Congruencia

$$aRb \Leftrightarrow a \equiv b(n) \Leftrightarrow n|a-b$$

La congruencia en modulo n es una relación de equivalencia, por lo tanto es **reflexiva, simétrica y transitiva**

Por ser una clase de equivalencia genera una partición en el cojunto.

Clases de equivalencia:

$$\bar{x} : \{y \in \mathbb{Z} / y = nk + x \ \text{con} \ k \in \mathbb{Z}\}$$

Es decir, en la clase de x están todos los enteros cuyo resto al dividir por n es x.

Conjunto cociente:

$$Z_n = \{\bar{0}, \bar{1}, \bar{2}, \cdots, n \bar{-} 1\}$$

Está formado por las clases residuales, son todos los restos posibles al dividir por n.

Propiedad

$$\forall x, y \in \mathbb{Z} : \quad x \in \bar{a}(n) \ \wedge \ y \in \bar{b}(n) \Rightarrow x + y \in a \bar{+} b(n)$$

Es decir, al sumar dos elementos de clases de equivalencia no importa que elemento se tome de cada clase, el resultado de la operación siempre pertenece a la misma clase.

Lo mismo ocurre con el producto:

$$\forall x, y \in \mathbb{Z} : \quad x \in \bar{a}(n) \ \wedge \ y \in \bar{b}(n) \Rightarrow x \cdot y \in a \bar{\cdot} b(n)$$

Función de Euler

$$\varphi(n) = |\{x \in \mathbb{N} / x \leq n \ \wedge \ (x, n) = 1\}|$$

Esta función se aplica a los numeros enteros positivos, y nos da la cantidad de números menores o iguales al dado que son coprimos con dicho numero.

Propeidades de la funcion de Euler

1. Si p es un número primo, entonces:
$$\varphi(p) = p - 1,$$

2. Si n es un numero natural cualquiera y p es un numero primo:
$$\varphi(p^n) = p^{n-1}(p-1)$$

3. Si $n, m \in \mathbb{N}$ y $m.c.d(n,m) = 1$ entonces:
$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$$

Para cualquier n:

$$\varphi(n) = n \prod_{p_i | n} (1 - \frac{1}{p_i})$$

Siendo p_i los primos divisores de n.

Pequeño teorema de Fermat

Si p es primo y $m.c.d(a,p) = 1$ entonces: $a^{p-1} \equiv 1(p)$ o bien $a^p \equiv a(p)$

Este teorema se utiliza para investigar si un numero natural muy grande es o no primo. Si el numero dado fuera primo, con cualquier numero natural a menor que p debe cumplirse que $a^{p-1} \equiv 1(p)$. Se va calculando con distintos valores de a. Si para algún cvalor de a menor que n no se cumple la congruencia entonces n es compuesto.

Nosotros vamos a utilizarlo para hallar el resto de la división de un numero entero grando por un numero primo.

Ej:

Calculemos el resto de la division de 7^{122} por 11.

Como $122 = 10 \cdot 12 + 2$, se tiene que:

$7^{122} = 7^{10 \cdot 12 + 2} = 7^{10 \cdot 12} \cdot 7^2 = 7^{(11-1) \cdot 12} \cdot 7^2 = [7^{(11-1)}]^{12} \cdot 7^2$

Teniendo en cuenta que $a^{p-1} \equiv 1(p)$ resulta $[7^{(11-1)}] \equiv 1(11)$ entonces: $[7^{(11-1)}]^{12} \equiv 1(11)$

Entonces: $7^{122} \equiv 7^2(11) = 5$

Teorema de Euler Fermat

Si $m.c.d(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1(n)$

Ej:

Calculemos el resto de dividir $8^{1791485}$ por 21.

Como 21 no es primo, utilizaremos el teorema de Eueler-Fermat, para ello, primero calculamos $\varphi(21) = 12$

Como: $8^{\varphi(21)} \equiv 1(21)$ entonces: $8^{12} \equiv 1(21)$

Para poder usar este resultado, decomponemos el numero 1791485

$1791485 = 12 \cdot 149290 + 5 \Rightarrow 8^{1791485} = 8^{12 \cdot 149290 + 5} = (8^{12})^{149290} \cdot 8^5$

Como $8^{12} \equiv 1(21)$ entonces $8^{1791485} \equiv 1 \cdot 8^5(21)$

Y ya tenemos un nuúmero bastante mas chico, aunque lo podemos escribir por ejemplo: $8^5 = 8^2 \cdot 8^2 \cdot 8$ y como $8^2 = 64 \equiv 1(21) \Rightarrow 8^5 \equiv 8(21)$

Y por lo tanto $8^{1791485} \equiv 8(21)$ con lo cual el resto de dividir $8^{1791485}$ por 21 es 8

Ecuaciones lineales de congruencia

Son de la forma $a \cdot x \equiv b(n)$ siendo a, x, b enteros y n natural.

Si $x \in \mathbb{Z}$ es una solución de $a \cdot x \equiv b(n)$ entonces $x + kn$ también es una solución. Como son infintias soluciones consideramos, $0 \leq x < n$ y las llamaremos soluciones principales.

Las eucuaciones lineal de congruencia pueden tener una, mas de una o niguna solución en Z_n

Condición suficiente para que una ecuación de congruencia tenga solución

Sea $a \cdot x \equiv b(n)$ Si $m.c.d(a,n) = 1$ entonces hay solución. Y la solución será: $x = a^{\varphi(n)-1} \cdot b$

Condición necesaria y suficiente para que una ecuación de congruencia tenga solución

$a \cdot x \equiv b(n)$ admite solución $\Leftrightarrow m.c.d(a,n)|b$ la cantidad de soluciones es $m.c.d(a,n)$ y difieren en n

Propiedad

Si $a \cdot c \equiv b \cdot c(n)$ y $m.c.d(c,n) = 1$ entonces:

$$a \equiv b(n)$$