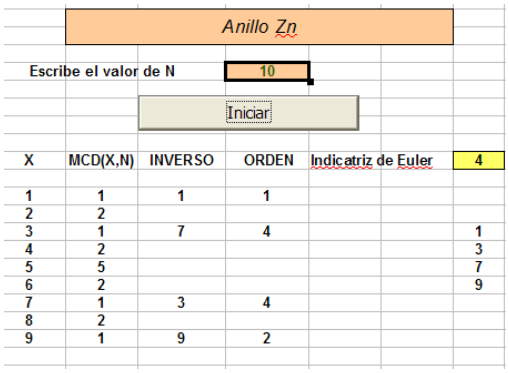
Orden de un elemento

Dado un elemento inversible **a**, llamaremos ***orden*** de ese elemento al mínimo número entero tal que **$a^r \equiv 1$**. 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…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.

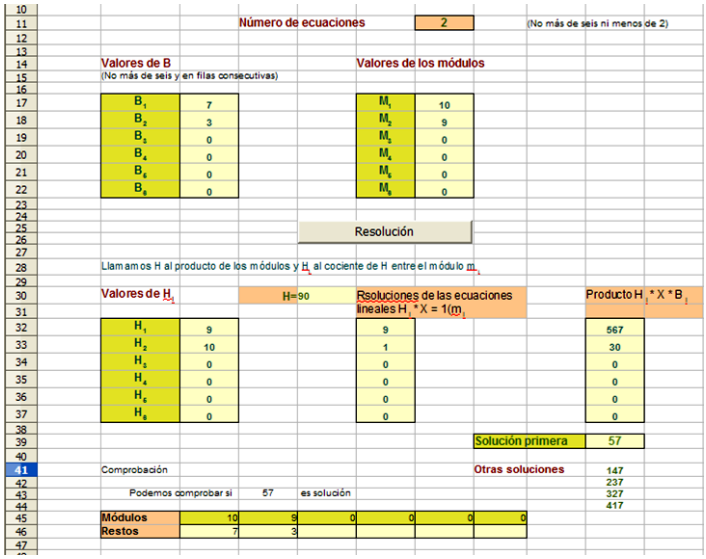
  $H=9.10 = 90$; $M'_1=9$; $M'_2=10$; $m_1=9$ (porque $9*9=81\equiv1$ (mod 10)); $m_2=1$ (porque $1*10=10\equiv1$ (mod 9)). Así tenemos que $E_1=9*9=81$ y $E_2=10*1=10$ y por último:

  $N=81.7+10.3= 597$. Lo reducimos a módulo 90 y queda 57. En efecto, $57\equiv7$ (mod 10) y $57\equiv3$ (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 $N=81.2+10.6=162+60=222\equiv42$ (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 $N \equiv a \pmod m$ y $N \equiv b \pmod n$. Por tanto, tenemos delante una correspondencia

biunívoca entre el conjunto $\mathbf{Z_m \times Z_n}$ y el conjunto $\mathbf{Z_{mn}}$. (Recuerda que **m** y **n** han de ser coprimos)

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 $N' \equiv p' \pmod m$ y $N' \equiv q' \pmod n$, podemos sumar y multiplicar miembro a miembro ambas congruencias y quedará: $N+N' \equiv p+p' \pmod m$ y de igual forma $N+N' \equiv q+q' \pmod n$. 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 $Z_m \times Z_n$ y el anillo 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 $Z^*_m \times Z^*_n$ es isomorfo a 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

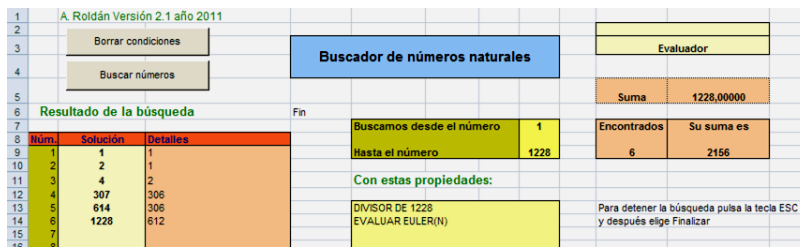
euler = e
End Function

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.

RESTOS CUADRÁTICOS

INTRODUCCIÓN

En esta entrada y otras posteriores trataremos el tema de las congruencias de segundo grado. Usaremos como siempre las hojas de cálculo, y, en especial una herramienta que hemos creado para este fin. Todo el tema gira alrededor de la ecuación

$$\mathbf{x^2 \equiv a \pmod p}$$

Imagina una clase de restos, por ejemplo la correspondiente a módulo 7, {0, 1, 2, 3, 4, 5, 6} Elige un resto, sea el 5. ¿Existirá otro resto que multiplicado por sí mismo dé como resultado 5, módulo 7? Probemos: $1*1\equiv1$, $2*2\equiv4$, $3*3\equiv2$, $4*4\equiv2$, $5*5\equiv4$, $6*6\equiv1$. Así que no es posible, los únicos resultados son 1, 4 y 2. Nunca resulta un 5, ni tampoco 3 ni 6.

Podemos resumir esta situación calificando 1, 2 y 4 como “restos cuadráticos” y 3, 5 y 6 como “no restos cuadráticos”. También podemos hablar de la “raíz cuadrada” de los primeros: $1^2=1$, $3^2=2$ y $2^2=4$. Es fácil ver que si k es raíz de n, también lo es m-k. Eleva esta última al cuadrado y lo comprobarás.

Restos	Raíz	No restos
1	1	3
2	3	5
4	2	6

Esta situación la tendrás siempre. Unos elementos podrán ser restos cuadráticos y otros no. El primer intento que hemos hecho para averiguarlo ha sido el probar los elementos uno a uno hasta conseguir que el cuadrado de uno de ellos coincida con el resto dado, o bien comprobar que esto es imposible y que se trata de un “no resto cuadrado”.

Para estudiar el tema con profundidad puedes acudir a

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

http://mate.dm.uba.ar/~pdenapo/teoria_analitica_de_numeros/clase11.pdf

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

Diremos que a es resto cuadrático módulo p, coprimo con él, cuando exista una solución a la ecuación

$$\mathbf{x^2 \equiv a \pmod{p}}$$

Con hoja de cálculo (o con ligeras variaciones, en cualquier lenguaje de programación) podemos automatizar este procedimiento. Definiremos una función, que dependa de un resto dado y del módulo correspondiente, que nos devuelva la raíz cuadrada,

con lo que sabremos que es resto cuadrático, o bien un cero si no lo es.

Public Function restocuad(n,modu) ‘los parámetros son el resto y el módulo
Dim k, r,s
Dim es As Boolean

es = False ‘ nos indica que aún no se ha encontrado una raíz
k = 1 ‘contador que busca la raíz
r = 0 ‘raíz encontrada
While k <= modu / 2 And Not es ‘va buscando las posibles raíces
s=(n-k*k)/modu
If s=int(s) Then es = True: r = k ‘se ha encontrado la raíz
k = k + 1 ’seguimos buscando
Wend
If es Then restocuad = r Else restocuad = 0 ‘devuelve un cero si no se ha encontrado
End Function

Con esta función implementada, puedes analizar qué restos son cuadráticos, formar tablas de restos y no restos y resolver la ecuación $x^2 \equiv a$, o, con los cambios adecuados, la ecuación general de segundo grado. Lo vemos con un ejemplo:

Resolver $x^2-26x+10 \equiv 7 \pmod{11}$

Damos estos pasos:
$X^2-26x+10 \equiv (x-13)^2-159 \equiv 7 \pmod{11}$

$(x-13)^2 \equiv 166 \pmod{11}$

$(x-13)^2 \equiv 1 \pmod{11}$

Buscamos la raíz cuadrada de 1 y resulta ser 1 o -1 (o 10) es decir:
$x-13 \equiv 1$ o $10 \pmod{11}$ Despejando: x=3 y x=1

Comprobamos: $3^2-26*3+10=-59 \equiv -4 \equiv 7 \pmod{11}$ y $1^2-26*1+10=-15 \equiv -4 \equiv 7 \pmod{11}$

Hemos elegido un ejemplo que tenía solución, pero si llega a aparecer un no resto en lugar de 1, no podríamos seguir. Por eso es tan importante saber previamente si un resto es cuadrático o no.

