Cryptography
Finite field

Anand Ballabh Joshi
Department of Mathematics
University of Lucknow, Lucknow, India

Modular integer Arithmetic

- **Modular Arithmetic**
- Division algorithm: $n > 0, a \in \mathbb{Z}, a = qn + r, 0 \leq r < n$
  $r = a(mod\ n), q = \lfloor \frac{a}{n} \rfloor, a = \lfloor \frac{a}{n} \rfloor + a(mod\ n)$
- Examples: $a = 11, n = 7, 11 = 1 \times 7 + 4,$
  $a = -11, n = 7, -11 = (-2) \times 7 + 3$
- Congruent modulo n; If $a\ mod n = b\ mod n$, i.e. remainder is same when a and b are divided by n, then we say
  $a \equiv b(mod\ n) \Leftrightarrow n | (a - b)$,
  $a = q_1 n + r, b = q_2 n + r$
  $\Leftrightarrow a - b = (q_1 - q_2)n \Leftrightarrow n | a - b$. So $a \equiv b\ (mod n)$
- eg. $100\ (mod 11) = 34 (mod 11)$, so $100 \equiv 34\ (mod 11)$

Modular integer Arithmetic

- The $\equiv$ is an equivalence relation on the set of integers,
  1. Reflexive: $a \equiv a(mod\ n)$
  2. Symmetric: If $a \equiv b(mod\ n)$ then $b \equiv a(mod\ n)$
  3. Transitive: If $a \equiv b(mod\ n)$ and $b \equiv c(mod\ n)$ then $a \equiv c(mod\ n)$
- **Fundamental theorem of equivalence relation**
  Equivalence relation partition the set into disjoint classes, union of disjoint classes is the whole set
- Example for $n = 5$
  $[0] = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$
  $[1] = \{\ldots, -14, -9, -4, 1, 6, 11, 16 \ldots\}$
  $[2] = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$
  $[3] = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}$
  $[4] = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$

Modular integer Arithmetic

- **Modular arithmetic:** can perform arithmetic with residues
  1. $[a(mod\ n) + b(mod\ n)](mod\ n) = (a + b)(mod\ n)$
     $a +_n b = (a + b)(mod\ n)$
  2. $[a(mod\ n) - b(mod\ n)](mod\ n) = (a - b)(mod\ n)$
     $a -_n b = (a - b)(mod\ n)]$
  3. $[a(mod\ n) \times b(mod\ n)](mod\ n) = (a \times b)(mod\ n)$
     $a \times_n b = (a \times b)(mod\ n)]$
- eg. $9 +_{13} 6 = 2(mod\ 13)$; $11 \times_{13} 11 = 4(mod\ 13)$
- **Fast exponential**: Square and multiplication method
  To find $a^e(mod n)$: write $e = \sum_{i=1}^{k} a_i 2^i$, $a_i = \{0, 1\}$
  $a^{73} = a^{2^6 + 2^3 + 2^0} = a^{2^6} a^{2^3} a$
  Find $a^2; (a^2)^2 = a^{2^2}; (a^{2^2})^2 = a^{2^3}; (a^{2^3})^2 = a^{2^4}; (a^{2^4})^2 = a^{2^5}$;
  $(a^{2^5})^2 = a^{2^6}$; Now calculate: $a^{2^6} a^{2^3} a$
- In ordinary multiplication we need 72 operations; In square and multiplication method only 6 squares and 3 multiplications

Modular integer Arithmetic

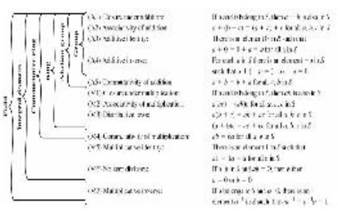
- Modular arithmetic in tabular form

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	4	1	2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- $(\mathbb{Z}_4, +_4)$ is a group but $(\mathbb{Z}_4, \times_4)$ is not a group. $(\mathbb{Z}_n, \times_n)$ is a group $\Leftrightarrow n = prime$, $(U(n), \times_n)$ is a group
- If $a \times b \equiv a \times c(mod\ n)$ then $b \equiv c(mod\ n)$ if a is relative prime to n.
- $gcd(a, n) = 1 \Rightarrow ax + ny = 1$ for some $x, y \in \mathbb{Z}$
  $\Rightarrow ax \equiv 1(mod\ n)$
  $\Rightarrow a$ is invertible $mod\ n$, $i.e.$, a^{-1} exist in (mod n)

