Campos Finitos

Roberto Gómez Cárdenas

March 24, 2009

Aclaración

La mayor parte de este material proviene del capítulo 4 FINITE FIELDS del libro:

> Cryptography and Network Security, Principles and Practices
> William Stallings
> Ed. Prentice Hall
> 3a. Edición, 2003
> ISBN: 0-13-091429-0
> Páginas: 103-137

Tipos de números

- Números naturales N: usados para cuantificar objetos
  $N = \{1, 2, 3, ...\}$
- Números enteros Z: se añade 0 y todos los números que aparecen al cambiar el signo a los naturales
  $Z = \{... - 3, -2, -1, 0, 1, 2, 3, ...\}$
  $N \subset Z$
- Números racionales Q: se incorporan las fracciones
  $Q = \{\frac{a}{b} | a, b \in Z \text{ y } b \neq 0\}$
  $Z \subset Q$
- Números irracionales I: todos los números decimales cuya parte decimal tienen infinitas cifras no periodicas
- Números reales R: unión números racionales e irracionales
  $R = Q \cup I$
- Números imaginarios: Im: resultados de obtener la raíz cuadrada de un número negativo.
- Números complejos: par de números, uno de tipo real y otro de tipo imaginario, expresados de la siguiente forma: $a \pm bi$

Grupos

Un grupo G, algunas veces denotado por $\{G, \bullet\}$ es un conjunto de elementos con una operación binaria $\bullet$, que asocia a cada par ordenado (a, b) de elementos en G un elemento $(a \bullet b)$, de tal forma que los siguientes axiomas se deben cumplir:

1. **Cerradura** Si a y b pertenecen a G, entonces $a \bullet b$ tambien se encuentra en G
2. **Asociativa** $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ para toda a, b, c en G.
3. **Elemento de identidad** Existe un elemento e en G tal que $a \bullet e = e \bullet a = a$ para toda a en G.
4. **Elemento simétrico** Para cada a en G existe un elemento a' en G tal que $a \bullet a' = a' \bullet a = e$

Tipos de grupos

1. **Grupo finito** si el grupo cuenta con un número finito de elementos. El *orden* del grupo es el número de elementos.
2. **Grupo infinito** el número de elementos es infinito.
3. **Grupo abeliano** si satisface la siguiente condición adicional (conmutativa):
   $a \bullet b = b \bullet a$ para toda a, b en G
   - Llamados así en honor al matemtico noruego Niels Henrik Abel.

Ejemplos grupos abelianos

El conjunto de enteros (positivos, negativos y cero) bajo la operación de suma. El conjunto de números reales diferentes a cero y bajo la operación de multiplicación.

Ejemplos Grupos Abelianos

1. Los conjuntos de números, $(Z, +)$, $(Q, +)$, $(R, +)$ donde la operación $+$ es la adición.
2. $(N, +)$ NO es un grupo ya que no cuenta con neutro aditivo, ni inverso de cada elemento
3. $(R, \times)$ donde $\times$ es la multiplicación, NO es un grupo, ya que el 0 no tiene inverso multiplicativo.

Grupo cíclico

- Se define la exponención dentro de un grupo como la aplicación repetitiva del operador de grupo, de tal forma que $a^3 = a \bullet a \bullet a$
- También se define: $a^0 = e$ como el elemento de identidad; y $a^{-n} = (a')^n$.
- Un grupo G es cíclico si cada elemento de G es una potencia a^k (siendo k un entero) de un elemento fijo de $a \in G$.
- Se dice que el elemento a genera el grupo G, o que es un generador de G.
- Un grupo cíclico siempre es abeliano, y puede ser finito o infinito.

Ejemplo grupo cíclico

El grupo aditivo de enteros es un grupo cíclico infinito generado por el elemento 1. En este caso, las potencias son interpretadas aditivamente, de tal forma que n es el $e - nesima$ potencia de 1.

Anillos

Un anillo A algunas veces denotados por $\{A, +, x\}$ es un conjunto de elementos con dos operaciones binarias, llamadas *adición* y *multiplicación*, de tal forma para todas a, b, c en A los siguientes axiomas se cumplen:

1. A es un grupo abeliano con el respecto a suma si satisface los axiomas relacionados con dicho grupo. En el caso de un grupo aditivo, el elemento identidad es 0 y la inversa de a es a.
2. **Cerradura bajo multiplicación:**
   Si a y b pertenecen a A, entonces ab también están en A.
3. **Asociativa para la multiplicación:**
   $a(bc) = (ab)c$ para toda a, b, c en A
4. **Leyes distributivas:**
   $a(b + c) = ab + ac$ para toda a, b, c en A.
   $(a + b)c = ac + bc$ para toda a, b, c en A.

Características Anillos

En esencia un anillo es un conjunto en el cual se pueden llevar a cabo operaciones de suma, substracción $[ab = a + (-b)]$ y multiplicación sin dejar el conjunto.

Ejemplo anillo

Con respecto a la adición y multiplicación, el conjunto de todas las matrices $n \times n$ sobre los números reales es un anillo.

Ejemplos Anillos

En todos los ejemplos las operaciones son la suma y la multiplicación.

1. $(Z, +, \times)$ NO es un anillo, ya que en N no existe neutro para la adición.
2. $(N, +, \times) \cup 0$: NO es un anillo, ya que carece de inversos aditivos.
3. $(Z, +, \times)$ ES un anillo conmutativo con unidad.

Dominio de integridad

- Un anillo es conmutativo con respecto a la multiplicación: $ab = ba$ para toda a, b en A
- Un dominio de integridad es un anillo conmutativo que obedece los siguientes axiomas:
  - Identidad multiplicativa: Existe un elemento 1 en A tal que $a1 = 1a = a$ para todo a en A
  - No divisores ceros: Un anillo $(A, +, \times)$ se dice sin divisores cero, sí y solo sí elementos no nulos de A dan un producto no nulo. $\forall a, b : a, b \in A$ si $a = 0$, y $b = 0$, entonces $a \times b = 0$

Ejemplo Dominio de Integridad

Sea S el conjunto de enteros, positivos, negativos bajo los operadores usuales de adición y multiplicación. S es un dominio de integridad.

