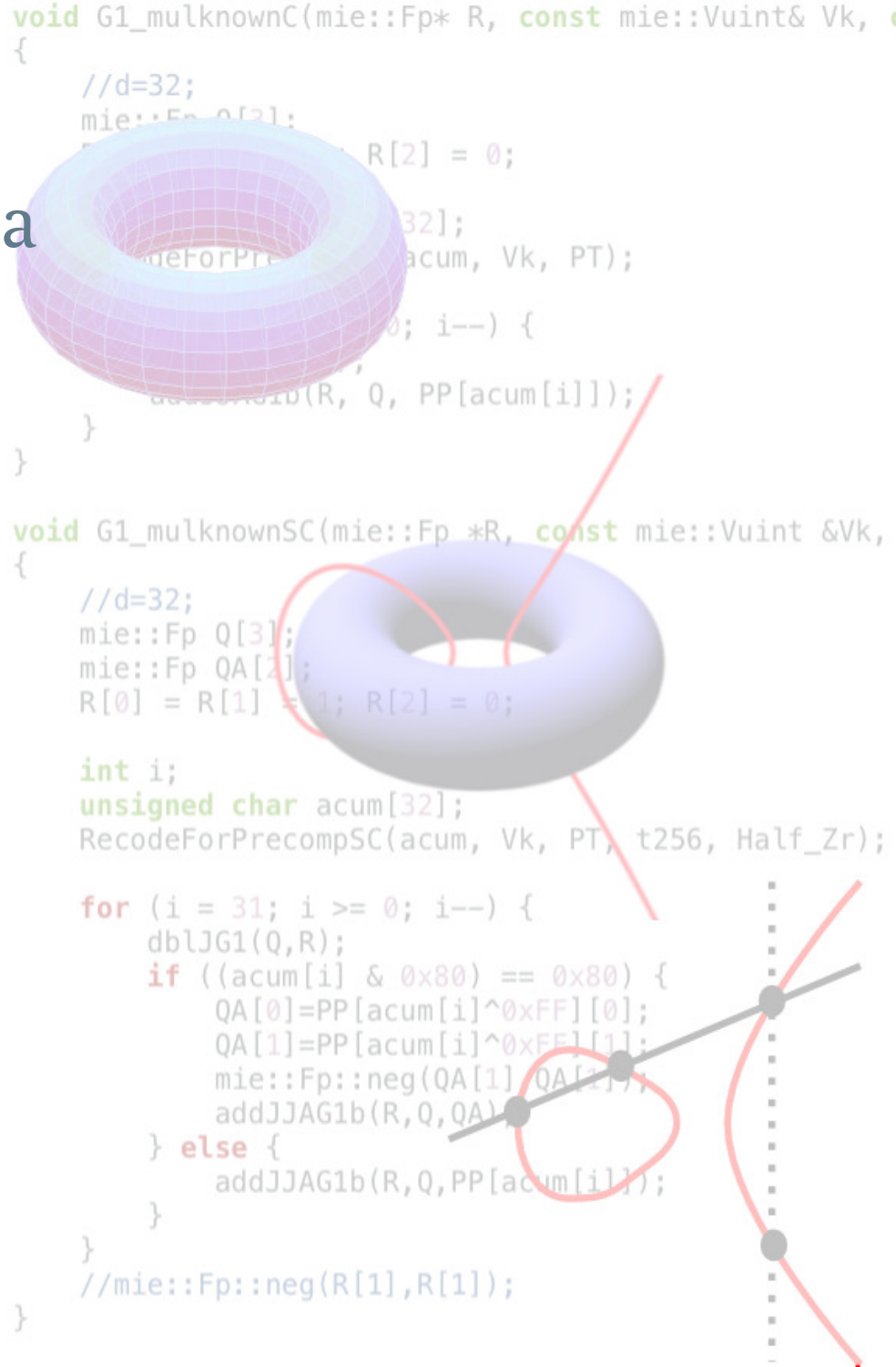
Matemáticas aplicadas a la criptografía

Unidad III - Campos finitos, y residuos cuadráticos

Dr. Luis J. Dominguez Perez

Universidad Don Bosco

Abril 24, 2013



Contenido de la sección 1

MCD revisitado

Hemos visto anteriorme cómo calculor el máximo común divisor de un número. Si $a, b \in \mathbb{Z}$, con $0 < b \leq a$, entonces:

- de el algoritmo tradicional de la división sabemos que existen $q, r \in \mathbb{Z}$, con $r < b$, y $a = bq + r$.
- si $g \in \mathbb{Z}$, y $g|a$ y $g|b$, entonces:

$$g|(a - bq) \Rightarrow g|r$$

MCD revisitado

Ahora bien:

- Si $\text{MCD}(a, b) = g$, entonces implica que $g|r$, donde r es el residuo que resulta de dividir a por b
- Si $r = 0$, entonces $b|a$, y el máximo común divisor de a, b es b.
- Si $r \neq 0$, entonces $\text{MCD}(a, b) = \text{MCD}(b, r)$, la cual es una operación más económica. Repitiendo este proceso hasa que $r = 0$ nos da el algoritmo MCD.

Algoritmo MCD

Algoritmo simple de MCD:

Input: Integers $0 < b \leq a$
Output: MCD(a, b)

$n = a$; $d = b$
$r = n - (d \times \lfloor \frac{n}{d} \rfloor)$
while $r \neq 0$ **do**
$n = d$
$d = r$
$r = n - (d \times \lfloor \frac{n}{d} \rfloor)$
end while
return MCD$(a, b) = d$

MCD extendido

El algoritmo MCD extendido es idéntico al algoritmo estándar, pero además carga con información adicional. Si $\text{MCD}(a, b) = g$, entonces sabemos que existen $x, y \in \mathbb{Z}$ tal que:

$$ax + by = g$$

y es la mínima combinación lineal positiva para a y b.

MCD extendido

- Note que si el MCD es 1, entonces esta ecuación nos da los inversos para a mod b, y b mod a: $x \equiv a^{-1} \bmod b$, y $y \equiv b^{-1} \bmod a$.
- Si el MCD no es 1, entonces, y dado que es la combinación linear más pequeña, se dice que no existen inversos para a mod b o b mod a.
- Extendiendo el algoritmo de MCD para calcular este dato extra, nos da un algoritmo eficiente para calcular los inversos multiplicativos.

Cómo extender el algoritmo MCD

Para extender el algoritmo MCD, la parte de la ecuación debe de agregarse a las iteraciones. Los valores iniciales de la ecuación son:

$$a(1) + b(0) = a$$
$$a(0) + b(1) = b$$

Algoritmo extendido de MCD

Input: Integers $0 < b \leq a$

Output: $x, y, \text{MCD}(a,b)$ tal que $ax + by = \text{MCD}(a,b)$

$v_0 = a$; $v_1 = b$

$x_0 = 1$; $y_0 = 0$

$x_1 = 0$; $y_1 = 1$

$i = 1$ {puntero al valor v más pequeño}

while $v_i \neq 0$ **do**

$i = i + 1 \bmod 2$

$q = \left\lfloor \frac{v_i}{v_{i+1 \bmod 2}} \right\rfloor$

$v_i = v_i - (q \times v_{i+1 \bmod 2})$

$x_i = x_i - (q \times x_{i+1 \bmod 2})$

$y_i = y_i - (q \times y_{i+1 \bmod 2})$

end while

$i = i + 1 \bmod 2$

return $x_i, y_i, \text{MCD}(a,b) = v_i$

Ejercicio

- Implemente el algoritmo extendido de Euclides (MCD)

- Calcule el inverso multiplicativo de $101 \bmod 1999$, y el inverso de $1999 \bmod 101$ utilizando el algoritmo.

Ejercicio

- Implemente el algoritmo extendido de Euclides (MCD)

- Calcule el inverso multiplicativo de 101 mod 1999, y el inverso de 1999 mod 101 utilizando el algoritmo.

