Congruencias

Edición 2024

Colección Hojamat.es

http://www.hojamat.es

CONTENIDO

INTRODUCCIÓN

Todo el tema de congruencias se desarrolla en el conjunto de los números enteros, pero por simplicidad, y para facilitar el uso con alumnos, haremos mención sólo de los naturales en los ejemplos, aunque los resultados se generalizan fácilmente.

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

NÚMEROS CONGRUENTES

DEFINICIÓN

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

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

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

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

PROPIEDADES

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

Esta ley tiene casos particulares interesantes:

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

* Si **a≡b (mod m)** y **c≡d (mod m)**, entonces:
  - a+b ≡ c+d (mod m)
  - a-b ≡ c-d (mod m)
  - a*b ≡ c*d (mod m)
  - ab ≡ cd (mod m)

* Si dos números **a** y **b** son congruentes respecto a varios módulos, también lo serán respecto a su mínimo común múltiplo.

* Dos números congruentes respecto a un módulo presentan el mismo MCD respecto a él.

* Si dos números **a** y **b** son congruentes respecto a un módulo **m**, también lo serán respecto a todos los divisores de m.

* La congruencia **es una relación de equivalencia**, porque es:

- Reflexiva: $a \equiv a \pmod{m}$
- Simétrica: Si $a \equiv b \pmod{m}$ entonces $b \equiv a \pmod{m}$
- Transitiva: Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$ entonces $a \equiv c \pmod{m}$

* Si en un polinomio con indeterminada x y coeficientes todos enteros, se sustituyen todos los elementos dos veces mediante pares de valores congruentes respecto a un módulo, los valores numéricos resultantes también serán congruentes respecto a ese módulo. Así: $2.2^2+3.2+7= 21$ es congruente con $2.7^2+3.7+2=121$ respecto al módulo 5.

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

CLASES DE RESTOS

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

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

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

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

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

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

Si a≡b (mod m) y c≡d (mod m) , entonces:

a+b ≡ c+d (mod m)
a*b ≡ c*d (mod m)

Estas dos propiedades nos permiten definir **la suma** y **el producto** entre clases de restos: sumar o multiplicar dos clases equivaldrá a

efectuar la operación entre los restos correspondientes a cada clase.

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

ESTRUCTURA ALGEBRAICA

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

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

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

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

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

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

Am'=A'D*m/D=A'm, que es congruente con cero, luego A*m'≡0 (mod m y por tanto divisor de cero.

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

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

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

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

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

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

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

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

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

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

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

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

Otra consecuencia es que si a es primo con m y se cumple que $a^x = a^y$, entonces han de ser x = y.

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

EXPONENCIACIÓN MODULAR

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

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

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

Para el conjunto Z la potenciación desemboca pronto en números grandes, pero no así en Z_m, pues los resultados siempre tendrán como cota m y este método puede ser muy útil. Incluso se puede intentar mentalmente. Por ejemplo, calcular 7^{63} (mod 5): $7\equiv2$ (mod 5); $7^2\equiv4$ (mod 5); $7^4\equiv1$ (mod 5); $7^8\equiv1$ (mod 5) y ya todos valen 1, luego

$7^{63}=7^{32+16+8+4+2+1}\equiv2*4*1*1*1*1\equiv8\equiv3$, luego $7^{63}\equiv3$ (mod 5)

Esta sería la exponenciación modular o binaria, que resulta imprescindible en cálculos con grandes números, porque sólo utiliza un número de multiplicaciones del orden del logaritmo de **n**, y no de **n** como el algoritmo clásico.

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

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

SISTEMAS DE RESTOS

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

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

Un conjunto de m elementos incongruentes siempre es completo.

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

La propiedad fundamental de estos conjuntos es:

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

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

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

TEOREMAS DE EULER, FERMAT Y WILSON

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

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

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

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

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

(Teorema de Fermat)

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

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

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

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

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

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

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

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

RESTOS POTENCIALES

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

Por ejemplo, los restos potenciales de 5 respecto al módulo 3 son:
De 5^0 el resto es 1, de 5^1 el resto es 2, de 5^2 el 1, de 5^3 el 2, etc. y así siguen de forma periódica.

