Pequeño diccionario de Congruencias

Es adaptación del archivo del mismo nombre ubicado en

http://www.hojamat.es/sindecimales/congruencias/diccio/diccong.htm

En esta versión en PDF no funcionarán los enlaces externos.

Selecciona una letra o un tema

A

Aritmética Modular

C

Clases

Congruencia

Criterio

CH

Chino

E

Ecuación

Euler

F

Fermat

G

Gausiano

I

Incongruente

Indicador

Índice modular

Inversible

Inverso

L

Ley de reciprocidad cuadrática

Logaritmo discreto

M

Módulo

P

Prueba

Pseudoaleatorio

R

Raíz digital

Raíz primitiva

Relación

Residual

Resto

S

Sistema

T

Teorema

W

Wilson

A

Aritmética Modular

Aritmética modular

Comprende el estudio de las clases de restos Z/nZ de los enteros respecto a un módulo n. Ver Congruencias.

C

Clase

Clases de restos (de congruencia, o residuales)

Son las clases que se forman al aplicar la relación de congruencia en el conjunto de los números enteros Z.

Se representan por Z/nZ, Así: Z/5Z = {0,1,2,3,4}

Congruencia

Relación de congruencia

Diremos que a y b (números enteros) son congruentes módulo **n** (natural), si la diferencia **b-a** es un múltiplo de n. Representaremos la relación de congruencia como **a=b (mod n)**.

La relación de congruencia es reflexiva, simétrica y transitiva, y por tanto da lugar a clases de equivalencia, llamadas también residuales.

Congruencias famosas

Congruencia de Fermat:

$A^{p-1}=1_{(\text{mod } p)}$ si **p** es primo.

Congruencia de Euler:

$A^{f(n)}=1_{(\text{mod } n)}$ donde **n** no ha de ser necesariamente primo y f(n) es el indicador de Euler de dicho número.

Congruencia de Wilson:

$(p-1)!+1=0_{(\text{mod } p)}$ con **p** primo.

Criterio de Congruencia

Criterio de congruencia

Dos números enteros **a** y **b** son congruentes módulo n, si y sólo si la diferencia b-a es un múltiplo de **n**

CH

Chino

Teorema chino de los restos

Si A_1, A_2, …A_n son números primos entre sí dos a dos y a_1, a_2, a_3,…a_n, enteros cualesquiera, existe un número entero N que cumple $N=a_{i\ (mod\ A_i)}$ para todo i entre 1 y n.

Para calcular ese número llamemos H al producto de todas las A_i y sea $A'_i = H/A_i$.

Se buscan unas m_i tales que $m_i.A'_i=1$ (mod A_i) y entonces la solución será:

$N = S\ A_i.m_i.a_i$

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.

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

$N=9.7.9+10.3.10= 867$

E

Ecuación

Ecuación de congruencias

Es toda ecuación definida sobre el anillo de las clases de restos Z/mZ

Ver Ecuación lineal

Euler

Indicador de Euler

Es una función **f(n)** que indica la cantidad de números inferiores a **n** y primos con él.

Si **n** es primo, su indicador será **n-1**

Una fórmula para esta función es

$f(n)=n(1-1/p_1)(1-1/p_2)(1-1/p_3)...$ siendo p_1 p_2 p_3 los factores primos de n

Así, f(7) = 6, f(8) = 3 porque sólo son primos con él 3, 5 y 7.

Criterio de Euler

Si **p** es un número primo impar, y **a** es coprimo con **p**, entonces si

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

será a resto cuadrático respecto a p, y no lo será si

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

F

Fermat

Teoremas de Fermat

Teorema núm. 1 (pequeño teorema): Si p positivo es primo, entonces para todo n extraño con p se cumple que $n^p = n \pmod p$

Es equivalente afirmar que

Teorema núm. 2

Si p es primo y a es primo con p se cumple que $a^{p-1} = 1 \pmod p$

Fue generalizado por Euler así: Si a y n son extraños, se cumple que $a^{f(n)} = 1 \pmod n$, siendo f(n) el indicador de n

---

G

Gausiano

Gausiano de un número respecto a un módulo.

Es el mínimo exponente al que hay que elevar ese número para que produzca resto 1 al dividirlo entre el módulo. Por ejemplo, el gausiano de 3 respecto a 4 es 2, porque $3^2=1 \pmod 4$

I

Incongruente

Números incongruentes

Varios números son incongruentes módulo **m**, cuando dan todos restos *distintos* al dividirlos entre m.

