Criptografía y Seguridad Computacional **2016-01**

Clase 7: 13/04/2016

Profesor: Fernando Krell *Notas: Tomás Andrighetti*

1. Algoritmos para teoría de números

En esta clase introduciremos algunos algoritmos básicos en teoría de números.

1.1. Algoritmo de Euclides

El algoritmo de euclides permite calcular el máximo común divisor entre 2 enteros. $\mathsf{mcd}(a, b)$ es máximo entero d tal que $d \mid a \wedge d \mid b$.

Para computar el mcd utilizaremos la siguiente proposición.

Proposición 1. *Sean a,b enteros mayores a 1. Si* $b \nmid a$*, entonces* $\mathsf{mcd}(a, b) = \mathsf{mcd}(b, [a \text{ mód } b])$.

Demostración. Si $a < b$, $a \mod b = a$. Si, en cambio, $a > b$, entonces computamos enteros q, r tales que $a = qb + r$, con $0 \leq r < b$. Veremos que $\mathsf{mcd}(qb + r, b) = \mathsf{mcd}(r, b)$. Como $b \nmid a$, r es mayor a 0. Sea d=$\mathsf{mcd}(a, b)$, por lo tanto $d \mid a$ y $d \mid b$, por lo tanto $d|r = a - qb$. Sea $d' = \mathsf{mcd}(b, r)$ es el *máximo* entero que divide a r y a b, $d \leq d'$. Análogamente, d' divide a b y tambien a r, por lo tanto también divide a $a = qb + r$. Como d es el *máximo* divisor de a y b, $d \geq d' \therefore \mathsf{mcd}(r, b) = d' = d = \mathsf{mcd}(a, b)$. □

$\underline{\mathsf{mcd}(\cdot, \cdot)}$

input: (a, b)
output: $\mathsf{mcd}(a, b)$

1. Si $b \mid a$, output b
2. Si $b \nmid a$, output $\mathsf{mcd}(b, a \mod b)$

Figura 1: Algoritmo de Euclides para calcular el máximo común divisor

1.2. Algoritmo extendido de Euclides

Sabemos que $\forall a, b \exists X, Y$ tal que $aX + bY = \mathsf{mcd}(a, b)$. Como veremos más adelante, es util saber el valor de X e Y. ¿Cómo encontrarlos?

$e\mathsf{mcd}(\cdot, \cdot)$

input: a, b
output: $MCD(a, b)$, X, Y tal que $aX + bY = MCD(a, b)$

1. Si $b \mid a$, output $\underbrace{b}_{MCD}, \underbrace{0}_{X}, \underbrace{1}_{Y}$

2. Si $b \nmid a$, $d, X, Y \leftarrow e\mathsf{mcd}(b, \overbrace{a \mod b}^{r})$ $\qquad a = qb + r$
output $d, Y, X - Yq$

Figura 2: Algoritmo extendido de Ecuclides

¿Por qué funciona?
$Xb + Y \underbrace{r}_{a-qb} = d = Xb + Ya - qYb = \underbrace{Y}_{X} a + \underbrace{(x - qY)}_{Y} b$

1.3. Cálculo de inversos modulo N

¿Cómo invertimos $a \mod N$?
Dado a, N calcular $a^{-1} \mod N$. Sabemos que $a^{-1} \mod N$ existe si $\mathsf{mcd}(a, N) = 1$

Invert

input: a, N
output: $\perp$ si a no es invertible o b tal que $ba = 1 \mod N$.
1. $d, X, Y \leftarrow e\mathsf{mcd}(a, N)$
2. si $d \neq 1$, output $\perp$
3. output X

Figura 3: Algortimo para invertir mod N

Dado que $aX + NY = d$, tenemos que si $d = 1$, entonces $aX = 1 \mod N$

1.4. Exponenciación modular

A continuación describimos 3 algoritmos de exponenciación modular.

ExpMod$(\cdot,\cdot)$

input: a, b, N
output: $a^b \mod N$
1. $r = 1$
2. For $i = 1$ to b:
3. $\quad r = r \cdot a \mod N$
4. **output** r

Figura 4: Algoritmo lineal de exponenciación modular

Tiempo: $O(b)$ operaciones.
El siguiente algoritmo aprovecha el hecho de que a^{2k} es igual a $(a^k)^2$.

ExpMod$(\cdot,\cdot)$

input: a, b, N
output: $a^b \mod N$
1. Si b es par:
2. $\quad r = \mathsf{ExpMod}(a, b/2)$
3. $\quad$ **output** $r \cdot r \mod N$
4. Si b es impar:
5. $\quad r = \mathsf{ExpMod}(a, (b-1)/2)$
6. $\quad$ **output** $a \cdot r \cdot r \mod N$

Figura 5: Algoritmo logaritmico de exponenciación modular

Tiempo: $O(\log b)$ operaciones.

