Práctico 9: Raíces Primitivas

Ejercicio 9. Resolver las siguientes congruencias:

a. $x^{27} \equiv 38 \pmod{43}$.

b. $x^{11} \equiv 38 \pmod{43}$.

c. $x^{20} \equiv 38 \pmod{43}$.

d. $28^{z} \equiv 38 \pmod{43}$

(sugerencia: utilizar que si g es raíz primitiva módulo 43, entonces si $x \in U(43)$, se tiene que $x = g^{\alpha}$ para algún $\alpha \in \{0, 1, \cdots 41\}$) 3

a. · Por el ej. anterior 3 es raíz primitiva $\Rightarrow \forall x \in U(43)\ \exists \alpha$ tq $x \equiv 3^{\alpha}\ (43)$

· Por otra parte $\log_3 38 \equiv 4\ (p-1) \rightsquigarrow 3^4 \equiv 38\ (p)$

· (a) $3^{\alpha \cdot 27} \equiv 3^4\ (p) \iff \alpha \cdot 27 \equiv 4\ (p-1)$ ✓

(b) $3^{\alpha \cdot 11} \equiv 3^4\ (p) \iff \alpha \cdot 11 \equiv 4\ (p-1)$

(c) $3^{\alpha \cdot 20} \equiv 3^4\ (p) \iff \alpha \cdot 20 \equiv 4\ (p-1)$

(d) $28^{z} \equiv 3^4\ (p)$

↳ Queremos $28 \equiv 3^{\alpha}$ y luego $3^{\alpha z} \equiv 3^4\ (p)$

↓

$28 \equiv 3^{\alpha}\ (43)$, queremos hallar α.

$3 \equiv 3^1 \quad 9 \equiv 3^2 \quad 27 \equiv 3^3 \quad 38 \equiv 3^4 \rightsquigarrow 3^5 \equiv 3 \cdot 38\ (43)$

$\equiv 3 \cdot (-5)\ (43)$

$\equiv -15$

$\equiv 28\ (43)$

(d) $3^{5 \cdot z} \equiv 3^4\ (p) \iff 5z \equiv 4\ (p-1)$

Resolvamos (a): $\alpha \cdot 27 \equiv 4\ (42)$ tiene sol. si y sólo si $3 = \operatorname{mcd}(\underbrace{42}_{2 \cdot 3 \cdot 7}, \underbrace{27}_{3^2}) \nmid 4 \Rightarrow$ no tiene solución.

Resolvamos (d) $5z \equiv 4\ (42)$ tiene sol $\iff \exists \beta, z$ tal que $5z - \beta 42 = 4$ $(\iff \operatorname{mcd}(42, 5) = 1$ ✓$)$

$\boxed{z = 68 \quad \beta = 8} \rightsquigarrow$ sol. $28^{68} \equiv 28^{26}$

Ejercicio 11. Sea p primo.

a. Probar que si p es impar y r es una raíz primitiva módulo p entonces $r^{p-1/2} \equiv -1 \pmod{p}$.

b. Probar el Teorema de Wilson utilizando raíces primitivas: Si p es primo, entonces $(p-1)! \equiv -1 \pmod{p}$.

$(p-1)! \equiv r^{\frac{p-1}{2}} \ (p)$

a. · r raíz primitiva módulo p si $mcd(r,p)=1$ y $o(r) = \varphi(p) = p-1$.

$r^{p-1} \equiv 1 (p)$ y $p-1$ es el mínimo tal que $r^{p-1} \equiv 1(p)$.

· $r^{\frac{p-1}{2}} \not\equiv 1 (p)$ porque $p-1$ es el mínimo que lo cumple.

Observar que $\left(r^{\frac{p-1}{2}}\right)^2 \equiv r^{p-1} \equiv 1 \ (p)$

$\Rightarrow r^{\frac{p-1}{2}} \equiv \begin{cases} 1(p) \longrightarrow \text{no puede ser } \times \\ -1(p) \end{cases}$

} obs. hay que $\frac{1}{2}$ elem de orden 2

b

· $(p-1)! = \underset{r^{a_1}}{(p-1)}\underset{r^{a_2}}{(p-2)} \dots \underset{r^{a_{p-1}}}{(2)}(1)$ ✓ $\rightarrow$ Aparecen todos los elementos de $U(p)$ sin repetir.

· Sea r raíz primitiva $\Rightarrow$ Existen raíces primitivas módulo p.

· Como hay una biyección entre $r^{\alpha} \mapsto \alpha$, cada elemento $(p-i)$ es de la forma r^{α_i} y si $(p-i) \neq (p-j) \Rightarrow \alpha_i \neq \alpha_j$.

Es decir, los exponentes no se repiten.