Contenido de la sección 2

Estructuras algebraicas

- Las estructuras algebraicas son el corazón de la mayoría de los criptosistemas y de los ataques criptoanalíticos.

- Sea G un conjunto de elementos, y $+, \times, \odot$ operadores binarios mapeando G a G, recordando las propiedades básicas discutidas en el inicio, tenemos que...

Objetos básicos

Los objetos matemáticos básicos son:

- Semigrupo: $\langle G, \odot \rangle$ es un semigrupo si G es cerrado y asociativo bajo $\odot$
- Monoide: $\langle G, \odot \rangle$ es un monoide si es un semigrupo, y existe un elemento identidad $e \in G$
- Grupo: $\langle G, \odot \rangle$ es un grupo si es un monoide, y existe un inverso para todo $a \in G$.
- Grupo abeliano: $\langle G, \odot \rangle$ es un grupo abeliano si es un grupo, y si $\odot$ es conmutativo
- Anillo: $\langle G, +, \times \rangle$ es un anillo si $\langle G, + \rangle$ es un grupo abeliano con identidad 0, $\langle G - \{0\}, \times \rangle$ es un monoide con identidad 1, y mantiene la propiedad distributiva bajo $+$
- Campo: $\langle G, +, \times \rangle$ es un campo si es un anillo, y $\langle G - \{0\}, \times \rangle$ es un grupo abeliano.

Ejemplos de estructuras algebraicas

Estructura	Monoide	Grupo	G. Abeliano	Anillo	A. Conmutativo	Campo
$\langle \mathbb{Q}^{n\times n}, \times \rangle$	✓	×	×	×	×	×
$\langle \mathbb{Q}^{n\times n}(inv), \times \rangle$	✓	✓	×	×	×	×
$\langle \mathbb{Z}, + \rangle$	✓	✓	✓	×	×	×
$\langle \mathbb{Q}^{n\times n}, +, \times \rangle$	–	–	–	✓	×	×
$\langle \mathbb{Z}/(15)\mathbb{Z}, +, \times \rangle$	–	–	–	✓	✓	×
$\langle \mathbb{Z}/(17)\mathbb{Z}, +, \times \rangle$	–	–	–	✓	✓	✓

- Las estructuras más utilizadas son los campos infinitos: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- En criptografía, las estructuras más utulizadas son las estructuras finitas, principalmente los grupos abelianos y los campos.

Observaciones sobre las estructuras

- En el caso de la criptografía, los campos utilizados son los *Campos Finitos* (también conocidos como *Campos de Galois*).
- Los campos finitos son los enteros módulo un primo p, o una potencia $q = p^m$, denotados como $\mathbb{F}_q$, o $\mathbb{Z}/q\,\mathbb{Z}$. Con $m \in \mathbb{Z}$, pudiendo ser un número compuesto.
- En el caso de ser una potencia prima, se les conoce como *extensión de campo*

observaciones

- Utilizar la q es una generalización para describir el campo finito. Algunos autores prefieres utilizar p, o la potencia explícita según les convenga.
- Un caso interesante es cuando el primo es 2, o 3. Adicionalmente, la potencia m compuesta por $2^i 3^j$, con $i, j \in \mathbb{Z}$, sin ser ambos cero, es popular.

- *Recientemente* se incluyen como estructuras algebraicas comunes a los grupos abelianos de puntos en curvas elípticas sobre un campo finito (o su extensión): $E(\mathbb{F}_p)$, $E_1(\mathbb{F}_{2^{1971}})$, $E'(\mathbb{F}_{p^d})$, ...

Ejercicio

- Defina campos finitos en Sage y verifique las propiedades algebraicas.

Subestructuras

Un subgrupo/campo es un subconjunto del conjunto original, el cual es cerrado bajo ciertas operaciones, y tiene las mismas propiedades que el original.

- Por ejemplo, $\mathbb{Z}/(15)\mathbb{Z}$ es un anillo, el subconjunto $\{0, 3, 6, 9, 12\}$ es cerrado, asociativo, y conmutativo bajo la adición, además, ya que tiene un elemento identidad, también es un subgrupo abeliano de $\mathbb{Z}/(15)\mathbb{Z}$ bajo la adición.

