19/04

Práctico 6: TCR – Teoremas de Euler y Fermat.

En gral. vamos a querer hallar $a^k \pmod n$, nos sirve encontrar $b>0$ t.q. $a^b \equiv 1 (n)$

Obs. dicho exponente no existe si a no es invertible: $a \cdot a^{b-1} \equiv 1 \pmod n$

$\varphi(n) = \#\{a : 0<a<n \text{ y } mcd(a,n)=1\}$

$\varphi(p) = p-1$

$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1-\frac{1}{p}\right)$

φ es multiplicativa: si $mcd(m,n)=1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

$$\varphi(50) = \varphi(2)\cdot\varphi(5^2) = (2-1)(5^2-5) = 1\cdot 20 = 20.$$

T. Euler: Si $mcd(a,n)=1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$

T. Fermat: Si $mcd(a,p)=1 \Rightarrow a^{p-1} \equiv 1 \pmod p$

Ejercicio 5. Cuando pedimos calcular $a \pmod m$ nos referimos a hallar el entero $0 \le x < m$ tal que $a \equiv x \pmod m$, en particular $a^{-1} \pmod m$ denota al inverso de a módulo m. En los siguientes casos, calcular:

a. los últimos dos dígitos de 7^{42} y de 23^{41};

b. $2^{61} \pmod{77}$ y $13^{31} \pmod{77}$ (sug. en el último caso descomponer módulo 7 y módulo 11);

c. $2^{-1} \pmod{55}$ y $2^{38} \pmod{55}$;

d. $123^{253} \pmod{490}$ (sug. descomponer módulo 2, 5 y 49).

(a) Tenemos que calcular $7^{42} \pmod{100}$ y $23^{41} \pmod{100}$

$mcd(7,100)=1$ y $mcd(23,100)=1$, entonces podemos usar T. Euler en ambos casos.

$7^{\varphi(100)} \equiv 1 \pmod{100}$

$\varphi(100) = \varphi(2^2\cdot 5^2) = \varphi(2^2)\cdot\varphi(5^2)$

$= (2^2-2)\cdot(5^2-5)$

$= 2\cdot 20 = 40.$

$7^{40+2} \equiv 7^{40} 7^2$

T. Euler: $7^{\varphi(100)} = 7^{40} \equiv 1 \pmod{100}$

$7^{42} \equiv 1\cdot 49 \pmod{100}$

$23^{\varphi(100)} \equiv 1 \pmod{100}$

$\varphi(100) = 40.$

$23^{41} \equiv 23^{40}\cdot 23 \equiv 23 \pmod{100}$

T. Euler $\equiv 1$

(b) $mcd(2,77)=1$, $mcd(13,77)=1$ } Podemos usar T. Euler en ambos casos.

$2^{61} \pmod{77}$: φ mult. $\varphi(p) = p-1$

$\varphi(77) = \varphi(7 \cdot 11) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60$.

T. Euler: $2^{60} \equiv 1 \pmod{77}$

$2^{61} \equiv 2^{60+1} \equiv 1 \cdot 2 \equiv 2 \pmod{77}$

↑ T. Euler

Necesitamos calcular $x \equiv 13^{31} \pmod{77}$, no nos sirve aplicar T. Euler directamente, pero descomponemos módulo 7 y 11.

Hallamos $*$ $\begin{cases} x \equiv 13^{31} \pmod 7 \\ x \equiv 13^{31} \pmod{11} \end{cases}$

que tiene sol. única mod 77 por Teo. Chino.

