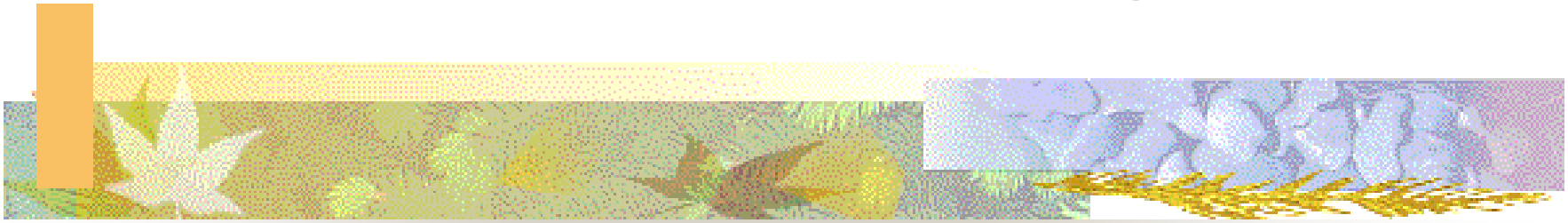
Introdução à Criptografia



Profa. Yeda

Aula 04 – Corpos Finitos

Cap. 4.3 Christof Paar & Jan Pelzl

Cap. 4 (parcial) Stallings

Introdução aos Corpos Finitos

- Utilizado por diversos algoritmos criptográficos
  - AES, Elliptic Curve, IDEA, Public Key
- Relaciona-se a operações sobre “números”
  - Onde o que constitui um “número” e o tipo de operações pode variar consideravelmente.
- Definições: grupos, anéis, corpos.

Grupo

- Definido por um conjunto G de elementos ou “números”,
- com alguma operação (•) cujo resultado também está no conjunto (fechamento)
  - Para todo $a,b \in G$, se $c = a \bullet b$ então $c \in G$.
- A operação de grupo obedece: (p/ qualquer $a,b \in G$)
  - lei associativa: $(a \bullet b) \bullet c = a \bullet (b \bullet c)$
  - tem elemento identidade e: $e \bullet a = a \bullet e = a$
  - tem inverso a^{-1}: $a \bullet a^{-1} = a \bullet a^{-1} = e$
- Se comutativa $a \bullet b = b \bullet a$, para qualquer $a,b \in G$
  - então forma um grupo abeliano
- Operação: normalmente chamada de adição ou multiplicação, com seus respectivos inversos, subtração ou divisão.

Grupo Cíclico

- define **exponenciação** como repetida aplicação do operador
  - exemplo: $a^3 = a \bullet a \bullet a$
- e a identidade seja: $e=a^0$
- um grupo é cíclico se todo elemento é uma potência de algum elemento fixo
  - $b = a^k$ para algum a e todo b no grupo
- a é dito ser um gerador do grupo

Anél

- Um conjunto de “números “ com 2 operações (adição e multiplicação) o qual forma:
- um grupo abeliano sobre a operação de adição,
- E a multiplicação:
  - se a multiplicação é comutativa, ela forma um anél comutativo

Corpo (F)

- Definido por um conjunto de números,
- com 2 operações as quais formam:
  - um grupo abeliano para a adição (+), com elemento neutro 0;
  - um grupo abeliano para a multiplicação (×) (ignorando 0), com elemento neutro 1.
  - Obs.: propriedade distributiva
- tem hierarquia com mais axiomas/leis
  - Grupo → anél → corpo

Corpo de Galois (GF)

- Corpo **finito** tem papel chave na criptografia.
  - Corpos com ***m*** elementos.
- TEOREMA: "Um corpo com ordem ***m*** somente existe se m é uma potência prima, isto é $m = p^n$, para algum inteiro positivo ***n*** e inteiro primo ***p***. Onde ***p*** é chamado a característica do corpo finito."
- Notação: $GF(p^n)$
- Normalmente usa-se os corpos:
  - $GF(p)$ e $GF(2^n)$

Corpo de Galois GF(p)

- GF(p) é o conjunto de inteiros *{0,1, ... , p-1}* com aritmética módulo um primo *p*.
- Formam um corpo finito, pois
  - Tem um inverso multiplicativo.
  - Assim como uma aritmética bem conhecida e pode-se adicionar, subtrair, multiplicar, e dividir sem deixar o corpo *GF(p)* (fechamento)

Corpo de Galois GF(p)

- Seja *a,b* inteiros positivos *{0,1, ... , p-1}*
- Adição: *(a + b) mod p*
- Inverso da adição (subtração): *(a + (-a)) mod p*
  - Qual é o elemento de *GF(p)* correspondente ao inverso de *a* para *p=5*?