Some algebraic structure



Finite Fields

- In field we can perform all fundamental arithmetics
- **Finite fields:** $GF(p^n)$ is Galois field of order p^n
- $GF^*(p^n) = GF(p^n) - \{0\}$ is a cyclic group
- For $n = 1$, $GF(p) = \mathbb{Z}_p = \{0, 1, \ldots, p-1\}, +_p, \times_p$
- For $n \in \mathbb{N}, 0 \neq a \in \mathbb{Z}_n$ has multiplicative inverse iff $gcd(a, n) = 1$ i.e., a is relative prime to n
- If $n = p$, then all non-zero integers in $\mathbb{Z}_n$ are relative prime to n. So, every non zero element in $\mathbb{Z}_p$ has multiplicative inverse
- Smallest field: $GF(2) = \{0, 2\}, +_2, \times_2$

$+_2$	0	1
0	0	1
1	1	0

$\times_2$	0	1
0	0	0
1	0	1

w	−w	w^{-1}
0	0	-
1	1	1

- addition is equivalent to **XOR** and multiplication **AND**
- Finding multiplicative inverse in $GF(p)$
  Extended Euclidean method

Finite Fields

- Arithmetic in $GF(7)$

$+_7$	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

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

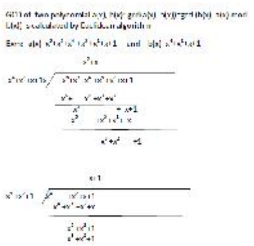
$\times_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

- **Polynomial arithmetic**
  1. Ordinary polynomial arithmetic $f(x) \in R[x]$, where is ring
  2. Polynomial arithmetic in $\mathbb{Z}_p$ i.e. $f(x) \in \mathbb{Z}_p[x]$
  3. Polynomial arithmetic in which coefficient are in $\mathbb{Z}_p$ and polynomial are defined modulo a polynomial $m(x)$
- Ordinary polynomial arithmetic
  $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i \in R[x]$
- A polynomial is called monic polynomial if $a_n = 1$
- We are not interested in evaluating a polynomial for a particular value of x. x is referred indeterminante
- Polynomial arithmetic: Addition, subtraction, multiplication
  $f(x) = \sum_{i=0}^{n} a_i x^i, \quad g(x) = \sum_{i=0}^{m} b_i x^i, \quad n > m$
- addition/subtraction:-
  $f(x) + g(x) = \sum_{i=0}^{m}(a_i + b_i)x^i + \sum_{i=m+1}^{n} a_i x^i$
- Multiplication $f(x)g(x) = \sum_{i=0}^{m+n} c_i x^i$, where
  $c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0$

- **Polynomial arithmetic with coefficient in $\mathbb{Z}_p$**
- addition, multiplication is possible same as in *mod p* with coefficient
- forms a polynomial ring
- If F is field then $F[x]$ is not field
- Let $f(x) = x^3 + x^2 \in \mathbb{Z}_2[x] and g(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$
  $f(x) + g(x) = x^3 + x + 1$
  $f(x) \times g(x) = x^5 + x^2$

- Polynomial division possible over a field (division does not mean exact division)
- We can apply division algorithm when $f(x), g(x) \in F[x]$ not both zero
  We can write $f(x) = q(x)g(x) + r(x)$
- If $deg[f(x)] = n$; $deg[g(x)] = m$, $n \geq m$ then $deg[q(x)] = n - m$ and $deg[r(x)]$ is at most $m - 1$
- An analogous to integer arithmetic we write $f(x) mod\ g(x)$ for remainder i.e. $r(x) = f(x) mod\ g(x)$
- If no remainder say $g(x)$ divide $f(x)$
- no divisor other than itself and 1 say it irreducible
- arithmetic modulo an irreducible polynomial forms a field