Caso de módulo primo e impar

En este caso, si consultas la teoría descubrirás que si p es el módulo primo e impar resulta que el número de restos cuadráticos es (p-1)/2, que son congruentes con 1^2, 2^2, 3^2…$((p-1)/2)^2$ y por tanto, este también es el número de no-restos.

Previamente estudia esta propiedad:

La ecuación $x^2 \equiv a \pmod{p}$ para un a dado, o no tiene solución, o tiene dos.

En efecto, si tiene una solución x_1 con $\mathbf{x_1^2 \equiv a \pmod{p}}$ también será solución $\mathbf{-x_1}$ y sólo tenemos que demostrar que ambas son distintas. Es fácil: si fueran iguales tendríamos que $2x_1=0$, pero ni 2 ni x_1 son divisores del cero, por ser p primo impar. La segunda solución la puedes expresar como $p-x_1$

Por tanto, el número de restos cuadráticos no sobrepasará (p-1)/2. Es más, es igual que ese número, porque los restos de 1^2, 2^2, 3^2…$((p-1)/2)^2$ no se repiten , ya que una igualdad entre ellos haría que la ecuación $\mathbf{x^2 \equiv a \pmod p}$ tuviera cuatro soluciones en lugar de dos.

Esta propiedad te ofrece un procedimiento para encontrar todos los restos cuadráticos en este caso, y es calcular los valores de 1^2, 2^2, 3^2…$((p-1)/2)^2$ y los resultados serán los restos cuadráticos, y los demás será no restos.

Hemos preparado una herramienta en hoja de cálculo

(ver http://www.hojamat.es/sindecimales/congruencias/herramientas/herrcong.htm#restoscuad),

cuya primera prestación es la de encontrar el conjunto de restos y no restos para un módulo primo e impar.

En ella está implementado el procedimiento de ir calculando los valores de 1^2, 2^2, 3^2…$((p-1)/2)^2$. La novedad de este esquema es que va situando los restos en una columna y los no restos en otra.

En la imagen figuran los 15 restos módulo 31, sus raíces, y los 15 no restos. Para ver cómo lo logra tendrías que acceder al Basic, pero no lo analizaremos en este momento.

Su funcionamiento en esta parte es muy simple: escribes el nuevo módulo y después pulsas el botón de **Restos y no restos** para que aparezcan.
Puedes alternar tus cálculos manuales con los de la hoja para entenderlo todo mejor y comprobar resultados.

En la siguiente entrada simplificaremos los cálculos necesarios para saber si un resto es cuadrático o no mediante un criterio debido a Euler.

CRITERIO DE EULER

En la una entrada anterior iniciamos el estudio de los restos cuadráticos respecto a un módulo. Descubrimos un procedimiento algo lento para encontrar los restos y los no restos. En esta otra entrada simplificaremos algo el proceso y aprenderemos nuevos conceptos. Se aconseja leer previamente la primera entrada dedicada a este tema.

El recorrer todos los restos desde 1 hasta (p-1)/2 puede hacerse muy pesado en el caso de valores muy grandes. Euler descubrió un criterio que nos ayuda a distinguir los restos de los no restos con un solo cálculo. Es este:
Si a es un resto cuadrático respecto a p (primo e impar) se cumple

$$a^{\frac{p-1}{2}} \equiv 1(mod\ p)$$

Y si no lo es

$$a^{\frac{p-1}{2}} \equiv -1(mod\ p)$$

Es una consecuencia del Teorema de Fermat: $a^{p-1} \equiv 1 \pmod p$, luego, como p-1 es par, podemos escribir

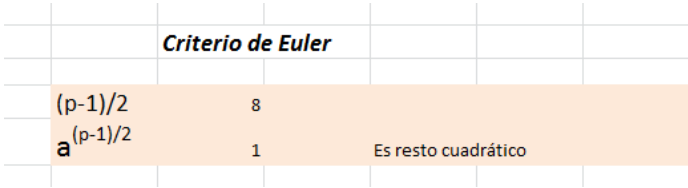
$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) \equiv 0(mod\ p)$$

De esta congruencia deducimos que uno de los paréntesis es congruente con cero, pero ambos no pueden serlo, porque entonces su diferencia, 2, cumpliría $2 \equiv 0$ y eso es imposible para p primo impar. De hecho, si **a** es resto cuadrático, el que se cumple es el segundo, ya que si existe un **x** tal que $\mathbf{x^2 \equiv a \pmod p}$ entonces $a^{(p-1)/2} \equiv x^{p-1} \equiv \mathbf{1 \pmod p}$ de nuevo por el Teorema de Fermat.

Como sólo se puede cumplir una congruencia, si **a** es no resto cuadrático, cumplirá la otra, con el -1.

Este criterio es bastante directo, para saber si un valor es resto cuadrático. Por ejemplo, ¿Es el 14 resto cuadrático respecto al 23?

$14^{(23-1)/2} = 14^{11}$ Calculamos el resto de este último por potencias sucesivas: $14^1 \equiv 14 \pmod{23}$, $14^2 \equiv 12 \pmod{23}$ $14^4 \equiv 12*12 \equiv 6 \pmod{23}$ $14^8 \equiv 6*6 \equiv 13 \pmod{23}$, luego $14^{11} \equiv 13*12*14 \equiv -1 \pmod{23}$, luego no es resto cuadrático.
La herramienta de hoja de cálculo que proponemos, en su tercera hoja, te realiza los cálculos la aplicación de este criterio:



Es conveniente que lo intentes sin hoja de cálculo para practicar. Puedes usar la exponenciación modular (http://hojaynumeros.blogspot.com.es/2012/03/de-la-multiplicacion-rusa-la.html). La usaremos en el siguiente ejemplo:

¿Es resto cuadrático el número 70 respecto al módulo 101?

El módulo 101 es primo e impar, luego podemos usar el criterio de Euler. Bastará elevar 70 a (101-1)/2=50.

Sabemos que 50=32+16+2, luego vamos calculando: $70^1 \equiv -31 \pmod{101}$, : $70^2 \equiv 31*31 \equiv -49 \pmod{101}$, $70^4 \equiv 49*49 \equiv -23 \pmod{101}$, $70^8 \equiv 23*23 \equiv 24 \pmod{101}$, $70^{16} \equiv 24*24 \equiv -30 \pmod{101}$, $70^{32} \equiv 30*30 \equiv -9 \pmod{101}$, y ahora construimos el 50:

$70^{50} \equiv 70^{32}70^{16}70^2 \equiv -9*30*49 \equiv 1 \pmod{101}$, luego según el criterio, 70 sí es resto cuadrático. Si lo compruebas con la herramienta que proponemos descubrirás que su raíz cuadrada es 26.

La aplicación de este criterio nos lleva a propiedades muy interesantes.
La primera es tan elemental que no tenemos que justificarla:

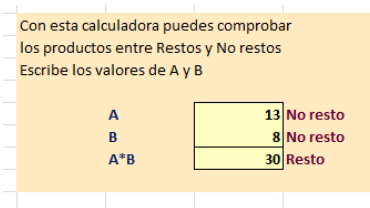
El producto de dos restos o de dos no-restos siempre da un resto, y el de resto con no resto produce un no-resto.