El conjunto de restos potenciales sigue unas pautas muy sencillas:

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

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

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

Aplicación a los decimales periódicos

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

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

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

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

LOS PSEUDOPRIMOS

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

Identificación de pseudoprimos

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

La primera operación es la de obtener el resto de una potencia respecto a un módulo, lo que hemos llamado ***resto potencial***. En nuestra web figura una hoja de cálculo de hace años, muy simple, que los calcula para datos no muy grandes

http://www.hojamat.es/sindecimales/congruencias/herramientas/hoja/potenciales.xls

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

Aquí partiremos de una función que actuará sobre tres datos:

- Base de la potencia b
- Exponente p
- Módulo m

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

Función RESTOPOT

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

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

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

26	2,54187E+12	2	2

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

Contando con la función RESTOPOT es fácil exigir que se cumplan las condiciones para ser pseudoprimo en una base dada.

```
Public Function espseudo(m, b) As Boolean

If Not esprimo(m) And mcd(m, b) = 1 And restopot(b, m - 1, m) =
1 Then espseudo = True Else espseudo = False

End Function
```

Nos limitamos a exigir que

- Sea compuesto
- Primo con la base
- El resto potencial b^m-1 respecto a m sea 1

Con esta función y un bucle de búsqueda podemos reproducir muchas sucesiones de pseudoprimos ya publicadas en OEIS. Por ejemplo, para b=23 obtenemos esta lista:

Pseudoprimos en base 23

22, 33, 91, 154, 165, 169, 265, 341, 385, 451, 481,…

La puedes comprobar en http://oeis.org/A020151

En base 11

Obtenemos: 10, 15, 70, 133, 190, 259, 305, 481, 645, 703, 793, 1105, 1330, 1729, 2047, 2257

http:/oeis.org/A020139)

Versión en PARI

Si deseas estudiar números mayores contando con la mayor velocidad de proceso de PARI, puedes usar este código debidamente adaptado a tus datos (está construido para base 23 y búsqueda hasta el 4000):

```
rpm(b,p,n)={my(r,m,i);r=b%n;m=1;for(i=1,p,m=(m*r)%n);m}
espseudo(m,b)=!isprime(m)&&gcd(m,b)==1&&rpm(b,m-1,m)==1
```

for(k=2,4000,if(espseudo(k,23),print1(k,", ")))

Lo hemos adaptado a base 17 y cota 20000, obteniendo:

4, 8, 9, 16, 45, 91, 145, 261, 781, 1111, 1228, 1305, 1729, 1885, 2149, 2821, 3991, 4005, 4033, 4187, 4912, 5365, 5662, 5833, 6601, 6697, 7171, 8481, 8911, 10585, 11476, 12403, 12673, 13333, 13833, 15805, 15841, 16705, 19345, 19729,…

Coinciden con los pseudoprimos publicados en http://oeis.org/A020145

Números de Carmichael

Si un número es pseudoprimo con base todos los números coprimos con él, se llama “de Carmichel”.

Los primeros los tienes en https://oeis.org/A002997:

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633,…

Bastará recorrer los números coprimos con uno de ellos y comprobar que es pseudoprimo con todos ellos.

Hay criterios más sencillos, que puedes consultar en https://en.wikipedia.org/wiki/Carmichael_number.

Números de Sarrus o Poulet

Estos son los pseudoprimos en base 2, también llamados números de Sarrus, Poulet o simplemente psudoprimos, sin especificar el módulo.

El primer pseudoprimo módulo 2 es el 341, porque es compuesto (341=11*31) y cumple que

$\mathbf{2}^{340} \equiv 1 \pmod{341}$

Esta condición se verifica fácilmente, ya que 210=1024=3*341+1 presenta resto 1 respecto al módulo 341, por lo que todas sus potencias, entre ellas 2340 también tendrán ese mismo resto.

El segundo pseudoprimo módulo 2 es 561, que es compuesto (561=3*11*17) y se verifica que

$\mathbf{2}^{560} \equiv 1 \pmod{561}$

La sucesión de números de Poulet la tienes en
http://oeis.org/A001567

341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911, 10261, 10585, 11305, 12801, 13741, 13747, 13981, 14491, 15709, 15841, 16705, 18705, 18721, 19951, 23001, 23377, 25761, 29341

Aquí nos hemos limitado a presentar conceptos básicos y facilitar la búsqueda de pseudoprimos. Se podría extender más su estudio, pero superaría los objetivos de este documento.

RESTOS CUADRÁTICOS

Un elemento **a** de unas clases de restos de módulo **m**, con **a** primo con **m**, es **resto cuadrático** cuando es resto potencial de algún cuadrado, es decir, que existe un n tal que $n^2 \equiv a \pmod{m}$.

En caso contrario diremos que **a** es **no resto cuadrático**. Bastará ensayar los cuadrados de los números 0, 1, 2, 3... m-1 para ver si alguno de ellos produce de resto **a**. En realidad sólo hay que probar la mitad, pues **r** produce el mismo resto cuadrático que **m-r**. Intenta demostrarlo.

Por ejemplo, con módulo 8, son restos cuadráticos 0, 1 y 4 y son no restos cuadráticos 2, 3, 5, 6 y 7.

