

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 módulo  $n$ ?

# Inversos modulares

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

# Inversos modulares

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  $n$ .

# Inversos modulares

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  $n$ ).

## Pequeño teorema de Fermat

### 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  $a + 1$ :

■  $(a + 1)^p \equiv_p (a + 1)$

## Paréntesis: Teorema del binomio

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

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

donde

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

## Pequeño teorema de Fermat

### 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  $a \geq 1$ .

$$\blacksquare a^p \equiv_p a$$

Debemos demostrar que se cumple para  $a + 1$ :

$$\blacksquare (a + 1)^p \equiv_p (a + 1)$$

Tenemos que:

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

Luego:

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



## Pequeño teorema de Fermat

### 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  $k \in \{1, \dots, p-1\}$ .

Por definición:

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

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

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

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

## Pequeño teorema de Fermat

### 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  $k \in \{1, \dots, p-1\}$ .

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

## Pequeño teorema de Fermat

### Corolario:

Sea  $p \geq 2$  un número primo.

Para todo  $a \geq 0$  tal que  $a \not\equiv_p 0$ , se cumple que  $a^{p-1} \equiv_p 1$ .

### Demostración:

Como  $p$  es primo y  $a \not\equiv_p 0$ , se cumple que  $\text{MCD}(a, p) = 1$ .

Luego,  $a$  tiene un inverso en módulo  $p$ , 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:

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

## Una aplicación: RSA

- Sistema criptográfico desarrollado por Rivest, Shamir y Adleman.
  - Muy utilizado en la actualidad.
- No requiere que las partes acuerden una misma clave secreta.
- Cada usuario tiene una **clave pública** y una **clave secreta**.
- Para enviar un mensaje al usuario  $A$ , se **cifra** con la **clave pública** de  $A$ , y el usuario  $A$  **decifra** el mensaje con su **clave secreta**.

## El sistema RSA

Un usuario  $A$  aplica el siguiente algoritmo para generar su clave pública  $P_A$  y clave secreta  $S_A$ :

1. Generar al azar dos números primos distintos  $P$  y  $Q$ .
2. Definir  $N = P \cdot Q$  y  $\varphi(N) = (P - 1) \cdot (Q - 1)$ .
3. Generar al azar un número  $d \in \{0, \dots, \varphi(N)\}$  tal que  $\text{MCD}(d, \varphi(N)) = 1$ .
4. Calcular un número  $e$  tal que  $(e \cdot d) \bmod \varphi(N) = 1$ .
5. Definir  $P_A = (e, N)$  y  $S_A = (d, N)$ .

## El sistema RSA

Sea un usuario  $A$  con clave pública  $P_A = (e, N)$  y secreta  $S_A = (d, N)$ .

Para cifrar un mensaje con la clave pública de  $A$  se usa la siguiente función.

Dado un mensaje  $m \in \{0, \dots, N-1\}$ :

$$\text{Cif}(P_A, m) = m^e \bmod N$$

Para decifrar un mensaje con la clave secreta de  $A$  se usa la siguiente función.

Dado un mensaje  $m \in \{0, \dots, N-1\}$ :

$$\text{Dec}(S_A, m) = m^d \bmod N$$

## El sistema RSA: ejemplo

### Ejemplo:

Sean  $P = 7$  y  $Q = 11$ .

- Se tiene que  $N = 77$  y  $\varphi(N) = 60$ .

Sea  $d = 37$ .

- Se tiene que  $\text{MCD}(37, 60) = 1$ .

Sea  $e = 13$ .

- Se tiene que  $(13 \cdot 37) \bmod 60 = 1$ .

Definimos  $P_A = (13, 77)$  y  $S_A = (37, 77)$ .

## El sistema RSA: ejemplo

### Ejemplo:

Ciframos y desciframos un mensaje  $m \in \{0, \dots, 76\}$  de la siguiente forma:

$$Cif(P_A, m) = m^{13} \bmod 77$$

$$Dec(S_A, m) = m^{37} \bmod 77$$

El sistema funciona correctamente:

$$Cif(P_A, 5) = 5^{13} \bmod 77 = 26$$

$$Dec(S_A, 26) = 26^{37} \bmod 77 = 5$$



## ¿Por qué funciona RSA?

¿Qué propiedades debemos demostrar que son ciertas?

- $Dec(S_A, Cif(P_A, m)) = m$ , para todo  $m \in \{0, \dots, N-1\}$ .

¿Qué problemas debemos demostrar que pueden ser resueltos de manera eficiente para que el sistema pueda ser utilizado?

