ELEC 473 Cryptography and Network Security

5. Introduction to Number Theory

Instructor: Dr. Jianbing Ni

Fall 2021

Review of C4 Topic 5

Bit Padding: The length of plaintext is not an exact multiple of the block size.

- The padding string is “1000…000”

Data Encryption Modes: How to use the block cipher to encrypt the data that are longer than a block.

- Electronic Codebook (ECB): $C_i=E(K, P_i)$
- Cipher Block Chaining (CBC): $C_i=E(K, P_i \oplus C_{i-1})$
- Output Feedback (OFB): $C_i=P_i \oplus MSB_s(E(K, LSB_{b-s}(I_{j-1})||C_{j-1}))$
- Cipher Feedback (CFB): $C_i=P_i \oplus E(K, C_{i-1} \oplus P_{i-1})$
- Counter (CTR): $C_i=P_i \oplus E(K,T_i)$

Advantages, disadvantages, and application scenarios.

Outline

- Euclidean Algorithm and Primality Test
- Modulo Arithmetic
- Intractable Problems

Integers

- $a|b$: a divides b, a is a divisor of b.
- $\gcd(a, b)$: greatest common divisor of a and b.
- Coprime or relatively prime: $\gcd(a, b)=1$.
- Euclidean algorithm: compute $\gcd(a, b)$
- Extended Euclidean algorithm: compute integers x and y such that $ax+by=\gcd(a, b)$

Euclidean Algorithm

Comment: compute $\gcd(a,b)$, where $a > b > 1$.

$r_0 := a$

$r_1 := b$

for $i := 1, 2, \ldots$ until $r_{n+1} = 0$

$r_{i+1} := r_{i-1} \bmod r_i$

return (r_n)

ex.
a = 30 b = 90
gcd (30, 95) =
=

Extended Euclidean Algorithm: Example

$\gcd(299,221) = ?$

$$299 = 1 \cdot 221 + 78$$
$$221 = 2 \cdot 78 + 65$$
$$78 = 1 \cdot 65 + 13$$
$$65 = 5 \cdot 13 + 0$$

$$\begin{aligned}\gcd(229,221) = 13 &= 78 - 65 \\ &= 78 - (221 - 2 \cdot 78) = 3 \cdot 78 - 221 \\ &= 3 \cdot (299 - 1 \cdot 221) - 221 \\ &= 3 \cdot 299 - 4 \cdot 221\end{aligned}$$

欧几里德, extension

$\gcd(a,b) = ax + by$

Prime Numbers

- Prime numbers only have divisors of 1 and self
  - They cannot be written as a product of other numbers
  - Note: 1 is prime, but is generally not of interest
- 2,3,5,7 are prime, 4,6,8,9,10 are not
- Prime numbers are central to number theory
- List of prime number less than 200 is:

  2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

Number Factorization

- To factor a number *n* as a product of other numbers:

$n = a \times b \times c$

- Factoring a number is relatively hard compared to multiplying the factors together to generate the number.
- **Prime factorisation** of a number n is when its written as a product of primes

$91 = 7 \times 13$; $3600 = 2^4 \times 3^2 \times 5^2$

$$n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$$

where $p_1 < p_2 < \cdots < p_t$ are prime numbers;
where each a_i is a positive integer.

Primality Testing

Trivial Division to test if n is a prime

```
for (p=2; p<n^(1/2); p++) {
    e=0;
    if (n%p ==0 ) {
      while (n%p ==0) { e++; n/=p; }
      printf("factor %d,  power %d\n", p, e);
    }
  }
```

Miller-Rabin Primality Test

Let $n>1$ be odd with $n-1=2^k m$ with an odd m.

Choose a random integer a, $1<a<n-1$. Compute $b_0 \equiv a^m \pmod{n}$,

if $b_0 \equiv \pm 1 \pmod{n}$, then stop and n is probably prime; otherwise let $b_1 \equiv (b_0)^2 \pmod{n}$.

