

CriptoTema2.pdf



onafolch



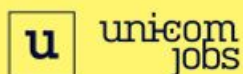
Criptografia i Seguretat



3º Grado en Ingeniería de Datos



Escuela de Ingeniería
Universidad Autónoma de Barcelona



Entra en la red donde pescan las mejores empresas

Descubre la app donde las empresas top buscan talentos del mañana. Escanea y empieza tu vida profesional hoy

Escanea el QR y entra a nuestra red social para comenzar tu futuro profesional





CRIPTOGRAFIA

FONAMENTS MATEMÀTICS DE LA CRIPTOGRAFIA

1. MATEMÀTICA DISCRETA

La **congruència** és la base en la que se sustenten les operacions de xifra en matemàtica discreta.

Si tenim dos nombres enters a i b , es diu que a és congruent amb b en el cos n (Z_n) si i només si existeix algun enter que divideix de forma exacta la diferència $(a-b)$.

$$\begin{aligned} a - b &= k * n \\ a &\equiv_n b \\ a &\equiv b \pmod n \end{aligned}$$

Exemple: Si estem treballant en Z_5 , els valors congruents amb l'1 serien el 6, 11, 16, 21,...

Propietats:

- **Reflexiva:** $a \equiv a \pmod n \quad \forall a \in Z$
- **Simètrica:** $a \equiv b \pmod n \rightarrow b \equiv a \pmod n \quad \forall a, b \in Z$
- **Transitiva:** si $a \equiv b \pmod n$ i $b \equiv c \pmod n \rightarrow a \equiv c \pmod n \quad \forall a, b, c \in Z$
- **Associativa:** $a + (b + c) \pmod n \equiv (a + b) + c \pmod n$
- **Commutativa:** $a + b \pmod n \equiv b + a \pmod n$ i $a * b \pmod n \equiv b * a \pmod n$
- **Distributiva:** $a * (b + c) \pmod n \equiv ((a * b) + (a * c)) \pmod n$
- **Identitat:** $a + 0 \pmod n = 0 + a \pmod n = a \pmod n = a$ i $a * 1 \pmod n = 1 * a \pmod n = a \pmod n = a$
- **Inversos:** $a + (-a) \pmod n = 0$ i $a * (a^{-1}) \pmod n = 1$ (si $a \neq 0$)
- **Reductibilitat:** $(a + b) \pmod n = [(a \pmod n) + (b \pmod n)] \pmod n$ i $(a * b) \pmod n = [(a \pmod n) * (b \pmod n)] \pmod n$

CCR (Conjunt complet de restos)

Per qualsevol enter positiu n , el CRR serà $CRR = \{0, 1, 2, \dots, n-1\}$.

Exemple: $CRR(11) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Homorfisme dels enters

Ens permet treballar amb números molt grans, ja que $(a \text{ op } b) \pmod n = [(a \pmod n) \text{ op } (b \pmod n)] \pmod n$.

Exemple: fer $8.184 \pmod{13}$. Sabem que 8.184 és $88 * 93$, aleshores:

$$[(88 \pmod{13}) * (93 \pmod{13})] \pmod{13} = (10 * 2) \pmod{13} = 20 \pmod{13} = 7$$

2. ALGORITME D'EUCLIDES

Divisibilitat dels números: moltes vegades ens interessa trobar el màxim comú denominador mcd entre dos números a i b . Per l'existència d'inversos en un cos n , la base a i el mòdul n han de ser primers entre si, és a dir, $\text{mcd}(a, n) = 1$. Per saber-ho, ho podem fer amb l'**algoritme d'Euclides**:

Sabem que $\text{mcd}(a, b) = \text{mcd}(b, r)$ on $a > b > r \geq 0$.

Exemple: Volem trobar el mcd entre 148 i 40. Anirem repetint l'expressió $a = (b * k) + r$.

Utilitzant la funció de l'algoritme d'Euclides, sabem que $\text{mcd}(148, 40) = \text{mcd}(40, 28) = \text{mcd}(28, 12) = \text{mcd}(12, 4) = \text{mcd}(4, 0)$.

Un cop hem acabat, hem obtingut que $\text{mcd}(148, 40) = 4$. En aquest cas no existeix inversa de 148 en el cos 40, ja que el mcd no és 1.

$$\begin{aligned} 148 &= (3 * 40) + 28 \\ 40 &= (1 * 28) + 12 \\ 28 &= (2 * 12) + 4 \\ 12 &= (3 * 4) + 0 \end{aligned}$$

Ona Folch

WUOLAH

3. INVERSOS EN Z_n

Si $a \cdot x = 1$, es diu que x és l'invers multiplicatiu d' a en Z_n , i serà a^{-1} . No sempre existeix inversos d'un element en Z_n . **Exemple:** si $n = 6$, no existeix l'invers de 2, ja que no hi ha cap valor x que $2 \cdot x = 1 \pmod 6$.

Si n és un nombre primer, tots els elements de Z_p menys el 0 tenen inversa. **Exemple:** si $n = 5$, l'invers d'1 és 1, l'invers de 2 és 3, l'invers de 3 és 2 i l'invers de 4 és 4.

- Existència del invers per primalitat: Si $\text{mcd}(a,n) = 1$, el resultat de $a \cdot i \pmod n$ (on i són els restos de n) seran valors diferents dintre del cos n .
- Inexistència de l'invers (no primalitat): Si $\text{mcd}(a,n)$ no és 1, no existeix invers.

En la suma sempre existirà l'invers per qualsevol número en qualsevol cos, i el seu valor serà únic. En la multiplicació, si el número i el mòdul són primers entre sí, sempre en tindrà. **Exemple:** si $n = 4$, el valor 2 no tindrà invers multiplicatiu, mentre que el 3 sí.