El último algoritmo que mostramos es utilizado cuando la base es usada en multiples evaluaciones. Dada la base a podemos preprocesar los valores de a^{2^i} para $i = 1, ..., \log N$. De esta forma, para cada exponente b podemos tomar su decomposición binaria y utilizar los valores precomputados anteriormente. Es decir, sea $b_0, ..., b_{\log N}$ los bits de b ((veremos más adelante que $\log N$ es una buena cota superior para el largo de b),

entonces

$$a^b = a^{\sum_{i=0}^{\log N} 2^i \cdot b_i} = \prod_{i|b_i=1} a^{2^i} \quad \text{mód } N$$

ExpMod$(\cdot,\cdot)$

input: a, b, N
output: a^b mód N

Preprocesamiento: Computar el conjunto $\{a^{2^i} \text{ mód } N\}_{i=1}^{\log N}$. (Tiempo $\log N$ operaciones).

Exponenciación
1. $r = 1$
2. For $i = 1$ to $|b|$:
2. si $b_i = 1$:
3. $r = r \cdot a^{2^i}$ mód N
4. **output** r

Figura 6: Algoritmo logaritmico de exponenciación modular con preprocesamiento de la base

Tiempo fase de exponenciación: $O(||b|| = \text{peso de hamming o cantidad de 1's en } b)$

2. Grupos Abelianos

Sea $\mathbb{G}$ un conjunto y $\circ$ una operacón binaria.

Definición 2. $(\mathbb{G}, \circ)$ *es un grupo si:*

1. $\circ$ *es cerrada para* $\mathbb{G}$*:* $g \circ h \in \mathbb{G} \qquad \forall g, h \in \mathbb{G}$
2. $\exists$ *elemento neutro* e*:* $g \circ e = e \circ g = g \qquad \forall g \in \mathbb{G}$
3. *inversos:* $\forall g \in \mathbb{G} \exists g' \in \mathbb{G}$ *tal que* $g \circ g' = e$
4. *asociatividad:* $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3 \qquad \forall g_1, g_2, g_3 in \mathbb{G}$
5. *conmutatividad:* $g_1 \circ g_2 = g_2 \circ g_1$ *(Para grupos abelianos abelianos)*

En muchas ocaciones la operación se puede obtener del contexto, y en tales casos denotaremos al grupo simplemente por su conjunto.

Definición 3. *Si $\mathbb{G}$ es finito, entonces $m = |\mathcal{G}|$ es el* orden *del grupo.*

Ejemplo 4.

- $(\mathbb{Z}, +)$ *sí es grupo abeliano.*
- $(\mathbb{Z}, \times)$ *no es grupo*
- *Sea* $\mathbb{Z}_N = \{0, 1, ..., N-1\}$, $(\mathbb{Z}_N, +_N)$ *sí es grupo abeliano ($+_N$: suma* mód N*).*
- *Sea* $\mathbb{Z}_N^* = \{x \in \mathbb{Z}_N | \mathsf{mcd}(x, N) = 1\}$. $(\mathbb{Z}_N^*, \times_N)$ *sí es grupo abeliano. ($\times_N$: multiplicación* mód N*).*
- $(\mathbb{R}, \times)$ *no es grupo, ya que 0 no tiene inverso.*
- $(\mathbb{R} \setminus \{0\}, \times)$ *sí es grupo.*

2.1. Exponenciación en grupos

$m \cdot g = \underbrace{g \circ g \circ ... \circ g}_{m \text{ veces}}$ (notación aditiva)

$g^m = g \circ g \circ ... \circ g$ (notación multiplcativa)

Podemos demostrar que la notación se "comporta bien":

$$g^{m+m'} = g^m \circ g^{m'}$$
$$(g^m)^{m'} = g^{m \cdot m'}$$
$$g^m \circ h^m = (g \circ h)^m$$

En la clase anterior vimos los siguientes resultados.

Teorema 5. *Si $\mathbb{G}$ es un grupo de orden m, entonces $g^m = 1 \forall g \in \mathbb{G}$ (en donde 1 es el elemento neutro para $\mathbb{G}$)*

Corolario 6. *Sea $\mathbb{G}$ un grupo de orden m, entonces para todo $g \in \mathbb{G}$, y para todo $x \in \mathbb{N}$, $g^x = g^{x \mod m}$*

Corolario 7. *Sea $f_e : \mathcal{G} \to \mathcal{G}$ una función definida como $f_e(g) = g^e$. f_e es una biyección si $\mathsf{mcd}(e, m) = 1$, y más aun, si $d = e^{-1}$* mód m*, entonces f_d es su función inversa.*

Un grupo muy importante es $\mathbb{Z}_N^*$ (todos los elementos de $\mathbb{Z}_N$ que tienen inversos multiplicativos.