If $b_1 \equiv 1 \pmod{n}$, then n is composite and $\gcd(b_0-1,n)$ is a nontrivial factor of n,

else if $b_1 \equiv -1 \pmod{n}$, stop and n is probably prime; otherwise let $b_2 \equiv (b_1)^2 \pmod{n}$.

If $b_2 \equiv 1 \pmod{n}$, then n is composite, else if $b_2 \equiv -1 \pmod{n}$, stop and n is probably prime.

Continue in this way until stopping or reaching b_{k-1}. If $b_{k-1} \not\equiv -1$, then n is composite.

Summary

- Euclidean Algorithm
- Prime Numbers
- Primality Testing

Assignment

- Please use the Euclidean Algorithm to compute gcd(1914,899).
- Please use trial division to determine if n=211 is a prime.
- Please use Miller-Rabin Primality Test to determine if n=561 is a prime (a=2).

Thanks

ELEC 473 Cryptography and Network Security

5. Introduction to Number Theory

Instructor: Dr. Jianbing Ni

Fall 2021

Review of C5 Topic 1

gcd(a,b): Greatest Common Divisor of a and b

Euclidean algorithm to computer gcd(a,b)

Prime numbers: Prime numbers only have divisors of 1 and self

Number Factorization: $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$

Co-prime: a, b have no common divisors apart from 1

Primality Testing: Trivial Division, Miller-Rabin Primality Testing

Outline

- Euclidean Algorithm and Primality Test
- Modulo Arithmetic
  - Additive Group Z_n or $(Z_n, +)$
  - Multiplicative Group Z_n^* or $(Z_n^*, *)$
  - Chinese Remainder Problem
  - Field
- Intractable Problems

Group

- A group, denoted by $(G,\circ)$, is a set G with an operation $\circ : G \circ G \to G$ such that
  1. $a \circ (b \circ c) = (a \circ b) \circ c$ (associative)
  2. $\exists\, e \in G$ s.t. $\forall x \in G,\ e \circ x = x \circ e = x$ (identity)
  3. $\forall x \in G,\ \exists\, y \in G$ s.t. $x \circ y = y \circ x = e$ (inverse)
- A group $(G,\circ)$ is abelian if $\forall x, y \in G,\ x \circ y = y \circ x$.
- Examples: $(Z,+)$, $(Q,+)$, $(Q \setminus \{0\},\ \times)$, $(R,+)$, $(R \setminus \{0\},\ \times)$.

Integers modulo n

- Let $n \geq 2$ be an integer.
- Def: a is congruent to b modulo n, written

  $a \equiv b \mod n$, if $n \mid (a-b)$, i.e., a and b have the same remainder when divided by n.
- Note: $a \equiv b \bmod n$ and $a = b \bmod n$ are different.
- Def: $[a]_n = \{\text{all integers congruent to } a \text{ modulo } n\}$.
- $[a]_n$ is called a residue class modulo n, and a is a representative of that class.

- $[a]_n = [b]_n$ if and only if $a \equiv b \bmod n$.
- There are exactly n residue classes modulo n:

  $[0],\ [1],\ [2],\ \ldots,\ [n-1]$.

  $[a]_n$ 中的 a 应小于 n.
- If $x \in [a],\ y \in [b],$ then $x + y \in [a + b]$ and $x \cdot y \in [a \cdot b]$.
- Define addition and multiplication for residue classes:

  $$[a] + [b] = [a + b]$$

  $$[a] \cdot [b] = [a \cdot b].$$

- Define $Z_n = \{[0],\ [1],\ ...,\ [n-1]\}$.
- Or, more conveniently, $Z_n = \{0,\ 1,\ ...,\ n-1\}$. ex. $Z_{26} = \{0, 1, 2, 3 \cdots 25\}$
- $(Z_n, +)$ forms an abelian additive group.
- For $a, b \in Z_n$,
  - $a + b = (a + b) \bmod n$. (Or, $[a] + [b] = [a + b] = [a + b \bmod n]$.)
  - 0 is the identity element.
  - The inverse of a, denoted by $-a$, is $n - a$. $a + a^{-1} = 0 \Rightarrow [a]_n + [n-a]_n = 0$
- When doing addition/substraction in Z_n, just do the regular addition/substraction and reduce the result modulo n. ex. $[6]_{10} + [10-6]_{10} = 0$
  - In Z_{10}, $5+5+9+4+6+2+8+3 = ? = 2$