Es decir, poseen estructura alternada, por lo que es fácil representar los restos mediante el signo + y los no restos con el -, y así poder usar la regla de los signos. Se razona fácilmente a partir del criterio de Euler.
Consecuencia inmediata:

El conjunto de restos cuadráticos forma un grupo multiplicativo en Z_p

Por ejemplo, si m=11, los restos son 1, 3, 4, 5 y 9 y los no restos 2, 6,7, 8 y 10 (o bien -1, -3, -4, -5 y -9). Los restos forman un grupo, como se puede verificar fácilmente.

En la segunda hoja de la herramienta que ofrecemos dispones de una calculadora para comprobar las afirmaciones anteriores.



En particular puedes estudiar que si llamamos C al grupo de los restos cuadráticos, las clases laterales tipo a*C tienen cardinal (p-1)/2 y que por tanto el índice de C respecto a Z_p es 2. Vemos una de esas clases. Multiplica el elemento 6 de Z_{11}, por todos los elementos de C, en este caso 1, 3, 4, 5, 9: $6*1\equiv 6 \pmod{11}$, $6*3\equiv 7 \pmod{11}$, $6*4\equiv 2 \pmod{11}$, $6*5\equiv 8 \pmod{11}$, $6*9\equiv 10$

(mod 11). Han resultado valores distintos, luego el cardinal de 6*C es (11-1)/2=5

Símbolo de Legendre

Esta estructura como grupo multiplicativo se expresa muy bien mediante el símbolo de Legendre (por comodidad tipográfica lo escribiremos como (m/p), con los dos números en línea, como hace Apostol).

Llamamos Símbolo de Legendre a una función que asigna a cada par de valores m y p, este último primo e impar, los siguientes valores:

(m/p)=1 si m es resto cuadrático respecto a p
(m/p)=-1 si m es no-resto cuadrático respecto a p
(m/p)=0 en el caso particular en el que m sea múltiplo de p.

En realidad, si recordamos el criterio de Euler, podemos usar una fórmula directa para encontrar el valor de un símbolo de Legendre:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (mod\ p)$$

Según lo explicado anteriormente, es fácil ver que **esta función es multiplicativa**:

(m/p)(n/p)=(mn/p)

Esto tiene una consecuencia práctica, y es que se pueden eliminar cuadrados al calcular el símbolo de un número compuesto.

Nótese que el valor del símbolo de Legendre es una propiedad de las clases de restos y no de los números concretos, por lo que es fácil entender que si a≡b (mod p). entonces (a/p)=(b(p)

PROPIEDADES DE LOS RESTOS CUADRÁTICOS

El criterio de Euler da lugar a propiedades interesantes de los restos cuadráticos respecto a ciertos tipos de primos. Los vemos:

-1 es un resto para todos los primos del tipo 4N+1 y no resto para los del tipo 4n+3

Es una consecuencia del criterio de Euler, pues (p-1)/2 sería par en el primer caso, e impar en el segundo, luego al elevar -1 a esa cantidad producirá un 1 (ser resto) para p=4N+1 y -1 (no resto) en el otro caso.

Esto quiere decir que la ecuación $\mathbf{x^2 + 1 \equiv 0 \pmod p}$ tiene solución para p=4N+1 y no la tiene en el segundo caso. Podemos expresarlo también como que 1 posee una raíz cuadrada entre las clases de restos módulo p

Podemos diseñar un pequeño esquema con la hoja de cálculo que usamos en esta serie:

Módulo	61
Raiz de -1	11

En la celda del 11 hemos escrito =RESTOCUAD(-1;61). Como este módulo es del tipo 4N+1, obtenemos la solución 11, ya que 11*11 módulo 61 es igual a 60, es decir, la clase de restos -1

Si hubiéramos usado módulo 11, que es del tipo 4N+3. Obtendríamos un cero, que es la señal de que -1 no es resto cuadrático:

Módulo	11
Raiz de -1	0

Esta propiedad se puede expresar así:

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

2 es resto cuadrático para todos los primos del tipo 8N+1 y 8N+7, y no resto para los demás

También podemos, en nuestra hoja de cálculo, crear un esquema para comprobar esta propiedad siguiendo la estructura que usamos en la anterior.

Módulo	11
Raiz de 2	0

Vemos que 11 no pertenece al tipo 8N+1 ni al 8N+7, y para el 2 no devuelve raíz cuadrada (el cero es una señal)

Módulo	31
Raiz de 2	8

Sin embargo, al usar el módulo 31, que es del tipo 8N+7, el 2 presenta raíz cuadrada 8, y es resto cuadrático.

No es sencilla la demostración. Tienes una en ***Fundamentos de la Teoría de los números*** de Vinogradov.

Encontrarás propiedades similares para el -3 y el 5 en el documento de Rafael Parra "Restos cuadráticos y Ley de reciprocidad cuadrática") http://www.hojamat.es/parra/restocuad.pdf. Las puedes comprobar con el esquema propuesto, sustituyendo el 2 por otros valores.

Ley de reciprocidad cuadrática

La propiedad más importante de estos restos es la ley de reciprocidad cuadrática, enunciada y demostrada por Gauss en 1801 en su libro Disquisitones Arithmeticae. Con palabras la podemos expresar así:

Dados dos primos impares p y q, si ambos pertenecen al tipo 4k+3, entonces p es resto cuadrático módulo q si y sólo si q no lo es de p. Si alguno de los primos pertenece al tipo 4k+1 entonces o bien ambos son restos uno del otro, o bien ninguno lo es.

Expresada así o de forma similar la propiedad resulta oscura. Sin embargo su significado queda claro con el uso de los símbolos de Legendre. En ese caso la propiedad se reduce a esta identidad:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Así se explica mejor: Si uno de los dos, p o q, es del tipo 4k+1, el exponente del -1 será par y el segundo miembro valdrá 1, con los que los símbolos del primero serán ambos iguales a 1 (restos recíprocos) o bien -1 (ninguno es resto).
Si ambos son del tipo 4k+3 el exponente será impar, el segundo miembro -1 y los símbolos tendrán signo opuesto: Si uno de los primos es resto del otro, no se dará la reciprocidad.

En textos y documentos varios dispones de ejercicios sencillos que muestran la utilidad de esta propiedad. Nosotros la hemos incluido en nuestra hoja de cálculo.

Escribe dos números primos e impares

	Valores	Tipo
P	43	4N+3
Q	37	4N+1

Símbolos de Legendre	(P/Q)	-1
	(Q/P)	-1

No son restos uno del otro

Al escribir los dos primos la hoja analiza si son del tipo 4N+3 o 4N+1, calcula después los restos y comprueba la propiedad.

Como se trabaja con valores 1 y -1, algunos manuales expresan esta propiedad mediante esta otra identidad equivalente:

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

Así se ve mejor cómo calcular un valor de (p/q) si se conoce el de (q/p).

GRUPOS DE POTENCIAS EN ZN

ÍNDICE O GAUSSIANO DE UN RESTO EN ZN

Iniciamos hoy el desarrollo de toda una teoría perteneciente a la Aritmética Modular, la de las raíces primitivas y temas afines.

Teoría previa

Resumimos brevemente la teoría previa que es conveniente conocer antes de seguir esta serie de entradas:

Comenzamos con la estructura $\mathbf{Z_m}$ formada por los restos posibles al dividir un número entre m. Ya sabes que este conjunto es la base de la Aritmética Modular (o del reloj)

Puedes repasar las páginas

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

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

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

Este conjunto $\mathbf{Z_m}$ con la suma y la multiplicación forma un **anillo cíclico de m elementos**. Por esta estructura cíclica se pensó en llamarles ***anillos*** por primera vez. Es un anillo con unidad, por lo que puede contener elementos inversibles. De ellos trataremos aquí.

