CÓDIGOS Y CRIPTOGRAFÍA. INFORMÁTICA DIEGO RUANO 8/11 2022

$\phi(n)$ FUNCIÓN DE EULER

$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m \equiv \mathbb{Z}/(m) = \{0, \dots, m-1\}$

DEF: SEA $n \in \mathbb{Z}$ DENOTAMOS POR $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ AL GRUPO MULTIPLICATIVO DE LAS UNIDADES DE $\mathbb{Z}/m\mathbb{Z}$ ES DECIR LOS QUE TIENEN INVERSO EN $\mathbb{Z}/m\mathbb{Z}$

LAS UNIDADES DE UN ANILLO SON AQUELLOS ELEMENTOS QUE TIENEN INVERSO

- SI $m=p$ PRIMO $\mathbb{Z}/p\mathbb{Z}$ ES UN CUERPO Y TODO ELEMENTO NO NO-NULO TIENE INVERSO $\left(\mathbb{Z}/p\mathbb{Z}\right)^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$
- SI $m \neq p$ PRIMO $\mathbb{Z}/m\mathbb{Z}$ NO ES UN CUERPO, HAY DIVISORES DE CERO Y NO TODO ELEMENTO TIENE INVERSO

EJ: $\mathbb{Z}/10\mathbb{Z}$ ¿$(\mathbb{Z}/10\mathbb{Z})^*$?

$a \cdot b = 1$
$b = a^{-1}$

¿QUIÉN TIENE INVERSO?

LOS RELATIVAMENTE PRIMOS CON 10 PORQUE NO SO DIVISORES DE CERO

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

0 NO $\quad 0 \cdot a = 0$

1 SI $\quad 1 \cdot 1 = 1, \quad 1^{-1} = 1$

2 NO $\quad 2 \cdot 5 = 10 = 0$ COMO ES DIVISOR DE CERO NO EXISTE SU INVERSO

IMAGINEMOS QUE 2 TUVIERA INVERSO:

ABSURDO

$0 = 2^{-1} \cdot 0 = 2^{-1} \cdot 10 = 2^{-1} 2 \cdot 5 = 1 \cdot 5 = 5$

$0 = 5$ ASURDO, VIENE DE SUPONER QUE $\exists 2^{-1}$

3 SI $\quad 3 \cdot 7 = 21 \quad 3^{-1} = 7$

4 NO $\quad$ 5 NO $\quad$ 6 NO $\quad$ 7 SI $\quad$ 8 NO $\quad$ 9 SI

$4\cdot 5 = 20 = 0$ $\quad$ $6\cdot 5 = 30 = 0$ $\quad$ $8\cdot 5 = 40 = 0$ $\quad$ $9\cdot 9 = 81 = 1$, $\quad 9^{-1} = 9$

$$\mathrm{mcd}(a, 10) = \begin{cases} 1 & \text{SI} \leftarrow \text{TIENE INVERSO} \\ \neq 1 & \text{NO} \leftarrow \text{ES UN DIVISOR CERO} \end{cases}$$

$$\mathrm{mcd}(6, 10) = 2 \qquad 6\cdot 5 = 30 = 3\cdot 10 = 0$$

$$\mathrm{mcd}(a, \overset{10}{\overset{\shortparallel}{m}}) = b > 1 \Rightarrow b \mid a \quad b \mid m$$

$$a = bk \qquad m = b\cdot l$$

$$a\cdot l = (bk)\cdot l = (bl)\cdot k = m\cdot k = 0 \;\; (\mathrm{MOD}\ m)$$

SI $\mathrm{mcd}(a, m) \neq 1 \Rightarrow a$ ES UN DIVISOR DE CERO Y NO TIENE INVERSO

$\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^*$ NÚMERO DE ELEMENTOS EN $\mathbb{Z}/m\mathbb{Z}$ QUE TIENEN INVERSO

$= \#\{a \mid 0 < a < m,\ mcd(a,m) = 1\}$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$\varphi(n)$	0	1	1	2	2	4	2	6	4	6	4	10	4	12

¿COMO CALCULAMOS $\varphi(n)$?