- Generar primos distintos  $P$  y  $Q$ .
- Generar un número  $d$  tal que  $MCD(d, \varphi(N)) = 1$ .
- Generar un número  $e$  tal que  $(e \cdot d) \bmod \varphi(N) = 1$ .
- Calcular funciones  $Cif$  y  $Des$ .

¿Qué problemas no pueden ser resueltos de manera eficiente para que el sistema sea seguro?

- Dado  $(e, N)$  calcular  $d$ , lo cual se reduce a encontrar los divisores de  $N$ .

## RSA funciona correctamente

Sean  $P_A$ ,  $S_A$ ,  $Cif$  y  $Dec$  definidas como antes.

- En particular  $P_A = (e, N)$  y  $S_A = (d, N)$ , con  $N = P \cdot Q$ .

### Teorema (Rivest-Shamir-Adleman):

Para cada  $m \in \{0, \dots, N-1\}$ , se tiene que  $Dec(S_A, Cif(P_A, m)) = m$ .

## RSA funciona correctamente: demostración

Tenemos que

$$\begin{aligned} \text{Dec}(S_A, \text{Cif}(P_A, m)) &= (m^e \bmod N)^d \bmod N \\ &= (m^e)^d \bmod N \\ &= m^{e \cdot d} \bmod N \end{aligned}$$

Por lo tanto, tenemos que demostrar que  $m^{e \cdot d} \equiv_N m$ .

Sabemos que  $(e \cdot d) \bmod \varphi(N) = 1$ .

■ Por lo tanto,  $e \cdot d = k \cdot \varphi(N) + 1$ .

Tenemos que demostrar que  $m^{k \cdot \varphi(N) + 1} \equiv_N m$ .

■ El siguiente lema es fundamental para la demostración.

## RSA funciona correctamente: demostración

### Lema:

$$m^{k \cdot \varphi(N)+1} \equiv_P m \text{ y } m^{k \cdot \varphi(N)+1} \equiv_Q m$$

### Demostración:

Veamos que  $m^{k \cdot \varphi(N)+1} \equiv_P m$  (el caso de  $Q$  es análogo).

Supongamos primero que  $m \equiv_P 0$ . Tenemos que:

$$\begin{aligned} m^{k \cdot \varphi(N)+1} \bmod P &= (m \bmod P)^{k \cdot \varphi(N)+1} \bmod P \\ &= 0^{k \cdot \varphi(N)+1} \bmod P \\ &= 0 \\ &= m \bmod P \end{aligned}$$

Concluimos que  $m^{k \cdot \varphi(N)+1} \equiv_P m$ .

## RSA funciona correctamente: demostración

### Lema:

$$m^{k \cdot \varphi(N)+1} \equiv_P m \text{ y } m^{k \cdot \varphi(N)+1} \equiv_Q m$$

### Demostración:

Veamos que  $m^{k \cdot \varphi(N)+1} \equiv_P m$  (el caso de  $Q$  es análogo).

Segundo, asumamos que  $m \not\equiv_P 0$ .

Por el pequeño Teorema de Fermat, sabemos que  $m^{P-1} \equiv_P 1$ .

Tenemos que:

$$\begin{aligned} m^{k \cdot \varphi(N)+1} \bmod P &= ((m^{P-1})^{k \cdot (Q-1)} \cdot m) \bmod P \\ &= ((m^{P-1} \bmod P)^{k \cdot (Q-1)} \cdot m) \bmod P \\ &= (1^{k \cdot (Q-1)} \cdot m) \bmod P \\ &= m \bmod P \end{aligned}$$

Concluimos que  $m^{k \cdot \varphi(N)+1} \equiv_P m$ .

## RSA funciona correctamente: Demostración

Del lema concluimos que:

$$m^{k \cdot \varphi(N)+1} - m = \alpha \cdot P$$

$$m^{k \cdot \varphi(N)+1} - m = \beta \cdot Q$$

Por lo tanto,  $\alpha \cdot P = \beta \cdot Q$ . Tenemos entonces que  $P \mid (\beta \cdot Q)$ .

Dado que  $P$  y  $Q$  son primos distintos tenemos que  $P \mid \beta$ .

- Por lo tanto,  $\beta = \gamma \cdot P$ .

Concluimos que  $m^{k \cdot \varphi(N)+1} - m = \gamma \cdot P \cdot Q$ .

- Es decir,  $m^{k \cdot \varphi(N)+1} \equiv_N m$ .

¿Cómo se pueden resolver los siguientes problemas de manera eficiente?

- Generar primos distintos  $P$  y  $Q$ .
- Generar un número  $d$  tal que  $\text{MCD}(d, \varphi(N)) = 1$ .
- Generar un número  $e$  tal que  $(e \cdot d) \bmod \varphi(N) = 1$ .
- Calcular funciones  $Cif$  y  $Des$ .