Orden

- Sea $\langle G, \odot \rangle$ un grupo con un elemento identidad e. El orden de G, escrito como $\text{ord}(G)$, u $|G|$ es el número de elementos en G. Si G es infinito, también lo es su orden.
- Otro tipo de orden existe para elementos en G. Si $a \in G$, entonces el orden de a es el entero positivo más chico $n > 0$, tal que:

$$\overbrace{a \odot a \odot \ldots \odot a}^{n \text{ times}} = 1$$

Si no existe n, entonces $\text{ord}(a) = \infty$.

Ejemplos

G	$\operatorname{ord}(G)$	a	$\operatorname{ord}(a)$
$\langle \mathbb{F}_{19}, \times \rangle$	18	7	3
$\langle \mathbb{F}_{19}, + \rangle$	19	7	19
$\langle \mathbb{F}_{17}, \times \rangle$	16	2	8
$\langle \{1, 3, 5, 9, 13\} \subset \mathbb{Z}/(14)\mathbb{Z}, \times \rangle$	6	11	3
$\langle \mathbb{Q}, \times \rangle$	∞	-1	2

Más sobre el orden

Teorema

Si G es un grupo finito abeliano con elemento identidad 1, y $\beta \in G$, entonces:

$$\beta^{\mathrm{ord}(G)} = 1$$

Análisis

Sea $\text{ord}(G) = n$, $G = \{\alpha_i\}_{i=0}^{n-1}$, y $\beta G = \{\beta\alpha_i\}_{i=0}^{n-1}$. $\beta G = G$ dado que:

- G es cerrado, por lo que: $\beta G \subseteq G$
- $\beta - 1\alpha_i \in G$, por lo que $\beta\beta - 1\alpha_i = \alpha_i \in \beta G$, por lo que $G \subseteq \beta G$, y $G \subseteq \beta G$.

$$\prod_{i=0}^{n-1} \alpha_i = \prod_{i=0}^{n-1} \beta\alpha_i$$

$$\prod_{i=0}^{n-1} \alpha^{-1} \prod_{i=0}^{n-1} \alpha_i = \beta^n \prod_{i=0}^{n-1} \alpha - 1 \prod_{i=0}^{n-1} \alpha_i$$

$$1 = \beta^n$$

Por lo que $\beta^{\text{ord}(G)} = 1$.

Generadores

- Si el orden de un elemento equivale al orden del grupo, se dice que ese elemento es *primitivo*, o *generador*. Por ejemplo, $3 \in \mathbb{F}_7$:

i	1	2	3	4	5	6
3^i	3	2	6	4	5	1

  Los generadores solo existen en algunos anillos finitos: $\mathbb{F}_2$, $\mathbb{F}_p$, $\mathbb{F}_{p^n}$, o $\mathbb{F}_{2^n}$, $\mathbb{Z}/4\mathbb{Z}$, o $\mathbb{Z}/(2p)\mathbb{Z}$, donde p es un primo impar.

- Los grupo finitos que tienen generadores se llaman *grupos finitos cíclicos*, ya que forman un ciclo simple conteniento cada elemento.

Encontrando generadores

Cuando existen generadores, se pueden encontrar seleccionando $\alpha \in_R G$, y probando su orden.

- Sea $\alpha \in G$, $\text{ord}(G) = \prod_{i=0}^{n-1} p_i^{e_i}$, $0 < e_i$, y $\{p_i\}_{i=0}^{n-1}$ primos distintos.
- Dado que el orden de cualquier elemento en G divide $\text{ord}(G)$, podemos escribir: $\text{ord}(\alpha) = \prod_{i=0}^{n-1} p_i^{s_i}$ con $0 \leq s_i \leq e_i$.
- Elevando α a la $\frac{\text{ord}(G)}{p_i}$, tenemos que:

$$\alpha^{\frac{\text{ord}(G)}{p_i}} = \begin{cases} 1 & p^{e_i} \nmid \text{ord}(\alpha) \Rightarrow s_i < e_i \\ \text{de otro modo} & p^{e_i} \mid \text{ord}(\alpha) \Rightarrow s_i = e_i \end{cases}$$