El caso más interesante se presenta cuando **m es primo impar**. En este caso se verifican estas propiedades:

* El número de restos cuadráticos es (m-1)/2, que son congruentes con 1^2, 2^2, 3^2… $((p-1)/2)^2$ y por tanto, este también es el número de no-restos.

* El producto de dos restos o de dos no-restos siempre da un resto, y el de resto con no resto produce un no-resto. Es decir, poseen estructura alternada, por lo que es fácil representar los restos mediante el signo + y los no restos con el -, y así poder usar la regla de los signos.

* El conjunto de restos cuadráticos forma un grupo multiplicativo en Z_p, de índice 2.
Por ejemplo, si m=11, los restos son 1, 3, 4, 5 y 9 y los no restos 2, 6, 7, 8 y 10 (o bien -1, -3, -4, -5 y -9). Los restos forman un grupo, como se puede verificar fácilmente.

Si a es un resto cuadrático respecto a p se cumple

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

Y si no lo es

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

SÍMBOLO DE LEGENDRE

Si **m** es primo, y **a** primo con él (es decir, no múltiplo, en este caso) usaremos el símbolo **(a/m)** (símbolo de Legendre) para indicar si **a** es resto cuadrático o no respecto a m.

Si lo es, declararemos que **(a/m)=1**, y si no lo es, que **(a/m)=-1** (Escribimos el símbolo de forma inclinada, pero se suele escribir verticalmente como una fracción)

Según se vio en el apartado anterior, podremos escribir

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

El símbolo de Legendre presenta varias propiedades interesantes:

$$\left(\frac{1}{p}\right) = 1$$

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

$$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) * \left(\frac{b}{m}\right)$$

La asignación de +1 o -1 **es un verdadero homomorfismo entre Z_p y el grupo multiplicativo {+1,-1}**, tal como se anunció en párrafos anteriores.

LEY DE RECIPROCIDAD CUADRÁTICA DE GAUSS

*Si **p** y **q** son primos impares, y uno de ellos tiene la forma **4n+1**, entonces **p** es resto cuadrático respecto de **q** si y solo si **q** es resto cuadrático de de **p**.*

Si ambos presentan la forma ***4n+3****, si* ***p*** *es resto cuadrático de* ***q****, entonces* ***q*** *no lo es de* ***p****, y a la inversa.*

Si se usa el símbolo de Legendre, la ley se puede expresar así:

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

En ese caso, si uno de los dos, p o q, tienen la forma 4n+1, la potencia tiene el valor de 1, por lo que si p es resto cuadrático de q, ocurrirá también que q lo será de p. Si ambos tienen la forma 4n+3, la potencia valdrá -1, y si p es resto de q, q no lo será de p.

CRITERIO DE EULER

Los símbolos de Legendre nos ayudan a expresar un criterio debido a Euler para saber si un entero es resto cuadrático:

Sea **m** primo y **a** entero coprimo con él. Entonces se cumple:

$$a^{\frac{m-1}{2}} \equiv \left(\frac{a}{m}\right) \bmod m$$

Lo podemos comprobar, por ejemplo, con los restos respecto a 11.
5^5 = 3125 ≡1 (mod 11), luego 5 sí es resto cuadrático.
7^5 = 16807≡10 (mod 11) ≡ -1 (mod 11), luego 7 no es resto cuadrático.

EL ALGORITMO EXTENDIDO DE EUCLIDES

Llamamos algoritmo extendido de Euclides al algoritmo clásico de ese nombre en el que se continúa con el desarrollo en fracciones continuas y del cálculo de convergentes o reducidas. También se puede interpretar como el recorrido inverso del algoritmo hasta llegar a la Identidad de Bezout.

El algoritmo extendido supone tres fases de calculo:

(1) El algoritmo para el cálculo del MCD. Lo recordamos en esta imagen:

	q_1	q_2	q_3	q_4	…	q_t
D	d	r_1	r_2	r_3	…	MCD
r_1	r_2	r_3	r_4	r_5	…	0

(2) Se despejan los restos a partir de las identidades de la división entera:

$r_1=D-d*q_1$
$r_2=d-r_1*q_2$
$r_3=r_1-r_2*q_3$
$r_4=r_2-r_3*q_4$
….