- Example GCD of two polynomial. Euclidean method



Finite Fields in cryptography

- Finite fields of the form $GF(2^n)$
- for every prime p and every positive number n, – field of order p^n
- $\mathbb{Z}_p$ is field, $\mathbb{Z}_{p^n}$ is not field
- Finite fields of the form $GF(2^n)$ are attractive for cryptographic algorithm
- Motivation: Both symmetric and public key encryption algorithm involve arithmetic operation on integers
  1. If one of the arithmetic is division, then we need to work in arithmetic defined over a field
  2. For implementation efficiency convenience, we would like to work with integers that fit exactly into a given number of bits, with no wasted bit patterns. We wish to work with integers in the range 0 through $2^n - 1$, which fit into an n bit word

Finite Fields in cryptography

8-bit example

Example. With 8-bits, we can represent integers in the range 0 through 255, but 256 is not prime number, nearest prime to 256 is 251. $\mathbb{Z}_{251}$ is a field, using arithmetic mod(251).
In this case the 8-bit pattern representing the integer 251 through 256 would not be used, resulting inefficient use of storage.

So, if all the arithmetic operations are to be used, and we wish to represent a full range of integers in n-bits, then arithmetic modulo 2^n will not work.

Finite Fields in cryptography

- Even if the encryption algorithm uses only addition and multiplication not division, use of set $\mathbb{Z}_{2^n}$ is questionable, following example illustrate:
- For 3-bit block encryption algorithm, which uses only addition and multiplication. In $\mathbb{Z}_{2^3} = \mathbb{Z}_8$ multiplication table the non-zero integers do not appears an equal number of times. For example occurrence of 3 is 4 and occurrence of 4 is 12, this is cryptographically weak, statistical attack possible
- Number of occurrence of non zero integers is uniform in $GF(2^3)$

Integers	1	2	3	4	5	6	7
Occurrence in $\mathbb{Z}_8$	4	8	4	12	4	8	4
Occurrence in $GF(2^3)$	7	7	7	7	7	7	7

- Following figures show multiplication in $\mathbb{Z}_8$ and multiplication in some field $GF(2^3)$

$\times_8$	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

Cryptographically weaker

$\times$	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

uniform distribution of integers

Finite Fields in cryptography

- Addition in $GF(2^3)$
- This is exclusive-or operation XOR

		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

Modular Polynomial Arithmetic

- One step beyond the modular integer arithmetic
- $f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0 = \sum_{i=0}^{n-1} a_ix^i \in \mathbb{Z}_p[x]$
- S set of all polynomial in $\mathbb{Z}_p[x]$ of degree less than or equal to $n - 1$, $|S| = p^n$
- with the appropriate definition of arithmetic operations, each such set is a finite field
- multiplication result in a polynomial of degree greater than $n - 1$, then the polynomial is reduced modulo some irreducible polynomial $m(x)$ of degree n.
- That is, we divide by $m(x)$ and keep the remainder
- for the polynomial $f(x)$ the remainder is expressed as $r(x) = f(x) mod (x)$

Modular Polynomial Arithmetic

- Advance encryption standard (AES) uses arithmetic in the finite field $GF(2^8)$, with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$
- Example: arithmetic under modulo polynomial $m(x)$
- $f(x) = x^6 + x^4 + x^2 + x + 1, g(x) = x^7 + x + 1$ then $f(x) + g(x) = x^7 + x^6 + x^4 + x^2$; $f(x) \times g(x) = x^{13} + x^{11} + x^9 + x^8 + x^7 + x^7 + x^5 + x^3 + x^2 + x + x^6 + x^4 + x^2 + x + 1$
- the degree of $f(x) \times g(x)$ is 13, we reduced it by modulo $m(x)$
- $f(x) \times g(x) = (x^5 + x^3)m(x) + (x^7 + x^6 + 1)$
- dividing $f(x) \times g(x)$ by $m(x)$ remainder is $x^7 + x^6 + 1$
- $f(x) \times g(x) \ mod \ m(x) = x^7 + x^6 + 1$

Modular Polynomial Arithmetic

- $\frac{F[x]}{<f(x)>}$ is field if and only if $f(x)$ is irreducible and order of field is $|F|^{deg(f(x))}$
- Irreducible Polynomial: can not factorize in two polynomial of degree greater than 1. $x^2 + 1$ not irreducible over $\mathbb{F}_2$ but irreducible over $\mathbb{R}$
- Construction of $GF(2^3)$: We take irreducible polynomial of degree 3 over $GF(2)$
- Only two irreducible polynomial of degree 3 $x^3 + x^2 + 1$ and $x^3 + x + 1$
- $m(x) = x^3 + x + 1$, polynomial arithmetic modulo$(x^3 + x + 1)$

