Teoría de números

Criptología y Seguridad de los Datos (CSD)

©Damián López

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf
Escola Tècnica Superior d'Enginyeria **Informàtica**

September 27, 2022

Índice

Bibliografía

- Handbook of applied crytography. *A. J. Menezes, P. C. van Oorshot and S. A. Vanstone*. CRC Press. 1996.
  (Capítulo 9)
- Introduction to algorithms. *C. E. Leiserson, C. Stein, R. Rivest and T. H. Cormen*. The MIT Press (3rd edition) 2009.
- Understanding Cryptography. *C. Paar and J. Pelzl*. Springer. 2010.

Teoría de grupos

Dado un conjunto finito G, el par $\langle G, \oplus \rangle$ es un grupo si se cumple que:

- La operación $\oplus$ es cerrada en G
- El elemento neutro para la operación $\oplus$ está incluido en G
- Para todo valor a en G se cumple que G contiene su inverso.

Habitualmente, utilizaremos la notación $\langle G, + \rangle$ o $\langle G, \cdot \rangle$.

Teoría de grupos

Dado un grupo $\langle G, +\rangle$ (o alternativamente $\langle G, \cdot\rangle$) y cualquier elemento $a \in G$, con ka (o alt. a^k) denotamos la composición de la operación k veces.

Con $< a >$ denotaremos el SUBGRUPO GENERADO POR a, esto es:

$$< a >= \{a^i \ : \ i \geq 1\}$$

Dado un elemento a en G y denotando con e el elemento neutro, diremos que el ORDEN DE a es el valor r tal que $ra = e$ (alt. $a^r = e$).

Teoría de grupos

El tamaño de cualquier subgrupo de un grupo es divisor del tamaño del grupo (TEOREMA DE LAGRANGE).

Un grupo es cíclico si existe un elemento a del grupo capaz de generarlo, en ese caso, a es un generador del grupo (sólo consideraremos grupos cíclicos).

Para cualquier grupo finito $\langle G, \oplus \rangle$ se cumple que si $a \in G$, entonces $ord(a) = card(< a >)$

Aritmética modular

- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
- Congruencia módulo n:

$$a \equiv b \pmod{n} \iff a - b = kn,\ k \in \mathbb{Z}$$

- Reducción módulo n (valor equivalente a uno dado en $\mathbb{Z}_n$):

$$a \bmod n$$

- Relación de equivalencia.

Aritmética modular

Grupos finitos módulo n. Operativa

Dados $a \equiv a' \pmod{n}$ y $b \equiv b' \pmod{n}$:

- $a + b \equiv a' + b' \pmod{n}$
- $ab \equiv a'b' \pmod{n}$

Por lo que, operando en $\mathbb{Z}_n$:

- $[a]_{\equiv_n} + [b]_{\equiv_n} = [a+b]_{\equiv_n}$
- $[a]_{\equiv_n}[b]_{\equiv_n} = [ab]_{\equiv_n}$

Aritmética modular

Grupos finitos módulo n. Operativa

Si $\langle G, \odot \rangle$ es un grupo finito con identidad e, entonces:

- Dado $a \in G$ con $ord(a) = r$, se cumple que:

$$a^i \equiv a^j \text{ si y sólo si } i \equiv j \pmod{r}$$

Es consistente con el resultado anterior definir $a^0 = e$ y $a^i = a^{i \bmod r}$, para todo $i \geq 0$

- COROLARIO para todo $a \in G$ se cumple que $a^{card(G)} = e$

Aritmética modular

Grupos finitos módulo n

$\langle \mathbb{Z}_n, + \rangle$

- La operación $+$ módulo n es cerrada en $\mathbb{Z}_n$
- Existe un elemento neutro para la operación $+$
- Para todo valor a en $\mathbb{Z}_n$ existe su inverso.

$\langle \mathbb{Z}_n, + \rangle$ tiene estructura de grupo.

Aritmética modular

Grupos finitos módulo n

$\langle \mathbb{Z}_n, \cdot \rangle$

- La operación $\cdot$ módulo n es cerrada en $\mathbb{Z}_n$
- Existe un elemento neutro para la operación $\cdot$
- Para todo valor a en $\mathbb{Z}_n$... ¿existe su inverso?

Aritmética modular

Grupos finitos módulo n

$\langle \mathbb{Z}_n, \cdot \rangle$

- La operación $\cdot$ módulo n es cerrada en $\mathbb{Z}_n$
- Existe un elemento neutro para la operación $\cdot$
- Para todo valor a en $\mathbb{Z}_n$... ¿existe su inverso?