· $(p-1)! = \prod_{i=1}^{p-1} r^{i} = r^{\sum_{i=1}^{p-1} i} \ (p)$

conmuta

parte previa $\equiv r^{\frac{(p-1)(p)}{2}} \ (p)$

p impar $\equiv (-1)^p \ (p)$

$\equiv (-1) \ (p)$

$(p-1)! \equiv \left(r^{\frac{p-1}{2}}\right)^p \ (p)$

$\equiv r^{\frac{p-1}{2}} \ (p)$

$\equiv (-1) \ (p)$

Ejercicio 13. Sea p un primo impar. Para cada $n \in \mathbb{Z}^+$ definimos $S_n = 1^n + 2^n + \ldots + (p-1)^n$. Probar que:

$$S_n \equiv \begin{cases} 0 \pmod{p} & \text{si } n \text{ no es múltiplo de } p-1 \\ -1 \pmod{p} & \text{si } n \text{ es múltiplo de } p-1 \end{cases}$$

$\boxed{n \text{ múltiplo de } p-1:}$ $S_n = 1^n + 2^n + \ldots + (p-1)^n \ (p)$

$n = (p-1) \cdot m$

$S_n \equiv (1^m)^{p-1} + (2^m)^{p-1} + \ldots + ((p-1)^m)^{p-1} \ (p)$

Euler (todos son coprimos con p) $\longrightarrow$ $\equiv 1 + 1 + \ldots + 1 \ (p)$

$\equiv (p-1) \ (p)$

$\equiv (-1) \ (p)$

$\boxed{n \text{ no es múltiplo de } p-1:}$ $S_n = 1^n + 2^n + \ldots + (p-1)^n \ (p).$

r raíz primitiva: igual que antes tenemos una biyección.

$S_n = r^{\alpha_1 \cdot n} + r^{\alpha_2 \cdot n} + \ldots + r^{\alpha_{p-1} \cdot n}$

Idea: $n=1$ $S_n = 1+2+3+\ldots+p-1 \pmod{p}$

$= \frac{p-1 \cdot p}{2} \equiv 0 \pmod{p}$

$S_n = 1^n + (p-1)^n + 2^n + (p-2)^n + \ldots$

$= 0 \qquad 0 \ldots$

$n=1$ ✓ n impar ✓

Otro caso: Idea: Con raíces primitivas. $\exists\, r$ r.p. módulo p.

$\Rightarrow S_1 = r^1 + r^2 + \ldots + r^{p-1}$ (Permutando)

$S_n = r^{1 \cdot n} + r^{2 \cdot n} + \ldots + r^{(p-1)n}$

Af: Si r^n también es raíz primitiva $\Rightarrow$ la suma S_n es igual a S_1 $= 0$.

En gral, si r es raíz primitiva

$o(r^n) = \frac{o(r)}{mcd(n, o(r))} = \frac{p-1}{mcd(n, p-1)}$

$\Rightarrow r^n$ va a ser raíz primitiva si y sólo si $mcd(n, p-1) = 1$

Es decir, vimos que la fórmula vale para — n múltiplo de $p-1$
— n no múltiplo de $p-1$ si: n impar
$mcd(n, p-1) = 1$

es decir n tq r^n es r.p. si r lo es.

Si r es raíz primitiva y r^n no lo es, entonces al sumar

$$1^n + 2^n + \dots + (p-1)^n \equiv r^{1\cdot n} + r^{2\cdot n} + \dots + r^{(p-1)n}$$
$$\equiv (r^n)^1 + \dots + (r^n)^{p-1}$$
$$\equiv \frac{p-1}{o(r^n)} \cdot \left(\underbrace{r^{n\,1} \quad \dots \quad r^{n\, o(n)}} \right)$$

y de forma análoga esto es $\equiv 0 \pmod p$

Una mejor forma de verlo es la siguiente:

$\boxed{\text{Si } n = (p-1)k}$ $\Rightarrow$ $S_n = (1^k)^{p-1} + \dots + (p-1)^{k\cdot p-1}$

Euler $\equiv \sum_{i=}^{p-1} 1 = p-1$

$\boxed{\text{Si } n \neq (p-1)\cdot k}$ $\Rightarrow$ sea r raíz primitiva

$\Rightarrow r^n \not\equiv 1 (p)$, además múltiplicar por r es biyectivo.

Luego

$$1^n + 2^n + \dots + (p-1)^n \equiv (r\cdot 1)^n + (r\cdot 2)^n + \dots + (r(p-1))^n$$
$$\equiv r^n \cdot (1^n + \longrightarrow (p-1)^n)$$

Como $r^n \not\equiv 1 \pmod p$ $\Rightarrow$ $S_n \equiv 0 \ (p)$.