CRR (Conjunt reduït de restos)

És el subconjunt de restos primers amb el cos n . Si n és primer, tots els restos seran primers amb ell. El zero no és una solució. **Exemple:** $\text{CRR}(8) = \{1,3,5,7\}$

4. FUNCIÓ D'EULER

La funció d'Euler $\phi(n)$ ens dirà el nombre d'elements del CRR.

- Si n és un nombre primer $\phi(n) = n - 1$

El resultat serà CCD menys el 0. **Exemple:** $\text{CRR}(7) = \{1,2,3,4,5,6\}$, per tant $\phi(7) = 6$

- Si n es representa com $n = p^k$, on p és primer i k un enter $\phi(n) = p^{k-1}(p - 1)$

Exemple: $\text{CRR}(16) = \{1,3,5,7,9,11,13,15\}$, per tant $\phi(16) = 8$

- Si n és $n = p \cdot q$, on p i q són primers $\phi(n) = (p - 1)(q - 1)$

Exemple: $\text{CRR}(15) = \{1,2,4,7,8,11,13,14\}$, per tant $\phi(15) = 8$

- Si n és un nombre qualsevol (forma genèrica) $\phi(n) = \prod_{i=1}^t p_i^{e_i-1}(p_i - 1)$

Exemple: $\text{CRR}(20) = \{1,3,7,9,11,13,17,19\}$, per tant $\phi(20) = 8$

$$\phi(20) = \phi(2^2 \cdot 5) = 2^{2-1}(2 - 1) \cdot 5^{1-1}(5 - 1) = 2 \cdot 1 \cdot 1 \cdot 4 = 8$$

Teorema d'Euler

Ens permet calcular l'invers d'un nombre. Si $\text{mcd}(a,n) = 1$, sabem que $a^{\phi(n)} \pmod n = 1$. Si igualem les dues funcions, tenim que $x = a^{\phi(n)-1} \pmod n$, on x és l'invers d' a en el cos n .

Exemple: Invers de 4 en el cos 9, és a dir, $\text{inv}(4,9)$. Com que $\text{mcd}(4,9) = 1$, sabem que té invers. Calculem $\phi(9)$ i ens dona 6. Si utilitzem la fórmula del teorema d'Euler, tenim que $x = 4^{6-1} \pmod 9 = 7$. Amb això diem que l'invers de 4 en el cos 9 és 7. $\text{inv}(4,9) = 7$ i $\text{inv}(7,9) = 4$.

Algoritme estès d'Euclides

Si no coneixem el $\phi(n)$ o no volem utilitzar el teorema d'Euler, sempre podem trobar l'invers amb aquest algoritme, ja que és el mètode més ràpid i pràctic.

Exemple: Si volem trobar $\text{inv}(9,25)$, fem el següent:

$$\left. \begin{array}{l} 25 = 2 * 9 + 7 \\ 9 = 1 * 7 + 2 \\ 7 = 3 * 2 + 1 \\ 2 = 2 * 1 + 0 \end{array} \right\} \begin{array}{l} \text{Amb això confirmem que } \text{mcd}(9,25) = 1. \\ \text{De les 3 primeres files aïllem el residu:} \end{array} \left\{ \begin{array}{ll} 7 = 25 - 2 * 9 & 2 = 9 - 1(25 - 2 * 9) = 3 * 9 - 1 * 25 \\ 2 = 9 - 1 * 7 & 1 = (25 - 2 * 9) - 3(3 * 9 - 1 * 25) \\ 1 = 7 - 3 * 2 & 1 = 4 * 25 - 11 * 9 \text{ mod } 25 \end{array} \right.$$


Amb aquests càlculs, tenim que $\text{inv}(9,25) = -11 \rightarrow -11 + 25 = 14$. Per tant, $\text{inv}(9,25) = 14$.

5. EXPONENCIACIÓ RÀPIDA

Ens serveix per quan tenim càlculs molt costosos. Es té $A^B \text{ mod } n$, on es representa l'exponent B en binari. Es calculen els productes A^{2^j} amb $j = 0$ fins $n-1$, sent n el nombre de bits que representen el valor binari de B. Només es tenen en compte els productes en els que la posició j del valor B apareix un 1.

Exemple: Volem calcular $x = 12^{37} \text{ mod } 221 = 207$. 12^{37} és un número de 40 dígit. Primer de tot passem el 37 a binari:

$B = 37_{10} = 100101_2$, i ens quedem només amb les j on tenim un 1.



Ara aplicarem l'operació $A^{2^j} \text{ mod } 221$ per les $j = 5, 2, 0$, on A és 12.

$$12^{2^0} \text{ mod } 221 = 12$$

$$12^{2^2} \text{ mod } 221 = 183$$

$$12^{2^5} \text{ mod } 221 = 1$$

I per obtenir el valor de x, multipliquem els valors resultants i fem mòdul 221.

$$x = 12 * 183 * 1 \text{ mod } 221 = 207$$

6. NOMBRES PRIMERS

Pel teorema dels nombres primers, es té que la probabilitat de trobar nombres primers a mesura que aquests es van fent més grans és menor.

Test de primalitat de Fermat

Sigui p un nombre primer, aleshores $a^{p-1} \text{ mod } p = 1$ per qualsevol valor tal que $1 \leq a < p$. Probabilitat de que el número sigui primer amb aquest teorema: $1 - 0.5^k$, on k és el nombre de valors aleatoris que agafes.

Test de primalitat de Miller-Rabin

És un test que combina la condició del teorema petit de Fermat amb la particularitat dels residus quadràtics en aritmètica popular.