Algoritmo de Euclides:
Es un método para calcular el Máximo Común Divisor (MCD) de dos números enteros. Se basa en la repetición de la siguiente operación: dividir el número mayor por el menor, y utilizar el residuo como nuevo divisor. El proceso continúa hasta que el residuo sea 0. En ese momento, el divisor actual es el MCD.

Algoritmo de Euclides Extendido: Extensión del algoritmo euclidiano que, además de calcular el MCD de dos números enteros, también encuentra dos enteros, x e y, que satisfacen la **ecuación de Bézout:** a * x + b * y = MCD(a, b).

La teoría de congruencias es un campo de la teoría de números que se ocupa del estudio de la relación entre números enteros que tienen el mismo resto al dividirlos por un número natural, llamado módulo. En este sentido, dos números a y b son congruentes módulo c (escrito como a ≡ b (mod c)) si su diferencia a - b es múltiplo de c.

Pequeño teorema de Fermat: Se formula de la siguiente manera:

- Si ***p*** es un número primo, entonces, para cada número natural ***a***, con ***a***>0 , ***a^p*** ≡ ***a*** (mod ***p***)
- Si ***p*** es un número primo, entonces, para cada número natural ***a***, con ***a***>0 , coprimo con ***p*** , ***a^(p***-1)≡ 1 (mod ***p***)

Esto quiere decir que, si se eleva un número ***a*** a la ***p***-ésima potencia y al resultado se le resta ***a*** lo que queda es divisible por ***p.***
Por tanto, a cada uno de los números ***p*** que cumple ésta condición, se le denomina: raíz primitiva de ***a***. Su interés principal está en su aplicación al problema de la primalidad y en criptografía.

Simbolo de Legrende: Es una función multiplicativa utilizada para determinar el carácter cuadrático de un número (mod p), es decir si es residuo cuadrático o no;la misma que toma como argumentos un entero ***a*** y un primo ***p*** y devuelve uno de los valores 0,1,-1 dependiendo de si ***a*** es o no residuo cuadrático módulo ***p***
es decir de si la congruencia tiene solución o no.

Residuo Cuadratico: Un residuo cuadrático es un número entero aaa que, al ser elevado al cuadrado, da como resultado un número $\mathbf{x^2}$ que es congruente a aaa módulo nnn. En otras palabras, aaa es un residuo cuadrático módulo nnn si existe un número xxx tal que:

$$\mathbf{x^2 \equiv a \bmod n}$$

Esto significa que el cuadrado de algún entero **x**, cuando se divide entre **n**, deja un residuo igual a **a**.

Cómo se Obtiene

Para determinar si un número aaa es un residuo cuadrático módulo nnn, se siguen los siguientes pasos:

1. **Elección de a y n**: Se selecciona un número **a** y un módulo **n**.
2. **Prueba con los cuadrados de los enteros**: Se calcula el cuadrado de los números enteros **x** y se determina el residuo cuando se divide por **n,** es decir, se calcula $\mathbf{x^2}$ mod **n** para diferentes valores de **x**.

3. **Verificación**: Si existe un número **x** tal que **$x^2 \equiv a$** (mod **n**), entonces **a** es un residuo cuadrático módulo **n.** Si no existe tal **x, a** no es un residuo cuadrático módulo **n**.

Teorema Chino del Resto

El **Teorema Chino del Resto** es un resultado fundamental en la teoría de números que permite resolver sistemas de congruencias simultáneas con módulos coprimos. En términos simples, el teorema garantiza que, dado un sistema de congruencias con módulos mutuamente primos, existe una única solución en un determinado rango.

Propiedades de la Exponenciación

- **Definición:** Si una base ***a*** se eleva a una potencia ***m*** y luego a otra potencia ***n***, el resultado es equivalente a elevar ***a*** al producto de ***m*** y ***n***:

$$(a^m)^n = a^{(m \cdot n)}$$

- Esto permite unificar las potencias de las dos ecuaciones elevando cada lado al exponente del otro, combinándolos en una sola potencia común.

Modularidad

- **Definición:** La aritmética modular trabaja con restos. Decimos que dos números son congruentes módulo ***N*** si tienen el mismo resto al dividir por ***N***:

$a \equiv b \pmod{N}$ si y solo si $(a-b)$ es divisible por N

Teorema Binomial de Newton

es una fórmula que se utiliza para expandir potencias de binomios, es decir, expresiones de la forma (a+b)n(a + b)^n(a+b)n. Generalmente, se expresa mediante una sumatoria que involucra coeficientes binomiales y términos de las variables aaa y bbb elevados a potencias decrecientes e incrementadas, respectivamente:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{(n-k)} b^k$$

Donde:

- **(n k)** es el coeficiente binomial y se calcula como $\binom{n}{k} = n!/(k!(n-k)!)$
- $a^{(n-k)} b^k$ representan las potencias respectivas de ***a*** y ***b***,
- ***k*** varía de 0 a ***n***

La forma simplificada del binomio de Newton se utiliza en aritmética modular para calcular expresiones de la forma ***(ap + bq)^n mod N*** , descartando términos intermedios de la expansión completa que no contribuyen significativamente al resultado debido a sus propiedades modulares. Solo se consideran los términos extremos de la expansión es válida cuando los términos intermedios no afectan el resultado bajo el módulo especificado. Es útil para cálculos rápidos y en contextos donde se manejan grandes potencias y módulos pequeños.

$$(ap+bq)^n \equiv (ap)^n+(bq)^n \bmod N$$

.