Encontrando generadores

- Si $\alpha^{\frac{\text{ord}(G)}{p_i}} = 1$, then $\text{ord}(\alpha) | \frac{\text{ord}(G)}{p_i}$, o:

$$\frac{p_i^{e_i} \prod_{j \neq i} p_j^{e_j}}{\prod_{j=0}^{n-1} p_j^{s_j}} = p_i^{e_i - s_i - 1} \prod_j^{e_j - s_j} \in \mathbb{Z}$$

por lo que $e_i - s_i - 1 \geq 0$, $s_i < e_i$, y $p^{e_i} \nmid \text{ord}(\alpha)$. Si $\alpha^{\frac{\text{ord}(G)}{p_i}} \neq 1$, then $\text{ord}(\alpha) \nmid \frac{\text{ord}(G)}{p_i}$, o:

$$p_i^{e_i - s_i - 1} \prod_{j \neq i} p_j^{e_j - s_j} \notin \mathbb{Z}$$

Encontrando generadores

- así que $e_i - s_i - 1 < 0$, $s_i = e_i$, y $p^{e_i} | \text{ord}(\alpha)$. Si $\alpha^{\frac{\text{ord}(G)}{p_i}} \neq 1$ para todo $p_i | \text{ord}(G)$, entonces el $\text{ord}(\alpha) = \text{ord}(G)$, ¡por lo que α es un generador!

Ejemplo

Ejemplo, encontrar un generador en $\mathbb{F}_{101}$.

- La factorización de $\phi(101) = 2^2 5^2$
- Verificar las dos exponenciaciones: α^{50}, y α^{20}. Si ninguna es 1, entonces α es un generador

α	α^{50}	α^{20}	¿generador?
2	100	95	✓
3	100	84	✓
77	1	36	×
69	100	1	×
17	1	1	×

Uso práctico

- El orden de un elemento facilita la suma y multiplicación en los exponentes.
  - Dado que $a^{\text{ord}(a)} = 1$: $a^{t+\text{ord}(a)} = a^t$
- Cálculo del inverso: $a^{-1} = a^{\text{ord}(a)-1}$
  - $3^{-1 \bmod 6} \equiv 3^5 \equiv 5 \bmod 7$
- Raíces: si el $\text{MCD}(\text{ord}(a), r) = 1$, entonces $\sqrt[r]{a} = a^{r^{-1} \bmod \text{ord}(a)}$
  - $\text{ord}(2) = 3 \in \mathbb{F}_7$, entonces $\sqrt{2} = 2^{2^{-1} \bmod 3} \equiv 4 \bmod 7$

Usos prácticos

- Calcular el orden de otro elemento: si $b = a^t$, y el $\text{MCD}(t, \text{ord}(a)) = g$, entonces el entero más pequeño n en $b^n = 1$ es:

$$n = \text{ord}(b) = \frac{\text{ord}(a)}{\text{MCD}(t, \text{ord}(a))}$$

  - $\text{ord}(3) = 6 \in \mathbb{F}_7$, por lo que $\text{ord}(2) = \text{ord}(3^2) = \frac{6}{\text{MCD}(6,2)} = 3$

Ejercicio

- Haga un programa para calcular el orden multiplicativo de todos los elementos en $\mathbb{F}_{101}$

Extensión de campos

- Las extensiones de campos, o de anillos polinomiales generales, se utilizan extensamente en la teoría de la información, además de en la criptografía. Se utilizan principalmente en los códigos de corrección de errores (para detectar bits erróneos en la transmisión de datos), en el procesamiento de señales y otras más.
- En el caso de la criptografía, se utilizan en los registros lineares de retroalimentación (que veremos más adelante), en los generadores de números aleatorios, cifrado AES, curvas elípticas, etc.