mod 10: $0 \quad 0 \quad 0 \quad 2$

- $(Z_n, *)$ is not a group, because 0^{-1} does not exist.
- Even if we exclude 0 and consider only $Z_n^+ = Z_n \setminus \{0\}$,

  $(Z_n^+, *)$ is not necessarily a group; some a^{-1} may not exist.
- For $a \in Z_n$, a^{-1} exists if and only if $\gcd(a, n) = 1$.
- $\gcd(a, n) = 1 \Leftrightarrow ax + ny = 1$ for some integers x and y

  $\Leftrightarrow [a] \cdot [x] + [n] \cdot [y] = [1]$ in Z_n

  $\Leftrightarrow [a] \cdot [x] = [1]$ in Z_n

  $\Leftrightarrow [a]^{-1} = [x]$ in Z_n

- Let $Z_n^* = \{a \in Z_n : \ \gcd(a,n) = 1\}$.
- $(Z_n^*, *)$ is an abelian multiplicative group.
- $a * b = ab \mod n$.
  - $a * b = ab \mod n$.
  - 1 is the identity element.
  - The inverse of a, written a^{-1}, can be computated by the Extended Euclidean Algorithm.
- For example, $Z_{12}^* = \{1,5,7,11\}$. $5 * 7 = 35 \bmod 12 = 11$.

How to compute $a^{-1} \bmod n$?

- Compute a^{-1} in Z_n^*.
- a^{-1} exists if and only if $\gcd(a,n) = 1$.
- Use extended Euclidean algorithm to find x, y such that $ax + ny = \gcd(a,n) = 1$

$$\Rightarrow ax = 1 \quad (\text{because } ny = 0 \text{ in } Z_n)$$

$$\Rightarrow a^{-1} = x.$$

- Note: every computation is reduced modulo n.

Example

- Compute $15^{-1} \mod 47$.

$47 = 15 \times 3 + 2$ (divide 47 by 15; remainder = 2)

$15 = 2 \times 7 + 1$ (divide 15 by 2; remainder = 1)

$$\begin{aligned} 1 &= 15 - 2 \times 7 && (\mod 47) \\ &= 15 - (47 - 15 \times 3) \times 7 && (\mod 47) \\ &= 15 \times 22 - 47 \times 7 && (\mod 47) \\ &= 15 \times 22 && (\mod 47) \end{aligned}$$

$15^{-1} \mod 47 = 22$

How many elements are there in Z_n^*?

- Euler's totient function:

$$\varphi(n) = \left|Z_n^*\right| = \left|\{a : \ 1 \le a \le n, \ \gcd(a,n) = 1\}\right|$$

- Facts:

1. $\varphi(p) = (p-1)$ for prime p.
2. $\varphi(pq) = \varphi(p)\varphi(q)$ if $\gcd(p,q) = 1$.
3. $\varphi(p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}) = p_1^{a_1}(1 - \frac{1}{p_1})p_2^{a_2}(1 - \frac{1}{p_2}) \cdots p_t^{a_t}(1 - \frac{1}{p_t})$

- Let G be a (multiplicative) finite group.
- The order of $a \in G$, written ord(a), is the smallest positive integer t such that $a^t = e$. (e, identity element.)
- The order of G, ord(G), is the number of elements in G.
- Example: Consider Z_{15}^*
  - $\text{ord}(Z_{15}^*) = \left|Z_{15}^*\right| = \varphi(15)$
  - $\text{ord}(8) = 4$, since $8^2 = 64 \bmod 15 = 4$