Campos/Cuerpos

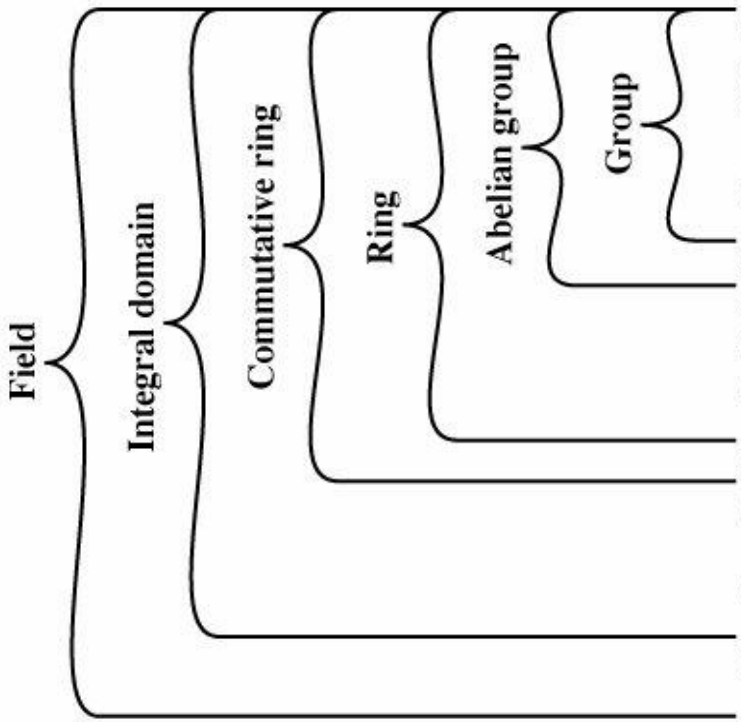
Un campo F, a veces denotado como $\{F, +, x\}$ el conjunto de elementos con dos operaciones binarias,llamadas *adición* y *multiplicación*, de tal forma para todas a, bc en F los siguientes axiomas se cumplen:

- F es un dominio de integridad, esto es F satisface todos los axiomas anteriores
- Inversa multiplicativa: para cada a en F, excepto 0 existe un elemento a^{-1} en F tal que $aa^{-1} = (a^{-1})a = 1$

En esencia, un campo es un conjunto en el cual se pueden llevar a cabo adiciones, substracciones, multiplicaciones y divisiones sin dejar el conjunto. La división es definida a partir de la siguiente regla:

$$a/b = a(b^{-1})$$

Comparación grupo, anillo y campo



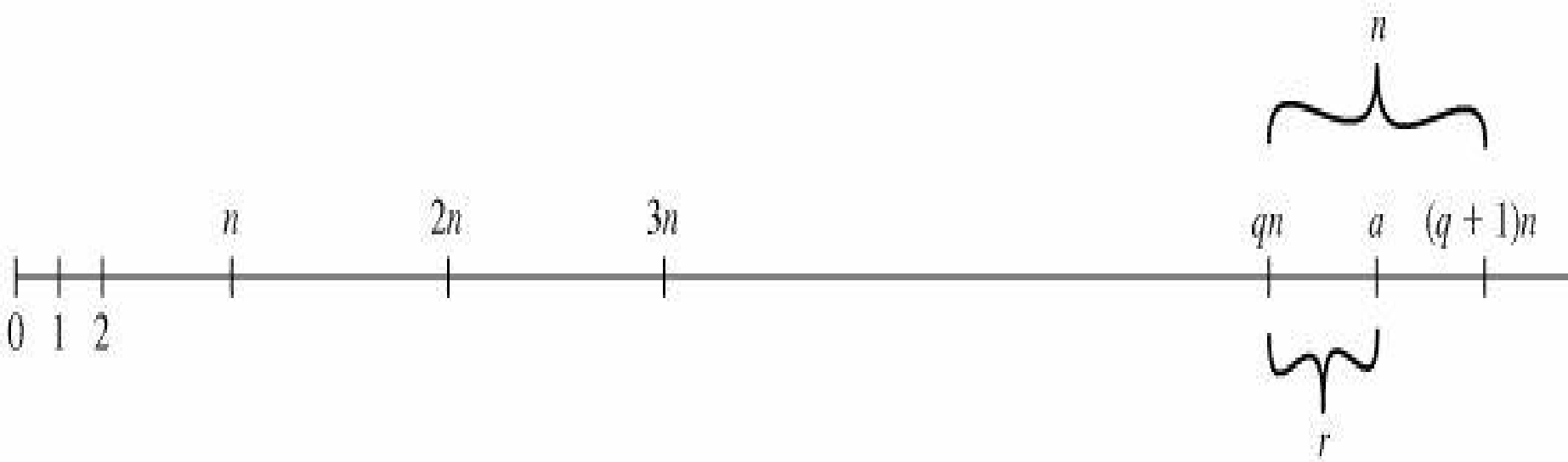
(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Dado un entero positivo n y cualquier entero no negativo a, si se divide a por n, se obtiene un cociente q y un residuo entero r que cumple con la siguiente relación:

$$a = qn + r; 0 \leq r < n; q = \lfloor a/n \rfloor$$

donde $\lfloor x \rfloor$ es entero más grande menor o igual a x.

La relación $a = qn + r; 0 \leq r < n$



$$a = 11; \quad n = 7; \quad 11 = 1 \times 7 + 4; \qquad r = 4 \quad q = 1$$
$$a = 11; \quad n = 7; \quad -11 = (-2) \times 7 + 3; \quad r = 3 \quad q = -2$$

El concepto de módulo

Si a es un entero y n es un entero positivo, se define a mod n como el residuo cuando a es dividido por n. El entero n es llamado el **modulo**. Entonces para cada entero a se puede aseverar que:

$$a = \lfloor a/n \rfloor \times n + (a \bmod n)$$

$$11 \bmod 7 = 4; \quad -11 \bmod 7 = 3$$

Congruencias

Se dice que dos enteros a y b son **congruentes modulo n**, si $(a \bmod n) = (b \bmod n)$. Esto se escribe como:

$$a \equiv b \bmod n$$

Ejemplo congruencia

$$73 \equiv 4 (\mathrm{mod} 23); \quad 21 \equiv -9 (\mathrm{mod} 10)$$

Divisores

Se dice que un no-cero b divide a si $a = mb$ para algún m, donde a, b y m son enteros. Esto es, b divide a si no existe ningún residuo en la división. La notación $b|a$ es usada para indicar que b divide a. También, si $b|a$, se dice que b es un **divisor** de a.

