Matemática Discreta I
Clase 17 - Teorema de Fermat / RSA

FAMAF / UNC

19 de mayo de 2022

El Teorema (pequeño) de Fermat

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

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) $p \mid \binom{p}{r}$, *con* $0 < r < p$,

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) $p \mid \binom{p}{r}$, *con* $0 < r < p$,

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

Demostración

Demostración

(a) Escribamos el número binomial de otra forma:

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

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

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

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

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

(2) $r < p \Rightarrow p \not| r!$.

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),

$$p \mid \binom{p}{r} \cdot r!(p-r)! \qquad \wedge \qquad p \not| \, r!(p-r)!$$

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

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

por lo tanto (p es primo)

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

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

$$p \Big| \binom{p}{r} \cdot r!(p-r)! \qquad \wedge \qquad p \nmid r!(p-r)!$$

por lo tanto (p es primo)

$$p \Big| \binom{p}{r}.$$

(b) Por el teorema del binomio sabemos que

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

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

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

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 $0 < i < p$.

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

$$p \mid \binom{p}{r} \cdot r!(p-r)! \qquad \wedge \qquad p \not| r!(p-r)!$$

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. $\square$

El siguiente es el llamado teorema de Fermat.

Teorema

Sea p un número primo y a número entero. Entonces

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

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

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) $a < 0$.

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:

$$k^p \equiv k \pmod{p}. \tag{HI}$$

Debemos probar,

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

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

$$k^p \equiv k \pmod{p}. \tag{HI}$$

Debemos probar,

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

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) $a < 0$.

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

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

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

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

Ahora bien,

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

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

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

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

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 (1) es equivalente a:

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

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

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

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 (1) es equivalente a:

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

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

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 $p|(a^{(p-1)} - 1)$,

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

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

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

$$\phi(n) := |\{x \in \mathbb{N} : \operatorname{mcd}(x, n) = 1 \wedge x < n\}|.$$

donde $|\cdot|$ significa la cardinalidad del conjunto.

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^{332} por 23.

Solución

Como 23 es un número primo (y es coprimo con 3), por el teorema de Fermat (2º versión):

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

Ahora bien: $332 = 22 \cdot 15 + 2$, Luego

$$3^{332} \equiv 3^{22\cdot 15+2} \equiv 3^{22\cdot 15}3^2 \equiv (3^{22})^{15}3^2 \equiv 1^{15}3^2 \equiv 3^2 \equiv 9 \pmod{23}$$

Luego el resto de dividir 3^{332} por 23 es 9. $\square$

Algoritmo RSA

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

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

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

- 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 $\mathrm{mcd}(e, (p-1)(q-1)) = 1$.
- La existencia de d está garantizada por la ecuación lineal de congruencia), pues e y $(p-1)(q-1)$ son coprimos.

Consideraciones finales sobre el algoritmo RSA

Hay dos "obstrucciones" para una implementación del algoritmo RSA:

(1) ¿Cómo calcular un número elevado a una potencia de más de 200 dígitos? Hay dos problemas

  (a) La cantidad de multiplicaciones necesarias va más allá de 2^{200}, imposibles de realizar.

  (b) Los números se tornan tan grandes que no entrarían en ninguna memoria.

(2) ¿Cómo saber si un número de más de 100 dígitos es primo o no? No es posible conocer los divisores de un número de ese tamaño.

Consideraciones finales sobre el algoritmo RSA

El problema (1) es fácil de resolver, se usa la técnica llamada *exponenciación modular*, explicada en el apunte, capítulo 4, sección 5.

- La idea para (1)(a) es usar la propiedad siguiente: si $m = 2q + r$, entonces
$$a^m = (a^q)^2 a^r$$
y definir recursivamente la potencia.
- La idea para (1)(b) es usar la idea de (1)(a) y en cada paso reducir módulo n. Es decir, utilizar la propiedad
$$a^m \equiv (a^q)^2 a^r \equiv s \pmod{n}$$
con $0 \leq s < n$.

Consideraciones finales sobre el algoritmo RSA

El problema (2) es más complicado y se usa el llamado el test de primalidad de Miller-Rabin probabilístico.

En el apunte, capítulo 4, sección 6 se explica en que consiste este test.