Unidad VII: Teoría de números

Teoría de números: Inversos modulares, Fermat y RSA

Clase 21 - Matemáticas Discretas (IIC1253)

Prof. Miguel Romero

Inversos modulares

Sea $n \geq 2$ un natural.

Definición:

Sean $a, b \in \mathbb{Z}$. Decimos que b es **inverso** de a en módulo n si:

$$(a \cdot b) \equiv_n 1.$$

Equivalentemente: $(a \cdot b) \bmod n = 1$.

Ejemplos:

- 3 es el inverso de 2 en módulo 5, ya que $3 \cdot 2 \equiv_5 1$.
- 2 **no** tiene inverso en módulo 4. (¿por qué?)

¿Cuándo existe inverso en modulo n?

Sea $n \geq 2$ un natural.

Teorema:

a tiene inverso en módulo n si y sólo si $\text{MCD}(a, n) = 1$.

Demostración ($\Rightarrow$):

Suponga que a tiene inverso en módulo n, digamos b.

- Entonces: $a \cdot b \equiv_n 1$.

Obtenemos que $a \cdot b - 1 = \alpha \cdot n$, luego $1 = a \cdot b - \alpha \cdot n$.

Sea $c \geq 1$ un divisor común de a y n, es decir, se cumple $c \mid a$ y $c \mid n$.

Obtenemos que $c \mid 1$, y luego $c = 1$.

Concluimos que $\text{MCD}(a, n) = 1$.

Sea $n \geq 2$ un natural.

Teorema:

a tiene inverso en módulo n si y sólo si $\text{MCD}(a, n) = 1$.

Demostración ($\Leftarrow$):

De la identidad de Bézout, obtenemos que existen $s, t \in \mathbb{Z}$ tal que:

$$1 = s \cdot a + t \cdot n$$

Luego: $1 - s \cdot a = t \cdot n$

Concluimos que $s \cdot a \equiv_n 1$.

- Es decir, s es inverso de a en módulo n.

Sea $n \geq 2$ un natural.

Teorema:

a tiene inverso en módulo n si y sólo si $\text{MCD}(a, n) = 1$.

Comentarios:

- Cuando $\text{MCD}(a, n) = 1$ decimos que a y n son **primos relativos**.
- Si a tiene inverso módulo n, entonces es único (modulo n):
  - Si b y c son inversos, entonces $b \equiv_n c$.
- Si a tiene inverso módulo n, entonces la ecuación

$$a \cdot x \equiv_n d$$

siempre tiene una única solución (modulo n).

Teorema:

Sea $p \geq 2$ un número primo. Para todo $a \geq 0$, se cumple que $a^p \equiv_p a$.

Demostración:

Aplicamos inducción en a.

Para $a = 0$ y $a = 1$ se cumple directamente.

Supongamos que la propiedad se cumple para $a \geq 1$.

- $a^p \equiv_p a$

Debemos demostrar que se cumple para $a + 1$

- $(a + 1)^p \equiv_p (a + 1)$.

Si $a, b, p > 0$, entonces:

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

donde

$$\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!}$$

Teorema:

Sea $p \geq 2$ un número primo. Para todo $a \geq 0$, se cumple que $a^p \equiv_p a$.

Demostración:

Supongamos que la propiedad se cumple para $a \geq 1$.

- $a^p \equiv_p a$

Debemos demostrar que se cumple para $a+1$

- $(a+1)^p \equiv_p (a+1)$.

Tenemos que:

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} \cdot a^k$$

Luego:

$$(a+1)^p - (a+1) = 1 + \sum_{k=1}^{p-1} \binom{p}{k} \cdot a^k + a^p - (a+1) = (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} \cdot a^k$$

Teorema:

Sea $p \geq 2$ un número primo. Para todo $a \geq 0$, se cumple que $a^p \equiv_p a$.

Demostración:

$$(a+1)^p - (a+1) \;=\; (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} \cdot a^k$$

Veamos que $p \mid \binom{p}{k}$, para $k \in \{1, \ldots, p-1\}$.

Por definición:

$$\binom{p}{k} \;=\; \frac{p!}{k! \cdot (p-k)!} \;=\; \frac{p \cdot (p-1) \cdot \ldots \cdot (p-k+1)}{k!}$$

Como p es primo y $k \in \{1, \ldots, p-1\}$:

$\frac{(p-1)\cdot\ldots\cdot(p-k+1)}{k!}$ debe ser un número entero (¿por qué?)

Obtenemos que $\binom{p}{k} = p \cdot \alpha$, para $\alpha \in \mathbb{Z}$.

Teorema:

Sea $p \geq 2$ un número primo. Para todo $a \geq 0$, se cumple que $a^p \equiv_p a$.

Demostración:

$$(a+1)^p - (a+1) \;=\; (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} \cdot a^k$$

Tenemos que $p \mid \binom{p}{k}$, para $k \in \{1, \ldots, p-1\}$.

Esto nos dice que $p \mid \sum_{k=1}^{p-1} \binom{p}{k} \cdot a^k$.

Por otra parte, por hipótesis inductiva, sabemos que $p \mid (a^p - a)$.

Concluimos que $p \mid (a+1)^p - (a+1)$, es decir, $(a+1)^p \equiv_p (a+1)$.

Corolario:

Sea $p \geq 2$ un número primo. Para todo $a \in \{1, \ldots, p-1\}$, se cumple que $a^{p-1} \equiv_p 1$.

Demostración:

Como p es primo y $a \in \{1, \ldots, p-1\}$, se cumple que $\text{MCD}(a, p) = 1$.

Luego, a tiene un inverso en modulo p, digamos b.

- Se tiene que $b \cdot a \equiv_p 1$.

Por el pequeño teorema de Fermat, sabemos que $a^p \equiv_p a$.

Multiplicando ambos lados por b, obtenemos:

$$b \cdot a^p \equiv_p b \cdot a \implies (b \cdot a) \cdot a^{p-1} \equiv_p 1 \implies a^{p-1} \equiv_p 1$$