Un elemento A de Z_m es inversible si existe otro elemento X de Z_m tal que $A*X \equiv 1 \pmod m$. Esta ecuación se sabe que tiene solución única siempre que A sea primo con el modulo m. **Luego los restos primos con m son inversibles**.

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

Llamamos **divisor de cero** en un anillo a aquel elemento A que multiplicado por cierto elemento no nulo C del anillo, da un producto nulo: A*C=0. Si que A tiene factores comunes con m, **es un divisor de cero**, porque si D=MCD(A,m), tendremos que A=A'*D y m=m'*D. Multiplicando A por m' (que es no nulo) resulta Am'=A'D*m/D=A'm, que es congruente con cero, luego $A*m' \equiv 0 \pmod m$ 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

  (http://hojaynumeros.blogspot.com.es/2012/06/la-herencia-de-euclides-1-el-algoritmo.html).

- **Si el elemento A no es primo con m, es un divisor de cero, y por tanto no inversible**.

  Grupo de inversibles

  El producto de dos inversibles A y B también lo es, y su inverso es $B^{-1}*A^{-1}$, 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** para la multiplicación**, 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.

Se cumple el llamado Teorema de Euler

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

para todo **a** primo con m o *unidad*.

Orden multiplicativo, índice o gaussiano de un elemento

Dado un elemento inversible **a**, llamaremos ***orden*** de ese elemento al mínimo número entero tal que $\mathbf{a}^r \equiv \mathbf{1}$. Según el teorema anterior, ese valor existe y puede ser φ(m) y todos sus múltiplos. Si es menor, ha de ser un divisor suyo. En efecto, supongamos que φ(m) no fuera múltiplo del orden r. Entonces efectuando la división entera entre ambos quedaría 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)**. Toda potencia que sea igual a 1 tendrá un exponente múltiplo de ese orden. Hay muchas formas de representar el orden o gaussiano. Aquí por comodidad tipográfica representaremos el gaussiano de N respecto al módulo M como G(N,M)

Podíamos habernos ahorrado el razonamiento anterior recordando el Teorema de Lagrange para grupos, que afirma que el orden de un subgrupo H es divisor del orden del grupo G. En este caso este último es **φ(m)** y como las potencias de **a** forman un grupo monógeno, su orden será divisor de **φ(m)**.

Vemos algunos ejemplos:

Orden de 5 módulo 8: Como 5 es primo con 8 y φ(8)=4, el orden podrá ser 2 o 4: 5^2=25≡1(8, luego el orden de 5 con módulo 8 es 2, o G(5,8)=2

Orden del 3 respecto al 7: φ(7)=6, luego el orden podrá ser 2, 3 o 6. Probamos: 3^2=9≡2(7, 3^3=27≡6(7, 3^6=729≡1 (7luego el orden o gaussiano de 3 es 6, G(3,7)=6

Estudio con hoja de cálculo

Deseamos desarrollar este tema con calma y en varias entradas. Así que nos pararemos un poco, con la ayuda de la hoja de cálculo alojada en

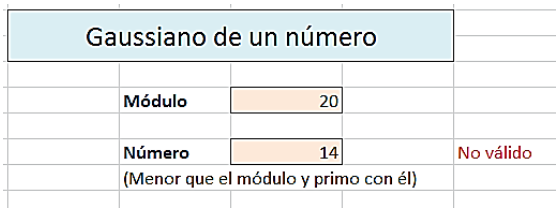
http://www.hojamat.es/sindecimales/congruencias/herramientas/herrcong.htm#gaussiano

Distinguiremos, en principio, tres niveles de complejidad en el descubrimiento del gaussiano de un número.

NIVEL 1

La hoja funciona sólo con las fórmulas de celdas, sin macros. Para ello basta escribir el número N y el módulo M, y calcular en columna las potencias de N en el **grupo de las unidades Z^*_m**. En la hoja hemos incluido el cálculo del MCD(N,M), que ha de ser 1 y, en caso contrario, se avisa del error.

En la imagen hemos escrito dos números no primos entre sí y la hoja nos avisa:



Simultáneamente, en las columnas del NIVEL 1, se construyen las potencias para ver cuál de ellas es igual a 1, con lo que obtendremos el gaussiano de N. A continuación reproducimos el cálculo correspondiente a 5 módulo 13:

	NIVEL 1	
	Potencias sin analizar	
	Exponente	Resto
5	1	5
	2	12
	3	8
	4	1
	5	5
	6	12
	7	8
	8	1
	9	5
	10	12
	11	8
	12	1

A simple vista se descubre que el gaussiano de 5 módulo 13 es 4, porque es el mínimo exponente al que hay que elevar 5 para obtener resto 1 módulo 13.

Si te interesa cómo se construyen estas columnas, revisa la hoja, y

estudia especialmente las fórmulas de las potencias, que son del tipo

=SI(C15<=G5;RESIDUO(B13*D14;G5);" ").

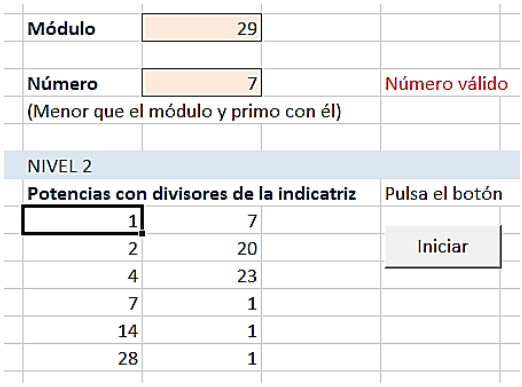
Podemos interpretarlas como “si el exponente no llega al módulo, multiplicamos la anterior potencia por N y calculamos el residuo”

De esta forma puedes descubrir el gaussiano por simple recorrido columna abajo hasta encontrar el primer 1. Como verás en próximas entradas, las potencias resultantes son periódicas, y su periodo es el orden del número, en este caso, 4.

NIVEL 2

Podemos simplificar las columnas si sólo probamos con los divisores de **φ(m)**. Esto ya requiere un poco de programación, ya que la hoja no puede encontrar los datos sólo con celdas y fórmulas. Hemos creado una subrutina y un botón para descubrir el gaussiano con menos pasos. Si te interesa la programación puedes investigar en el código Visual Basic. Lo que hace es calcular la indicatriz φ(m) y recorrer sus divisores para encontrar el exponente que se convierte en gaussiano.

En la imagen están contenidas las columnas correspondientes a 7 módulo 29:

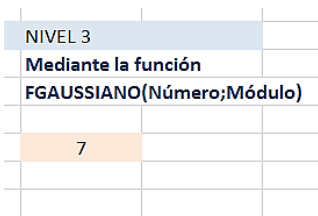


La indicatriz de 29 es 28, porque es primo. En la hoja se recorren los divisores de 28, lo que simplifica el esquema. Vemos que el primer 1 aparece en el exponente 7, luego ese será el gaussiano de 7.

NIVEL 3

Es muy útil para nuestros estudios posteriores disponer del gaussiano en forma de función que tenga como parámetros un número y un módulo y nos devuelva el orden de ese número (o cero si no es primo con el módulo)

En la parte derecha de la hoja hemos utilizado esa función para encontrar rápidamente el gaussiano de un número, en el caso de la imagen, de 7 módulo 29.