Indicador de Euler

Ver Euler

Indice modular

Si **n** es una raíz primitiva respecto a un módulo primo **p**, diremos que el número **a** es *índice modular* de otro número **b** respecto a la base **p**, cuando $n^a=b \pmod p$

Inversible

Número inversible

Un número es inversible si posee inverso para una operación determinada

Inverso

Inverso de un número natural en Z/mZ

Dos números naturales **a** y **b** son inversos respecto al módulo **m**, si se cumple que **a.b=1 (mod m**)

L

Ley de reciprocidad cuadrática (ya descubierta por Legendre)

Si **p** y **q** son primos impares se cumple que el sistema de ecuaciones $x^2 = q \pmod p$ y $x^2 = p \pmod q$ tiene solución siempre, excepto si tanto p como q tienen la forma 4n+3, en cuyo caso, una tiene solución y la otra no.

Logaritmo discreto

Si una raíz primitiva engendra todo el grupo de inversibles, cada uno de estos vendrá representado por su exponente respecto a esa raíz primitiva. Es decir, que si **a** es raíz primitiva y **b** un elemento inversible, existirá un exponente **g** tal que $\mathbf{a^g = b}$. A ese número **g** le llamaremos **logaritmo discreto o índice** de b con base a.

M

Módulo

Módulo en una congruencia

Es el número **m** que tiene el papel de divisor en la definición de congruencia

---

P

Prueba

Prueba del 9

Consiste en sustituir cada número en una operación por su resto al dividirlo entre 9 y someter los restos a las mismas operaciones para ver si son congruentes respecto a 9. El resto se calcula fácilmente sumando las cifras del número y restando 9 cuando sea posible. Por ejemplo:

Comprobar mediante restos respecto a 9 la corrección de esta operación:
568*899+23 = 510655
Pasando a restos: 1*8 + 5 = 13 que es congruente con 4, resto del resultado.

Pseudoaleatorio

Números naturales pseudoaleatorios

Son sucesiones de números, procedentes de fórmulas, que sin embargo parecen haber sido generados al azar. Para ello usan las propiedades de las congruencias.

R

Raíz

Raíz digital de un número entero positivo (en base 10)

La raíz digital de un número entero positivo es el dígito, entre 0 y 10, que resulta al sumar las cifras de su expresión decimal, volviendo a sumar reiteradamente los resultados de esa suma y de las siguientes hasta que la suma sea un número de una cifra, al que llamaremos raíz digital del número. Por ejemplo, la raíz digital del número 23451 es 6 , porque 2+3+4+5+1 = 15 y sumando las cifras del 15 resulta 6.

Se obtiene el mismo resultado calculando el resto módulo 9 de ese número, pero en caso de ser 0 se sustituye por 9.

Raíz primitiva respecto a un módulo primo

Un número **n** constituye una *raíz primitiva* respecto a un módulo primo **p**, cuando el gausiano de **n** respecto a **p** es exactamente **p-1**

Relación

Relación de congruencia

Dos números están relacionados por una congruencia cuando son *congruentes* respecto a un módulo dado. Esta relación es reflexiva, simétrica y transitiva y produce, por tanto, **clases de equivalencia**, llamadas también clases de restos o residuales.

Residual

Ver Clases

Resto

Resto potencial

Llamaremos restos potenciales de un número natural **z** respecto a un módulo **m** a los restos de dividir las potencias de z entre m. Por ejemplo, los restos potenciales del número 7 respecto a 5 son:

$r_0=1$ $r_1=2$ $r_2=4$ $r_3=3$ ...

Resto cuadrático

Un elemento **a** de unas clases de restos es ***resto cuadrático*** cuando es resto potencial de algún cuadrado, es decir, que existe un **n** tal que $n^2 = a \pmod m$. En caso contrario diremos que **a** es ***no resto cuadrático.***

S

Sistema

Sistema de ecuaciones en congruencias

Es un conjunto de ecuaciones de congruencia con soluciones comunes.

Ver el Teorema Chino

Sistema de números incongruentes

Es un conjunto de números naturales cuyos restos respecto a un módulo dado son todos diferentes.

Por ejemplo: los números 13, 24 y 31 forman un sistema de números incongruentes respecto al 5.

Sistema completo de números incongruentes

Un sistema de números incongruentes se llama *completo* cuando sus restos completan todo el conjunto de los posibles respecto a un módulo.

Por ejemplo: El sistema 2,7,8,13 es completo respecto a 4, porque produce los restos 2,3,0 y 1.

T

Teorema

Ver Teoremas Chino, Fermat,

W

Wilson

Teorema de Wilson

Para que **n** divida a (n-1)!+1 es necesario y suficiente que **n** sea primo.

Por tanto, para p>0 primo tendremos que (p-1)! Es congruente con –1 módulo p