Ejemplo divisores

Los divisores positivos de 24 son $1, 2, 3, 4, 6, 8, 12$ y 24.

Relaciones divisores

Se establecen las siguiente relaciones:

- Si $a|1$, entonces $a = \pm 1$.
- Si $a|b$ y $b|a$, entonces $a = \pm b$.
- Cualquier $b \neq 0$ divide 0.
- Si $b|g$ y $b|h$, entonces $b|(mg + nh)$ para enteros arbitrarios m y n.
  - Para este último punto es necesario notar que:
    - Si $b|g$, entonces g es de la forma $g = b \times g_1$ para algún entero g_1.
    - Si $b|h$, entonces h es de la forma $h = b \times h_1$ para algún entero h_1.

Entonces:

$$mg + nh = mbg_1 + nbh_1 = b \times (mg_1 + nh_1)$$

y por lo tanto b divide $mg + nh$.

Ejemplo divisores

Considerando los siguientes valores:

$$b = 7; g = 14; h = 63; m = 3; n = 2$$

- $7|14$ y $7|53 \Rightarrow 7|(3 \times 14 + 2 \times 63)$
- Lo anterior se demuestra:
  $(3 \times 14 + 2 \times 63) = 7(3 \times 2 + 2 \times 9)$
  Y es obvio que: $7|(7(3 \times 2 + 2 \times 9))$

A notar que si $a \equiv 0 (\mathrm{mod}\, n)$ entonces $n|a$

Propiedades de las congruencias

Las congruencias cuentan con las siguientes propiedades:

1. $a \equiv \mod n$ si $n|(a\ b)$.
2. $a \equiv b \bmod n$ implica que $b \equiv a \bmod n$...
3. $a \equiv b \bmod n$ y $b \equiv c \bmod n$ implica que $a \equiv c \bmod n$

Ejemplo congruencias

$$
\begin{array}{lll}
23 \equiv 8 (\mod 5) & \text{ya que} & 23 - 8 = 15 = 5 \times 3 \\
11 \equiv 5 (\mod 8) & \text{ya que} & -11 - 5 = -16 = 8 \times (-2) \\
81 \equiv 0 (\mod 27) & \text{ya que} & 81 - 0 = 81 = 27 \times 3
\end{array}
$$

Operaciones de la aritmética modular

- El operador $(\mod n)$ mapea todos los enteros en el conjunto de enteros $\{0, 1, ..., (n-1)\}$
- **Pregunta:** Se pueden llevar a cabo operaciones aritméticas dentro de los confines de este conjunto
  - Respuesta: Si se puede, la tecnica se conoce como **aritmética modular**
- La aritmética modulos exhibe las siguientes propiedades:
  1. $[(a \bmod n) + (b \bmod n)] mod n = (a + b) \bmod n$.
  2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$.
  3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$.

Ejemplos operaciones modulares

- Considerando los siguientes valores:
  $11 \bmod 8 = 3;$
  $15 \bmod 8 = 7$
- Ejemplo adición:

$$\begin{aligned}[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 &= [(3) + (7)] \bmod 8 \\ &= 10 \bmod 8 \\ &= 2 \bmod 8\end{aligned}$$

$$\begin{aligned}[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 &= (11 + 15) \bmod 8 \\ &= 26 \bmod 8 \\ &= 2 \bmod 8\end{aligned}$$

- Ejemplo substracción:

$$\begin{aligned}[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 &= [(3) - (7)] \bmod 8 \\ &= -4 \bmod 8 \\ &= 4 \bmod 8\end{aligned}$$

$$\begin{aligned}[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 &= (11 - 15) \bmod 8 \\ &= -4 \bmod 8 \\ &= 4 \bmod 8\end{aligned}$$

Ejemplos operaciones modulares

- Considerando los siguientes valores:
  $11 \bmod 8 = 3;$
  $15 \bmod 8 = 7$
- Ejemplo multiplicación:

$$
\begin{aligned}
[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 &= [(7) \times (3)] \bmod 8 \\
&= 21 \bmod 8 \\
&= 5 \bmod 8 \\
[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 &= 5(11 \times 15) \bmod 8 \\
&= 165 \bmod 8 = 5 \\
&5 \bmod 8
\end{aligned}
$$

La exponenciación en aritmética modular

Se lleva a cabo por repetidas multiplicaciones, tal y como se hace en aritmética ordinaria.
Por ejemplo para encontrar 11^7 mod 13, se procede como sigue:
$11^2 = 121 \equiv 4 \bmod 13$
$11^4 \equiv 4^2 \equiv 3 \bmod 13$
$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \bmod 13$

Conclusión

Las reglas para aritmética ordinaria involucrando adición, substracción y multiplicación se aplican a la aritmética modular.

Propiedades aritmética modular

Se define el conjunto Z_n como el conjunto de enteros no negativos menores a n:

$$Z_n = \{0, 1, ..., (n-1)\}$$

A esto se le conocer como el **conjunto de residuos** o **clases de residuos** modulo n. Cada entero en Z_n representa una clase de residuo. Se puede nombrar las clases de residuo modulo n como $[0], [1], [2], ..., [n\ 1]$, donde:
$[r] = \{a : \text{a es un entero}, a \equiv r (\mathrm{mod}\, n)\}$

Las clases residuo del modulo 4

$$\begin{aligned}
[0] &= \{..., -16, -12, -8, -4, 0, 4, 8, 12, 16, ...\} \\
[1] &= \{..., -15, -11, -7, -3, 1, 5, 9, 13, 17, ...\} \\
[2] &= \{..., -14, -10, -6, -2, 2, 6, 10, 14, 18, ...\} \\
[3] &= \{..., -13, -9, -5, -1, 3, 7, 11, 15, 19, ...\}
\end{aligned}$$

Reduciendo k al modulo n

- De todos los enteros en una clase residual, el entero negativo más pequeño es el utilizado generalmente para representar la clase residual.
- Encontrar el entero negativo para el cual k es congruente modulo n es conocido como **reducir** k **al modulo** n.
- Si se lleva a cabo aritmética modular dentro Z_n, las propiedades conmutativas, asociativas, distributivas, de identidad y simétricas se mantienen para los enteros en Z_n.
- Entonces, Z_n es un anillo conmutativo con un elemento de identidad multiplicativo.