Modular Polynomial Arithmetic

		000	001	010	011	100	101	110	111
	+	0	1	x	x+1	x²	x²+1	x²+x	x²+x+1
000	0	0	1	x	x+1	x²	x²+1	x²+x	x²+x+1
001	1	1	0	x+1	x	x²+1	x²	x²+x+1	x²+x
010	x	x	x+1	0	1	x²+x	x²+x+1	x²	x²+1
011	x+1	x+1	x	1	0	x²+x+1	x²+x	x²+1	x²
100	x²	x²	x²+1	x²+x	x²+x+1	0	1	x	x+1
101	x²+1	x²+1	x²	x²+x+1	x²+x	1	0	x+1	x
110	x²+x	x²+x	x²+x+1	x²	x²+1	x	x+1	0	1
111	x²+x+1	x²+x+1	x²+x	x²+1	x²	x+1	x	1	0

Addition modulo polynomial $m(x)=x^3+x+1$

Modular Polynomial Arithmetic

		000	001	010	011	100	101	110	111
	×	0	1	x	x+1	x²	x²+1	x²+x	x²+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	x+1	x²	x²+1	x²+x	x²+x+1
010	x	0	x	x²	x²+x	x+1	1	x²+x+1	x²+1
011	x+1	0	x+1	x²+x	x²+1	x²+x+1	x²	1	x
100	x²	0	x²	x+1	x²+x+1	x²+x	x	x²+1	1
101	x²+1	0	x²+1	1	x²	x	x²+x+1	x+1	x²+x
110	x²+x	0	x²+x	x²+x+1	1	x²+1	x+1	x	x²
111	x²+x+1	0	x²+x+1	x²	x²+1	x	x+1	0	1

Modular Polynomial Arithmetic

- In $GF(2^3)$, $x^2 + 1$ is 101_2 and $x^2 + x + 1$ is 111_2. So, addition is $(x^2 + 1) + (x^2 + x + 1) = x$, 101_2 XOR $111_2 = 010_2$
- multiplication is $(x^2 + 1).(x^2 + x + 1) = x^4 + x^3 + x + 1$
- polynomial modulo reduction $m(x) = x^3 + x + 1$ is $x^3 - x^2 - x + 1 \ (moox^3 - x + 1) = 1.(x^3 - x - 1) - x^2 = x^2$
- Multiplicative inverse modulo $m(x)$ Using Extended Euclid algorithm

$$(x^7 + x + 1)x^7 = 1 \ mod \ (x^8 + x^4 + x^3 + x + 1)$$
$$\Rightarrow (x^7 + x + 1)^{-1} \equiv x^7 \ mod \ (x^8 + x^4 + x^3 + x + 1)$$

Computational considerations

- A polynomial $f(x)$ in $GF(2^n)$ $f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0 = \sum_{i=0}^{n-1} a_i x^i$ can be uniquely represented by its n binary coefficients $(a_{n-1}a_{n-2}\dots a_0)$
- Every polynomial in $GF(2^n)$ can be represented by an n-bit number
- Addition: Addition of polynomial is performed by adding corresponding coefficients
- In case of $\mathbb{Z}_2$, addition is just XOR
- addition of two polynomial in $GF(2^n)$ a bitwise XOR operation
- Example:

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$$
$$(01010111) \oplus (10000011) = (11010100)$$

Computational considerations

- Multiplication: There is no simple XOR
- Example. $GF(2^8)$, $m(x) = x^8 + x^4 + x^3 + x + 1$
- The technique is based on the observation that

$$x^8 \ mod \ m(x) = (m(x) - x^8) = x^4 + x^3 + x + 1$$

- In general in $GF(2^n)$ $x^n \ mod \ p(x) = p(x) - x^n$
- Consider $f(x) =$ $b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0 \in GF(2^8)$
- $xf(x) =$ $(b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \ mod \ m(x)$
- If $b_7 = 0$, result a poly. of degree less than 8
  If $b_7 = 1$ reduce by $m(x)$
- $xf(x) =$ $(b_6x^7+b_5x^6+b_4x^5+b_3x^4+b_2x^3+b_1x^2+b_0x)+(x^4+x^3+x+1)$
- Multiplication by x(i.e.00000010) can be implemented 1-bit left shift followed by a conditional bitwise XOR with (00011011) i.e. $(x^4 + x^3 + x + 1)$.