Su sintaxis es FGAUSSIANO(NÚMERO;MÓDULO), en el ejemplo, FGAUSSIANO(7;29)

Está implementado para números pequeños. Para otros mayores sería preferible usar la descomposición factorial. La versión que insertamos a continuación no es demasiado eficiente, pero es sencilla de entender. Quizás no puedas reproducirla, por carecer de algunas funciones, pero lo importante es que entiendas su estructura.

Public Function fgaussiano(n, m)
Dim f, i, p, e
f = 0 ‘se comienza declarando nula la función, por si no son coprimos
If mcd(n, m) = 1 Then ‘son coprimos
p = n ‘inicio de las potencias del número
i = 1 ‘contador
e = euler(m) ‘encontramos la phi de Euler
While i <= e And f = 0 ‘nos detenemos cuando encontremos potencia 1
p = p Mod m ‘encontramos el residuo de la potencia
If p = 1 Then f = i ‘se encontró el orden f
p = p * n ‘siguiente potencia
i = i + 1
Wend
End If
fgaussiano = f ‘se recoge el valor de f
End Function

Gaussiano de las potencias de un resto

Supongamos que un resto a tiene como gaussiano t, es decir g(a)=t. Es fácil demostrar que el gaussiano de una potencia de a, sea por ejemplo a^k, equivale a

$$g(a^k) = \frac{t}{MCD(k,t)}$$

Por ejemplo, G(4,29)=14 y si elevamos el 4 a la sexta se tendrá G(4^6,29)=14/MCD(6,14)=14/2=7

Se puede razonar así: t divide a MCM(k,t), luego se cumplirá que $a^{MCM(k,t)} \equiv 1$, por ser t el menor exponente con esa propiedad. Efectuamos unos cambios en la expresión:

$a^{MCM(k,t)} = (a^k)^{MCM(k,t)/k} = (a^k)^{t/MCD(k,t)} \equiv 1$, luego t/MCD(k,t) puede ser el gaussiano de a^k. Sólo falta demostrar que es el más pequeño con esa propiedad. En efecto, si $(a^k)^m \equiv 1$, será $a^{km} \equiv 1$, con lo que km será múltiplo de t, pero como también es múltiplo de k, lo será del MCM(k,t), luego m>= MCM(k,t)/k=t/MCD(k,t), luego esta expresión t/MCD(k,t) es la menor con esta propiedad, lo que la convierte en el gaussiano de a^k.

En esta tabla tienes un ejemplo de lo demostrado. El resto 4 tiene un gaussiano igual a 14 respecto al

módulo 29, luego el gaussiano de sus potencias será un divisor de 14, precisamente el MCD de 14 y el exponente. Estúdialo bien:

Exponente K	Potencia	Gaussiano	MCD(K,14)
1	4	14	1
2	16	7	2
3	6	14	1
4	24	7	2
5	9	14	1
6	7	7	2
7	28	2	7
8	25	7	2
9	13	14	1
10	23	7	2
11	5	14	1
12	20	7	2
13	22	14	1

Observamos 6 potencias con el mismo gaussiano 14, que se corresponden con los exponentes primos con 14, que son 6, porque **φ(14)**=6

Otras seis potencias tienen gaussiano igual a 7. Se trata de los números pares, en los que MCD(2N,14)=2, y por la fórmula anterior su gaussiano será 14/2=7

Por último, la potencia de exponente 7 presenta un gaussiano igual a 14/7=2.

Hemos descubierto que en el grupo monógeno engendrado por las potencias de un elemento de Zm no tienen que poseer el mismo valor del gaussiano, pero eso era de esperar, porque ocurre lo mismo en todo el grupo Zm.

SUBGRUPOS CÍCLICOS EN ZM*

Según la entrada anterior, todo elemento **a** perteneciente a Z_m^* (conjunto de inversibles del grupo multiplicativo Z_m) posee un ***orden g(a)***, que es el mínimo número entero tal que $\mathbf{a^r \equiv 1}$. Ese orden siempre es divisor de la indicatriz de Euler de m, φ(m), o igual a ella.

$$a^{g(a)} \equiv 1 \ (mod\ m$$

Sabemos que las potencias de un mismo elemento **a** forman siempre un grupo cíclico **< a >**. En el caso de un elemento de Z_m^* estos grupos tendrán el mismo orden que el elemento que los genera, es decir g(a). En efecto, las potencias a^0, a^1, a^2,…$a^{g(a)-1}$ son todas distintas (si dos fueran iguales, al dividirlas resultaría una potencia del elemento igual a la unidad con exponente menor que g(a), en contra de la definición de g(a)). Sus productos pertenecen al conjunto, ya que si sobrepasan $a^{g(a)}$, al ser este la unidad, se puede eliminar de dicho producto.

Por ejemplo, con módulo 13, el orden o gaussiano de 5 es 4, luego $5^0 \equiv 1$ (mod 13, $5^1 \equiv 5$ (mod 13, $5^2 \equiv 12 \equiv -1$ (mod 13 y $5^3 \equiv 8 \equiv -5$ (mod 13 formarán un subgrupo de Z_{13}. Lo podemos representar así: < 5 > = {1, 5, -1, -5}

Así que el concepto de orden de un elemento coincide aquí con el de orden del grupo cíclico que

engendra. Este grupo es el más pequeño que contiene ese elemento. Según la teoría general de grupos cíclicos, será abeliano (conmutativo) y ***único***, para un valor dado del orden.

Según los párrafos anteriores, en un subgrupo de potencias de un elemento de gaussiano g, existen φ(g) elementos con el mismo gaussiano, pero como hemos señalado que este grupo es único para ese valor de g, podremos afirmar:

El conjunto de elementos pertenecientes a Z_m* con un gaussiano concreto g tiene un cardinal de φ(g).

Si volvemos al ejemplo concreto del módulo 29 que vimos más arriba, esta sería la descomposición de los elementos de Z_{29} según su gaussiano. Cada uno de los elementos engendrará un subgrupo de orden idéntico a su gaussiano, y todos los que compartan el mismo valor g de ese gaussiano formarán un subconjunto de φ(g) elementos:

Gaussiano	Conjunto con el mismo gaussiano	Función de Euler
28	2, 3, 8, 10, 11, 14, 15, 18, 19,26, 27	ϕ(28)=12
14	4, 5, 6, 9, 13,22	ϕ(14)=6
7	7, 16, 20, 23, 24, 25	ϕ(7)=6
4	12, 17	ϕ(4)=2
2	28	ϕ(2)=1
1	1	ϕ(1)=1
	Suma	28

Esta tabla es muy útil para repasar lo que hemos explicado hasta ahora:

29 es primo, luego Z^*_{29} contendrá 28 elementos inversibles, y poseerán como gaussiano uno de los divisores de 28: 28, 14, 7, 4, 2 y 1. Según lo explicado, cada conjunto de elementos con el mismo gaussiano k tendrá un cardinal de φ(k). En la tabla vemos que aparecen 12 elementos con gaussiano 28, y φ(28)=12. Luego, tenemos 6 con gaussiano 14 y otros 6 con el valor 7. Finalmente, otros cuatro presentan los gaussianos 4, 2 y 1. Si los sumamos todos, obtenemos 28= φ(29), que es el cardinal de Z^*_{29}.

Con esta tabla hemos comprobado la expresión de 28 en suma de φ(28)+φ(14)+φ(7)+φ(4)+ φ(2)+φ(1), que es un caso de la fórmula general:

$$n = \sum_{d:n} \varphi(d)$$

Un número entero coincide con la suma de las indicatrices de sus divisores.