Tabla de suma (mod 10)

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Tabla de multiplicación (mod 10)

*	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Inversas aditivas y multiplicativas (mod 10)

w	$-w$	w^{-1}
0	0	–
1	9	1
2	8	–
3	7	7
4	6	–
5	5	–
6	5	–
7	3	3
8	2	–
9	1	9

Tabla de suma (mod 8)

+	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Tabla de multiplicación (mod 8)

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Inversas aditivas y multiplicativas (mod 8)

w	$-w$	w^{-1}
0	0	–
1	7	1
2	6	–
3	5	3
4	4	–
5	3	5
6	2	–
7	1	7

Propiedades de Aritmética Modular para enteros en Z_n

Propiedad	Expresión
Leyes Conmutativas	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Leyes Asociativas	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Leyes Distributivas	$[w + (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$ $[w + (x \times y)] \bmod n = [(w + x) \times (w + y)] \bmod n$
Identidades	$(0 + w) \bmod n = w \bmod n$ $(1 + w) \bmod n = w \bmod n$
Inversa aditiva$(-w)$	$\forall w \in Z_n \; \exists \vert z$ tal que: $w + z \equiv 0 \bmod n$

Propiedades inversa aditiva en mod n

- Si $(a+b) \equiv (a+c) (\mathrm{mod}\, n) \Rightarrow b \equiv c (\mathrm{mod}\, n)$
  Ejemplo: $(5+23) \equiv (5+7) (\mathrm{mod} 8)$
  $23 \equiv 7 (\mathrm{mod} 8)$
- La ecuación anterior es consistente con la existencia de un inverso aditivo de a. Añadiendo el inverso aditivo a ambos lados de la ecuación se tiene:
  $((-a)+a+b) \equiv ((-a)+a+c) (\mathrm{mod}\, n)$
  $b \equiv c (\mathrm{mod}\, n)$
- El siguiente enunciado es verdad, siempre y cuando se cumpla la condición que la acompaña:
  Si $(a \times b) \equiv (a \times c) (\mathrm{mod}\, n) \Rightarrow b \equiv c (\mathrm{mod}\, n)$ si y solo si a es relativamente primo a n

Números relativamente primos

- Dos enteros son relativamente primos si el único entero positivo de factor común entre los dos es 1.
- Se puede decir que la ecuación: Si $(a \times b) \equiv (a \times c)(\mod n) \Rightarrow b \equiv c(\mod n)$ es consistence con la existencia de un inverso multiplicativo.
- Aplicando un inverso multiplicativo de ambos lados:
  $((a^1)ab) \equiv ((a^{-1})ac)(\mod n)$
  $b \equiv c(\mod n)$

El máximo común divisor

- El entero b diferente de cero es un divisor de a si $a \equiv mb$ para alguna m, donde a, b y m son enteros.
- Se utiliza la notación $gcd(a, b)$ para designar el máximo común divisior de a y b.
- El entero c es el náximo común divisor de a y b si
  1. c es el divisor de a y de b
  2. cualquier divisor de a y b es un divisor de c

  Una definición equivalente es la siguiente:
  $gcd(a, b) = max[k,$ tal que $k|a$ y $k|b]$

Ejemplo

$gcd(60, 24) = gcd(60, 24) = 12$

El mximo común divisor y los números relativamente primos

- Dos enteros a y b son relativamente primos si el único factor común que comparten es 1.
- Esto es equivalente a decir que a y b son relativamente primos si $gcd(a, b) = 1$

Ejemplos

8 y 15 son relativamente primos porque:

- los divisores positivos de 8 son 1,2,4 y 8
- los divisores positivos de 15 son 1,3,5 y 15

El algoritmo Euclidiano

- Se basa en la siguiente ecuación:

$$gcd(a, b) = gcd(b, a \bmod b)$$

- Por ejemplo:

$$gcd(55, 22)$$

- La primera ecuación se puede usar repetitivamente para calcular el máximo común divisor:
  $gcd(18, 12) = gcd(12, 6) = gcd(6, 0) = 6$
  $gcd(11, 10) = gcd(10, 1) = gcd(1, 0) = 1$
- El algoritmo euclidiano hace un uso repetitivo de la primera ecuación. El algoritmo asume que $a > b > 0$

Especificacón del algoritmo Euclidiano

Asumiendo que $a > b > 0$, y la siguiente ecuación:$a = b \times q + r$
Para calcular $gcd(a, b)$:

1. $A \leftarrow a;\ \ B \leftarrow b$
2. Si $B = 0$ regresa $A = gcd(a, b)$
3. $R = A \bmod B$
4. $A \leftarrow B$
5. $B \leftarrow R$
6. Ir a paso 2

El algoritmo presenta la siguiente progresión:

$$A_1 = B_1 \times Q_1 + R_1$$
$$A_2 = B_2 \times Q_2 + R_2$$
$$A_3 = B_3 \times Q_3 + R_3$$
$$A_4 = B_4 \times Q_4 + R_4$$

Ejemplo algoritmo Euclides

Para encontrar $gcd(1970, 1066)$

$$
\begin{aligned}
1970 &= 1 \times 1066 + 904 && gcd(1066, 904)\\
1066 &= 1 \times 904 + 162 && gcd(904, 162)\\
904 &= 5 \times 162 + 94 && gcd(162, 94)\\
162 &= 1 \times 94 + 68 && gcd(94, 68)\\
94 &= 1 \times 68 + 26 && gcd(68, 26)\\
68 &= 2 \times 26 + 16 && gcd(26, 16)\\
26 &= 1 \times 16 + 10 && gcd(16, 10)\\
16 &= 1 \times 10 + 6 && gcd(10, 6)\\
10 &= 1 \times 6 + 4 && gcd(6, 4)\\
6 &= 1 \times 4 + 2 && gcd(4, 2)\\
4 &= 2 \times 2 + 0 && gcd(2, 0)
\end{aligned}
$$

Campos infinitos vs finitos

- Anteriormente se definió un campo como un conjunto que obedece a ciertos axiomas y se dieron ejemplos de campos infinitos.
- Campos infinitos no son de interes para el área de criptografia.
- Los campos finitos juegan un rol crucial en varios algoritmos criptográficos.
- El orden de un campo finito (número elementos) debe ser potencia de un número primo p: p^n, (donde n es un entero positivo).