$$8^3 = (8^2 \cdot 8) \bmod 15 = (4 \cdot 8) \bmod 15 = 2$$

$$8^4 = (8^2 \cdot 8^2) \bmod 15 = (4 \cdot 4) \bmod 15 = 1$$

Example: $n = 15$

- $Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$
- $\left|Z_{15}^*\right| = \varphi(15) = \varphi(3) \times \varphi(5) = 2 \times 4 = 8$
- $$\begin{array}{l|cccccccc} a \in Z_{15}^*: & 1 & 2 & 4 & 7 & 8 & 11 & 13 & 14 \\ \hline \text{ord}(a): & 1 & 4 & 2 & 4 & 4 & 2 & 4 & 2 \end{array}$$
- For all $a \in Z_{15}^*$, we have $a^{\varphi(15)} = a^8 = 1$

- Theorem: For any element $a \in G$, $\text{ord}(a) \mid \text{ord}(G)$.
- Corollary: For any element $a \in G$, $a^{\text{ord}(G)} = e$.
- Fermat's little theorem:

  If $a \in Z_p^*$ (p a prime), then $a^{\varphi(p)} = a^{p-1} = 1$.
- Euler's theorem:

  If $a \in Z_n^*$, then $a^{\varphi(n)} = 1$. $\quad (\because \text{ord}(Z_n^*) = \varphi(n).)$

  That is, for any integer a relatively prime to n,

  $a^{\varphi(n)} \equiv 1 \mod n$.

Fermat's Little Theorem

If $a \in Z_p^*$, p is a prime, $a^{\varphi(p)} = a^{p-1} = 1$.

Considering the set of multiples of a up to $(p\text{-}1)a$: $\{a, 2a, 3a, \cdots, (p\text{-}1)a\}$.

gcd(a, p)=1, such that a and p are relatively prime, and their greatest common divisor is 1.

- For any element $x \in Z_p^*$, since a and p are coprime, x and p are coprime, so we have ax and p are coprime, such that $ax \in Z_p^*$.
- For any two elements $x, y \in Z_p^*$, $x \neq y$, we have $ax \bmod p \neq ay \bmod p$.

So $a \cdot 2a \cdot 3a \cdot \cdots \cdot (p\text{-}1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p\text{-}1) \bmod p$

$$a^{p-1}(p\text{-}1)! \equiv (p\text{-}1)! \bmod p$$

$$a^{p-1} = 1 \bmod p$$

Euler's Theorem

If $a \in Z_n^*$, $a^{\varphi(n)}=1$.

Suppose $Z_n^*=\{x_1, x_2, \cdots, x_{\varphi(n)}\}$
Considering the set of multiples: $\{ax_1, ax_2, ax_3, \cdots, ax_{\varphi(n)}\}$.

gcd(a, n)=1, such that a and n are relatively prime, and their greatest common divisor is 1.

- For any element $x_i \in Z_p^*$, since x_i and n are coprime, a and n are coprime, so we have ax_i and n are coprime, such that $ax_i \in Z_n^*$.
- For any two elements $x_i, x_j \in Z_n^*$, $x_i \neq x_j$, we have $ax_i \bmod n \neq ax_j \bmod n$.

So $ax_1 \cdot ax_2 \cdot ax_3 \cdot \cdots \cdot ax_{\varphi(n)} \equiv x_1 \cdot x_2 \cdot \cdots \cdot x_{\varphi(n)} \bmod n$

$a^{\varphi(n)} x_1 \cdot x_2 \cdot \cdots \cdot x_{\varphi(n)} \equiv x_1 \cdot x_2 \cdot \cdots \cdot x_{\varphi(n)} \bmod n$

$a^{\varphi(n)}=1 \bmod n$

Topic 2 Modulo Arithmetic

Chinese Remainder Problem

Instructor: Dr. Jianbing Ni

Fall 2021

Chinese Remainder Problem

- A problem described in an ancient Chinese arithmetic book.
- Problem: We have a number of things, but we do not know exactly how many.
  - If we count them by threes we have two left over.
  - If we count them by fives we have three left over.
  - If we count them by sevens we have two left over.