Aritmética polinomial

- Las extensiones comienzan sobre un *campo base*, como $\mathbb{F}_p$, y después la ``extienden'' al añadirle la raíz de un polinomio (solución a una ecuación irreducible en un campo dado).
  - Los números complejos son una extensión de campo sobre los números reales con la raíz $f(x) = x^2 + 1$ agregada: $i = \sqrt{-1}$ es una raíz de $f(x)$, y las potencias de i se reducen (simplifican) utilizando la relación $f(i) = 0$, o $i^2 = i$.
  - El conjunto de polinomios sobre un anillo R, $R[x] = \{\sum_{i=-1\infty}^{\infty} a_i x^i | a_i \in R\}$, utilizando operaciones normales de polinomios como suma y multiplicación, forman un anillo

Divisibilidad de polinomios

Definición

Sea R un anillo, y $R[x]$ el anillo de polinomios con elementos $g(x), h(x) \in R[x]$. Se dice que $g(x)$ divide a $h(x)$, si existe un $k(x) \in R[x]$ tarl que $g(x)k(x) = h(x)$.

Ejemplos

Divisibilidad de polinomios:

- $(x-2)(x+2) = (x^2-4)$
  - (x^2-4) factoriza sobre $\mathbb{Z}$, y sobre cualquier anillo sobre los enteros

- $\left(x+(-1)^{\frac{1}{2}}\right)\left(x-(-1)^{\frac{1}{2}}\right) = (x^2+1)$
  - (x^2+1) no factoriza sobre los enteros, y sólo se factorizaría sobre anillos conteniendo un elemento de orden 4. Si R es un campo, note que la fórmula cuadrática genera las raíces, factorizando el polinomio cuadrático.

Ejemplos

- $(x+2)^2 \equiv x^2 + x + 1 \bmod 3$
- $(x+3)(x+5) \equiv x^2 + x + 1 \bmod 7$
- Para $x^2 + x + 1$, la fórmula cuadrática es:

$$x = 2^{-1}\left(-1 \pm (-3)^{\frac{1}{2}}\right)$$

  - Para el campo $\mathbb{F}_7$ la raíz cuadrada de (-3) es ± 2, en $\mathbb{F}_3$ es cero, por lo que $x^2 + x + 1$ es factorizable en los dos campos.
  - En el caso de $\mathbb{F}_2$, 2 no tiene raíz cuadrada.
  - En el caso de $\mathbb{F}_5$ ($-3 \equiv 2$) no es residuo cuadrático, así que no existen racíces para $x^2 + x + 1$, por lo que no es factorizable.

Extensiones de campo sobre campos finitos

- En lugar de agregar *i*, agregamos raíces de polinomios sobre un campo. Por ejemplo, si $\mathbb{F}_2$ se exitende al añadir una raíz de $f(x) = x^+x + 1$, y llamamos esa raíz α, entonces $f(\alpha) = \alpha^3 + \alpha + 1 = 0$, y $\alpha^3 \equiv \alpha + 1$.
- Cabe destacar que las operaciones en $\mathbb{F}_2$ son peculiares: los valores negativos y los positivos son equivalentes, por lo que $\alpha^3 \equiv \alpha + 1$.

Ejemplo

Potencias de α, en donde α es una raíz de $f(x) = x^3 + x + 1$ sobre $\mathbb{F}_2$:

i	α	α^2	α^3	α^4	α^5	α^6	α^7
α^i	α	α^2	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$	1

Extensiones de campo sobre campos finitos

- Los campos con p^n elementos, como $\mathbb{F}_{2^3}$ se llaman *extensiones de campos*. El grado de la extensión de campos es el grado del polinomio cuya raíz se va a agregar.