Computational considerations

To summarize

$$x \times f(x) = \begin{cases} (b_6 b_5 b_4 b_3 b_2 b_1 b_0 0) & if \ b_7 = 0 \\ (b_6 b_5 b_4 b_3 b_2 b_1 b_0 0) \oplus (00011011) & if \ b_7 = 1 \end{cases}$$

multiplication by higher power of x can be achieved by repeated application of equation.
By adding intermediate results, multiplication by any constant in $GF(2^8)$ can be achieved.

Computational considerations

Example: Let $f(x) = x^6 + x^4 + x^2 + x + 1)$, $g(x) = x^7 + x + 1$
and $m(x) = x^8 + x^4 + x^3 + x + 1$
Compute $f(x) \times g(x) \ mod \ m(x) = x^7 + x^6 + 1$
In binary arithmetic, we need to compute (01010111) × (10000011)
First we determine the results of multiplication by powers of x:

(01010111) × (00000010) = (10101110)
(01010111) × (00000100) = (01011100) ⊕ (00011011) = (01000111)
(01010111) × (00001000) = (10001110)
(01010111) × (00010000) = (00011100) ⊕ (00011011) = (00000111)
(01010111) × (00100000) = (00001110)
(01010111) × (01000000) = (00011100)
(01010111) × (10000000) = (00111000)

Computational considerations

So, we can compute $f(x) \times g(x)$ using the above table as follows
(01010111) × (10000011)
(01010111) × [(00000001) ⊕ (00000010) ⊕ (10000000)]
= (01010111) ⊕ (10101110) ⊕ (00111000) = (11000001)
which is equivalent to $x^7 + x^6 + 1$.

Example of modular polynomial arithmetic

Generalized ElGamal system
Based on discrete logarithmic problem (DLP)
and Diffie-Hillman key exchange

- **Public domain parameters:** Select a cyclic group G of order n, with a primitive element a.
- **Private key:** Some random secret $x \in \{1, 2, \ldots, n-1\}$.
- **Public key:** a (primitive element of group) and $y = a^x$.
- **Encryption:** Let $m \in G$ be the message.
  Choose some random secret $k \in \{1, 2, \ldots, n-1\}$,
  Compute $K = y^k$ in G,
  generate the cryptogram $C = (C_1, C_2)$ with $C_1 = a^k$ and $C_2 = K.m$ in G.
- **Decryption:** Compute $C_1^x = K$ (since $C_1^x = a^{kx} = y^k = K$), recover $m = K^{-1}C_2$

Example of modular polynomial arithmetic

Example:
$G = \mathbb{F}_{2^4}^*$. Elements are polynomials of degree ≤ 3 over $\mathbb{F}_2$ and the multiplication is taken modulo the irreducible polynomial $f(u) = u^4 + u + 1$. The element $a_3u^3 + a_2u^2 + a_1u + a_0 \in \mathbb{F}_{2^4}$ is represented by the binary sting $(a_3a_2a_1a_0)$. G has order 15, $G = < a >$, $a = (0010)$ is a generator, since $a^k, k = 1, 2, \ldots, 15$ is $u, u^2, u^3, u+1, u^2+u, u^3+u^2, u^3+u+1, u^2+1, u^3+u,$ $u^2+u+1, u^3+u^2+u, u^3+u^2+u+1, u^3+u^2+1, u^3+1, 1$

Example of modular polynomial arithmetic

- A chooses $x = 7$,
  A's public key: $a = (0010), y = a^7 = (1011)$
- Encryption : $m = (1100) = a^6$
  B select $k = 11$,
  compute $K = y^{11} = a^{7.11} = a^{15.5+2} = a^2 = (0100)$,
  $C_1 = a^{11} = (1110)$, and
  $C_2 = K.m = a^2.a^6 = a^8 = (0101)$.
- Decryption: A computes $C_1^x = (0100) = a^2 = K$,
  $K^{-1} = a^{13} = (1101)$, and
  $m = K^{-1}C_2 = a^{13}a^8 = a^6 = m$.