- SI p PRIMO: $\varphi(p) = p - 1$
- SI m y n SON RELATIVAMENTE PRIMOS

(*) $(mcd(m,n) = 1)$: $\varphi(mn) = \varphi(m)\varphi(n)$ $\quad \mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ TEOREMA CHINO RESTOS

(**)
- SI p PRIMO: $\phi(p^r) = p^r - p^{r-1}$

ESTO SIGNIFICA QUE PODEMOS CALCULAR $\phi(n)$ SI CONOCEMOS LA FACTORIZACIÓN DE n

$$n = p_1^{r_1} \cdot \dots \cdot p_s^{r_s}$$

$$\varphi(n) \overset{*}{=} \varphi(p_1^{r_1}) \cdot \dots \cdot \varphi(p^{r_s})$$

$$\overset{**}{=} \left(p_1^{r_1} - p_1^{r_1-1}\right) \cdots \left(p_s^{r_s} - p_s^{r_s}\right)$$

EJ: $\varphi(100)$
$= \varphi(2^2 \cdot 5^2) =$
$\overset{*}{=} \varphi(2^2)\,\varphi(5^2)$
$\overset{**}{=} (2^2 - 2)(5^2 - 5)$
$= 2 \cdot 20 = 40$

EL PROBLEMA ES QUE FACTORIZAR UN NÚMERO GRANDE ES COSTOSO

EN PARTICULAR, SI p, q SON PRIMOS

$$\varphi(n) = \varphi(p \cdot q) = \varphi(p)\,\varphi(q) = (p-1)(q-1)$$

SI NOS DAN n PERO NO NOS DAN $n = pq$

$\varphi(n)$? NECESITAMOS FACTORIZAR $n = p \cdot q$

PORQUE ENTONCES $\varphi(n) = (p-1)(q-1)$

SI NO PODEMOS CALCULAR LA FACTORIZACION DE n

$\{0, 1, 2, \ldots\ldots, n-1\}$

$\mathrm{mcd}(\ \cdot\ , n) = \begin{cases} 1 \\ \neq 1 \end{cases}$

TENEMOS QUE IR MIRANDO UNO POR UNO

MUY COSTOSO

TEOREMA CHINO DE LOS RESTOS

SEAN $m_1, \dots, m_n$ ENTEROS POSITIVOS QUE SON CO-PRIMOS DOS A DOS (ES DECIR $mcd(m_i, m_j) = 1$ (*) PARA $i \neq j$)

SEAN $a_1, \dots, a_n$ ENTEROS

QUEREMOS ENCONTRAR LA SOLUCIÓN DE

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \vdots \\ x \equiv a_n \mod m_n \end{cases}$$

VEREMOS QUE EXISTE UNA SOLUCIÓN ÚNICA

$$0 \leq x < m_1 \cdot m_2 \cdot \dots \cdot m_n = m$$

ES DECIR, LA SOLUCIÓN EXISTE Y ES ÚNICA MÓDULO m.

SEA $m=\prod_{i=1}^{n} m_i$, $M_i = \frac{m}{m_i}$ $i=1,\dots,n$

POR ⊛ $\Rightarrow$ $\gcd(m_i, M_i) = 1$, $1 \le i \le n$

POR EL ALGORITMO DE EUCLIDES EXTENDIDO PODEMOS CALCULAR $y_i \in \mathbb{Z}$, $i=1,\dots,n$ TAL QUE

$$y_i M_i \equiv 1 \bmod m_i, \quad 1 \le i \le n \quad (**)$$

$(y_i = M_i^{-1} \bmod m_i)$

ENTONCES DEFINIMOS $x = \sum_{i=1}^{n} a_i y_i M_i \bmod m$

VEAMOS QUE x ES UNA SOLUCIÓN DEL SISTEMA DE ECUACIONES MODULARES

$$x \bmod m_i = a_i \underbrace{y_i M_i}_{\overset{(**)}{=} 1} \bmod m_i = a_i$$

PORQUE $\underset{j \neq i}{a_j y_j \underbrace{M_j}_{\overset{\shortparallel}{0}}} = 0$ MOD m_i PORQUE $m_i \mid M_j$.