Campos finitos de la forma $GF(p)$

- El campo finito de orden p^n generalmente se escribe como $GF(p^n)$.
- Se le conoce como campo de Galois.
- Dos casos especiales son interesantes para el área de criptografia:
  1. Para $n = 1$, se cuenta con el campo $GF(p)$
  2. Para $n > 1$
- El primero tiene una estuctura diferente que el segundo.

Campos finitos del orden p

Para un número primo p el campo finito de orden p, $GF(p)$ es definido como el conjunto Z_p de enteros $\{0, 1, ...p-1\}$, junto con las operaciones aritméticas modulo p.
Observaciones, recordar que:

- El conjunto Z_n de enteros $\{0, 1, ..., n-1\}$ junto con las operaciones aritméticas modulo n, es un anillo conmutativo.
- Cualquier entero en Z_n cuenta con una inversa multiplicativa, si y solo si el entero es relativamente primo a n.
- Si n es primo, entonces todos los enteros diferentes de cero en Z_n son relativamente primos a n y por lo tanto existe un inverso múltiplicativo para todos los enteros diferentes de cero en Z_n.

Propiedades de Aritmética Modular para enteros en el campo finito de orden p

Se añade una propiedad a las de la aritmética modular para enteros en Z_n:

Propiedad	Expresión
Leyes Conmutativas	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Leyes Asociativas	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Leyes Distributivas	$[w + (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$ $[w + (x \times y)] \bmod n = [(w + x) \times (w + y)] \bmod n$
Identidades	$(0 + w) \bmod n = w \bmod n$ $(1 + w) \bmod n = w \bmod n$
Inversa aditiva$(-w)$	$\forall w \in Z_n \; \exists \vert z$ tal que: $w + z \equiv 0 \bmod n$
Inversa multiplicativa(w^{-1})	$\forall w \in Z_n, w \neq 0, \; \exists \vert z$ tal que: $w \times z \equiv 1 (\bmod n)$

Observaciones

- Ya que w es relativamente primo a p, si se multiplican todos los elementos de Z_p por w, el residuo resultantes son todos los elementos de Z_p permutados.
- Entonces uno de los residuos cuenta con el valor de 1.
- Por lo tanto, existe algún entero en Z_p que, cuando es multiplicado por w, da el residuo 1.
- Este entero es el inverso multiplicativo de w designado por w^{-1}
- Por lo tanto Z_p es un campo finito.
- En base a lo anterior se puede decir que
  Si $(a \times b) \equiv (a \times c) (\mathrm{mod}\, p)$ entonces $b \equiv c (\mathrm{mod}\, p)$
- Multiplicando la ecuación anterior por el inverso multiplicativo de a, tenemos que:
  $((a^{-1}) \times a \times b) \equiv ((a^{-1}) \times a \times c) (\mathrm{mod}\, p)$
  $b \equiv c (\mathrm{mod}\, p)$

Primer ejemplo campo finito $GF(p)$

- El más simple ejemplo es $GF(2)$
- La operación de suma se muestra en la siguiente tabla:

$+$	0	1
0	0	1
1	1	0

- La operación de multiplicación es:

X	0	1
0	0	0
1	0	1

- Las inversas son las siguientes:

w	$-w$	w^{-1}
0	0	1
1	1	0

- En este caso la suma es equivalente a la operación XOR y la multiplicación a la operación lógica AND

Adición en $GF(7)$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Multiplicación e inversas en $GF(7)$

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

w	$-w$	w^{-1}
0	0	—
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Encontrando inversos multiplicativos en $GF(p)$

- Si el valor de p es pequeño se puede construir una tabla de multiplicar y ver el resultado directamente en la tabla.
- Para valores de p el enfoque anteior no es práctico.
  - Si $gcd(m, b) = 1$ entonces b tiene un inverso multiplicativo modulo m.
  - Para un entero positivo $b < m$, entonces existe un $b^{-1} < m$ tal que $bb^{-1} = 1 \bmod m$.
  - El algoritmo Euclidiano puede extenderse para que, aparte de encontrar $gcd(m, b)$, si $gcd(m, b) = 1$, el algoritmo regrese el inverso múltiplicativo de b.

El algoritmo Euclidiano Extendido

El algoritmo encuentra el $gcd(m, b)$ y si este es 1, regresa el inverso multiplicativo de b mod m.

1. $(A1, A2, A3) \leftarrow (1, 0, m); (B1, B2, B3) \leftarrow (0, 1, b)$
2. Si $B3 = 0$ regresa $A3 = gcd(m, b)$; no hay inversa
3. Si $B3 = 1$ regresa $B3 = gcd(m, b)$; $B2 = b^{-1}$ mod m
4. $Q = \lfloor \frac{A3}{B3} \rfloor$
5. $(T1, T2, T3) \leftarrow (A1 - QB1, A2 - QB2, A3 - QB3)$
6. $(A1, A2, A3) \leftarrow (B1, B2, B3)$
7. $(B1, B2, B3) \leftarrow (T1, T2, T3)$
8. Ir a paso 2

A notar que si $b^{-1} < 0 \Rightarrow b^{-1} = m - |B2|$

Ejemplo algoritmo Euclides Extendido

Para encontrar $gcd(1970, 1066)$

Q	A1	A2	A3	B1	B2	B3
	1	0	1759	0	1	550
3	0	1	550	1	3	109
5	1	3	109	5	16	5
21	5	16	5	106	339	4
1	106	339	4	111	355	1

Aritmética Polinomial

- Polinomios basado en una sola variable x.
- Se pueden distinguir tres tipos de aritmética polinomial:
  1. Aritmética polinomial ordinaria, usando las reglas básicas del algebra.
  2. Aritmética polinomial en la que la aritmética de los coeficientes son realizadas modulo p, es decir, los coeficientes están en $GF(p)$.
  3. Aritmética polinomial en la que los coeficientes están en $GF(p)$, y los polinomios estan definidos modulo un polinomo $m(x)$ cuya mayor potencia es algún entero n.