  How many things are there?

$$x \equiv 2 \bmod 3, \quad x \equiv 3 \bmod 5, \quad x \equiv 2 \bmod 7$$

$$x = ?$$

Chinese Remainder Theorem

Let $m_1, \cdots, m_r$ be pairwise co-prime numbers, i.e., $\gcd(m_i, m_j) = 1$ if $i \neq j$, and let $a_1, \cdots, a_r$ be integers. Then the following system of r congruent equations:

$$x \equiv a_1 \bmod m_1$$

$$x \equiv a_2 \bmod m_2$$

$$\cdots,$$

$$x \equiv a_r \bmod m_r$$

has a unique solution X modulo $M = m_1 m_2 \cdots m_r$, which is given by

$$X = \sum_{i=1}^{r} a_i M_i \, yi \bmod M$$

where $M_i = M/m_i$, and $y_i = M_i^{-1} \bmod m_i$, for $1 \leq i \leq r$.

Question of Chinese Remainder Theorem

Suppose

$x \equiv 1 \mod 3$

$x \equiv 6 \mod 7$

$x \equiv 8 \mod 10$

By the Chinese remainer theorem, the solution is:

$$x \equiv 1\times 70\times(70^{-1} \bmod 3)+6\times 30\times(30^{-1} \bmod 7)+8\times 21\times(21^{-1} \bmod 10)$$

$$\equiv 1\times 70\times(1^{-1} \bmod 3)+6\times 30\times(2^{-1} \bmod 7)+8\times 21\times(1^{-1} \bmod 10)$$

$$\equiv 1\times 70\times 1+6\times 30\times 4+8\times 21\times 1 \bmod 210$$

$$\equiv 958 \bmod 210$$

$$\equiv 118 \bmod 210$$

$30^{-1} \mod 7$

$= 2^{-1} \mod 7$

$30 \mod 7$

$= 2$

$30^{-1} \cdot 30 \equiv 1$

$70x \equiv 1 \mod 3$

$x \equiv 1 \mod 3$

$x = 1$

$2 \cdot 6^{-1} \equiv 1 \mod 7$

$2a - 1 \equiv 7y \mod 7$

$2a - 7y = 1 \mod 7$

$\gcd(2,7) = 1$

$7 = 2\times 3 + 1$

$2 = 1\times 2 + 0$

$1 = 7 - 2\times 3 = 2^{-1}$

$2^{-1} \mod 7$

$= 3 \mod 7$

$= 4$

Topic 2 Modulo Arithmetic

Field

Instructor: Dr. Jianbing Ni

Fall 2021

Field

A nonempty set F of elements with two operations "+" and "·" satisfying the following axioms. $\forall a, b, c \in F$

(i) F is closed under + and ·; i.e., a+b and a·b are in F.

(ii) Commutative laws: a+b=b+a, a·b=b·a

(iii) Associative laws: (a+b)+c=a+(b+c) , (a·b)·c=a·(b·c)

(iv) Distributive law: a·(b+c) = a·b + a·c

(v) (vi) Identity: a+0 = a , a·1 = a for all a ∈ F. 0·a = 0.

(vii) Additive inverse: for all a ∈ F, there exists an additive inverse (-a) such that a+(-a)=0

(viii) Multiplicative inverse: for all a ∈F, a≠0, there exists a multiplicative inverse a^{-1} such that $a \cdot a^{-1}=1$

Field

Lemma: F is a field.

(i) $(-1) \cdot a = -a$

(ii) $ab = 0$ implies $a = 0$ or $b = 0$.

Proof:

(i) $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = ((-1)+1) \cdot a = 0 \cdot a = 0$

Thus, $(-1) \cdot a = -a$

(ii) If $a \neq 0$, then $b = 1*b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}* 0 = 0$.

Field

Z_m is a field if and only if m is a prime.

- (➔) Suppose that m is a composite number and let m = ab for two integers 1< a, b< m. Thus, a≠0, b≠0. 0=m=ab in Z_m. This is a contradiction to Lemma ii. Hence Z_m is not a field.