(3) Sustituimos $\mathbf{r_1}$ en la fórmula de $\mathbf{r_2}$, con lo que éste dependerá sólo de **D** y **d**. Proseguimos sustituyendo $\mathbf{r_2}$ en $\mathbf{r_3}$, éste en $\mathbf{r_4}$ y así hasta llegar al **MCD** que dependerá entonces sólo de **D** y **d** y habremos obtenido la identidad de Bezout: **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 (Ver la teoría de fracciones continuas en nuestro documento teorarit.pdf)

ECUACIÓN LINEAL EN CONGRUENCIAS

Llamaremos ecuación lineal a la de forma **a*x ≡ b (mod m).** Los tipos de solución que presenta son:

1. Si **a** es primo con **m**, existe una sola solución $\mathbf{x \equiv b*a^{-1} \pmod m}$, por ser **a** inversible en el anillo Zm

2. Si **MCD(a,m)=d**, con d mayor que 1, para que exista solución ha de ser b múltiplo de d. En ese caso se simplifican los tres números a,b y m con lo que se pasa al primer caso. Se puede encontrar una primera solución $\mathbf{x_0 = b*a^{-1} \pmod m}$ y existirán en total d soluciones, que vienen dadas por la fórmula $\mathbf{x_r = x_0 + r*m/d}$

Para resolver esta ecuación deberemos encontrar el inverso a^{-1}. Esto se puede conseguir de las dos formas explicadas más arriba:

- Una fórmula para calcular el inverso de un número a es $\mathbf{a^{-1} = a^{\varphi(m)-1}}$, siendo φ (m) la indicatriz del módulo m
- Otra forma es acudir a la identidad de Bezout, pues si a y m son coprimos, existen dos enteros p y q tales que ap+mq=1 (Estos números p y q se calculan mediante el algoritmo de Euclides extendido) Despejando, ap=1-mq será congruente con 1 módulo m, luego A será el inverso pedido.

Caso homogéneo

Si **b** es cero, esta ecuación queda como a*x ≡ 0 (mod m) por lo que además de la solución trivial x=0 existirán otras si M.C.D(a,m)>1, y entonces **a** se confirmará como divisor de cero. Por ejemplo, si se resuelve 6*x ≡ 0 (mod 9) y obtendrás las soluciones 0, 3 y 6, ya que M.C.D(6,9)=3>1. Sin embargo, resuelve 6*x ≡ 0 (mod 7) y sólo obtendrás x=0, ya que en este caso 6 es inversible.

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 $A*x \equiv B \pmod m$

SISTEMAS DE ECUACIONES LINEALES

Sólo se incluye el caso del llamado Teorema Chino de los restos:

Si $M_1, M_2, M_3 \ldots M_n$ son números enteros primos entre sí dos a dos y $B_1, B_2, B_3, \ldots B_n$, 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.

Esta solución es única. Su fundamento está en que si dos números son congruentes respecto a módulos primos entre sí, también lo serán congruentes respecto al producto de los módulos. Así, en este caso, si N_1 y N_2 fueran dos soluciones distintas, serían congruentes respecto a todos los módulos $M_1, M_2, M_3 \ldots M_n$ y por tanto congruentes respecto a H, que es lo que garantiza su unicidad.

Para calcular ese número se sigue el proceso, llamado algoritmo de Gauss:

Llamemos H al producto de todos los módulos M_i y sea $M'_i = H/M_i$. Se buscan unas m_i tales que $m_i.M'_i=1 \pmod{M_i}$, es decir, sus inversos, y entonces la solución será:

$$N = \sum_{i=0}^{n} M_i\, m_i B_i = \sum_{i=0}^{n} E_i\, B_i$$

Se han destacado los coeficientes $E_i=M_i*m_i$ porque sólo dependen de los módulos, y no de las B_i, lo que significan que se pueden seguir usando para esos módulos aunque cambiemos otros datos.

Por ejemplo: Encontrar un número n tal que al dividirlo entre 10 nos dé de resto 7, y al dividirlo entre 9 obtengamos un resto de 3.

H=9.10 = 90 ; $A'_1=9$; $A'_2=10$; $m_1=9$; $m_2=1$ y por último:

N=9.7.9+10.3.1= 81*7+10*3=597. Si reducimos a módulo 90 nos quedará 57, que es la solución única en Z_{90}.

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

El caso de dos ecuaciones

Si la solución de este problema es única, podríamos definir una función $\Psi(a,b,m,n)$ tal que a cada par de enteros **a** y **b** y dos módulos **m** y **n** primos entre sí les asignara la solución N tal que $N\equiv a \pmod{m}$ y $N\equiv b \pmod{n}$. Si los módulos no fueran primos entre sí le podríamos asignar el valor de alarma, por ejemplo el cero.

