CS557: Cryptography

Elementary Number Theory-VI

S. Tripathy
IIT Patna

Finite Fields

- finite fields play a key role in cryptography
- The number of elements in a finite field **must** be a power of a prime P (p^n)
  - known as Galois field
  - denoted GF(p^n)
- in particular often use the fields:
  - GF(p)
  - GF(2^n)

Summary- Fields

Def (field): A set F with two binary operations $+$ (addition) and $\cdot$ (multiplication) is called a *field* if

1 $\forall\ a,b\in F,\ a+b\in F$

2 $\forall\ a,b,c\in F,\ (a+b)+c=a+(b+c)$

3 $\forall\ a,b\in F,\ a+b=b+a$

4 $\exists\ 0\in F,\ \forall\ a\in F,\ a+0=a$

5 $\forall\ a\in F,\ \exists\ -a\in F,\ a+(-a)=0$

6 $\forall\ a,b\in F,\ a\cdot b\in F$

7 $\forall\ a,b,c\in F,\ (a\cdot b)\cdot c=a\cdot(b\cdot c)$

8 $\forall\ a,b\in F,\ a\cdot b=b\cdot a$

9 $\exists\ 1\in F,\ \forall\ a\in F,\ a\cdot 1=a$

10. $\forall\ a\neq 0\in F,\ \exists\ a^{-1}\in F,\ a\cdot a^{-1}=1$

11 $\forall\ a,b,c\in F, a\cdot(b+c)=a\cdot b+a\cdot c$

- Equivalently, $(F,+)$ is a commutative (additive) group and $(F \setminus \{0\}, \cdot)$ is a commutative (multiplicative) group.

- A field is a commutative ring with identity where each non-zero element has a multiplicative inverse.

Polynomials over Fields

Polynomials:

<u>Finite field):</u> A field $(F,+,\cdot)$ is called a finite field if the set F is finite.

Example: Z_p denotes $\{0,1,\ldots,p-1\}$. We define $+$ and $\cdot$ as addition and multiplication modulo p, respectively.

One can prove that $(Z_p,+,\cdot)$ is a field iff p is prime.

Theorem: There is a unique polynomial $r(x)$ of degree $< m$ over F such that

$$f(x) = h(x) \cdot g(x) + r(x).$$

where, $r(x)$ is called the remainder of $f(x)$ modulo $g(x)$.

Galois Fields GF(p^k)

Theorem: For every prime power p^k ($k=1,2,\dots$) there is a unique finite field containing p^k elements. These fields are denoted by GF(p^k).
There are no finite fields with other cardinalities.

Évariste Galois (1811-1832)

Remarks:

1. For $F=GF(p^k)$, $char(F)=p$.

2. GF(p^k) and Z_{pk} are not the same!

NB>: Operations (+, x) require additional steps in Galois field

Galois Fields GF(p)

- GF(p) is the set of integers {0,1, … , p-1} with arithmetic operations modulo prime p
- these form a finite field
  - since have multiplicative inverses

Multiplication in 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

Polynomial Arithmetic

- can compute using polynomials

  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum a_i x^i$
  - not interested in any specific value of x
- Ordinary Polynomial Arithmetic
  - add or subtract corresponding coefficients
  - multiply all terms by each other

  - Eg: $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$

    $f(x) + g(x) = x^3 + 2x^2 - x + 3$

    $f(x) - g(x) = x^3 + x + 1$

    $f(x) \times g(x) = x^5 + 3x^2 - 2x + 2$

Polynomial Arithmetic with Modulo Coefficients

- when computing value of each coefficient
  - do calculation modulo some value
  - forms a polynomial ring
  - could be modulo any prime

- but we are most interested in mod 2
  - i.e all coefficients are 0 or 1
  - eg. let $f(x) = x^3 + x^2$ and $g(x) = x^2 + x + 1$

$$f(x) + g(x) =$$
$$x^3 + x + 1$$

$$f(x) \times g(x) =$$
$$x^5 + x^2$$

Polynomial Division

- can write any polynomial in the form:
  - $f(x) = q(x)\ g(x) + r(x)$
  - can interpret $r(x)$ as being a remainder
  - $r(x) = f(x) \bmod g(x)$
- if no remainder, we say $g(x)$ divides $f(x)$

- if $f(x)$ has no divisors other than itself & 1 we say it is **irreducible** polynomial

- Arithmetic modulo an irreducible polynomial forms a field

Polynomial GCD

- can find greatest common divisor for polys
  - $c(x) = GCD(a(x), b(x))$ if $c(x)$ is the poly of greatest degree which divides both $a(x)$, $b(x)$
- can adapt Euclid's Algorithm to find it:

EUCLID[$a(x)$, $b(x)$]

1. $A(x) = a(x)$; $B(x) = b(x)$

2. **if** $B(x) = 0$ **return** $A(x) = gcd[a(x), b(x)]$

3. $R(x) = A(x) \bmod B(x)$

4. $A(x) \leftarrow B(x)$

5. $B(x) \leftarrow R(x)$

6. **goto** 2

Computational Consideration

- since coefficients are 0 or 1, can represent any such polynomial as a bit string

- addition becomes XOR of these bit strings
- multiplication is shift & XOR

- modulo reduction done by repeatedly substituting highest power with remainder of irreducible poly (also shift & XOR)

Computational Example

- in GF(2^3) have (x^2+1) is 101_2 & (x^2+x+1) is 111_2
- so addition is
  - $(x^2+1) + (x^2+x+1) = x$
  - $101 \text{ XOR } 111 = 010_2$
- and multiplication is
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1)$
    $= x^3+x+x^2+1 = x^3+x^2+x+1$
  - $011.101 = (101){<<}1 \text{ XOR } (101){<<}0 =$
    $1010 \text{ XOR } 101 = 1111_2$
- polynomial modulo reduction is
  - $(x^3+x^2+x+1) \bmod (x^3+x+1) = 1.(x^3+x+1) + (x^2) = x^2$
  - $1111 \bmod 1011 = 1111 \text{ XOR } 1011 = 0100_2$

Galois Field (polynomial)

- The field defined over the set of residues $F[x]/p(x)$ with the addition and multiplication modulo $p(x)$, where $p(x)$ is irreducible, is called Galois filed GF.

- If the field F is Z_N (N is prime) then the corresponding galois field $Z_N[x]/p(x)$ is denoted by $GF(N^n)$ (n=degree($p(x)$))

- GF(N) is the set of integers {0,1, … , N-1} with arithmetic operations modulo prime N
  - these form a finite field
  - since have multiplicative inverses
  - **Most General use GFs are $GF(2^n)$ and GF(N)| N is prime**

Example GF(7): GF(N: N is prime)

+	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

(a) Addition modulo 7

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

(c) Additive and multiplicative inverses modulo 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

(b) Multiplication modulo 7

Example GF(2^3): $p(x) = x^3 + x + 1$

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

(a) Addition

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

(c) Additive and multiplicative inverses

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

(b) Multiplication

Thanks