Ejercicio 6. (Logaritmo discreto) Sea p un primo impar y r una raíz primitiva módulo p.

a. Probar que $r^a \equiv r^b \pmod{p} \Leftrightarrow a \equiv b \pmod{p-1}$.

b. Esto permite definir la función $e : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$, tal que: $e\,(a \pmod{p-1}) = r^a \pmod{p}$. Probar que esta función es biyectiva (*sugerencia: probar que es inyectiva*). A la función inversa de e la llamamos *logaritmo discreto en base* r, y se caracteriza por la propiedad: $\log_r b = \beta \Leftrightarrow r^\beta \equiv b \pmod{p}$.

c. Probar que si $a \not\equiv 0 \pmod{p}$ y $n \in \mathbb{Z}^+$, entonces $\log_r(a^n) \equiv n \log_r a \pmod{p-1}$.

d. Probar que 3 es raíz primitiva módulo 43, y hallar $\log_3 38 \in \mathbb{Z}_{42}$.

p un primo impar y r una raíz primitiva modulo p.

a) $r^a \equiv r^b \pmod{p} \Leftrightarrow a \equiv b \pmod{p-1}$

r es raíz primitiva modulo $p \Rightarrow \langle \bar{r} \rangle = U(p)$

$\Rightarrow o(\bar{r}) = \varphi(p) = p-1$

$\bar{r}^\alpha = \bar{1} \Leftrightarrow o(\bar{r}) \mid \alpha$

$$\begin{aligned} r^a \equiv r^b \pmod{p} &\Leftrightarrow r^a r^{-b} \equiv 1 \pmod{p} \\ &\Leftrightarrow r^{a-b} \equiv 1 \pmod{p} \\ &\Leftrightarrow \bar{r}^{a-b} = \bar{1} \quad (\text{en } U(p)) \\ &\Leftrightarrow o(\bar{r}) \mid a-b \\ &\Leftrightarrow p-1 \mid a-b \\ &\Leftrightarrow a \equiv b \pmod{p-1} \end{aligned}$$

$$\boxed{r^a \equiv r^b \pmod{p} \Leftrightarrow a \equiv b \pmod{p-1}}$$

b) Vamos a definir

$$e : \mathbb{Z}_{p-1} \longrightarrow \underbrace{\mathbb{Z}_p^*}_{= U(p)}$$

$\mathbb{Z}_{p-1} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{p-2}\}$

$\mathbb{Z}_p = \{\bar{0}, \underbrace{\bar{1}, \bar{2}, \dots, \overline{p-1}}\}$

$\mathbb{Z}_p^* = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$

$U(p) = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$

$$e : \mathbb{Z}_{p-1} \longrightarrow \mathbb{Z}_p^*$$ un elemento que está en la clase de a en $\mathbb{Z}_{p-1}$

$$e(\underbrace{a \pmod{p-1}}_{\substack{= \text{la clase de} \\ a \text{ en } \mathbb{Z}_{p-1}}}) = r^{a} \pmod p$$

* e está bien definida

queremos ver que si $a \equiv b \pmod{p-1}$ entonces

$$\underbrace{e(a \pmod{p-1})}_{r^a \pmod p} = \underbrace{e(b \pmod{p-1})}_{r^b \pmod p}$$

es decir queremos ver que

$$a \equiv b \pmod{p-1} \implies r^a \equiv r^b \pmod p$$

y esto es cierto por el recíproco de a)

* e es biyectiva

$$e : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^* \qquad e(a \pmod{p-1}) = r^a \pmod p$$

$|\mathbb{Z}_{p-1}| = p-1$

$|\mathbb{Z}_p^*| = |U(p)| = \varphi(p) = p-1$

Alcanza con ver que e es inyectiva

Para ver que es inyectiva queremos ver que

$$\underbrace{e(a \pmod{p-1})}_{r^a \pmod p} = \underbrace{e(b \pmod{p-1})}_{r^b \pmod p} \implies a \pmod{p-1} = b \pmod{p-1}$$

o sea queremos ver que

$$r^a \equiv r^b \pmod p \implies a \equiv b \pmod{p-1}$$

y esto es cierto por el directo de a)

entonces $e : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ es invertible y la inversa es lo que llamamos el logaritmo discreto en base r : $\log_r : \mathbb{Z}_p^* \to \mathbb{Z}_{p-1}$

* se verifica: $\log_r b \equiv \beta \pmod{p-1} \iff b \equiv r^{\beta} \pmod p$

$$\log_r b \equiv \beta \pmod{p-1} \iff e(\log_r b \pmod{p-1}) = e(\beta \pmod{p-1})$$
$$\iff b \pmod p = r^{\beta} \pmod p$$
$$\iff b \equiv r^{\beta} \pmod p$$

c. Probar que si $a \not\equiv 0 \pmod p$ y $n \in \mathbb{Z}^+$, entonces $\log_r(a^n) \equiv n \log_r a \pmod{p-1}$.

$$\log_r(a^n) \equiv n \log_r(a) \pmod{p-1} \iff e(\log_r a^n \pmod{p-1}) = e(n \log_r(a) \pmod{p-1})$$
$$\iff a^n \pmod p = r^{n\log_r(a)} \pmod p$$
$$\iff a^n \pmod p = (r^{\log_r(a)})^n \pmod p$$
$$\iff a^n \pmod p = a^n \pmod p \checkmark$$

$\log_r(a)$

$r^{\log_r(a)}$ = que potencia de r da a?