Exponente	Resto
1	5
2	25
3	13
4	9
5	17
6	1
7	5
8	25
9	13
10	9
11	17
12	1
13	5
14	25
15	13
16	9
17	17
18	1

Periodicidad de las potencias

Si en lugar de considerar sólo las potencias de exponente menor que g(a) las estudiamos todas, es evidente que son periódicas, pues $a^{k+tg(a)}=a^k*a^{tg(a)}=a^k*1=a^k$

De paso hemos demostrado que el periodo de las potencias de a es precisamente g(a). Lo puedes comprobar con la hoja de cálculo que presentamos en anteriores párrafos.

En la tabla figuran las potencias de 5 respecto al módulo 28. El orden de Z_{28}^* es 12 (φ(28)), el orden del 5 respecto a 28 es 6 (divisor de 12), y se produce, como puedes comprobar, una periodicidad de periodo 6.

Además, los integrantes de cada ciclo son los elementos del grupo engendrado por el elemento 5: {5, 25, 13, 9, 17, 1} En la anterior entrada descubrimos que cada elemento de este tipo de grupos tiene un gaussiano diferente, como puedes ver en la siguiente tabla:

Exponente K	Potencia	Gaussiano
1	5	6
2	25	3
3	13	2
4	9	3
5	17	6
6	1	1

Todos los gaussianos son divisores de 12 (φ(28)).

Subgrupos generados

Ha quedado claro que las potencias de un elemento no tienen que compartir el mismo gaussiano, luego los

subgrupos que vamos a recorrer ahora no tienen por qué coincidir con los conjuntos estudiados más arriba. Lo que sí queda claro es que, dentro del subgrupo engendrado por un elemento, pueden aparecer subgrupos formados a partir de una potencia con un gaussiano menor.

Hemos preparado nuestra hoja GAUSSIANO para que dado un resto en Z^*_n encuentre el subgrupo que engendra mediante sus potencias. En la siguiente entrada estudiaremos los elementos que engendran todo Z^*_n, pero ahora los repasaremos todos. Para entenderlo mejor, estudia esta primera tabla que hemos creado, con módulo 13 y resto 11:

Subgrupo de potencias

Exponente	*G0*	*Gaussiano*	*Subgrupos*					
1	11	12						
2	4	6	4	3	12	9	10	1
3	5	4	5	12	8	1		
4	3	3	3	9	1			
5	7	12						
6	12	2	12	1				
7	2	12						
8	9	3	9	3	1			
9	8	4	8	12	5	1		
10	10	6	10	9	12	3	4	1
11	6	12						
12	1	1	1					

En la primera columna figuran las potencias de 11, que como su gaussiano es 12, posee ese número de elementos. Este es G0, el subgrupo creado por las potencias de 11 en Z^*_{13}. Tal como vimos anteriormente, los elementos de ese grupo no han de tener gaussiano 12. De hecho aparecen todos los divisores de 12: 6, 4,

3, 2 y 1. También vimos que las potencias de cada uno de ellos forman subgrupos del principal. Según la teoría de grupos, estos son únicos para cada orden, aunque se engendren con elementos distintos. Compruébalo:

- G6: Grupo de orden 6: {4, 3, 12, 9, 10, 1} Engendrado en la tabla por 4 y 10.
- G4: Grupo de orden 4: {5, 12, 8, 1} con generadores 5 y 8
- G3: Grupo de orden 3: {3, 9, 1} engendrado por 3 y 9.
- G2: Grupo de orden 2: {12, 1} con generador 12.
- GE: Grupo trivial: {1}

Obsérvese que el número de generadores de cada subgrupo coincide con el valor de su indicatriz de Euler. Así tenemos $\varphi(6)= \varphi(4)=\varphi(3)=2$ y por eso los primeros subgrupos poseen dos generadores. Sin embargo, como $\varphi(2)=1$, el penúltimo tiene un solo generador.

Como son grupos de potencias, se cumple que si el gaussiano de **a** es divisor del de **b**, el grupo engendrado por **a** es subgrupo del engendrado por **b**.

Todas las potencias de 11 pertenecen a un grupo, y algunas a varios.

Para construir estas tablas, busca en Gaussiano.xlsm la hoja “Subgrupo engendrado” y rellena tan sólo el módulo y el elemento dado. El resto lo construye la

hoja. Aquí tienes otro ejemplo, con módulo 15 y elemento 7:

Subgrupos engendrados con potencias

				Módulo	14		Su gaussiano es	6
				Número	5		Número válido	
				(Menor que el módulo y primo con él)				
Subgrupo de potencias								
Exponente	***G0***	***Gaussiano***	***Subgrupos***					
1	5	6						
2	11	3	11	9	1			
3	13	2	13	1				
4	9	3	9	11	1			
5	3	6						
6	1	1	1					

Indicador de un elemento

Dado cualquiera de los subgrupos que estamos estudiando, cualquier elemento de Z^*_n posee una potencia perteneciente a cada uno de ellos. En efecto, dado un subgrupo S, si un elemento **a** pertenece a él, bastará elevarlo a 1. Si no pertenece, lo elevamos a **n** para engendrar la unidad, pero hay casos en los que existen otros enteros positivos k<n tales que a^k pertenece a S. Al menor de ellos le llamaremos *indicador de* ***a*** con respecto a S. Hemos visto que puede valer **1** o **n**. Observa la tabla anterior: el indicador de 5 respecto al subgrupo {11, 9, 1} es 2, porque 5^2=11 es la potencia positiva más pequeña que pertenece al subgrupo. Igualmente, el 3 es el indicador respecto a {13, 1}

RAÍCES PRIMITIVAS

En los apartados anteriores estudiamos el grupo multiplicativo Z^*_n de las unidades en Z_n (números

coprimos con **n**). Su orden coincide con φ(n). Cualquier elemento **a** de ese grupo engendrará a su vez un subgrupo cíclico **< a >** mediante sus potencias. Por el Teorema de Lagrange, el orden de ese subgrupo será un divisor de φ(n) y recibe el nombre de gaussiano g de ese elemento. Recordemos que esto implica que $\mathbf{a^g \equiv 1}$ **(mod n**. También vimos que el número de generadores de < a > coincide con φ(g).

En esta entrada estudiaremos **las raíces primitivas**, que son aquellos elementos que engendran todo Z^*_n, o lo que es equivalente, aquellos cuyo gaussiano coincide con **φ(n)**. Según lo que hemos recordado, el número de esas raíces primitivas puede coincidir con φ(φ(n)), y de hecho es así **si $\mathbf{Z^*_n}$ es cíclico**. Usamos la palabra "puede" pues, como ya veremos, **no todos los módulos poseen raíces primitivas**.

En la tercera hoja de nuestra herramienta Gaussiano.xlsm

http://www.hojamat.es/sindecimales/congruencias/herramientas/herrcong.htm#gaussiano

podemos descubrir el valor del gaussiano de todos los elementos de Z^*_n e identificar las raíces primitivas como aquellas cuyo gaussiano sea igual a φ(n). Aquí tienes la tabla correspondiente al módulo 14

			Módulo	14
			Indicatriz	6
			Núm. Posible de raíces	2
Inversibles	Gaussiano	Es raíz primitiva		
1	1			
3	6	Raíz primitiva		
5	6	Raíz primitiva		
9	3			
11	3			
13	2			

Explicamos la tabla: El módulo es 14, luego existirán tantos inversibles como indique φ(14)=6. En efecto, Z^*_{14} = {1, 3, 5, 9, 11, 13}, conjunto de 6 elementos, como puedes comprobar en la tabla. Ahora bien, las raíces primitivas son generadores de todo Z^*_{14}, y su número ha de ser φ(φ(14)) = φ(6) = 2.