Definición 8. *La función de Euler es* $\phi(N) = |\mathbb{Z}_N^*|$.

- si P es primo, ¿cuánto es $\phi(P)$?

  $$\mathbb{Z}_P^* = \{1, ..., P-1\} \Rightarrow \phi(P) = P - 1$$

  pues todo elemento positivo menor a P tiene inverso mod P ($\mathsf{mcd}(x, P) = 1$).

- si $N = P \cdot Q$, $P \neq Q$, ambos primos

  $|\mathbb{Z}_N^*| = ?$

  elementos divisibles por P: $P, 2P, 3P, ..., (Q-1)P$

  elementos divisibles por Q: $Q, 2Q, 3Q, ..., (P-1)Q$

  $\therefore \phi(PQ) = PQ - (P-1) - (Q-1) = (P-1)(Q-1)$

- EN general si, $N = \prod P_i^{e_i}$ (decomposición única de N en numeros primos $\{P_i\}$), entonces $\phi(N) = \prod P_i^{e_i - 1}(P_i - 1)$.

(A continuación los mismos corolarios anteriores aplicados a $\mathbb{Z}_N^*$)

Corolario 9. $\forall a \in \mathbb{Z}_N^*$

$$a^{\phi(N)} = 1 \ mod \ N$$

Corolario 10. *$f_e(a)$: a^e mód N es biyección si $e \in \mathbb{Z}_{\phi(N)}^*$*
Sea $d = e^{-1}$ mód $\phi(N)$, entonces

$$f_d(f_e(a)) = f_d(a^e \mod N) = a^{e \cdot d} \mod N = a^{e \cdot d \mod \phi(N)} \mod N = a \mod N$$

3. Isomorfismos

En esta sección veremos que si $N = pq$, entonces el grupo $\mathbb{Z}_N$, se pueden representar en base a $\mathbb{Z}_p$ y $\mathbb{Z}_q$ (análogo para $\mathbb{Z}_N^*$ también).

Definición 11. *$f : \mathbb{G} \to \mathbb{H}$ es isomorfismo de $\mathbb{G}$ a $\mathbb{H}$ si*

1. *f es biyección*
2. *$f(g_1 \circ_{\mathcal{G}} g_2) = f(g_1) \circ_{\mathcal{H}} f(g_2)$*

Si existe tal función f entonces decimos que $\mathbb{G}$ y $\mathbb{H}$ son isomorfos, *y lo denotamos como $\mathbb{G} \cong \mathbb{H}$.*

3.1. Teorema del resto chino

Si $\mathsf{mcd}(p,q) = 1 \wedge N = pq$, entonces $\mathbb{Z}_N \cong \underbrace{\mathbb{Z}_P \times \mathbb{Z}_Q}_{(X,Y):X\in\mathbb{Z}_P\wedge Y\in\mathbb{Z}_Q} \wedge \mathbb{Z}_N^* \cong \mathbb{Z}_P^* \times \mathbb{Z}_Q^*$.

$f(X) = (X \mod P, X \mod Q)$ es el isomorfismo.
operaciones:

- $\mathbb{Z}_p \times ZZ_q$: $(X_1, Y_1) \boxplus (X_2, Y_2) = (X_1 + X_2 \mod p, Y_1 + Y_2 \mod q)$
- $\mathbb{Z}_p^* \times ZZ_q^*$: $(X_1, Y_1) \boxtimes (X_2, Y_2) = (X_1 \cdot X_2 \mod p, Y_1 \cdot Y_2 \mod q)$

Ejemplo 12. *Calculemos* $18^{25} \mod 35$.

$$\begin{aligned} 18^{25} \mod \underbrace{35}_{5\cdot 7} &\leftrightarrow ((18 \mod 5)^{25}, (18 \mod 7)^{25}) \\ &= (3^{25} \mod 5, 4^{25} \mod 7) \\ &= (3^{25 \mod \overbrace{4}^{|\mathbb{Z}_5^*|}} \mod 5, 4^{25 \mod \overbrace{6}^{|\mathbb{Z}_7^*|}} \mod 7) \\ &= (3 \mod 5, 4 \mod 7) \end{aligned}$$

