Ejercicio 6 - Logaritmo discreto

p un primo impar

r raíz primitiva modulo p $\Rightarrow \langle \bar{r} \rangle = U(p) \Rightarrow o(\bar{r}) = |U(p)| = \varphi(p) = p-1$

$$U(p) = \{\bar{r}, \bar{r}^2, \bar{r}^3, \dots, \bar{r}^{p-1}\}$$

$$U(p) = \{\bar{1}, \bar{2}, \bar{3}, \dots, \overline{p-1}\}$$

sea $\bar{a} \in U(p) \Rightarrow \bar{a} = \bar{r}^n$ para algún $n \in \{1, \dots, p-1\}$

$$\log_r(a) = n$$

$$\log_r : U(p) \longrightarrow \mathbb{Z}_{p-1}$$
$$\bar{a} \longmapsto n \text{ tal que } \bar{r}^n = \bar{a}$$

idea: * vamos a definir $\exp: \mathbb{Z}_{p-1} \longrightarrow U(p)$, $\bar{n} \longmapsto \bar{r}^n$

* vamos a ver que exp está bien definido y es biyectiva

* como es biyectiva, tiene inversa y la inversa es

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

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 $\log_3 38 \in \mathbb{Z}_{42}$.

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

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

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

$$e : \mathbb{Z}_{p-1} \longrightarrow U(p) = \mathbb{Z}_p^* = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$$

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

$e(\bar{a})$ = $\bar{r}^a$ ← la clase de r en $U(p)$

↑ la clase de a en $\mathbb{Z}_{p-1}$

* e está bien definida

$$\bar{r}^a = \bar{r}\cdot\bar{r}\cdot\bar{r}\cdots\bar{r} = \overline{r\cdot r\cdot r\cdots r} = \bar{r}^a$$

Queremos ver que

$$\underbrace{\bar{a} = \bar{b}}_{\text{en } \mathbb{Z}_{p-1}} \Rightarrow \underbrace{\bar{r}^a = \bar{r}^b}_{\text{en } U(p)}$$

$\bar{r}^a$ $\bar{r}^b$

es decir queremos ver que

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

y esto es cierto por el recíproco de la parte a)

* e es biyectiva

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

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

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

$|U(p)| = \varphi(p) = p-1$

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

como $|\mathbb{Z}_{p-1}| = p-1$ y $|U(p)| = p-1$ alcanza con ver que es inyectiva

entonces queremos ver que

$$\underbrace{e(a \pmod{p-1})}_{\bar{r}^a \text{ en } U(p)} = \underbrace{e(b \pmod{p-1})}_{\bar{r}^b \text{ en } U(p)} \Rightarrow a \pmod{p-1} = b \pmod{p-1}$$

es decir queremos ver que

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

y esto es cierto por el directo de a)

Conclusión:

la función $e: \mathbb{Z}_{p-1} \to U(p)$

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

es biyectiva

$\Rightarrow$ tiene una inversa que llamamos logaritmo discreto

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

$\bar{x} \longmapsto$ a qué potencia tenemos que elevar la raíz primitiva para que nos de $\bar{x}$.

$$\boxed{\bar{r}^{\log_r(\bar{x})} = \bar{x}}$$

* veamos que $\log_r(b) \equiv \beta \pmod{p-1} \iff b \equiv r^\beta \pmod p$

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

$$\iff r^{\log_r(b)} \pmod p = r^\beta \pmod p$$

$$\iff b \pmod p = r^\beta \pmod p$$

$$\iff b \equiv r^\beta \pmod p$$

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

$\varphi(43) = 42 = 2 \cdot 3 \cdot 7$

$\rightarrow$ los divisores primos de $\varphi(43)$ son 2, 3 y 7

3 es raíz primitiva modulo 43 $\iff$

$$\begin{cases} 3^{\varphi(43)/7} \not\equiv 1 \pmod{43} \\ 3^{\varphi(43)/3} \not\equiv 1 \pmod{43} \\ 3^{\varphi(43)/2} \not\equiv 1 \pmod{43} \end{cases}$$

$\iff$

$$\begin{cases} 3^{6} \not\equiv 1 \pmod{43} \checkmark \\ 3^{14} \not\equiv 1 \pmod{43} \checkmark \\ 3^{21} \not\equiv 1 \pmod{43} \checkmark \end{cases}$$

exponenciación rápida:

$6 = 4+2 = 2^2 + 2^1$

$14 = 8+4+2 = 2^3 + 2^2 + 2^1$

$21 = 16+4+1 = 2^4 + 2^2 + 2^0$

n	$3^{2^n} \pmod{43}$	
0	3	$\leftarrow 3^1$
1	9	$\leftarrow 3^2$
2	$9 \cdot 9 \equiv 38 \equiv -5 \pmod{43}$	$\leftarrow 3^4$
3	25	$\leftarrow 3^8$
4	23	$\leftarrow 3^{16}$

$3^6 \equiv 3^{2^2+2^1} \equiv 3^{2^2} 3^{2^1} \equiv (-5) \cdot 9 \equiv 2 \pmod{43}$

$3^{14} \equiv 3^{2^3} \cdot 3^{2^2} 3^{2^1} \equiv 25 \cdot 2 \equiv 7 \pmod{43}$

$3^{21} \equiv 3^{2^4} 3^{2^2} 3^{2^0} \equiv 23 \cdot (-5) \cdot 3 \equiv 26(-5) \equiv 42 \pmod{43}$

$\Rightarrow$ 3 es raíz primitiva modulo 43

$\log_3(38) = ?$

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

$3^4 \equiv 38 \pmod{43} \Rightarrow \log_3(38) = 4$

Ejercicio 7

r raiz primitiva modulo p con p primo impar

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

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

3 es raiz primitiva modulo 43

* $\log_3(38) = 4 \Rightarrow 38 \equiv 3^4 \pmod{43}$
* $x \equiv 3^k \pmod{43}$

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

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

$\iff 11k \equiv 4 \pmod{42}$

$42 = 7 \cdot 3 \cdot 2$

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

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

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

$$\Leftrightarrow \begin{cases} k \equiv 1 \pmod 7 \rightsquigarrow 1, \underline{8} \\ k \equiv 2 \pmod 3 \rightarrow 8 \checkmark \\ k \equiv 0 \pmod 2 \rightarrow 8 \checkmark \end{cases}$$

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

$x'' \equiv 38 \pmod{43} \Leftrightarrow k \equiv 8 \pmod{42}$

$x \equiv 3^k \pmod{43}$

$x'' \equiv 38 \pmod{43} \Leftrightarrow x \equiv 3^8 \pmod{43}$

$\Leftrightarrow x \equiv 25 \pmod{43}$