Esto es así porque si una raíz primitiva se eleva a un exponente primo con φ(m), resulta otra raíz primitiva, en virtud de la fórmula que estudiamos en una entrada anterior

$$g(a^k) = \frac{t}{MCD(k,t)}$$

En efecto, aparecen las dos raíces primitivas 3 y 5. Recorre sus potencias y comprobarás que engendran todo el grupo: $3^0 \equiv 1$, $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 13$, $3^4 \equiv 11$ y $3^5 \equiv 5$. Igualmente, $5^0 \equiv 1$, $5^1 \equiv 5$, $5^2 \equiv 11$, $5^3 \equiv 13$, $5^4 \equiv 9$ y $5^5 \equiv 3$.

Es fácil comprender entonces que si Z^*_k admite raíces primitivas tendrá carácter de cíclico, ya que está generado por las potencias de un mismo elemento. Según esto, en virtud de una propiedad general de

estos grupos, Z^*_k estaría engendrado por cualquier potencia de una raíz primitiva cuyo exponente fuera coprimo con φ(k), ya que, en caso contrario engendraría sólo un subgrupo propio de Z^*_k. Todas esas potencias serían también raíces primitivas, luego su número será φ(φ(k)), como ya comprobamos más arriba. Observa esta tabla y comprueba que todas las raíces primitivas tienen exponentes coprimos con la indicatriz:

Módulo	19	
Indicatriz	18	
Núm. Posible de raíces	6	
Potencias de 2		Gaussiano
1	2	18
2	4	9
3	8	6
4	16	9
5	13	18
6	7	3
7	14	18
8	9	9
9	18	2
10	17	9
11	15	18
12	11	3
13	3	18
14	6	9
15	12	6
16	5	9
17	10	18
18	1	1

El módulo es 19, su indicatriz 18, 2 es una raíz primitiva, con gaussiano 18, y observa hacia abajo que las demás raíces primitivas son potencias del 2 con exponentes coprimos con 18: {1, 5, 7, 11, 13, 17}, seis en total.

Otros módulos no tienen raíces primitivas, como el 30:

				Módulo	30
				Indicatriz	8
				Núm. Posible de raíces	4
	Inversibles	Gaussiano	Es raíz primitiva		
	1	1			
	7	4			
	11	2			
	13	4			
	17	4			
	19	2			
	23	4			
	29	2			

Vemos en la tabla que ningún elemento presenta gaussiano máximo 8 (φ(30)=8), luego con módulo 30 no existen raíces primitivas. Se puede demostrar (no es simple, es un conjunto de teoremas que puedes consultar en los textos especializados) que sólo poseen raíces primitivas **los módulos 2, 4, p^k y $2p^k$, siendo p primo impar y k>=1**. El 30=2*3*5 no es de ninguno de estos cuatro tipos, y carece de raíces primitivas. El 14 es del tipo **$2p^k$** y sí tiene raíces primitivas.

Para ayudarte a entender y practicar con esta situación hemos añadido dos rutinas a nuestra hoja Gaussiano.xlsm. Una encuentra la menor raíz primitiva de un módulo **m**, y te avisa si no existe tal raíz. Se basa en una búsqueda sistemática desde 1 hasta m-1. Este es su código:

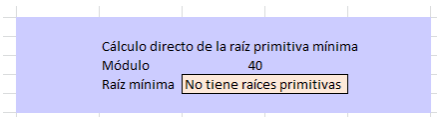
Public Function minraiz(m) As Variant
Dim o, g, j, mr

mr = 0: o = sacaprimos(m): g = euler(m) ‘encuentra la indicatriz y los factores primos

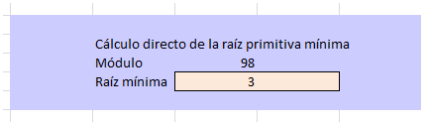
If m = 2 Or m = 4 Or (o = 1 And primo(1) <> 2) Or (o = 2 And primo(1) = 2 And expo(1) = 1 And primo(2) <> 2) Then
j = 1 ‘esta parte actúa si el módulo posee la factorización adecuada
While j < m And mr = 0
If fgaussiano(j, m) = g Then mr = j ‘búsqueda de la primera raíz primitiva
j = j + 1
Wend
minraiz = mr
Else
minraiz = "No tiene raíces primitivas" ‘caso en el que el módulo no tiene raíces primitivas
End If
End Function

No tienes que usar ningún botón, porque el resultado aparece automáticamente.

Por ejemplo, con módulo 40=2^3*5 nos devuelve el resultado



40 no pertenece a ninguno de los cuatros tipos de números que poseen raíces primitivas. Sin embargo, con el 98 nos resulta:



Cálculo directo de la raíz primitiva mínima	
Módulo	98
Raíz mínima	3

Este resultado coincide con el obtenido mediante el botón “Inicio”:

Inversibles	Gaussiano	Es raíz primitiva
1	1	
3	42	Raíz primitiva
5	42	Raíz primitiva
9	21	
11	21	
13	14	
15	7	
17	42	Raíz primitiva
19	6	

Este módulo de hoja de cálculo no te añade ningún aprendizaje nuevo, pero te lo facilita. El siguiente sí es más conceptual.

Criterio de los factores de la indicatriz

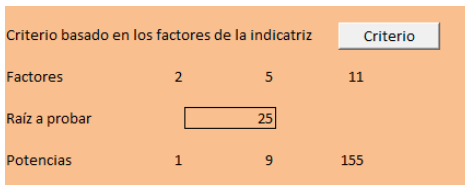
Si buscamos la indicatriz del módulo, φ(m), y la descomponemos en factores primos, sean estos p_1, p_2, p_3,…(escritos sin exponentes), un resto **a** será raíz primitiva si se cumple

$$a^{\varphi(m)/p_i} \equiv r, con\ r \neq 1\ \forall i$$

Si todas las potencias presentan restos distintos de 1, **a** será raíz primitiva, y si por el contrario, alguna de las potencias es congruente con 1, ese resto **a** no será raíz primitiva. La justificación no es muy complicada:

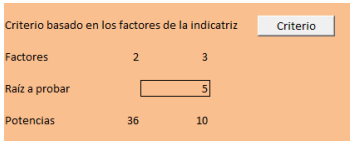
Si una de las potencias es congruente con 1, el gaussiano de a sería menor que φ(m), y no podría ser raíz primitiva. Por el contrario, si ninguna es congruente con 1, sí ha de serlo, ya que, en caso contrario, existiría un divisor propio de φ(m), sea **g**, que sería el gaussiano de a y $a^g \equiv 1$. Además, como los cocientes $\varphi(m)/p_i$ son los divisores maximales de φ(m), uno al menos de ellos sería múltiplo o igual al gaussiano, con lo que la potencia $a^{\varphi(m)/pi} \equiv 1$ en contra de lo supuesto.

El siguiente módulo es una simple curiosidad y comprobación de lo anterior.



La anterior imagen se corresponde con el módulo 242, cuya indicatriz, 110, posee los factores primos 2, 5 y 11. Hemos aplicado el criterio al resto 25, y vemos que no es raíz primitiva, porque la primera potencia $25^{110/2}$ es congruente con 1. Efectivamente, su gaussiano es casualmente ese: 110/2=55.

El siguiente ejemplo es el criterio aplicado al resto 5 respecto al módulo 37



La indicatriz de 37 es 36, con factores 2 y 3. La aplicación del criterio nos da dos potencias congruentes con 36 y 10 respectivamente, luego 5 es una raíz primitiva.

ÍNDICES MODULARES

En el apartado anterior estudiamos las raíces primitivas, elementos del grupo multiplicativo Z^*_n de las unidades en Z_n (números coprimos con **n**), tales que su gaussiano es máximo y coincidente con φ(n). Estas raíces, mediante sus potencias, engendran todo Z^*_n, luego un elemento inversible cualquiera coincidirá con una potencia de la raíz primitiva. El exponente comprendido entre 0 y φ(n)-1 que logra esta coincidencia recibe el nombre de **índice del elemento respecto a la raíz primitiva**. También es llamado **logaritmo discreto**.