  No... sólo para aquellos relativamente primos con n

Aritmética modular

Grupos finitos módulo n: MCD

El $mcd(a,b)$ es el menor entero estrictamente positivo del conjunto $\{xa + yb \;:\; x, y \in \mathbb{Z}\}$ (combinaciones lineales de a y b)

$$mcd(a,b) = mcd(b, a \mod b)$$

Aritmética modular

Grupos finitos módulo n: MCD

EuclidesExt(a, b):

if $b = 0$ **then**

$\quad Return(a, 1, 0)$

else

$\quad (d', x', y') = EuclidesExt(b, a \bmod b))$

$\quad (d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$

$\quad Return(d, x, y)$

end if

Aritmética modular

Grupos finitos módulo n: MCD

a	b	d	x	y
27	8	1	3	$-1 - \lfloor 27/8 \rfloor \cdot 3 = -10$
8	3	1	-1	$1 - \lfloor 8/3 \rfloor \cdot (-1) = 3$
3	2	1	1	$0 - \lfloor 3/2 \rfloor \cdot 1 = -1$
2	1	1	0	$1 - \lfloor 2/1 \rfloor \cdot 0 = 1$
1	0	1	1	0

$$(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$$

Aritmética modular

Grupos finitos módulo n

$\langle \mathbb{Z}_n, \cdot \rangle$

- Si denotamos con $\mathbb{Z}_n^*$ el conjunto de valores invertibles de $\mathbb{Z}_n$, entonces $\langle \mathbb{Z}_n^*, \cdot \rangle$ tiene estructura de grupo.
- El número de elementos invertibles en $\mathbb{Z}_n^*$ puede calcularse conociendo la descomposición de n en factores primos, siendo $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$:

$$\phi(n) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_i - 1})$$

Aritmética modular

Grupos finitos módulo n. Operativa

Dado $\langle \mathbb{Z}_n^*, +, \cdot \rangle$

- El inverso de a para la operación $+$ es $-a \equiv n - a \pmod{n}$
- El inverso de a para la operación $\cdot$ es b tal que $ab \equiv 1 \bmod n$

  (necesario recurrir al cálculo del $mcd(a, n)$)
- El inverso de a para la potencia es b tal que $ab \equiv 1 \bmod \phi(n)$

  (necesario conocer la descomposición en factores de n para después calcular $mcd(a, \phi(n))$.

Aritmética modular

Grupos finitos módulo n. Operativa

El CÁLCULO EFICIENTE de la composición de la operación $+$ o $\cdot$ puede hacerse teniendo en cuenta:

$$\begin{cases} a^{2c} \bmod n = (a^c)^2 \bmod n \\ a^{2c+1} \bmod n = (a^c)^2 a \bmod n \end{cases}$$

Aritmética modular

Grupos finitos módulo n. Operativa

El CÁLCULO EFICIENTE de la composición de la operación $+$ o $\cdot$ puede hacerse teniendo en cuenta:

$$\begin{cases} a^{2c} \bmod n = (a^c)^2 \bmod n \\ a^{2c+1} \bmod n = (a^c)^2 a \bmod n \end{cases}$$

$$\begin{cases} (2c)a \bmod n = 2(ca) \bmod n \\ (2c+1)a \bmod n = 2(ca) + a \bmod n \end{cases}$$

Aritmética modular

Grupos finitos módulo n. Operativa: Exponenciación por cuadrados sucesivos

Require: Enteros a, b y n
Ensure: $a^b \bmod n$

$sol = 1$
$< b_1, b_2, \ldots, b_k >$ representación binaria de b
//bit más representativo b_1
for i=1 **to** k **do**
  $sol = sol \cdot sol \bmod n$
  if $b_i = 1$ **then**
    $sol = sol \cdot a \bmod n$
  end if
end for
return sol

Aritmética modular

Ejemplo:
Para obtener $5^{11} \bmod 16$ tenemos en cuenta que $11_{10} = 1011_2$

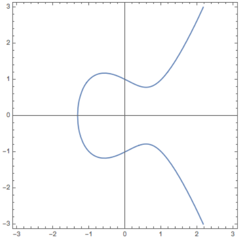
i	b_i	exp_2	*sol*
		0	1
1	1	1	$(1 \cdot 1 \bmod 16) \cdot 5 \bmod 16 = 5$
2	0	10	$(5 \cdot 5 \bmod 16) = 9$
3	1	101	$(9 \cdot 9 \bmod 16) \cdot 5 \bmod 16 = 5$
4	1	1011	$(5 \cdot 5 \bmod 16) \cdot 5 \bmod 16 = 13$