Por otra parte, para todo entero N existen dos enteros únicos a y b tales que $N\equiv a \pmod{m}$ y $N\equiv b \pmod{n}$. Por tanto, tenemos delante

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

Por tanto, nuestra función Ψ quedará como un isomorfismo entre anillo $\mathbf{Z_m \times Z_n}$ y el anillo $\mathbf{Z_{mn}}$ si la aplicamos a módulos **m** y **n** coprimos, cumpliendo

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

Correspondencia entre inversibles

Si el resto **p** es inversible en $\mathbf{Z_m}$, será porque no tiene factores primos comunes con **m**. De igual forma, si **q** es inversible en $\mathbf{Z_n}$, no compartirá factores con **n**. Si aplicamos la función $\Psi(p,q)=N$ (si suponemos que m y n son coprimos), este resultado N será coprimo con m y con n, pues en caso contrario produciría divisores de cero tanto en $\mathbf{Z_m}$ como en $\mathbf{Z_n}$. Por tanto, N es inversible en $\mathbf{Z_{mn}}$

La correspondencia $\Psi(p,q)=N$ convierte inversibles en inversibles.

ECUACIONES POLINÓMICAS EN Z_M

Al ser Z_m un anillo, será posible definir polinomios con una indeterminada. Esto permite definir ecuaciones polinómicas como la siguiente:

$$\mathbf{f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a_0 \equiv 0 \pmod m}$$

Para este tipo de ecuaciones es cierto el Teorema de Lagrange

Si en la ecuación polinómica $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a_0 \equiv 0 \pmod m$ el módulo m no divide a todas las a_i , entonces el número de soluciones de la ecuación no puede ser superior a m.

GRUPOS DE POTENCIAS EN ZN

ÍNDICE O GAUSSIANO DE UN RESTO EN ZN

Teoría previa

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

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

Puedes repasar las páginas

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

http://hojamat.es/sindecimales/congruencias/39teoria/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'≡0 (mod m) y por tanto divisor de cero.

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

Así que:

- **Si el elemento A es primo con el módulo m, entonces es inversible**, es decir, que existe algún otro elemento B tal que A*B=B*A=1. Anteriormente vimos cómo encontrarlo mediante el algoritmo extendido de Euclides

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

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

Grupo de inversibles

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

Gaussiano de las potencias de un resto

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

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

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

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

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

En esta tabla tienes un ejemplo de lo demostrado. El resto 4 tiene un gaussiano igual a 14 respecto al módulo 29, luego el gaussiano de sus potencias será un divisor de 14, precisamente el MCD de 14 y el exponente. Estúdialo bien:

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

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

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

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

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

SUBGRUPOS CÍCLICOS EN Z_M*

Según el tema 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.

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 $a^{k+tg(a)}=a^k*a^{tg(a)}=a^k*1=a^k$

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

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

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

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

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

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

Subgrupos generados

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

Más adelante estudiaremos los elementos que engendran todo Z^*_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.

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 este apartado 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 Z^*_n es cíclico**. Usamos la palabra "puede" pues, como ya veremos, **no todos los módulos poseen raíces primitivas**.

Aquí tienes la tabla correspondiente al módulo 14

Módulo	14
Indicatriz	6
Núm. Posible de raíces	2

Inversibles	Gaussiano	Es raíz primitiva
1	1	
3	6	Raíz primitiva
5	6	Raíz primitiva
9	3	
11	3	
13	2	

Explicamos la tabla: El módulo es 14, luego existirán tantos inversibles como indique φ(14)=6. En efecto, Z^*_{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 anteriormente

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

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

Criterio de los factores de la indicatriz

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

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

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

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

ÍNDICES MODULARES

En el apartado anterior estudiamos las raíces primitivas, elementos del grupo multiplicativo Z^*_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.

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:

$6*ind_5(x) \equiv ind_5(37)$ (mod 54 ≡12

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

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

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

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:

$X^7 \equiv 12$ (mod 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 $a^4=15$ (mod 22 y analizamos:

Formamos la tabla de índices módulo 22

A. Roldán 2015

Tablas de índices

		Módulo	22		Tabla
		Indicatriz	10		
	Raíces primitivas				
Inversibles		**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

$\varphi(22)=10$ 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)

TEMAS DE CALENDARIOS

NOTA PREVIA

La página web ***hojamat.es*** contiene varios temas de calendarios. Esta página puede sufrir cambios importantes en un futuro, o incluso desaparecer. Por ello, se incluyen aquí esos temas, como una especie de copia de seguridad, pero sin enlaces a las herramientas de hoja de cálculo.

Las herramientas de cálculo en hojas de cálculo se encuentran actualmente en esta dirección:
http://www.hojamat.es/sindecimales/congruencias/herramientas/calendarios/inicalend.htm
Allí se desarrollan algunos esquemas que incluiremos en este apartado.