Es decir; si **a** es una raíz primitiva y **b** un elemento inversible, existe un exponente k en el intervalo (0, φ(n)-1) tal que $\mathbf{a^k \equiv b}$, y a ese exponente le llamaremos índice de **b** respecto a **a**.

Por ejemplo, el módulo 7 posee dos raíces primitivas. La raíz 3 engendra mediante potencias todos los elementos desde 1 a 6 (por ser 7 primo son todos inversibles), $3^0 \equiv 1$, $3^1 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$,$3^4 \equiv 4$, $3^5 \equiv 5$. Cada uno de los exponents es el índice de ese elemento.

La función índice que asigna a cada elemento inversible el exponente de la menor potencia de la raíz primitiva que lo engendra la podemos representar por $ind_a(b)$ o simplemente ind(b) si se conoce la raíz. También podemos representarlo como un logaritmo, que en este caso recibe el nombre de *logaritmo discreto*. En el ejemplo anterior $ind_3(6)=3$, $ind_3(4)=4$,…Si existe una raíz primitiva, todos los elementos inversibles de Z_m tendrán definido el índice.

Al ser un exponente, las propiedades del índice o logaritmo discreto son previsibles (supongamos módulo m):

- $Ind_a(1)=0$
- $Ind_a(a)=1$
- $Ind(a*b)=ind(a)+ind(b)$
- $Ind(a^k)=k*ind(a)$
- $Ind_a(x)=ind_a(b)*ind_b(x)$ (fórmula del cambio de base)
- $Ind_a(x^{-1})= \varphi(m)-Ind_a(x)$

El cálculo de los índices en grupos complejos no es fácil, aunque se han creado muchos algoritmos eficientes, y por eso los índices son usados en algunos sistemas criptográficos.

Aquí nos limitaremos, como siempre, a casos sencillos con los que aprender los conceptos. Hemos creado en nuestra hoja Gaussiano.xlsm

http://www.hojamat.es/sindecimales/congruencias/herramientas/herrcong.htm#gaussiano

un confeccionador automático de tablas de índices para un módulo dado. Sólo tienes que escribir dicho módulo, y pulsar un botón para que aparezca la tabla, si es que existen raíces primitivas. Aquí tienes la del módulo 54:

Módulo 54 Tabla

	Raíces primitivas					
Inversibles	**5**	**11**	**23**	**29**	**41**	**47**
1	18	18	18	18	18	18
5	1	17	7	5	13	11
7	14	4	8	16	2	10
11	17	1	11	13	5	7
13	16	2	4	8	10	14
17	3	15	3	15	3	15
19	6	12	6	12	6	12
23	13	5	1	11	7	17
25	2	16	14	10	8	4
29	11	7	5	1	17	13
31	4	14	10	2	16	8
35	15	3	15	3	15	3
37	12	6	12	6	12	6
41	7	11	13	17	1	5
43	8	10	2	4	14	16
47	5	13	17	7	11	1
49	10	8	16	14	4	2
53	9	9	9	9	9	9

En columna aparecen los elementos inversibles de Z_{54}, que hay 18, porque $\varphi(54)=18$. En la fila superior tenemos las raíces primitivas, que por ser 54 de la forma $2p^k$ ($2*3^3$), existen con seguridad, y son 6, ya que

φ(φ(54))=6. Con ella podemos encontrar el índice de cualquier inversible. Por ejemplo, el índice de 37 respecto a 23 es 12, lo que indica que 23^{12}=37.

Ecuaciones potenciales

Las tablas de índices nos pueden servir para resolver la ecuación

$$x^n \equiv a \ (mod\ m$$

El comportamiento de los índices como logaritmos nos permite transformar esta ecuación en otra lineal, eligiendo cualquier raíz primitiva **b** y aplicando índices en ambos miembros respecto a ella.

$$n \times ind_b(x) \equiv ind_b(a)\ (mod\ \varphi(m)$$

Según la teoría de las ecuaciones lineales en Z_m, si llamamos **d** al MCD(n, φ(m)), el índice de **a** ha de ser múltiplo de **d** para que exista solución. En ese caso basta despejar el índice de x y buscar después el valor de x en las tablas. Podíamos haber automatizado todo el proceso, pero parece que se aprende más de esta forma.

Ejemplo: Resolver $x^6 \equiv 37$ (mod 54

En primer lugar encontramos que φ(54)=18 (ver tabla y párrafos anteriores), luego d=MCD(6,18)=6. En la tabla citada buscamos el índice de 37 respecto a la raíz primitiva 5 y encontramos que es 12. Por tanto, como 12 es múltiplo de 6, deberá existir una solución (en realidad, según las propiedades de las ecuaciones lineales, deberían aparecer 6). Tomamos índices respecto al 5:

$6*ind_5(x) \equiv ind_5(37) \pmod{54} \equiv 12$

$ind_5(x) \equiv 12/6=2.$

Buscamos en la tabla qué inversible tiene índice 5 respecto a la raíz primitiva 5, y nos resulta 25. Comprobamos:

$25^1 \equiv 25;\ 25^2 \equiv 25*25 \equiv 31;\ 25^3 \equiv 25*31 \equiv 19;\ 25^4 \equiv 25*19 \equiv 43;$
$25^5 \equiv 25*43 \equiv 49;\ 25^6 \equiv 25*49 \equiv 37$

Así comprobamos que 25 es una solución de la ecuación propuesta. Pero hemos asegurado que existen otras cinco soluciones, que se pueden leer en la tabla si hubiéramos usado otra raíz primitiva. Son estas: 13, 43, 31, 7 y 49. Esto completa el conjunto de seis soluciones de la ecuación propuesta.

Otras ecuaciones de ese tipo no tienen solución. Por ejemplo:

$X^7 \equiv 12 \pmod{49}$

Formamos la tabla de índices módulo 49 y vemos que $ind_3(12)=11$, que $\varphi(49)=42$ y $MCD(7,42)=7$, pero 11 no es múltiplo de 7, luego no existe solución. Hemos creado una tabla con las séptimas potencias de los inversibles de Z^*_{49} y sólo nos resultan seis resultados posibles: {1, 30, 31, 18, 19, 48}, y el 12 no está entre ellos.

El ejemplo anterior nos da una pista para descubrir si un resto dado es cúbico, bicuadrado o de otro orden en un módulo dado. Por ejemplo, ¿es resto bicuadrado 15 en módulo 22? Planteamos $a^4=15 \pmod{22}$ y analizamos:

Formamos la tabla de índices módulo 22

A. Roldán 2015

Tablas de índices

Módulo 22 — Indicatriz 10 — Tabla

Inversibles	Raíces primitivas 7	13	17	19
1	10	10	10	10
3	4	8	2	6
5	2	4	6	8
7	1	7	3	9
9	8	6	4	2
13	3	1	9	7
15	6	2	8	4
17	7	9	1	3
19	9	3	7	1
21	5	5	5	5

φ(22)=10 y MCD(4,10)=2, luego ind(15) ha de ser múltiplo de 2. Según la tabla, se cumple para cualquier raíz primitiva, luego sí es un resto bicuadrado. Podemos encontrar su raíz cuarta:

4ind(a)=2, luego ind(a)=2/4 (mod 22 = 6

El 3 posee índice 6, y cumple 3^4=15 (mod 22, luego existe la raíz bicuadrada de 15, y este valor 15 es resto bicuadrado (sólo hemos investigado una posibilidad, pero con una basta)