- Hay muchas maneras de representar elementos en una extensión de campo de grado n. Además de agregar una raíz formal, se puede representar utilizando vectores de longitud n módulo $\mathbb{F}_p$, o polinomios con grado menor a n. Por ejemplo, $\alpha + 1$ se puede representar:
  - $\begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$
  - $(x + 1)$

Suma

La suma es una simple adición vectorial directa, módulo p. Utilizando $\mathbb{F}_{2^3}$ como ejemplo, tenemos los 8 elementos del grupo:

$$\begin{bmatrix} 0 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

Así que la suma se hace así:

$$\begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \oplus \begin{bmatrix} 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$$

Multiplicación

- La multiplicación es máscomplicada. Si x se utiliza como una raíz de $f(x)$, los elementos módulo $f(x)$ se pueden interpretar como polinomios sobre $\mathbb{F}_p$.

- La multiplicación de elementos módulo $f(x)$ es una multiplicación polinomial simple, seguida de una reducción poinomial.

Ejemplo

- Sea el campo base $\mathbb{F}_5$, y $f(x) = x^4 + 4x^3 + 4$. Así que $x^4 \equiv x^3 + 1 \bmod f(x)$.
- Multiplicación de elementos en $\mathbb{F}_{5^4}$, $g(x) = x^3 + 2x + 3$, y $h(x) = 2x^2 + 4$.

En la primera fila se utiliza la notación polinomial estándar, mientras que en la segunda, se utilizan polinomios.

$g(x)$	$h(x)$	$g(x)h(x) \bmod f(x)$
$x^3 + 2x + 3$	$2x^2 + 4$	$(2x^5 + 4x^3 + x^2) + (4x^3 + 3x + 2)$
$[\ 1\ \ 0\ \ 2\ \ 3\ ]$	$[\ 0\ \ 2\ \ 0\ \ 4\ ]$	$[\ 0\ \ 0\ \ 2\ \ 0\ ] \cdot [\ 1\ \ 0\ \ 0\ \ 1\ ]$
		$+[\ 3\ \ 1\ \ 3\ \ 2\ ] \cdot 2[\ 1\ \ 0\ \ 0\ \ 1\ ]$
		$+[\ 3\ \ 1\ \ 0\ \ 2\ ] \cdot [\ 0\ \ 1\ \ 0\ \ 4\ ]$

Anillos y campos

Estas estructuras polinomiales forman anillos y campos dependiendo de la *irreducibilidad* del módulo.

- La estructura $\mathbb{Z}/(n)\mathbb{Z}$ es un anillo el entero compuesto n, y para el primo n; la misma estructura se mantiene para $\mathbb{Z}[x]/f(x)$.
- Si $f(x)$ es irreducible -divisible por los elementos del campo base y $f(x)$- entonces la estructura forma un campo.

Ejemplos

Campo base	$f(x)$	Irreducible	Factores
$\mathbb{F}_2$	x^2+x+1	✓	$\times$
$\mathbb{F}_3$	x^2+x+1	$\times$	$(x+2)^2$
$\mathbb{F}_5$	x^2+x+1	✓	$\times$
$\mathbb{F}_7$	x^2+x+1	$\times$	$(x+3)(x+5)$

Los polinomios *unitarios* (monic) tienen su coeficiente de mayor order igual a uno. Si el polnomio no es unitario, entonces se puede convertir al multiplicarlo por el inverso del término de mayor orden.

Polinomios unitarios

Observación

Cuando se utilizan polinomios como módulo o cuando se discute irreducibilidad, se asume que se está hablando de polinomios unitarios.

- Factorizar y verificar la irreducibilidad de los polinomios es trivial para grado $n \leq 3$. En estos casos, los polinomios deben de tener una raíz en el campo base, sino, son irreducibles.
- El polinomio $f(x)$ sobre $\mathbb{F}_p$ tiene una raíz r en el campo base: $f(r) \equiv 0 \bmod p$, sí y solo si $(x - r)$ divide a $f(x)$.
- Los polinomios de grado menor o igual a 3 tienen al menos un factor de grado 1, sino, son irreducibles.