  (🡐) If m is a prime. $\forall a \in Z_m$, 0<a<m, a is prime to m. There exist two integers u,v such that ua +vm =1. ua≡1 (mod m). u =a^{-1}. This implies that axiom (viii) in field definition is also satisfied and hence Z_m is a field.

Finite Field

- **Galois Field**: A field with finite number of elements
- GF(p) is the set of integers $\{0, 1, \ldots, p-1\}$ with arithmetic operations modulo prime p
- It is possible to extend the prime field GF(p) to a field of p^n elements, GF(p^n), which is called an extension field of GF(p)
- The number of elements is always a power of a prime number. denoted as GF(p^n)
- Can do addition, subtraction, multiplication, and division without leaving the field GF(p)
  - GF(2) = Mod 2 arithmetic; GF(8) = Mod 8 arithmetic
  - There is no GF(6) since 6 is not a power of a prime.

Summary

- Group
- Integer Modulo
- Additive Group Z_n
- Multiplicative Group Z_n^*
- Order of an Element
- Order of a Group
- Euler's Totient Function
- Fermat's Little Theorem
- Euler's Theorem
- Chinese Remainder Theory
- Field and Finite Field

Practice Question

(1) Use the extended Euclidean algorithm to compute the multiplicative inverses:

a. $17^{-1} \bmod 101$

b. $357^{-1} \bmod 1234$

(2) Compute gcd (57, 93), and find integers s and t such that $57s+93t= \gcd(57, 93)$.

(3) Compute Euler's totient functions: $\varphi(41)$, $\varphi(27)$, and $\varphi(440)$.

Practice Question

(4)

$x \equiv 5 \bmod 7$

$x \equiv 3 \bmod 11$

$x \equiv 10 \bmod 13$

Please calculate $x \bmod 1001$

Thanks

Review of C5 Topic 2

- Group: closure, associativity, identity, and invertibility. $(Z, +)$
- $a \equiv b \bmod n$: a is congruent to b modulo n.
- $[a]_n$: a residue class modulo n (all integers congruent to a modulo n).
- There are exactly n residue classes modulo n: [0], [1], [2], …, [n-1].
- $(Z_n, +)$ is an abelian additive group, where $Z_n = \{0, 1, 2, \ldots, n-1\}$
- $(Z_n^*, *)$ is an abelian multiplicative group, where $Z_n^* = \{a \in Z_n, \gcd(a, n)=1\}$.
- Compute $a^{-1} \bmod n$: Use extended Euclidean Algorithm
- Euler totient Function: $\varphi(n) = |Z_n^*| = |\{a: 1 \le a \le n, \gcd(a, n)=1\}$
- Order(a): The small positive integer t such that $a^t = e \bmod n$.
- Order(G): The number of elements in G.
- Fermat's Little Theorem: If $a \in Z_p^*$, p is a prime, $a^{\varphi(p)} = a^{p-1} = 1$.
- Euler's Theorem: If $a \in Z_n^*$, $a^{\varphi(n)} = 1$.

ELEC 473 Cryptography and Network Security

5. Introduction to Number Theory

Instructor: Dr. Jianbing Ni

Fall 2021

Review of C5 Topic 2

- Group: closure, associativity, identity, and invertibility. $(Z, +)$
- $a \equiv b \bmod n$: a is congruent to b modulo n.
- $[a]_n$: a residue class modulo n (all integers congruent to a modulo n).
- There are exactly n residue classes modulo n: [0], [1], [2], …, [n-1].
- $(Z_n, +)$ is an abelian additive group, where $Z_n = \{0, 1, 2, \ldots, n-1\}$
- $(Z_n^*, *)$ is an abelian multiplicative group, where $Z_n^* = \{a \in Z_n, \gcd(a, n)=1\}$.
- Compute inverse $a^{-1} \bmod n$: Use extended Euclidean Algorithm
- Euler totient Function: $\varphi(n) = |Z_n^*| = |\{a: 1 \le a \le n, \gcd(a, n)=1\}$
- Order(a): The small positive integer t such that $a^t = e \bmod n$.
- Order(G): The number of elements in G.
- Fermat's Little Theorem: If $a \in Z_p^*$, p is a prime, $a^{\varphi(p)} = a^{p-1} = 1$.
- Euler's Theorem: If $a \in Z_n^*$, $a^{\varphi(n)} = 1$.