FUNDAMENTOS

Los calendarios están formados por múltiples congruencias y todos los elementos fundamentales de la hora, día y año pertenecen a las clases Z/mZ. Por ejemplo:
* Los días de la semana pertenecen a Z/7Z (identificamos Domingo=0, Lunes=1, etc.)
* Los meses del año a Z/12Z (Por ejemplo Enero=0, Febrero=1, etc.)
* Los minutos y segundos a Z/60Z
* La aparición o no de años bisiestos forma el conjunto {0,1,2,3} = Z/4Z
E igual con los siglos, los años terminados en 0 no bisiestos y otros.

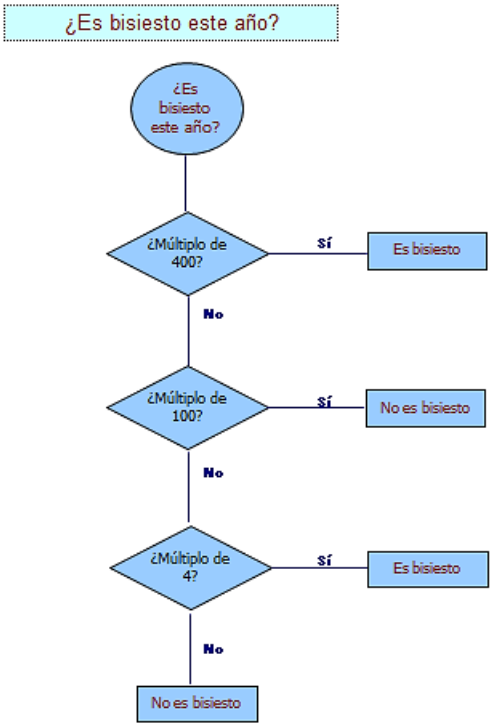
AÑOS BISIESTOS

Se considera año bisiesto a aquel que contiene 366 días en lugar de 365. Aquí nos interesará la definición y los algoritmos para averiguar si un año es bisiesto. Los temas históricos se pueden consultar en otras publicaciones.

Los algoritmos para averiguar esta cuestión se basan en las tres reglas que se establecieron en el calendario gregorianoen el año 1582:

- Si el número de año es múltiplo de 400, no se considera bisiesto
- Si es múltiplo de 100, pero no de 400, se considera bisiesto
- En los demás casos, sólo si es múltiplo de 4 será bisiesto

Por tanto, basta responder a las tres preguntas y decidir.



Lo podemos plasmar en esta fórmula de hoja de cálculo:

=SI(O(Y(RESIDUO(D5;4)=0;RESIDUO(D5;100)<>0);RESIDUO(D5;400)=0);"SÍ";"NO")

Si el año lo escribimos en la celda D5, esta fórmula nos responderá “SÍ” o “NO”.

Estas preguntas se desprenden del valor del año trópico, (tiempo medio que tarda el Sol, en su movimiento aparente entre dos pasos consecutivos por el equinocio, por ejemplo el de primavera)

El mejor valor que se conoce de este año trópico es el de 365,242199074 días

El calendario juliano sustituyó este valor por 365 + 1/4 -1/100 + 1/400, que equivale a 365,2425

1/4 Se acumula un día cada 4 años
1/100 Se descuenta un día cada 100
1/400 Se añade otro día cada 400

Sigue habiendo un error, pues hay diferencia entre el verdadero valor de 365,242199074 y 365,2425. El error es

365,2425 – 365,242199074, es decir: 3,01E-004

Si dividimos un día entre la diferencia de ambos nos dan: 3323,076105 años, que es lo que el calendario actual nos garantiza de exactitud en días.

CÁLCULO DEL DÍA DE LA SEMANA

Dada un fecha cualquiera del calendario gregoriano (el vigente en la actualidad), constituye un problema muy interesante el calcular en qué día de la semana cae.

Todos los algoritmos existentes hacen uso de los siguientes hechos:

El día de la semana correspondiente a una fecha siempre proviene de considerar una congruencia respecto al número 7, porque la sucesión de días de la semana siempre es un elemento de Z/7

Este hecho nos permite representar los días de la semana como los números del 0 al 6 en un “reloj” de siete números.

Como el número de días de un año no bisiesto, 365, es congruente con 1 módulo 7, cada año que transcurra se incrementa en una unidad el día de la semana. Si el año pasado una fiesta cayó en viernes, este año lo hará en sábado.

$365 = 52 * 7 + 1$ $\qquad$ $365 \equiv 1$ (mód 7

Si el año es bisiesto, se incrementará el número en dos días por año. Recordando que son bisiestos los múltiplos de 4 que no lo sean de 100 y los múltiplos de 400, deberemos considerar también las congruencias respecto a 4, 100 y 400

Así, el avance de días que se produce en T años vendrá dado por

A = T + COCIENTE(T;4) – COCIENTE(T;100) + COCIENTE(T;400)

La función COCIENTE se refiere al entero, sin decimales, por lo que equivale a ENTERO(T/4). Por ejemplo.