Corpo de Galois GF(p)

- Seja *a,b* inteiros positivos *{0,1, ... , p-1}*
- Adição: *(a + b) mod p*
- Inverso da adição (subtração):
  - *(a + (-a)) mod p = 0 mod p*
  - Qual é o elemento de *GF(p)* correspondente ao inverso aditivo de *a* para *p=5*?

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

-0 = 0
-1 = 4
-2 = 3
-3 = 2
-4 = 1

Corpo de Galois GF(p)

- Seja *a,b* inteiros positivos *{0,1, ... , p-1}*
- Multiplicação: $(a \times b) \bmod p$
- Inverso da multip.(divisão):
  - $(a \times a^{-1})) \bmod p = 1 \bmod p$
  - Qual é o elemento de *GF(p)* correspondente ao inverso multiplicativo de *a* para *p=5*?

x	0	1	2	3	4
0					
1					
2					
3					
4					

Corpo de Galois GF(p)

- Seja *a,b* inteiros positivos *{0,1, ... , p-1}*
- Multiplicação: $(a \times b) \bmod p$
- Inverso da multip.(divisão): $(a \times a^{-1})) \bmod p$
  - Qual é o elemento de *GF(p)* correspondente ao inverso multiplicativo de *a* para *p*=5?

x	0	1	2	3	4
0					
1					
2					
3					
4					

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Corpo de Galois GF(p)

- Seja *a,b* inteiros positivos *{0,1, ... , p-1}*
- Multiplicação: $(a \times b) \bmod p$
- Inverso da multip.(divisão): $(a \times a^{-1})) \bmod p$
  - Qual é o elemento de *GF(p)* correspondente ao inverso multiplicativo de *a* para *p*=5?

x	0	1	2	3	4
0					
1					
2					
3					
4					

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

0^{-1} = não existe
$1^{-1} = 1$
$2^{-1} = 3$
$3^{-1} = 2$
$4^{-1} = 4$

Corpo de Galois GF(2)

- GF(2) = {0,1}
- Adição:

+	0	1
0	0	1
1	1	0

XOR

- Multiplicação:

x	0	1
0	0	0
1	0	1

AND

Corpos de Extensão

- Se a ordem ***m*** de um corpo finito não é primo, as operações de adição e multiplicação não podem ser definidas para aritmética modular para p^n. Exemplo: $m = 2^n$.
- São os chamados corpos de extensão.
  - Elementos representados como polinômios,
  - Aritmética polinomial módulo polinômio irredutível.

Corpo de Galois GF(2^n)

- Pode-se obter um corpo GF(2^n) :
  - Polinômios com coeficientes módulo 2
    - cujo grau é menor que n
  - assim deve reduzir módulo um polinômio irredutível de grau *n* (p/ multiplicação somente)
- Pode-se sempre achar um inverso
  - pode-se estender o algoritmo do inverso de Euclides para achar.

Example GF(2^3)

Table 4.6 Polynomial Arithmetic Modulo ($x^3 + x + 1$)

	+	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(a) Addition

	×	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

(b) Multiplication

Módulo (x^3+x+1)

Considerações Computationais

- Uma vez que os coeficientes são 0 or 1, pode-se representar qualquer polinômio como uma string de bits
- **Adição e subtração** torna-se **XOR** destes bits
- Multiplicação obtida por shift & XOR
  - Contra multiplicações longas
- A redução modular é feita repetidamente substituindo a potência mais alta pelo resto do polinômio irredutível (shift & XOR também)

Computational Example

- Em GF(2^3) tem-se que(x^2+1) é 101_2 e (x^2+x+1) is 111_2
- Assim a adição é:
  - $(x^2+1) + (x^2+x+1) = x$
  - $101 \text{ XOR } 111 = 010_2$
- E multiplicação é
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1)$
    $= x^3+x+x^2+1 = x^3+x^2+x+1$
  - $011.101 = (101)<<1 \text{ XOR } (101)<<0 =$
    $1010 \text{ XOR } 101 = 1111_2$

Computational Example

- Redução módulo polinomial(q(x) & r(x)) is
  - $(x^3+x^2+x+1) \bmod (x^3+x+1) = 1.(x^3+x+1) + (x^2) = x^2$
  - $1111 \bmod 1011 = 1111 \text{ XOR } 1011 = 0100_2$
  - Observe o módulo para elementos individuais, como x^4, x^5, etc.
    - O resto corresponde a um XOR do operando e polinômio irredutível (deslocado a esquerda)
    - $x^3 \bmod (x^3+x+1) = 1.(x^3+x+1) + (x+1) = (x+1) \bmod (x^3+x+1)$
    - $x^5 \bmod (x^3+x+1)$
      $= x^2.(x^3+x+1) + (x^3+x^2) = x^2.(x^3+x+1) + (x+1+x^2)$
      $= x^2+x+1$