Review of C5 Topic 2

- Chinese Remainder Theorem
- Field: closure, commutative laws, associative laws, distributive law, identity, additive inverse, multiplicative inverse.
- F is a field, *(i) (-1)•* $a = -a$*; (ii)* $ab=0$ implies $a=0$, *or* $b=0$.
- Z_m is a field if and only if m is a prime.
- Finite Field (Galois Field): A field with finite number of elements
- GF(p) is the set of integers $\{0,1, \ldots, p-1\}$ with arithmetic operations modulo prime p
- It is possible to extend the prime field GF(p) to a field of p^n elements, GF(p^n), which is called an extension field of GF(p)

Outline

- Euclidean Algorithm and Primality Test
- Modulo Arithmetic
- Intractable Problems

The Structure of Z_p^*

Z_p^* is a **cyclic group**, that is

$\exists\ g \in Z_p^*$ such that $\{1, g, g^2, g^3, \ldots, g^{p-2}\} = Z_p^*$

g is called a **generator** of Z_p^*

Example: p=7. $\{1, 3^1, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = Z_7^*$

Not every element is a generator: $\{1, 2, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\}$

How to find the generator of Z_p^*?

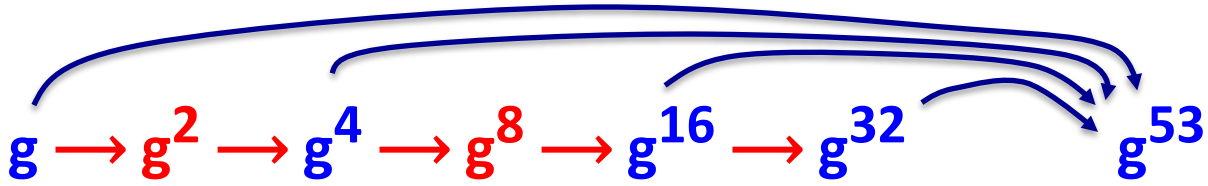
Exponentiation

Finite cyclic group G (for example $G = \mathbb{Z}_p^*$)

Goal: given g in G and x compute g^x

Example: suppose $x = 53 = (110101)_2 = 32+16+4+1$

Then: $g^{53} = g^{32+16+4+1} = g^{32} \cdot g^{16} \cdot g^4 \cdot g^1$



The Repeated Squaring Algorithm

Input: g in G and x>0; **Output**: g^x

write $x = (x_n\, x_{n-1} \ldots x_2\, x_1\, x_0)_2$

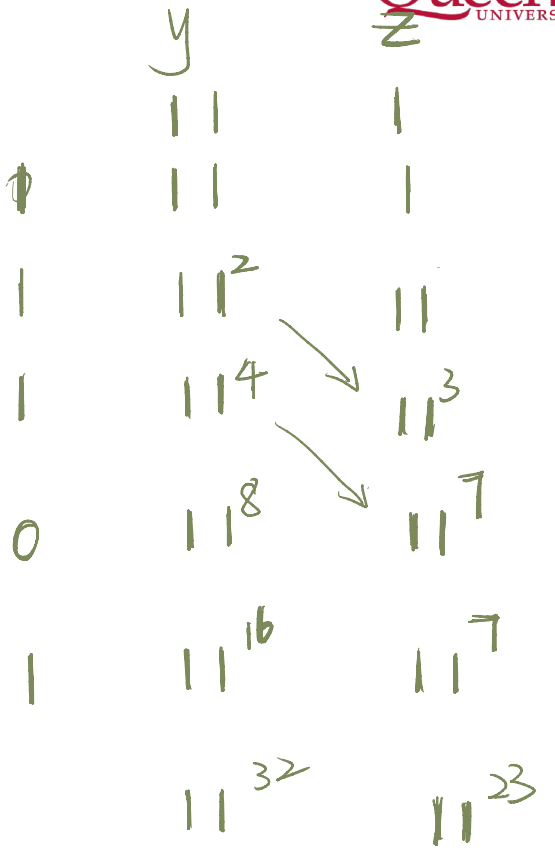
```
y ← g,   z ← 1
for i = 0 to n do:
        if (x[i] == 1):
                z ← z·y
        y ← y^2
output z
```