Los distintos algoritmos que se basan en esta idea difieren de cómo tratar el problema de la fecha inicial a partir de la cual se incrementa el día de la semana. Aquí incluimos el de Zeller, que se basa en la siguiente congruencia (tomada de la Wikipedia)

$$h = \left(q + \left\lfloor \frac{(m+1)26}{10} \right\rfloor + K + \left\lfloor \frac{K}{4} \right\rfloor + \left\lfloor \frac{J}{4} \right\rfloor - 2J\right) \mod 7$$

Si llamamos D al día de la fecha, M al mes, C a la centuria (siglo menos 1) y A al año dentro de la centuria, la congruencia de Zeller es la siguiente:

DIASEM= RESIDUO(D + COCIENTE((M+1)*26;10) + A + COCIENTE(A;4)+COCIENTE(C;4) + 5*C) ; 7)

Si el mes es Enero o Febrero, se les suma 12 y se resta un año.

El esquema para la fecha 19/07/22 sería:

D	19
COCIENTE((M+1)*26;10)	20
A	22
COCIENTE(A;4)	5
COCIENTE(C;4)	5
5C	100
SUMA	171
MÓDULO 7	3
Día de la semana	Martes

CÁLCULO DE LA FECHA JULIANA

La fecha juliana o día juliano es una forma de situar cualquier fecha independientemente de que pertenezca a un calendario concreto. Se basa en el cómputo de días transcurridos desde el 1 de Enero del año 4713 aC a las 12h del mediodía.

Así, José Scaliger creó una escala continuada en el tiempo, válida para comparar fechas lejanas o pertenecientes a distintos calendarios.

Existen varios algoritmos para calcular el día juliano de cualquier fecha, sea anterior al 4 de Octubre de 1582 (calendario juliano) o posterior al 15 del mismo mes, día en el que comienza el calendario gregoriano en varios países. Otros se retrasaron en adoptarlo, como Inglaterra, y otros aún usan el calendario juliano.

Así, el día en el que se escribe este texto, 25 de Noviembre de 2007, posee una fecha juliana equivalente a 2.454.429,5

Esta escala nos proporciona un método fiable para contar el número de días transcurridos entre dos fechas. Basta restar las dos fechas julianas correspondientes.

Incluimos los esquemas del algoritmo para números reales y el correspondiente a enteros, aplicados ambos a la fecha 19/07/22:

Números reales

Llamo A1 al cociente del año entre 100	A1	20
Llamo A2 a A1/4	A2	5
Llamo A3 a 2-A1+A2	A3	-13
Llamamos A4 a 365.25*(año+4716)	A4	2461054
A5 será igual a 30,6001*(mes+1)	A5	244

Día juliano es la suma sde D+A3+A4+A5-1524,5	2459779,5

Números enteros

JD1 es (a1/4000)*1460969	JD1	0
A2 es el módulo de A1 respecto a 4000	A2	2022
JD2 es ((A1/100*146097)/4	JD2	730485
JD3 es ((A1 mod 100)*1461)/4	JD3	8035
JD$ es (153*M1+2)/5	JD4	122

Sumo JD1+JD2+JD3+JD4+D+1721119-0,5	DIAJUL	2459779,5

FECHA DE LA PASCUA

Este cálculo era fundamental en las iglesias cristianas, por lo que se estudió mucho y justificó cargos de astrónomos. Aquí tampoco entraremos en detalles históricos, pues solo copiaremos el esquema del algoritmo de Butcher, aplicado al año 2022:

	Cociente		Resto	
Se divide el año entre 19		106	A	8
Se divide el año entre 100	B	20	C	22
Se divide B entre 4	D	5	E	0
Se divide (B+8) entre 25	F	1		
Se divide (B-F+1) entre 3	G	6		
Dividimos (19A+B-D-G+15) entre 30			H	26
Se divide C entre 4	I	5	K	2
Dividimos 32+2E+2I-H-K entre 7			L	0
Se divide A+11H+22L entre 451	M	0		
Se divide H+L-7M+114 entre 31	N	4	P	16

Fecha	17	de	Abril

OTROS TEMAS RELACIONADOS CON LAS CONGRUENCIAS

Estos temas se desarrollan de forma sucinta, tan sólo para presentarlos. Si deseas adquirir más conocimientos debes acudir a manuales o direcciones de Internet que los tratan.

