

# Matemática Discreta I

## Clase 18 - Congruencia 3

FAMAF / UNC

19 de mayo de 2020

# El Teorema (pequeño) de Fermat

El siguiente lema nos sirve de preparación para la demostración del Teorema (o fórmula) de Fermat.

## Lema

*Sea  $p$  un número primo, entonces*

$$(a) \quad p \mid \binom{p}{r}, \text{ con } 0 < r < p,$$

$$(b) \quad (a + b)^p \equiv a^p + b^p \pmod{p}.$$

## Demostración

(a) Escribamos el número binomial de otra forma:

$$\binom{p}{r} = \frac{p!}{r!(p-r)!} = p \cdot \frac{(p-1)!}{r!(p-r)!},$$

luego

$$\binom{p}{r} \cdot r!(p-r)! = p \cdot (p-1)!.$$

Por lo tanto,

(1)  $p \mid \binom{p}{r} \cdot r!(p-r)!$ . Además,

(2)  $r < p \Rightarrow p \nmid r!$ .

(3)  $r > 0 \Rightarrow p-r < p \Rightarrow p \nmid (p-r)!$ .

De (1), (2) y (3),

$$p \mid \binom{p}{r} \cdot r!(p-r)! \quad \wedge \quad p \nmid r!(p-r)!$$

por lo tanto ( $p$  es primo)

$$p \mid \binom{p}{r}.$$

(b) Por el teorema del binomio sabemos que

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

Por (a) es claro que  $\binom{p}{i} a^i b^{p-i} \equiv 0 \pmod{p}$ , si  $0 < i < p$ .

Luego se deduce el resultado. □

El siguiente es el llamado teorema de Fermat.

### Teorema

*Sea  $p$  un número primo y  $a$  número entero. Entonces*

$$a^p \equiv a \pmod{p}.$$

### Demostración

Dividiremos la demostración en 2 casos (1)  $a \geq 0$ , (2)  $a < 0$ .

(1)  $a \geq 0$ . Por inducción sobre  $a$ .

*Caso base  $a = 0$ .  $0^p \equiv 0 \pmod{p}$ , es trivial.*

*Paso inductivo.* Si  $k \geq 0$ , la hipótesis inductiva es:

$$k^p \equiv k \pmod{p}. \quad (\text{HI})$$

Debemos probar,

$$(k+1)^p \equiv k+1 \pmod{p}. \quad (\text{T})$$

Ahora bien,

$$\begin{aligned} (k+1)^p &\equiv k^p + 1^p \pmod{p} && (\text{por (b) del lema}) \\ &\equiv k+1 \pmod{p} && (\text{por HI}). \end{aligned}$$

Es decir  $(k+1)^p \equiv k+1 \pmod{p}$ , que es lo que queríamos probar.

(2)  $a < 0$ . Como  $a < 0$ , entonces  $-a > 0$ , luego por (1):  
 $(-a)^p \equiv -a \pmod{p}$  o, equivalentemente

$$(-1)^p a^p \equiv (-1)a \pmod{p} \quad (1)$$

Ahora bien,

$p > 2$ , entonces  $(-1)^p = -1$ , en particular  $(-1)^p \equiv -1 \pmod{p}$ .

$p = 2$ , entonces  $(-1)^p = 1$ , pero como  $1 \equiv -1 \pmod{2}$ ,  $(-1)^p \equiv -1 \pmod{p}$ .

Luego  $(-1)^p \equiv -1 \pmod{p}$  para todo  $p$  primo y la ecuación (??) es equivalente a:

$$(-1)a^p \equiv (-1)a \pmod{p}$$

Multiplicando por  $-1$  la ecuación obtenemos  $a^p \equiv a \pmod{p}$ . □

Supongamos que  $a$  y  $p$  son coprimos, por Fermat

$$p|(a^p - a) = a(a^{(p-1)} - 1).$$

Como  $p$  no divide a  $a$ , tenemos que  $p|(a^{(p-1)} - 1)$ , es decir

### Teorema

*Si  $a$  y  $p$  coprimos y  $p$  es primo, entonces*

$$a^{(p-1)} \equiv 1 \pmod{p}.$$

Este último enunciado es también conocido como teorema de Fermat.



## Definición

Sea  $n \geq 1$ , La *función de Euler* se define

$$\phi(n) := |\{x : \text{mcd}(x, n) \wedge 1 \leq x < n\}|.$$

El teorema de Fermat, 2° versión, admite la siguiente generalización, llamada teorema de Euler:

## Teorema

*Si  $n$  un entero positivo y  $a$  un número entero coprimo con  $n$ , entonces*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

## Ejemplo

Usar el teorema de Fermat, 2° versión, para calcular el resto de dividir  $3^{47}$  por 23.

## Solución

Podemos calcular  $3^i \equiv a_i \pmod{23}$  para  $0 \leq i < 23$ . Como alguno se va a repetir, podemos usar eso para hacer el cálculo.

El teorema de Fermat nos evita unos cuantos pasos.

Como 23 es un número primo (y es coprimo con 3)

$$3^{22} \equiv 1 \pmod{23},$$

Luego

$$3^{47} \equiv 3^{22 \cdot 2 + 3} \equiv 3^{22 \cdot 2} 3^3 \equiv (3^{22})^2 3^3 \equiv 3^3 \equiv 27 \equiv 4 \pmod{23}$$

Luego el resto de dividir  $3^{47}$  por 23 es 4. □

# Algoritmo RSA

Dados primos distintos  $p$  y  $q$  suficientemente grandes tomamos  $n = pq$ .

- Sea  $e$  con  $1 < e < (p-1)(q-1)$  tal que

$$\text{mcd}(e, (p-1)(q-1)) = 1.$$

- Sea  $d$  tal  $0 \leq d < (p-1)(q-1)$  y que

$$ed \equiv 1 \pmod{(p-1)(q-1)}.$$

## Proposición

Si  $0 \leq m < n$ , entonces

$$m \equiv m^{ed} \pmod{n}.$$

# Algoritmo RSA - procedimiento

Decimos que:

- $(e, n)$  es la *clave pública*.
- $d$  es la *clave privada*.

$A$  le quiere enviar un mensaje encriptado a  $B$ .

## Preliminares

- $A$  conoce la clave pública  $(e, n)$ .
- $B$  conoce la clave pública y una clave privada  $d$ .

## Protocolo

- $A$  le quiere enviar el mensaje  $m$  a  $B$ .
- $A$  calcula  $c \equiv m^e \pmod{n}$  y le envía  $c$  a  $B$
- $B$  descifra el mensaje:  $c^d \equiv (m^e)^d \equiv m \pmod{n}$ .

## Observación

- Los dos primos  $p$  y  $q$  deberían tener alrededor de 100 dígitos cada uno (longitud considerada segura en este momento).
- El número  $e$  puede elegirse pequeño y se selecciona haciendo prueba y error con el algoritmo de Euclides, es decir probando hasta encontrar un  $e$  tal que  $\text{mcd}(e, (p-1)(q-1)) = 1$ .
- La existencia de  $d$  está garantizada por la ecuación lineal de congruencia), pues  $e$  y  $(p-1)(q-1)$  son coprimos.