example: g^{53}

	y	z
$x_0=1$	g	1
$x_1=0$	g^2	g
$x_2=1$	g^4	g
$x_3=0$	g^8	g^5
$x_4=1$	g^{16}	g^5
$x_5=1$	g^{32}	g^{21}
	g^{64}	$\mathbf{g^{53}}$

$11^{23} \bmod 187$

$23 = \{10111\}$



Intractable Problems with Primes

Fix a prime $p > 2$ and g in Z_p^* of order q.

Consider the function: $\mathbf{x \mapsto g^x \quad in \ Z_p^*}$

Now, consider the inverse function:

$\mathbf{Dlog_g (g^x) = x}$ **where** $\mathbf{x}$ **in** $\mathbf{\{0,\cdots, q-1\}}$

Example:

in $\mathbb{Z}_{11}$:	1,	2,	3,	4,	5,	6,	7,	8,	9,	10
$Dlog_2(\cdot)$:	0,	1,	8,	2,	4,	9,	7,	3,	6,	5

$2^x \bmod 11$

Discrete Logarithm (DLog)

Let **G** be a finite cyclic group and **g** is a generator of G

$$G = \{ 1 , g , g^2 , g^3 , \ \dots \ , \ g^{q-1} \} \qquad (q \text{ is called the order of } G)$$

Def: We say that **DLog is hard in G** if for all efficient alg. A:

$$\Pr_{g \leftarrow G,\, x \leftarrow Z_q} [A(G, q, g, g^x) = x] < \text{negligible}$$

Examples:

(1) Z_p^* for large p, (2) Elliptic curve groups mod p

Computing DLog in Z_p^* (n-bit prime p)

Best known algorithm (GNFS): run time $\exp(\tilde{O}(\sqrt[3]{n}))$

cipher key size	modulus size
80 bits	1024 bits
128 bits (AES)	**3072** bits
256 bits	15360 bits

An Application: Collision Resistance

Choose a group G where DLog is hard (e.g. Z_p^* for large p)

Let $q = |G|$ be a prime. Choose generators g, h of G

For $x,y \in \{1,\ldots,q\}$ define $\mathbf{H(x,y) = g^x \cdot h^y \text{ in } G}$

Lemma: finding a collision for H(.,.) is as hard as computing $\text{Dlog}_g(h)$

Proof: Suppose we are given a collision $H(x_0,y_0) = H(x_1,y_1)$

$$g^{x_0} \cdot h^{y_0} = g^{x_1} \cdot h^{y_1} \Rightarrow g^{x_0 - x_1} = h^{y_1 - y_0} \Rightarrow h = g^{(x_0 - x_1)/(y_1 - y_0)}$$

Intractable Problems with Composites

Consider the set of integers: (e.g. for n=1024)

$$\mathbb{Z}_{(2)}(n) := \{N = p \cdot q \text{ where } p,q \text{ are n-bit primes}\}$$

Problem 1: Factor a random N in $\mathbb{Z}_{(2)}(n)$ (e.g. for n=1024)

Problem 2: Given a polynomial **f(x)** where degree(f) > 1

and a random N in $\mathbb{Z}_{(2)}(n)$

find x in $\mathbb{Z}_N$ s.t. f(x) = 0 in $\mathbb{Z}_N$

Summary

- The structure of Z_p^*
- Exponentiation
- Intractable Problems with Primes
- DLog in Z_p^*
- Intractable Problems with Composites

Thanks