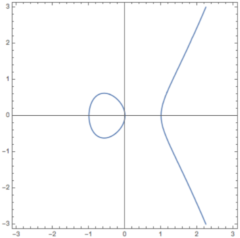
Aritmética modular

Curvas elípticas

Una CURVA ELÍPTICA es el conjunto de puntos definido por una ecuación de la forma

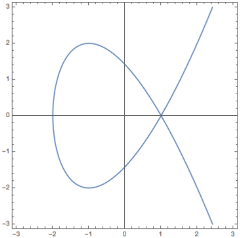
$$y^2 = x^3 + ax + b$$

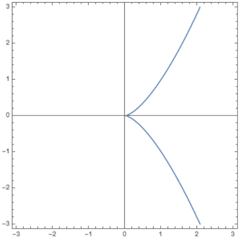




Aritmética modular

Curvas elípticas





Para uso criptográfico, es interesante que la curva no tenga discontinuidades, para ello los valores de a y b deben cumplir la ecuación:

$$4a^3 + 27b^2 \neq 0.$$

Aritmética modular

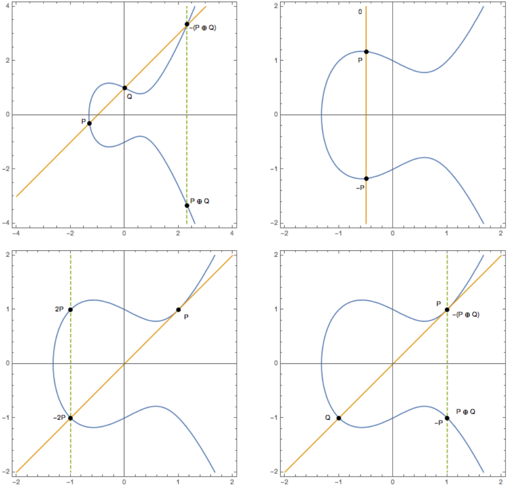
Curvas elípticas

Puede definirse un grupo a partir del conjunto de los puntos de una curva elíptica C:

- Añadiendo un punto adicional 0 ubicado en el infinito como elemento neutro.
- Definiendo una operación $\oplus$ (suma) de puntos a partir de la consideración que la suma de tres puntos alineados de la curva da siempre el elemento neutro.

Aritmética modular

Curvas elípticas



Aritmética modular

Curvas elípticas. Operativa

Dados dos puntos $P = (x_P, y_P)$ y $Q = (x_Q, y_Q)$:

$$\begin{cases} m = \frac{y_P - y_Q}{x_P - x_Q} & \text{si la recta es secante a dos puntos} \\ m = \frac{3x_P^2 + a}{2y_P} & \text{si la recta es tangente a un punto} \end{cases}$$

$$\begin{aligned} x_R &= m^2 - x_P - x_Q \\ y_R &= y_P + m(x_R - x_P) \\ &\text{(alternativamente, } y_R = y_Q + m(x_R - x_Q)) \end{aligned}$$

Por lo tanto, para obtener las coordenadas de $P \oplus Q$, basta considerar el punto $(x_R, -y_R)$.

Aritmética modular

Curvas elípticas. Operativa

Es posible trabajar en un dominio finito considerando aritmética módulo n. Dados dos puntos $P = (x_P, y_P)$ y $Q = (x_Q, y_Q)$:

$$\begin{cases} m = (y_P - y_Q)(x_P - x_Q)^{-1} \bmod n & \text{//si la recta es secante} \\ m = (3x_P^2 + a)(2y_P)^{-1} \bmod n & \text{//si la recta es tangente} \end{cases}$$

$$\begin{aligned} x_R &= m^2 - x_P - x_Q \bmod n \\ y_R &= y_P + m(x_R - x_P) \bmod n \\ &\quad (\text{alternativamente, } y_R = y_Q + m(x_R - x_Q) \bmod n) \end{aligned}$$

y, de nuevo, obtener las coordenadas de $P \oplus Q$ como las del punto $(x_R, -y_R)$.

Aritmética modular

Cuerpos

La terna $\langle G, +, \times \rangle$ tiene estructura de *cuerpo* (o campo, por el témino en inglés *field*) si:

- El par $\langle G, + \rangle$ tiene estructura de grupo donde $0 \in G$ es el elemento neutro.
- El par $\langle G - \{0\}, \times \rangle$ tiene estructura de grupo donde $1 \in G$ es el elemento neutro.
- Las operaciones cumplen la propiedad distributiva respecto $+$, esto es:
$$a \times (b + c) = (a \times b) + (a \times c).$$

El orden de un cuerpo es siempre potencia de un primo.