$= a$

$e: \mathbb{Z}_{p-1} \longrightarrow \mathbb{Z}_p^*$

$e(a \pmod{p-1}) = r^a \pmod p$

$\log_r : \overbrace{\mathbb{Z}_p^*}^{U(p)} \longrightarrow \mathbb{Z}_{p-1}$

sea $x \in \mathbb{Z}_p^*$

$\Rightarrow x \equiv r^{\alpha} \pmod p$

$\log_r(r^{\alpha}) = \alpha$

$r^{\alpha} = e(\log_r r^{\alpha}) = e(\alpha) =$

$\log_r(a)$ = la potencia que hay que tomar de r para que de a

$r^{\log_r(a)} = a$

d. Probar que 3 es raíz primitiva módulo 43, y hallar $\log_3 38 \in \mathbb{Z}_{42}$.

Ejercicio 7. 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. $28^z \equiv 38 \pmod{43}$

r raíz primitiva modulo p con p primo impar

a) $x^{27} \equiv 38 \pmod{43}$ $\qquad r^a \equiv r^b \pmod{p} \iff a \equiv b \pmod{p-1}$

Asumimos que 3 es raíz primitiva modulo 43

* $x \equiv 3^k \pmod{43}$ para algún $k \in \{1, \dots, 42\}$

* $38 \equiv 3^{?} \pmod{43}$

$3^3 \equiv 27 \pmod{43}$

$3^4 \equiv 81 \equiv 38 \pmod{43}$

entonces:

$$x^{27} \equiv 38 \pmod{43} \iff (3^k)^{27} \equiv 3^4 \pmod{43}$$
$$\iff 3^{27k} \equiv 3^4 \pmod{43}$$
$$\iff 27k \equiv 4 \pmod{\underbrace{42}}$$

$42 = 7 \cdot 3 \cdot 2$

$$27k \equiv 4 \pmod{42} \iff \begin{cases} 27k \equiv 4 \pmod{7} \\ 27k \equiv 4 \pmod{3} \\ 27k \equiv 4 \pmod{2} \end{cases}$$

$$\iff \begin{cases} 6k \equiv 4 \pmod{7} \\ 0 \equiv 1 \pmod{3} \end{cases}$$ ← no tiene solución

entonces $x^{27} \equiv 38 \pmod{43}$ no tiene solución

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

3 es raiz primitiva modulo 43

* $x \equiv 3^k \pmod{43}$ para algún $k \in \{1, \dots, 42\}$
* $38 \equiv 3^4 \pmod{43}$

$$x^{11} \equiv 38 \pmod{43} \iff (3^k)^{11} \equiv 3^4 \pmod{43}$$
$$\iff 3^{11k} \equiv 3^4 \pmod{43}$$
$$\iff 11k \equiv 4 \pmod{42}$$

$42 = 7 \cdot 3 \cdot 2$

$$11k \equiv 4 \pmod{42} \iff \begin{cases} 11k \equiv 4 \pmod{7} \\ 11k \equiv 4 \pmod{3} \\ 11k \equiv 4 \pmod{2} \end{cases}$$

$$\iff \begin{cases} 4k \equiv 4 \pmod{7} \\ 2k \equiv 1 \pmod{3} \\ k \equiv 0 \pmod{2} \end{cases}$$

$4 \cdot \underset{\uparrow}{2} + 7(-1) = 1$

$\Rightarrow 4 \cdot 2 \equiv 1 \pmod{7}$

$2 \cdot 5 + 3(-3) = 1$

$$\iff \begin{cases} 2 \cdot 4k \equiv 2 \cdot 4 \pmod{7} \iff k \equiv 1 \pmod{7} \\ 5 \cdot 2k \equiv 5 \pmod{3} \iff k \equiv 2 \pmod{3} \\ k \equiv 0 \pmod{2} \end{cases}$$

$$\iff \begin{cases} k \equiv 1 \pmod{7} & 1, \underline{8}, 15, \dots \\ k \equiv 2 \pmod{3} & 2, 5, \underline{8} \\ k \equiv 0 \pmod{2} & 0, 2, 4, 6, \underline{8} \end{cases}$$

$$\iff k \equiv 8 \pmod{42}$$

$$x^{11} \equiv 38 \pmod{43} \iff 3^{11k} \equiv 3^4 \pmod{43} \iff 11k \equiv 4 \pmod{42}$$

$x \equiv 3^k \pmod{43}$ $\qquad \iff k \equiv 8 \pmod{42}$

Entonces: $x^{11} \equiv 38 \pmod{43} \iff x \equiv 3^{8} \pmod{43}$