

Teoría de Números

Jaime Sebastian Chavarria Fuertes

January 6, 2025

1 Aritmética Modular

1.1 Teoría de Congruencias

Una congruencia es una relación de equivalencia entre enteros que se basa en sus restos al dividirse por un número dado.

Definición 1.1 (Congruencia). *Decimos que dos números enteros a y b son congruentes módulo n , y escribimos $a \equiv b \pmod{n}$, que significa que:*

$$a \% n == b \% n$$

Tambien podemos decir que si $a \equiv b \pmod{n}$ entonces se puede decir que:

$$n | (a - b)$$

Es decir que n divide a: $(a - b)$

Ejemplo 1.2. $17 \equiv 2 \pmod{5}$, ya que $17 - 2 = 15$ es divisible por 5.

Propiedades:

- Si $a \equiv b \pmod{n}$, entonces $a + x \equiv b + x \pmod{n}$.
- Si $a \equiv b \pmod{n}$, entonces $a \cdot x \equiv b \cdot x \pmod{n}$.
- Si $a \equiv b \pmod{n}$ y $x \equiv y \pmod{n}$, entonces $a + x \equiv b + y \pmod{n}$.
- $a^n \equiv b^n \pmod{m} \forall n \in \mathbb{N}$
- Dispuesto a completar y/o agregar cosas

2 Fibonacci

La secuencia tiene un monton de propiedades interesantes. Algunas de ellas son:

Teorema 2.1 (Identidad de Cassini).

$$F_{n-1}F_{n+1} - F_n^2 = (-1)^n$$

Teorema 2.2 (Regla de adición).

$$F_{n+k} = F_k F_{n+1} + F_{k-1} F_n$$

Teorema 2.3 (Aplicando la regla previa a $k = n$ conseguimos:).

$$F_{2n} = F_n(F_{n+1} + F_{n-1})$$

Teorema 2.4. *Con la definicion anterior se puede probar que para cualquier entero positivo k , F_{nk} es multiplo de F_n*

Teorema 2.5. *El inverso del anterior tambien es verdad, si F_m es multiplo de F_n entonces m es multiplo de n*

Teorema 2.6 (Identidad del GCD).

$$GCD(F_m, F_n) = F_{GCD(m,n)}$$

- Solo para saber, los numeros de Fibonacci son el peor caso en la entrada del gcd extendido

2.1 Formula de Binet

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$

Podemos deducir la formula siguiente, redondeando hacia el entero mas proximo:

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$

Como estas dos formulas requieren alta precision casi no tienen uso practico.

2.2 Calculando el F en $O(\log n)$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

El codigo que lo implementa esta en la pagina xxx

Expandiendo la matriz para $n = 2k$

$$\begin{pmatrix} F_{2k+1} & F_{2k} \\ F_{2k} & F_{2k-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{2k} = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix}^2$$

Encontramos estas ecuaciones simples:

$$F_{2k+1} = F_{k+1}^2 + F_k^2 \tag{1}$$

$$F_{2k} = F_k(F_{k+1} + F_{k-1}) = F_k(2F_{k+1} - F_k) \tag{2}$$

Gracias a estas ecuaciones tenemos el codigo en la pagina xx para calcular el fibonacci en tiempo logaritmico

2.3 Suma de $F_0 + F_1 + \dots + F_n$

La suma resulta en $F_{n+2} - 1$

2.4 Es Fibonacci?

Un numero x pertenece a la secuencia de fibonacci si y solo si alguna (o ambas) expresiones siguientes son cuadrado(s) perfecto(s):

$$5x^2 + 4$$

$$5x^2 - 4$$

3 Funciones Aritméticas

Las funciones aritméticas son aquellas que se definen en los números enteros y tienen aplicaciones importantes en teoría de números.

3.1 Función ϕ de Euler

La función $\phi(n)$ cuenta el número de enteros positivos menores o iguales que n que son coprimos con n .

Dos numeros son "coprimos" cuando el $\gcd(a, b) = 1$

La funcion *phi* hasta 21:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8	12

3.1.1 Propiedades

- Si p_1, p_2, \dots, p_k son los factores primos distintos de n , entonces:

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

- Si p es un numero primo, entonces el $\gcd(p, q) = 1$ para todo $1 \leq q < p$ Entonces tenemos:

$$\phi(p) = p - 1.$$

- Si p es un numero primo y $k \geq 1$ entonces hay exactamente $\frac{p^k}{p}$ entre 1 y p^k que son divisibles por p Lo que nos da:

$$\phi(p^k) = p^k - p^{k-1}.$$

- Si a y b son coprimos, entonces:

$$\phi(ab) = \phi(a) \cdot \phi(b).$$

- De la propiedad de arriba se extiende que, si a es un número con una factorización prima:

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$$

donde p_1, p_2, \dots, p_k son primos distintos y e_1, e_2, \dots, e_k son exponentes enteros positivos, entonces la función $\phi(a)$ se calcula como:

$$\phi(a) = \phi(p_1)^{e_1} \cdot \phi(p_2)^{e_2} \cdot \dots \cdot \phi(p_k)^{e_k}$$

Ojo, si ya tienes la criba con los primos, facil puedes precalcular la funcion phi de un numero, entonces con la factorizacion del numero en $\mathcal{O} \log(n)$ podemos facil tener el resultado del la funcion ϕ

4 Conclusiones

La teoría de números es una de las ramas más antiguas de las matemáticas y sigue siendo un área activa de investigación. Desde su aplicación en criptografía hasta su influencia en otras ramas matemáticas, los resultados de esta teoría continúan jugando un papel crucial.