Un polinomio de grado n (entero $n \geq 0$ es una expresión de la forma:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

donde a_i son elementos de algún designado conjunto de numeros S, llamado el conjunto de coeficientes, y $a_n \neq 0$. Se dice que tales polinomios son definidos sobre el conjunto de coeficientes S.

Características polinomios

- Un polinomio de grado cero es llamado un **polinomio constante** y es simplemente un elemento del conjunto de coeficientes.
- Se dice que un polinomio de grado enésimo es un polinomio monico, si $a_n = 1$.
- En el contexto de algebra abstracta, no se esta interesado en evaluar el polinomio para un determinado valor.
- Para enfatizar lo anterior, la variable x se conoce como **indeterminada**.

Aritmética polinomial

- Incluye las operaciones de suma, substracción y multiplicación.
- Operaciones definidas tomando en cuenta que x es un elemento de S.
- Lo mismo pasa para la divisón, pero se requiere que S sea un campo. Ejemplos de campos incluye a los numeros reales, los numeros racionales, y Z_p siendo p un número primo.
- A notar que el conjunto de todos los enteros no es un campo y no soporta la división polinomial.

Definición operaciones ordinarias en polinomios

Para todos los casos se considera:

$$f(x) = \sum_{i=0}^{n} a_i x^i; \quad g(x) = \sum_{i=0}^{n} b_i x^i; \quad n \geq m$$

- Adición y substracción se lleva a cabo sumando y restando los correspondientes coeficientes:

$$f(x) + g(x) = \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{m} b_i x^i; \quad n \geq m$$

- La multiplicación se define como:

$$f(x) \times g(x) = \sum_{i=0}^{n+m} c_i x^i$$

donde: $c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0$

En la última formula, se trata a_i como cero para $i > n$ y b_i como cero para $i > m$. A notar que el grado del producto es igual a la suma de los grados de los dos polinomios.

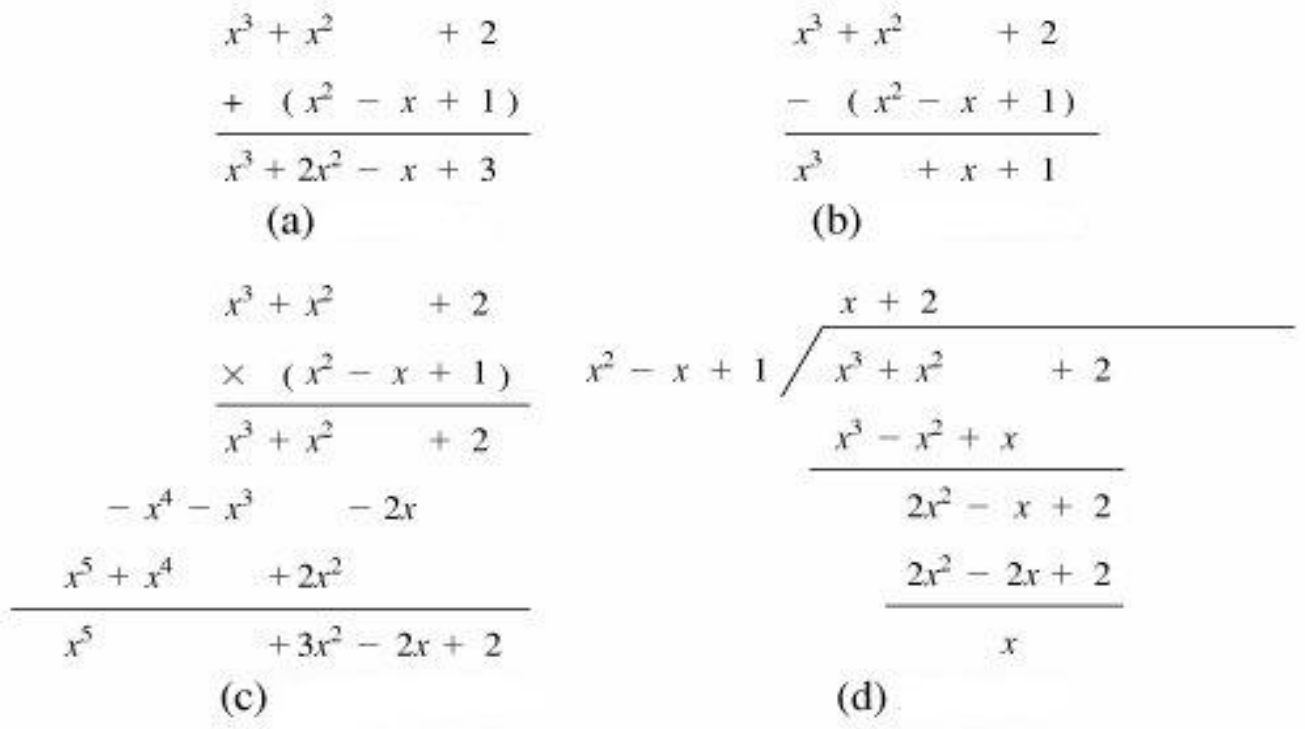
Ejemplo operaciones

Sea, $f(x) = x^3 + x^2 + 2$ y $g(x) = x^2 - x + 1$, donde S es el conjunto de enteros, entonces:

- Adición: $f(x) + g(x) = x^3 + 2x^2 - x + 3$
- Substracción: $f(x)g(x) = x^3 + x + 1$
- Multiplicación: $f(x) \times g(x) = x^5 + 3x^2 - 2x + 2$
- División: $f(x)/g(x) = x + 2$ con residuo: x

Desarrollo de las operaciones

(a) Adición (b) Substraccón
(c) Multiplicación (d) División



Operaciones aritméticas con coeficientes en Z_p

- Se consideran polinomios con coeficientes elementos de algun campo F. A esto se le conoce como polinomio sobre el campo F.
- Es fácil ver que el conjunto de tales polinomios es un anillo, conocido como un **anillo de polinomio**.
- Si se considera cada polinomio distinto como un elemento del conjunto, entonces el conjunto es un anillo.
- Cuando la aritmetica polinomial es realizada en polinomios sobre un campo, la división es posible.
  - Esto no significa que la división exacta sea posible.
  - Dentro de un campo, dados dos elementos a y b, el cociente a/b también es un elemento del campo.
  - Sin embargo, dado que un anillo R no es un campo, en una división no dara como resultado un cociente y un residuo; esto no es una división exacta.

Operaciones de polinomios con coeficientes en $GF(2)$

- Se consideran polinomios sobre GF(2).
- Tomar en cuenta que en GF(2):
  - La adición es equivalente a la operación XOR.
  - La multiplicación es equivalente a la operación AND.
  - Adición y substracción son equivalentes.
- Ejemplo operaciones, tomando en cuenta que
  $f(x) = (x^7 + x^5 + x^4 + x + 1)$
  $g(x) = (x^3 + x + 1)$
  Entonces:
  $f(x) + g(x) = x^7 + x^5 + x^4$
  $f(x) - g(x) = x^7 + x^5 + x^4$
  $f(x) \times g(x) = x^{10} + x^4 + x^2 + 1$
  $f(x)/g(x) = x^4 + 1$

Desgloce operaciones aritméticas con coeficientes en $GF(2)$

- Adición

$$\begin{array}{rrrrrrrr} x^7 & +x^5 & +x^4 & +x^3 & & +x & +1 \\ & & & & +(x^3 & +x & +1) \\ \hline x^7 & +x^5 & +x^4 & & & & \end{array}$$

- Substracción

$$\begin{array}{rrrrrrrr} x^7 & +x^5 & +x^4 & +x^3 & & +x & +1 \\ & & & & -(x^3 & +x & +1) \\ \hline x^7 & +x^5 & +x^4 & & & & \end{array}$$

Desgloce operaciones aritméticas con coeficientes en $GF(2)$

- Multiplicación

$$
\begin{array}{rrrrrrrrrrr}
 & & & & x^7 & + x^5 & + x^4 & + x^3 & + x & + 1 \\
 & & & & & & & \times (x^3 & + x & + 1) \\
\hline
 & & & & x^7 & + x^5 & + x^4 & + x^3 & + x & + 1 \\
 & & & x^8 & & + x^6 & + x^5 & + x^4 & + x^2 & + x \\
 & x^{10} & + x^8 & + x^7 & + x^6 & & + x^4 & + x^3 & & \\
\hline
 & x^{10} & & & & & + x^4 & & + x^2 & + 1
\end{array}
$$

- División

$$
\begin{array}{rrrrrrrrrrr}
 & & & & & & x^4 & + 1 & & \\
 & & & & & \multicolumn{7}{l}{\hline} \\
x^3 & + x & + 1 & \Big/ & x^7 & + x^5 & + x^4 & + x^3 & + x & + 1 \\
 & & & & x^7 & + x^5 & + x^4 & & & \\
 & & & & \multicolumn{3}{l}{\hline} & & & \\
 & & & & & & & x^3 & + x & + 1 \\
 & & & & & & & x^3 & + x & + 1 \\
 & & & & & & & \multicolumn{3}{l}{\hline}
\end{array}
$$

Polinomios irreductibles y primos

- Un polinomio $f(x)$ sobre un campo F es llamado **irreductible** si y solo si $f(x)$ no puede ser expresado como un producto de dos polinomios, ambos sobre F, y ambos de un grado menor que el de $f(x)$.
- Por analogía a los enteros, a un polinomio irreductible tambien se le llama **polinomio primo**.

Ejemplos

- El polinomio $f(x) = x^4 + 1$ sobre $GF(2)$ es reductible, ya que $(x^4 + 1) = (x + 1)(x^4 + x^2 + 1)$
- El polinomio $f(X) = x^3 + x + 1$ es irreductible.
  - x no es un factor de $f(x)$
  - $x + 1$ no es un factor de $f(x)$
  - no tiene factores de grado 1
  - si $f(x)$ es reductible debe contar con un factor de grado 2 y un factor de grado 1
  - Por lo tanto $f(x)$ es irreductible

Encontrando el máximo común divisor

Posible extender la analogía entre aritmética polinomial sobre un campo y la aritmética entera definiendo el concepto de máximo común divisor como sigue:
Se dice que el polinomio $c(x)$ es el máximo común divisor de $a(x)$ y $b(x)$ si

1. $c(x)$ divide a $a(x)$ y a $b(x)$
2. cualquier divisor de $a(x)$ y $b(x)$ es un divisor de $c(x)$

Una definición equivalente es la siguiente: $gcd[a(x), b(x)]$ es el polinomio de grado máximo, que divide a ambos $a(x)$ y $b(x)$.
Se puede adaptar el algoritmo Euclidiano para calcular el máximo común divisor de dos polinomios. Se puede definir la siguiente ecuación:

$$gcd[a(x), b(x)] = gcd[b(x), a(x) \bmod b(x)]$$

Algoritmo Euclidiano para polinomios

El algoritmo asume que el grado de $a(x)$ es mayor que el grado de $b(x)$. Para encontrar el $gcd[a(x), b(x)]$ se define el siguiente algoritmo:

1. $A(x) \leftarrow a(x);\ \ B(x) \leftarrow b(x)$
2. Si $B(x) = 0$ regresa $A(x) = gcd[a(x), b(x)]$
3. $R(x) = A(x) \bmod B(x)$
4. $A(x) \leftarrow B(x)$
5. $B(x) \leftarrow R(x)$
6. Ir a paso 2