EJ:

$$\begin{cases} x \equiv 2 \mod 4 \\ x \equiv 1 \mod 3 \\ x \equiv 0 \mod 5 \end{cases}$$

$m = 4 \cdot 3 \cdot 5 = 60$

$M_1 = \frac{m}{m_1} = \frac{60}{4} = 3 \cdot 5 = 15$ $\quad M_2 = 4 \cdot 5 = \frac{60}{3} = 20$ $\quad M_3 = \underset{\overset{\shortparallel}{60/5}}{4 \cdot 3} = 12$

$y_i = M_i^{-1} \mod m_i$

$$\begin{cases} y_1 = 15^{-1} \mod 4 \\ y_2 = 20^{-1} \mod 3 \\ y_3 = 12^{-1} \mod 5 \end{cases} \quad \begin{cases} y_1 = 3^{-1} \mod 4 \implies y_1 = 3 \\ y_2 = 2^{-1} \mod 3 \implies y_2 = 2 \\ y_3 = 2^{-1} \mod 5 \implies y_3 = 3 \end{cases}$$

$$x = \sum_{i=1}^{3} a_i y_i M_i = 2 \cdot 3 \cdot 15 + 1 \cdot 2 \cdot 20 + 0 \cdot 3 \cdot 12$$

$$= 90 + 40 + 0 = 130$$

$$130 \bmod \underset{m}{\underset{\shortparallel}{60}} = 10$$

TODAS LAS SOLUCIONES ENTERAS

$$\{ 10 + \lambda \cdot 60 \ / \ \lambda \in \mathbb{Z} \}$$

$$\mathbb{Z}_{60} \simeq \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$m \longmapsto (m \text{ MOD } 4, m \text{ MOD } 3, m \bmod 5)$$

TEOREMA

SEAN $m_1, \ldots, m_n$ ENTEROS COPRIMOS DOS A DOS

Y SEA $m = m_1 \cdot \ldots \cdot m_n$ ENTONCES

$$\mathbb{Z}_m \longrightarrow \prod \mathbb{Z}_{m_i}$$

$$a + m\mathbb{Z} \longmapsto (a + m_1\mathbb{Z}, \ldots, a + m_n\mathbb{Z})$$

ES UN ISOMORFISMO DE ANILLOS

DEM

- ESTÁ BIEN DEFINIDA
- INYECTIVA Y SOBREYECTIVA POR EL TEOREMA CHINO DE LOS RESTOS

TEOREMA ⊛

SEAN m, n COPRIMOS, ENTONCES $\varphi(mn) = \varphi(m)\varphi(n)$

$\text{mcd}(m,n) = 1$

DEMOSTRACIÓN:

$$\left(\mathbb{Z}_{mn}\right)^* \longrightarrow \left(\mathbb{Z}_m\right)^* \times \left(\mathbb{Z}_n^*\right)$$

$$(a + mn\mathbb{Z}) \longmapsto (a + m\mathbb{Z},\ a + n\mathbb{Z})$$

ES UN ISOMORFISMO DE ANILLOS, EN PARTICULAR ES BIYECTIVA Y TIENEN EL MISMO TAMAÑO. POR LO QUE $\varphi(mn) = \varphi(m) \times \varphi(n)$

TEOREMA (**)

SEA p PRIMO, ENTONCES $\phi(p^r) = p^r - p^{r-1}$

DEMOSTRACIÓN

SEA $a \in \{0, 1, 2, \ldots, p^r - 1\}$, a SE PUEDE ESCRIBIR DE FORMA ÚNICA EN BASE p COMO

$$a = a_0 + a_1 p + a_2 p^2 + \cdots + a_{r-1} p^{r-1}$$

CON $a_i \in \{0, \ldots, p-1\}$ PARA $i = 1, \ldots, r-1$

SE TIENE QUE $\gcd(a, p^r) = 1 \iff a_0 \neq 0$

(CON $a_0 = 0$ p ES UN FACTOR COMÚN)

$$\Rightarrow \phi(p^r) = \underbrace{(p-1)}_{\substack{\text{ELECCIONES} \\ a_0}} \underbrace{p^{r-1}}_{\substack{\text{ELECCIONES} \\ a_1 \ldots a_{r-1}}} = p^r - p^{r-1}$$

Th PEQUEÑO DE FERMAT:

p PRIMO, $a \in \mathbb{N}$ TAL QUE $mcd(a,p)=1$

$$\Rightarrow a^{p-1} \equiv 1 \mod p$$

COROLARIO: p PRIMO, $0 \leq a < p$

$$\Rightarrow a^{p} \equiv a \mod p$$

Th EULER: $a, m \in \mathbb{N}$ TALES QUE $mcd(a,m)=1$

$$\Rightarrow a^{\phi(m)} \equiv 1 \mod m$$

COROLARIO: $m \in \mathbb{N}$ Y $0 < a < m$ Y TAL QUE $mcd(a,m)=1$

$$\Rightarrow a^{\phi(m)} \equiv 1 \mod m$$