¿Cómo invertimos $(3 \mod 5, 4 \mod 7)$ *a* $\mathbb{Z}_{35}^*$*?*

En general, sea $X_p = X \mod p$, $X_q = X \mod q$. *Queremos converir* (X_p, X_q) *a* $X \in \mathbb{Z}_N^*$. *Por teorema del resto chino, sabemos que*

$$(X_p, X_q) \to X_p \cdot (1,0) + X_q \cdot (0,1)$$

¿Cuál es la representación de $(1,0) \wedge (0,1)$ *en* $\mathbb{Z}_N^*$*?*

Como $\mathsf{mcd}(p,q) = 1$, *entonces* $\hat{X} \cdot p + \hat{Y} \cdot Q = 1$ */ mod p, por lo que,* $\hat{Y} \cdot q = 1 \mod p$. *De forma análoga, obtenemos que* $\hat{X} \cdot p = 1$. *Por lo tanto, podemos concluir que:* $(1,0) \leftrightarrow \hat{Y} \cdot q \mod N$ *y* $(0,1) \leftrightarrow X \cdot p \mod N$.

Volviendo al ejemplo, necesitamos X, Y *tal que* $X \cdot 5 + Y \cdot 7 = 1 \mod 35$

Por ejemplo, $X = 3$ *e* $Y = -2 \mod 35 = 33$. *Calculamos entonces,* $33 \cdot 7 = 34 \cdot 7 \mod 35 = 21$ *y* $3 \cdot 5 = 15$. *Por lo tanto, el resultado es* $3 \cdot 21 + 15 \cdot 4 \mod 35 = 18$.

3.2. Demostración del teorema del resto chino

Está claro que para cualquier $x \in \mathbb{Z}_N$ el output $f(x)$ es un par de elementos (x_p, x_q) con $x_p \in \mathbb{Z}_p$ y $x_q \in \mathbb{Z}_q$. Además, decimos que si $x \in \mathbb{Z}_N^*$ entonces $(x_p, x_q) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Es más, si (por ejemplo) $x_p \notin \mathbb{Z}_p^*$ entonces esto significa que el $\mathsf{mcd}([x \mod p], p) \neq 1$. Pero entonces $\mathsf{mcd}(x, p) \neq 1$. Esto implica que $\mathsf{mcd}(x, N) \neq 1$, contradiciendo el supuesto de que $x \in \mathbb{Z}_N^*$.

Ahora mostramos que f es un isomorfismo de $\mathbb{Z}_N$ a $\mathbb{Z}_p \times \mathbb{Z}_q$. (La demostración de que es un isomorfismo de $\mathbb{Z}_N^*$ a $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ es similar.) Comenzamos probando que f es inyectiva. Sean $x \neq x' \in ZZ_N$, tal que $f(x) = (x_p, x_q) = f(x')$. Entonces $x = x_p = x' \mod p$ y $x = x_q = x' \mod q$. Esto implica que $(x - x')$ es divisible por p y por q. Como $\mathsf{mcd}(p, q) = 1$, $pq = N$ divide a $(x - x')$. Pero entonces $x = x' \mod N$. Por lo tanto f es inyectiva.

Como $|\mathbb{Z}_N| = N = p \cdot q = |\mathbb{Z}_p| \cdot |\mathbb{Z}_Q|$, los conjuntos $\mathbb{Z}_N$ y $\mathbb{Z}_p \times \mathbb{Z}_q$ son del mismo tamaño. Esto, junto con el hecho de que f es inyectiva implica que f es biyectiva.

En el siguiente párrafo, sean $+_N$, $+_p$, $+_q$ adición módulo N, p y q respectivamente. $\boxplus$ denota la operación de grupo en $\mathbb{Z}_p \times \mathbb{Z}_q$ (es decir, adición módulo p en la primera componente y módulo q en la segunda). Para concluir la demostración de que f es un isomorfismo de $\mathbb{Z}_N$ a $\mathbb{Z}_p \times \mathbb{Z}_q$, tenemos que mostrar que para todo $a, b \in \mathbb{Z}_N$ se cumple que $f(a +_N b) = f(a) \boxplus f(b)$. Para ver que esto es cierto, note que

$$f(a +_N b) = \Big([(a +_N b) \mod p], [(a +_N b) \mod q]\Big)$$

$$= \Big([(a +_p b) \mod p], [(a +_q b) \mod q]\Big)$$

$$= \Big([a \mod p], [a \mod q]\Big) \boxplus \Big([b \mod p], [b \mod q]\Big) = f(a) \boxplus f(b).$$

Ejercicio: Demostrar para $\mathbb{Z}_N^*$