Ejemplo

- $f(x) = x^2 + x + 1$ sobre $\mathbb{F}_7$ tiene una raíz en 4: $f(4) \equiv 0 \bmod 7$, y $(x - 4) \equiv (x + 3) \bmod 7$ divide a $f(x)$.
  - $(x + 3)x = x^2 + 3x$: $(x^2 + x + 1) - (x^2 + 3x) = -2x + 1$
  - $-2x + 1 \equiv 5x + 1 \bmod 7$
  - $(x + 3)5 = 5x + 15 \equiv 5x + 1$
- $(x + 3)(x + 5) | x^2 + x + 1$ en $\mathbb{F}_7$.

Polinomios primitivos y orden

- La reducción módulo un polinomio irreducible sobre un campo finito genera la extensión de campo de grado n, en donde n es el grado de dicho polinomio: $\mathbb{F}_{p^n}$

- Al igual que en el caso de los campos primos, las extensiones de campo tienen el concepto de orden, tanto para el grupo multiplicativo, como para los elementos individuales.

Contenido de la sección 3

q-ésima raíz y residuos

Definición

Sea G un grupo con $\alpha, \beta \in G$ tal que $\alpha^q = \beta$. Entonces, β es un q-ésimo *residuo* en G, y α es una q-ésima *raíz* de β. Los *residuos cuadráticos* son elementos para los cuales existe una raíz cuadrática. La q-ésima *residuocidad* es la propiedad de ser un residuo q-éismo.

Ejemplo

- Raíces cuadradas, cúbicas y quintas, y residuos

α	1	2	3	4	5	6
α^2	1	4	2	2	4	1
α^3	1	1	6	1	6	6
α^5	1	4	5	2	3	6

En otras palabras, $\sqrt[2]{1} \in \{1, 6\}$, y $\sqrt[3]{1} \in \{1, 2, 4\}$ en $\mathbb{F}_7$. Cada elemento en $\mathbb{F}_7^*$ es un 5-ésimo residuo, mientras que solo $\phi(7)/2$ son residuos cradráticos, y $\phi(7)/3$ residuos cúbicos.

Notas sobre los residuos

- ¿Cuántos residuos q-écimos existen?
- ¿Cómo se verifica la q-écima residualidad?
- ¿Cuántas raíces existen para una q-ésimo residuo?
- ¿Cómo se calcula la q-ésima raíz?

La respuesta depende de si q es co-primo a n ($\text{MCD}(q, n) = 1$), o si comparten algún factor.

$\mathbf{MCD}(q, n) = 1$

- Cada elemento es un q-ésimo residuo
- No hay necesidad de verificar
- Existe solamente una raíz para cada elemento
- $\sqrt[q]{\alpha} = \alpha^{q^{-1}} \bmod n$

$\mathbf{MCD}(q, n) = g > 1$

- $\beta \in G$ es un q-ésimo residuo sí y solo si es un g-ésimo residuo. Hay $\frac{\alpha}{g} g$-ésimos residuos: $\{\alpha^{gx}\}_{x=0}^{\frac{n}{g}}$
- Elevar $\beta \in G$ a la $\frac{n}{g}$-ésima potencia nos da como resultado 1 si β es un g residuo, por lo que también es un q-ésimo residuo
- Si β es un q-ésimo residuo, existen g raíces para β. Si δ es una raíz, entonces el conjunto de todas las q-ésimas raíces es: $\{\delta\alpha^{x\frac{n}{g}}\}_{x=0}^{g-1}$
- El cálculo de raíces es complicado, para el caso de que el $\text{MCD}(g, \frac{n}{g}) = 1$, si β es un q-ésimo residuo, entonces:

$$(\beta)^{\frac{1}{q}} = \beta^{q^{-1 \bmod \frac{n}{g}}}$$

Material de lectura

- El principal repositorio público de artículos de investigación es el ArXiv.org de la Universidad de Cornell (de la Ivy League)
- Sin embargo, para el caso de la criptología, utilizamos el eprint de la IACR: eprint.iacr.org. La cual es una organización no lucrativa dedicada a la criptología y áreas relacionadas.

Lectura

- Lectura sección 3 de Implementing Cryptographics Pairings, por Scott.

- Fin de la unidad 3