

Teoría de Números

Jaime Sebastian Chavarria Fuentes

December 30, 2024

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 $a + x \equiv b + y \pmod{n}$.
- $a^n \equiv b^n \pmod{n} \quad \forall n \in \mathbb{N}$
- 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 definición anterior se puede probar que para cualquier entero positivo k , F_{nk} es múltiplo de F_n

Teorema 2.5. El inverso del anterior también es verdad, si F_m es múltiplo de F_n entonces m es múltiplo de n

Teorema 2.6 (Identidad del GCD).

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

- Solo para saber, los números 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 fórmula siguiente, redondeando hacia el entero más próximo:

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

Como estas dos fórmulas requieren alta precisión casi no tienen uso práctico.

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 código que lo implementa está en la página 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 código en la página xx para calcular el fibonacci en tiempo logarítmico

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 Números Primos

Definición 3.1 (Número Primo). *Un numero es primos si y solo si tiene únicamente dos divisores*

4 Funciones Aritméticas

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

Definición 4.1 (Función ϕ de Euler). *La función $\phi(n)$ cuenta el número de enteros positivos menores o iguales que n que son coprimos con n .*

Teorema 4.2 (Propiedad de la función ϕ). *Si p_1, p_2, \dots, p_k son los factores primos distintos de n , entonces:*

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

Ejemplo 4.3. Para $n = 12$, los factores primos son 2 y 3, por lo que:

$$\phi(12) = 12 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 12 \times \frac{1}{2} \times \frac{2}{3} = 4$$

5 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.