Teoría de Números

Congruencias y Potencias módulo m

Víctor Castellanos V.

Entrenamiento para la OMET
Julio de 2025.

Índice

1. Congruencias **1**

1.1. Definición 1
1.2. Propiedades fundamentales 2
1.3. Clases residuales 2
1.4. Ejemplo 1 2
1.5. Ejemplo 2 2
1.6. Ejercicios 3

2. Potencias módulo m **3**

2.1. Orden de un elemento 3
2.2. Teorema pequeño de Fermat 3
2.3. Teorema de Euler 3
2.4. Ejemplo 1 3
2.5. Ejemplo 2 4
2.6. Ejercicios 4

3. Problemas tipo Olimpiada **4**

Introducción

Estas notas están dirigidas a estudiantes de nivel medio superior que se preparan para competencias nacionales de matemáticas. El énfasis está en el razonamiento, la correcta manipulación de congruencias y el uso estratégico de resultados clásicos como los teoremas de Fermat y Euler.

1. Congruencias

1.1. Definición

Sean $a, b, m \in \mathbb{Z}$ con $m > 0$. Decimos que a es congruente con b módulo m si

$$m \mid (a - b).$$

Esto se denota por

$$a \equiv b \pmod{m}.$$

1.2. Propiedades fundamentales

Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces:

- $a + c \equiv b + d \pmod{m}$,
- $a - c \equiv b - d \pmod{m}$,
- $ac \equiv bd \pmod{m}$,
- $a^k \equiv b^k \pmod{m}$ para todo $k \in \mathbb{N}$.

1.3. Clases residuales

Los enteros se dividen en m clases residuales:

$$[0], [1], \ldots, [m-1],$$

donde

$$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}.$$

1.4. Ejemplo 1

Determinar si $137 \equiv 17 \pmod{10}$.

Solución paso a paso

1. Calculamos la diferencia: $137 - 17 = 120$.
2. Como $10 \mid 120$, la congruencia es verdadera.
3. Por tanto, $137 \equiv 17 \pmod{10}$.

1.5. Ejemplo 2

Resolver la congruencia

$$7x \equiv 1 \pmod{26}.$$

Solución paso a paso

1. Buscamos el inverso de 7 módulo 26.
2. Aplicamos el algoritmo de Euclides:

$$26 = 3 \cdot 7 + 5, \quad 7 = 1 \cdot 5 + 2, \quad 5 = 2 \cdot 2 + 1.$$

3. Retrocediendo:

$$1 = 5 - 2 \cdot 2 = 3 \cdot 5 - 2 \cdot 7.$$

4. Como $5 = 26 - 3 \cdot 7$, obtenemos
$$1 = 3 \cdot 26 - 11 \cdot 7.$$
5. Entonces $-11 \equiv 15 \pmod{26}$ es el inverso de 7.
6. La solución es $x \equiv 15 \pmod{26}$.

1.6. Ejercicios

1. Determinar el residuo de 2^{1001} módulo 3.
2. Resolver $12x \equiv 8 \pmod{20}$.
3. Probar que si $a \equiv b \pmod{m}$, entonces $a^3 \equiv b^3 \pmod{m}$.
4. Encontrar todos los enteros x tales que $5x \equiv 10 \pmod{15}$.
5. Calcular el último dígito de 7^{2023}.
6. Probar que $n^2 \equiv 0, 1 \pmod{4}$ para todo entero n.

2. Potencias módulo m

2.1. Orden de un elemento

Sea a un entero coprimo con m. El *orden de a módulo m* es el menor entero positivo k tal que
$$a^k \equiv 1 \pmod{m}.$$

2.2. Teorema pequeño de Fermat

Teorema 1. *Si p es primo y $\gcd(a, p) = 1$, entonces*
$$a^{p-1} \equiv 1 \pmod{p}.$$

2.3. Teorema de Euler

Teorema 2. *Si $\gcd(a, m) = 1$, entonces*
$$a^{\varphi(m)} \equiv 1 \pmod{m},$$
donde φ es la función indicatriz de Euler.

2.4. Ejemplo 1

Calcular $3^{100} \pmod{7}$.

Solución

1. Por Fermat, $3^6 \equiv 1 \pmod{7}$.

2. Escribimos $100 = 6 \cdot 16 + 4$.

3. Entonces
$$3^{100} \equiv 3^4 \equiv 81 \equiv 4 \pmod 7.$$

2.5. Ejemplo 2

Calcular $7^{222} \pmod{40}$.

Solución

1. $\gcd(7, 40) = 1$ y $\varphi(40) = 16$.
2. Entonces $7^{16} \equiv 1 \pmod{40}$.
3. Como $222 = 16 \cdot 13 + 14$, se obtiene
$$7^{222} \equiv 7^{14} \equiv 9 \pmod{40}.$$

2.6. Ejercicios

1. Calcular $2^{1000} \pmod 9$.
2. Hallar el orden de 3 módulo 10.
3. Determinar $5^{1234} \pmod{11}$.
4. Probar que el orden de a módulo m divide a $\varphi(m)$.
5. Encontrar el último dígito de 9^{999}.
6. Calcular $11^{2025} \pmod{12}$.

3. Problemas tipo Olimpiada

Problemas

1. Demostrar que para todo entero n,
$$n^5 - n \equiv 0 \pmod{30}.$$
2. Sea $p > 3$ un primo. Probar que $p^2 - 1$ es divisible por 24.
3. Calcular el residuo de $2^{2025} + 3^{2025}$ módulo 5.
4. Sea a un entero impar. Probar que
$$a^{2^n} \equiv 1 \pmod 8$$
para todo $n \geq 1$.

5. Determinar todos los enteros n tales que

$$n^2 \equiv 1 \pmod{24}.$$

6. Probar que si $\gcd(a, 10) = 1$, entonces

$$a^4 \equiv 1 \pmod{10}.$$

Pistas

- Factorizar y trabajar módulo 2, 3 y 5.
- Usar que $p^2 - 1 = (p-1)(p+1)$.
- Aplicar Fermat y separar potencias.
- Proceder por inducción.
- Analizar el problema módulo 8 y módulo 3.
- Usar que $\varphi(10) = 4$.

Bibliografía

1. W. Mora, *Introducción a la Teoría de Números. Ejemplos y algoritmos*, ITCR, 2010.
2. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer.
3. G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford.
4. M. Rosen, *Elementary Number Theory and Its Applications*, Pearson.