Ejemplo algoritmo Euclides para polinomios

Encontrar $gcd[a(x), b(x)]$ para:
$a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1;$
$b(x) = x^4 + x^2 + x + 1$
$A(x) = a(x);\ B(x) = b(x)$

$$
\begin{array}{r}
x^2 + x \\
x^4 + x^2 + x + 1 \overline{)\ x^6 + x^5 + x^4 + x^3 + x^2 + x + 1} \\
\underline{x^6 \quad + x^4 + x^3 + x^2} \\
x^5 \qquad\qquad + x + 1 \\
\underline{x^5 \quad + x^3 + x^2 + x} \\
x^3 + x^2 \quad + 1
\end{array}
$$

Ejemplo algoritmo Euclides para polinomios

$R(x) = R(x) = A(x) mod B(x) = x^3 + x^2 + 1$
$A(x) = x^4 + x^2 + x + 1; B(x) = x^3 + x^2 + 1$

$$
\begin{array}{r}
x + 1 \\
x^3 + x^2 + 1 \overline{)\, x^4 + x^2 + x + 1} \\
\underline{x^4 + x^3 \quad + x} \\
x^3 + x^2 + 1 \\
\underline{x^3 + x^2 + 1} \\
\end{array}
$$

$R(x) = A(x) mod B(x) = 0$
$gcd[a(x), b(x)] = A(x) = x^3 + x^2 + 1$

Campos finitos de la forma $GF(2^n)$

- El orden de un campo finito debe ser de la forma p^n donde p es un número primo y n es un número positivo.
- En el caso de $n = 1$, usando aritmetica modular en Z_n, todos los axiomas para un campo se satisfacen.
- Para polinomios sobre p^n, con $n > 1$, las operaciones modulo p^n no producen un campo.
- Es necesario encontrar que estructura satisface los axiomas en un conjunto con p^n elementos, i.e. $GF(2^n)$.

Motivación

- Casi todos los algoritmos, simétricos y asimétricos, involucran operaciones aritméticas sobre enteros.
- Si una de las operaciones usadas en el algoritmo es división, entonces es necesario trabajar con aritmética definida sobre un campo.
- Por conveniencia y por eficiencia en implementación, es recomemdable trabajar con enteros que se acomoden dentro de un determinado número de bits, sin bits de desperdicio.
- Se desea trabajar con enteros en el rango 0 a $2^n - 1$, que caben en una palabra de n bits.

Ejemplo

- Considerar que se define un algoritmo convencional de cifrado, que opera en 8 bits de datos, y que se desea llevar a cabo una división.
- Con 8 bits se pueden representar enteros en el rango de 0 a 255.
- Sin embargo, 256 no es un número primo, por lo que si la aritmética se lleva a cabo en Z_{256} (aritmética modulo 256), este conjunto de enteros no es un campo.
- El número primo más cercano menor a 256 es 251.
- Por lo que el conjunto Z_{251}, usando aritmética modulo 251, es un campo.
- Sin embargo en este caso los patrones de 8 bits que representan los enteros 251 a 255 no serán usados, resultando en un desperdicio en el almacenamiento.

Cifrado y operaciones aritméticas

- Si todas las operaciones aritméticas se van a usar, y es necesario representar un rango completo de enteros en n bits, entonces la aritmética modulo 2^n no trabajará.
- El conjunto de enteros modulo 2^n, para $n > 1$, no es campo.
- Además, aún si el algoritmo de cifrado solo usa adición y multiplicaci'on, pero no división, el uso del conjunto Z_{2^n} es cuestionable.

Ejemplo uso aritmética para cifrado

- Suponer que usa bloques de 3 bits en un algoritmo de cifrado y solo se usan operaciones de adición y multiplicación.
- Posible usar aritmetica modulo 8, ya que $2^3 = 8$, sin embargo en la tabla de multiplicar:
  - Los enteros no-cero no aparecen el mismo número de veces
  - Cuatro ocurrencias de 3, pero doce de 4
- Por otro lado, existen campos finitos de la forma $GF(2^n)$, por lo que hay en particular un campo finito de orden $2^3 = 8$
- Observando las tablas aritméticas se puede observar que las ocurrencias de enteros no-cero es uniforme.
- Resumiendo:

Entero	1	2	3	4	5	6	7
Ocurrencias en Z_8	4	8	4	12	4	8	4
Ocurrencias en $GF(2^3)$	7	7	7	7	7	7	7

Tabla de suma en $GF(2^3)$

	+	000	001	010	011	100	101	110	111
		0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

Tabla de multiplicación en inversa en $GF(2^3)$

	×	000	001	010	011	100	101	110	111
		0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

w	$-w$	w^{-1}
0	0	—
1	1	1
2	2	5
3	3	6
4	4	7
5	5	2
6	6	3
7	7	4

Observaciones sobre operaciones aritméticas en $GF(2^3)$

1. La adición y multiplicación son simétricos acerca de la diagonal principal, conforme a la propiedad comnumtativa de adición y muliplicación.
2. Todos los elementos no cero definidos en las tablas de aritmética de $GF(2^3)$ tienen inversos multiplicativos.
3. El esquema definido en las tablas satisfacen todos los requerimientos de un campo finito. Entonces se puede hacer referencia a este esquema como $GF(2^3)$.
4. Por conveniencia, se mostro una asignación de 3 bits usado para elemento de $GF(2^3)$.

Concluyendo

- Un algoritmo que mapea los enteros de forma desigual entre ellos mismos puede ser criptograficamente más debil que uno que proporciona un mapeo uniforme.
- Entonces, los campos de la forma $GF(2^n)$ son atractivos para algoritmos criptográficos.
- Se esta buscando por un conjunto de 2^n elementos, junto con una definición de adición y multiplicación sobre el conjunto que define un campo.
- Se puede asignar un entero único en el rango de 0 a $2^n - 1$ a cada elemento del conjunto.
- A tomar en cuenta que no se usará aritmética modular, ya que esto no resulta en un campo.
- Posible usar aritmética polinomial para construir el campo deseado.