Calculemos $13^{31} \pmod 7$:

$\varphi(7) = 6 \Rightarrow 13^6 \equiv 1 \pmod 7$

$13^{31} \equiv 13^{5 \cdot 6 + 1} \equiv (13^6)^5 \cdot 13 \equiv 13 \pmod 7$

↑ Fermat

Calculemos $13^{31} \pmod{11}$

$\varphi(11) = 10 \Rightarrow 13^{10} \equiv 1 \pmod{11}$

$13^{31} \equiv (\underbrace{13^{10}}_{1})^3 \cdot 13 \equiv 13 \pmod{11}$

$*$ nos queda $*$ $\begin{cases} x \equiv 13 \pmod 7 \\ x \equiv 13 \pmod{11} \end{cases}$

La sol. a $*$ es $13 \pmod{77}$

(c) $2^{-1} \pmod{55}$

En gral. $2^{-1} \pmod n$ n impar es $2^{-1} \equiv \text{coc}(n,2) + 1 \pmod n$

En este caso $2^{-1} \pmod{55} \equiv 27 + 1 \equiv 28 \pmod{55}$

$2^{38} \pmod{55}$

$\mcd(2,55)=1 \Rightarrow$ podemos usar T. Euler.

$\varphi(55) = \varphi(5\cdot 11) = \varphi(5)\varphi(11) = 4\cdot 10 = 40.$

T. Euler $2^{40} \equiv 1 \ (55)$

$$2^{38} \equiv 2^{40}\cdot 2^{-2} \equiv (2^{-1})^2 \equiv 28^2 \pmod{55}$$
$$\equiv 784 \pmod{55}$$
$$\equiv 14 \pmod{55}$$

(d) $123^{253} \pmod{490}$

$$\begin{cases} x \equiv 123^{253} \ (49) \\ x \equiv 123^{253} \ (5) \\ x \equiv 123^{253} \ (2) \end{cases}$$

$\varphi(49)=42$, $\varphi(5)=4$ $\longleftrightarrow$ T. Euler módulos 2, 5, 49.

$$\begin{cases} \dots \\ x \equiv 1 \ (5) \\ x \equiv 1 \ (2) \end{cases}$$

descomponer + T. Chino

Ejercicio 9.

a. Probar que 2 es invertible módulo n si y solamente si n es impar. En tal caso, hallar el inverso.

El inverso de 2 mod n es $x \pmod n$ tq

$2x \equiv 1 \pmod n$

tiene sol. si $\mcd(2,n)=1$.

n impar: $n = 2k+1$

$\exists x$ tq $2x \equiv 1 \pmod n \iff \exists x, y$ tq $2x = 1 + ny$

$\iff \exists x,y \ 2x - ny = 1$

Queremos hallar x, sustituimos n por $2k+1$, queremos x e y t.q.

$$\begin{cases} x = k+1 \\ y = 1 \end{cases}$$

$$\iff 2x - (2k+1)y = 1$$
$$\iff 2(k+1) - (2k+1) = 1$$
$$\iff 2k+2-2k-1 = 1$$

El inverso es $x \equiv k+1 \pmod n$ donde $n = 2k+1$.

Ejercicio 6. Sean p y q primos distintos tales que $a^p \equiv a \pmod{q}$ y $a^q \equiv a \pmod{p}$. Probar que $a^{pq} \equiv a \pmod{pq}$.

$$a^{pq} \equiv (a^p)^q \pmod{q} \equiv a^q \pmod{q}$$

T. Fermat: $a^{q-1} \equiv 1 \pmod{q}$ a y q coprimos. (i.e. $a \not\equiv 0 \ (q)$)

$a^q \equiv a \pmod{q}$ $\forall a$.

$\Rightarrow a^{pq} \equiv a^q \equiv a \pmod{q}$

↖ Fermat

Analogo:

$a^{pq} \equiv (a^q)^p \pmod{p} \equiv a^p \pmod{p}$

Fermat $\rightarrow \equiv a \pmod{p}$

Entonces tenemos: $*$ $\begin{cases} a^{pq} \equiv a \pmod{p} \\ a^{pq} \equiv a \pmod{q} \end{cases}$

Por el Teo. Chino $a^{pq} \equiv a \pmod{pq}$ es la única sol. a $*$ módulo pq.