Aritmética modular

Cuerpos

- Si el cuerpo tiene orden primo p, entonces el grupo se denota como $\mathcal{F}_p$ (o $GF(p)$) y:

$$G = \{0, 1, 2, \ldots p - 1\}$$

- Cuando el tamaño del cuerpo no es un número primo hablamos de *cuerpos extendidos*, en estos casos:
  - El conjunto de elementos del cuerpo **no pueden representarse como enteros**.
  - Las operaciones suma y producto **no son las operaciones de aritmética módulo**.

Aritmética modular

Cuerpos: Operativa

- Los elementos se pueden representar como polinomios:

$$a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_2x^2 + a_1x + a_0,$$

donde los coeficientes toman valores en $GF(p)$.

- Las operaciones suma y producto **no son las operaciones de aritmética módulo**.

Aritmética modular

Cuerpos: Operativa

- La suma de dos elementos a y b en $GF(p^m)$ consiste en sumar coeficientes en a y b del mismo grado y reducir esta suma módulo p.
- El producto de dos elementos a y b en $GF(p^m)$ se basa en el producto de polinomios estándar, considerando aritmética módulo p en la operación con coeficientes.
  Es necesario un polinomio *módulo* para reducir el resultado.

Aritmética modular

Cuerpos: Ejemplos

En el cuerpo $GF(2^8)$:

$$\begin{array}{rr} & x^7 \quad\quad +x^5+x^3+x^2 \quad\quad +1 \\ + & x^6+x^5 \quad\quad +x^2+x+1 \\ \hline \end{array}$$

Aritmética modular

Cuerpos: Ejemplos

En el cuerpo $GF(2^8)$:

$$
\begin{array}{rcccccccccc}
 & x^7 & & +x^5 & & +x^3 & +x^2 & & +1 \\
+ & & x^6 & +x^5 & & & +x^2 & +x & +1 \\
\hline
 & x^7 & +x^6 & & & +x^3 & & +x &
\end{array}
$$

Aritmética modular

Cuerpos: Ejemplos

En el cuerpo $GF(2^8)$, trabajando módulo el polinomio irreducible $x^8 + x^4 + x^3 + 1$:

$$\begin{array}{r r} & x^6 + x^2 + 1 \\ \times & + x^3 + 1 \\ \hline \end{array}$$

Aritmética modular

Cuerpos: Ejemplos

En el cuerpo $GF(2^8)$, trabajando módulo el polinomio irreducible $x^8 + x^4 + x^3 + 1$:

$$
\begin{array}{rcccccc}
 & & & x^6 & & +x^2 & +1 \\
\times & & & & +x^3 & & +1 \\
\hline
 & & & x^6 & & +x^2 & +1 \\
 & x^9 & & +x^5 & +x^3 & & \\
\hline
 & x^9 & +x^6 & +x^5 & +x^3 & +x^2 & +1
\end{array}
$$

Aritmética modular

Cuerpos: Ejemplos

En el cuerpo $GF(2^8)$, trabajando módulo el polinomio irreducible $x^8 + x^4 + x^3 + 1$:

$$
\begin{array}{rl}
 & x^6 + x^2 + 1 \\
\times & x^3 + 1 \\
\hline
 & x^6 + x^2 + 1 \\
 & x^9 + x^5 + x^3 \\
\hline
 & x^9 + x^6 + x^5 + x^3 + x^2 + 1
\end{array}
$$

$$
\begin{array}{r|l}
x^9 + x^6 + x^5 + x^3 + x^2 + 1 & x^8 + x^4 + x^3 + 1 \\
\cline{2-2}
x^9 + x^5 + x^4 + x & x \\
\cline{1-1}
x^6 + x^4 + x^3 + x^2 + x + 1 &
\end{array}
$$

Funciones unidireccionales

Logaritmo discreto

Dado un grupo cíclico $\langle G, \cdot \rangle$ de orden t y α un generador de G

Para cualquier $\beta \in G$, el cálculo del *logaritmo discreto* de β en base α (que denotaremos con $log_\alpha \beta$) el el problema de encontrar el único entero $x \in \mathbb{Z}_t$ tal que $\alpha^x = \beta$.

No se conoce solución eficiente al problema para el caso general.

Funciones unidireccionales

Factorización de enteros

Si consideramos el grupo $\langle \mathbb{Z}_n^*, \cdot \rangle$ donde $n = pq$ con p y q primos, entonces, para un valor $x \in \mathbb{Z}_n^*$ cualquiera, a partir de:

$$y = x^e \bmod n$$

considerando el valor e como público, el problema de obtener x a partir de y implica obtener primero los factores de n, problema para el que NO SE CONOCE SOLUCIÓN EFICIENTE PARA EL CASO GENERAL.