Teoría de Números - Órdenes

Jesús Liceaga
jose.liceaga@cimat.mx
25 de Febrero de 2022

---

1. Un breve recordatorio

En este documento, utlizaremos la siguiente notación:

- Dado un entro positivo n, denotamos como $\varphi(n)$ al número de enteros positivos menores o iguales a n que son primos relativos con n.
- Si p es un número primo y $a \in \mathbb{Z}$, denotamos como $\nu_p(a)$ al mayor entero no negativo tal que $p|a^{\nu_p(a)}$.

Teorema 1.1. Supongamos que la descomposición en primos de n es $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Entonces

$$\varphi(n) = p_1^{\alpha_1 - 1} \dots p_n^{\alpha_n - 1}(p_1 - 1) \dots (p_n - 1)$$

Teorema 1.2 (Euler). Sea n un entero positivo y $a \in \mathbb{Z}$ tal que $(a, n) = 1$. Entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$.

1.1. Ejercicios

Ejercicio 1.1. ¿Qué residuo deja 3^{120} al dividirlo entre 20?

Ejercicio 1.2. ¿Qué residuo deja 2^{2023} al dividirlo entre 120?

Ejercicio 1.3. Sean m, n enteros positivos. Demuestra que $\varphi(m^n - 1)$ es divisible entre n.

2. El orden de un número módulo n

Definición 2.1. Sean a, n enteros positivos primos relativos. Al menor entero positivo k tal que $a^k \equiv 1(\text{mod } n$ se le conoce como el *orden de a módulo n* y se denota como $o_n(a)$.

Teorema 2.1. Si a, n, k son enteros positivos tales que $(a, n) = 1$ y $a^k \equiv 1(\text{mod } n)$. Entonces $\text{ord}_n(a)|k$.

Corolario 2.1. Si a, n son enteros positivos primos relativos, entonces $\text{ord}_n(a)|\varphi(n)$.

2.1. Ejercicios

Ejercicio 2.1. Encuentra $o_5(4)$.

Ejercicio 2.2. Encuentra $o_{101}(2)$.

Ejercicio 2.3. Encuentra el menor múltiplo de 19 cuyos dígitos son todos iguales a 1.

Ejercicio 2.4. Encuentra el menor entero positivo n tal que 2^{2023} divide a $17^n - 1$.

Ejercicio 2.5. Sea n un entero positivo. Demuestra que $n|\varphi(a^n - 1)$ para todo entero positivo a.

Ejercicio 2.6. Demuestra que no existe un entero positivo $n > 1$ tal que $n|2^n - 1$.

Ejercicio 2.7. Demuestra que $3^n - 2^n$ no es divisible por n para ningún entero $n \geq 2$.

Ejercicio 2.8. Demuestra que si p es un número primo mayor a 3, entonces cualquier divisor positivo del número

$$\frac{2^p + 1}{3}$$

es de la forma $2kp + 1$, donde k es un entero no negativo.

Ejercicio 2.9. Demuestra que $o_{3^n}(2) = 2 \cdot 3^{n-1}$.

Ejercicio 2.10. Sea $k \geq 2$ un entero y $n_1, \ldots, n_k$ enteros positivos tales que $n_1|2^{n_2} + 1$, $n_2|2^{n_3} + 1$, … , $n_k|2^{n_1} + 1$. Demuestra que $n_1 = n_2 = \cdots = n_k = 1$.

Ejercicio 2.11. Encuentra el menor entero $n > 1$ que no sea una potencia de 3 tal que $n|2^n + 1$.

Ejercicio 2.12. Determina todos los enteros positivos $m, n \geq 2$ tales que

$$\frac{1 + m^{3^n} + m^{2 \cdot 3^m}}{n}$$

es un número entero.