NÚMEROS PSEUDOALEATORIOS

Las congruencias nos permiten generar números naturales, que aunque procedentes de fórmulas o algoritmos, semejan haber sido generados al azar.
Una técnica muy sencilla para ello es la siguiente:
* Se fija un módulo grande, que se ha estudiado previamente y se ha visto que funciona bien. Por ejemplo 199017 (usado en algunas calculadoras Texas Instrument).
* Un primer número pseudoaleatorio se elige entre 0 y el módulo, por ejemplo el 34900, al que llamaremos semilla.
* Sobre la semilla se aplica reiteradamente una fórmula de recurrencia lineal del tipo xn+1 = a.xn+c (mod 199017)
En este caso se puede elegir a=24298 y como c=99991
En los ordenadores, la semilla se toma del estado actual del reloj interno, lo que aumenta la sensación de aleatoriedad.
Como ejemplos de generadores populares podemos recordar dos:
Si a=75, c=0 y m=231 - 1, resulta el generador usado durante muchos años por IBM y el programa MATLAB
Si a=1103515425, c=12345 y m=232, obtendremos el generador del sistema UNIX

CRITERIOS DE DIVISIBILIDAD

Los criterios que estudiábamos de niños (Un número es divisible entre 9 si la suma de sus cifras...) están basados en los restos potenciales.

Si deseamos ver si el número abcde es divisible entre m, podríamos descomponer ese número en unidades, decenas, centenas, de la forma

abcde = a104 + b103 + c102+d10+e con lo que el resto de dividirlo entre m, según los teoremas de las congruencias, equivale a

Resto: (ar4 + br3 + cr2 + dr1 + er0) (mod m) (1)

siendo r4,r3... los restos potenciales de 10 respecto a m.

Estos restos pueden ser:

Módulo 2: r0=1, r1=0,r2=0, r3=0,... La expresión (1) se reduce a a MOD m

En el criterio sólo habrá que mirar las unidades, que corresponden al único resto no nulo.

Módulo 3: r0=1, r1=1,r2=1, r3=1,... Todos los restos valen 1. En este caso la expresión (1) del resto será a +b +c +d +e MOD m

por lo que habrá que sumar todas las cifras y ver su resto respecto a m

y así con todos.

No es imprescindible usar el número 10. Con el número 1000 se pueden construir criterios para el 13, 11 y 7, porque sus restos potenciales son r0=1, r1=1,r2=1, r3=1,...lo que permite usar sumas alternadas de números de tres cifras.

CÁLCULO CON NÚMEROS GRANDES

El Teorema Chino nos garantiza que dados A1, A2, …An primos entre sí dos a dos, todo número natural menor que A1* A2* …*An viene determinado por a1, a2, a3,…an, tales que que cumple N=ai (mod Ai) para todo i entre 1 y n. Esto nos permite representar N de forma unívoca por el vector (a1, a2, a3,…an)

Por ejemplo, 9 y 10 son primos entre sí, luego todos los números menores que su producto 90 vendrán representados de forma unívoca por sus restos respecto a ellos. Así, el número 57 se representaría por el par de coordenadas (3,7), porque 57=3(mod9 y 57=7(mod 10. Recíprocamente, si resolvemos por el teorema chino estas dos condiciones nos daría como solución 9*9*7 + 10*1*3 = 597, que reducido a módulo 90 se convierte en 57.
Como las operaciones de suma y producto son compatibles con la relación de congruencia, a veces nos puede convenir sustituir números grandes por sus coordenadas, operar con ellas y después reconstruir los números. En Informática, si una unidad aritmética posee sus registros limitados, puede ser la única forma de operar.

DÍGITOS DE CONTROL

Los dígitos de control se introducen en números grandes para verificar la corrección de su escritura. Los más populares son los de las cuentas bancarias, que tienen la forma EEEE OOOO CD NNNN NNNN, en la que EEEE representa a la entidad, OOOO a la oficina, CD son los dígitos de control y NN... la cuenta de referencia. Tanto C como D se calculan mediante congruencias módulo 11 a partir del resto de dígitos. En concreto, C proviene de una suma ponderada de los EEEE y OOOO y D procede del número de cuenta.

DNI

La letra del NIF se obtiene a partir del número del DNI hallándole su resto módulo 23 y usando después una tabla de equivalencia:

Resto	0	1	2…
Letra T	R	W…	

FUNCIONES HASH

Están basadas en las congruencias, y se usan para asignar posiciones de memoria de un ordenador a partir del número clave de un registro en una base de datos. Por ejemplo, si un alumno tiene una clave de seis dígitos, como 344 231, y sólo tenemos 512 posiciones de memoria para almacenar las claves, se utiliza la función de tipo hash (direccionamiento calculado)

$$f(344231) = 344231 \bmod 512$$

El problema de esto reside en que dos claves pueden ser asignadas a una misma posición. Diremos que se ha producido una colisión y a las claves se les llama sinónimas. Existen técnicas informáticas para resolverlo.