Práctico 9: Raíces primitivas

Ejercicio 6. Sean $r, s \in \mathbb{N}$ con $1 < r < s$ y $\text{mcd}(r, s) = 1$.

a. Probar que si $a \in U(rs)$ entonces $a^{\text{mcm}(\varphi(r),\varphi(s))} \equiv 1 \pmod{rs}$.

b. Probar que si $r > 2$ entonces $\text{mcd}(\varphi(r), \varphi(s)) > 1$ (sugerencia: probar que ambos son pares).

c. Probar que sólo pueden existir raíces primitivas módulo m para $m = 2, 4, p^\alpha$ o $2p^\alpha$ con p primo impar y $\alpha \in \mathbb{N}$ (sugerencia: utilizar los ejercicios anteriores).

a) $a \in U(rs)$ sii $\text{mcd}(a, rs) = 1$ ⟵ $\text{mcd}(a,r) = 1 \Rightarrow a \in U(r)$; $\text{mcd}(a,s) = 1 \Rightarrow a \in U(s)$

Fermat - Euler:
$$\begin{cases} a^{\varphi(r)} \equiv 1 \ (r) \\ a^{\varphi(s)} \equiv 1 \ (s) \\ a^{\varphi(rs)} \equiv 1 \ (rs) \end{cases}$$

$m = \text{mcm}(\varphi(r), \varphi(s)) \Rightarrow m = d \cdot \varphi(r)$, $m = d' \cdot \varphi(s)$ $\Rightarrow$
$$\begin{cases} a^m = (a^{\varphi(r)})^d \equiv 1 \ (r) \\ a^m = (a^{\varphi(s)})^{d'} \equiv 1 \ (s) \end{cases}$$

Teorema Chino
$$\begin{cases} a^m \equiv 1 \ (r) \\ a^m \equiv 1 \ (s) \end{cases}$$
$\Rightarrow$ Como r y s son coprimos por el T. Chino $a^m \equiv 1 \ (rs)$.

b) $2 < r < s \Rightarrow$ Basta probar que $\varphi(n)$ $n > 2$ es par.

Caso 1: $\exists$ p impar tal que $p \mid n \Rightarrow n = p^k \cdot q$ con $\text{mcd}(p, q) = 1$.

Caso 2: $\nexists$ p impar tal que $p \mid n \Rightarrow n = 2^k$ con $k > 1$.

Caso 1: $\varphi(n) = \varphi(p^k q) = \varphi(p^k) \cdot \varphi(q) = \varphi(q) \cdot p^{k-1}(p-1) = \varphi(q) \cdot p^{k-1} \cdot (p-1)$ ($p-1$: par)

Caso 2: $\varphi(2^k) = 2^{k-1}$, par pues $k > 1$.

$2 \mid \varphi(r)$, $2 \mid \varphi(s)$ $\Rightarrow \text{mcd}(\varphi(r), \varphi(s)) \geq 2$

c. Hay que ver que fuera de esos casos no hay raíces primitivas.

Caso 1: 2^k con $k \geq 3$. (Ejercicio 5)

Otros casos: pq, p, q primos
$2^k pq$,
$pqs \ldots$ p, q, s primos,
$2^k p^a$ con $k \geq 1$
$\vdots$

} rs con $r, s > 2$ coprimos.

Caso 2: rs con $r, s > 2$ coprimos.

Supongamos que $\exists\, g$ raíz primitiva módulo $rs \Rightarrow mcd(g, rs) = 1$ y
$o(g) = \varphi(rs) = \varphi(r)\varphi(s)$ (coprimos)

Queremos ver que $\exists\, d < o(g) = \varphi(r)\varphi(s)$ tq $g^d \equiv 1 \ (rs)$.

$$mcm(\varphi(r), \varphi(s)) = \frac{\varphi(r)\varphi(s)}{mcd(\varphi(r), \varphi(s))} \Rightarrow^{(a)} g^{mcm(\varphi(r), \varphi(s))} = 1 \ (rs)$$

$$= g^{\frac{\varphi(r)\varphi(s)}{mcd}} \equiv 1 \ (rs)$$

$\Rightarrow$ tenemos $g^d \equiv 1$ con $d = \frac{\varphi(r)\varphi(s)}{mcd \ldots} < \varphi(r)\varphi(s)$. ↯ (Contradice minimalidad del orden de g).

Ejercicio 8. (Logaritmo discreto) Sea p un primo impar y r una raíz primitiva módulo p.

a. Probar que $r^a \equiv r^b \mod p \Leftrightarrow a \equiv b \mod (p-1)$.

b. Por lo tanto podemos definir la función $e : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ definida por $e(a \mod (p-1)) = r^a \mod p$. 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 $\log_r b = \beta \Leftrightarrow r^\beta \equiv b \mod p$.

" $e^{-1}(b)$ "

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

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

a. En el teórico vieron: G grupo $r^a = r^b \Leftrightarrow a \equiv b \ (o(r))$.

Obs: Como r es raíz primitiva $o(g) = |U(p)| = p-1$.

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

$a \ (p-1) \mapsto r^a \ (p)$

Biyectivo:

Inyectiva: Queremos ver que si $e(x) = e(y) \Rightarrow x = y$

Esto es: $r^x \equiv r^y \ (p) \Rightarrow x \equiv y \ (p-1)$,

y se cumple por la parte (a).

Sobreyectivo: Es inyectivo y $|\mathbb{Z}_{p-1}| = |\mathbb{Z}_p^*| = p-1 \Rightarrow$ es sobreyectivo.

c. Hay que ver que $\log_r(a^n) = n \cdot \log_r(a)$.

Por definición, $\log_r(a^n) = \beta \in \mathbb{Z}_{p-1}$ tal que $r^\beta \equiv a^n \ (p)$

$r^{\log_r(a^n)} = r^\beta \equiv a^n \ (p)$

De la misma manera $\log_r(a) = \alpha \in \mathbb{Z}_{p-1}$ tal que $r^\alpha \equiv a \ (p)$

$\Rightarrow$ $r^{n \cdot \log_r(a)} \equiv \left(r^{\log_r(a)}\right)^n \equiv (a)^n \ (p)$ $\Rightarrow \beta = n \log_r(a)$.

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

d. Cuenta: $3^{\varphi(43)/p} \not\equiv 1 \ (43) \quad \forall p \mid \varphi(43)$.

$\log_3 38$: En la def: $r = 3$

$b = 38$

$\beta = \log_3 38$ (queremos hallar).

β tq $3^\beta \equiv 38 \ (43)$

$3 \not\equiv 38 \ (43)$

$3^2 \equiv 9 \not\equiv 38 \ (43)$

$3^3 \equiv 27 \not\equiv 38 \ (43)$

$3^4 \equiv 81 \equiv 38 \ (43)$ ✓ $\Rightarrow \beta = 4$.