Discrete Mathematics
Lecture 6

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

Summary of Lecture 5

Extended Euclidean Algorithm:

- **Input**: a, b $(a \geq b > 0)$
- **Output**: $d = \gcd(a, b)$, s, t such that $d = as + bt$

Linear congruence equation: $ax \equiv b (\mathrm{mod}\ n)$

- **Solvable** if and only if $\gcd(a, n) \mid b$
- **Solution**: $x \equiv \frac{b}{d} t \ \left(\mathrm{mod} \frac{n}{d}\right)$, $t = \left(\frac{a}{d}\right)^{-1} \ \mathrm{mod}\ \frac{n}{d}$

System of linear congruences:

$$\begin{cases} a_1 x \equiv b_1 \ (\mathrm{mod}\ n_1) \\ a_2 x \equiv b_2 \ (\mathrm{mod}\ n_2) \\ \qquad\qquad \vdots \\ a_k x \equiv b_k \ (\mathrm{mod}\ n_k) \end{cases}$$

CRT Map

THEOREM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ and $\gcd(n_i, n_j) = 1$ for all $i \neq j$.

Let $n = n_1 \cdots n_k$. The **CRT map** $\theta([x]_n) = ([x]_{n_1}, \ldots, [x]_{n_k})$ is a well-defined bijection from $\mathbb{Z}_n$ to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

- θ **is well-defined**: show that $[x]_n = [y]_n \Rightarrow \theta([x]_n) = \theta([y]_n)$
  - $[x]_n = [y]_n$
  - $x \equiv y \pmod{n}$
  - $x \equiv y \pmod{n_i}$ for every $i \in [k]$;
  - $[x]_{n_i} = [y]_{n_i}$ for every $i \in [k]$
  - $\theta([x]_n) = ([x]_{n_1}, \ldots, [x]_{n_k})$
    $= ([y]_{n_1}, \ldots, [y]_{n_k})$
    $= \theta([y]_n)$

Residue Class

DEFINITION: Let $\alpha \in \mathbb{R}$.

- $\lfloor \alpha \rfloor$: **floor** of α, the largest integer $\leq \alpha$
- $\lceil \alpha \rceil$: **ceiling** of α, the smallest integer $\geq \alpha$
  - If $a = bq + r$, then $q = \lfloor a/b \rfloor$ and $r = a - bq$

DEFINITION: Let $a \in \mathbb{Z}, n \in \mathbb{Z}^+$. We denote the equivalence class of a under the equivalence relation mod n with $[a]_n$ and call it the **residue class of** a mod n.

- $[a]_n = a + n\mathbb{Z} = \{a + nx : x \in \mathbb{Z}\}$
  - any element of $[a]_n$ is a **representative** of $[a]_n$

EXAMPLE: $[0]_6 = \{0, \pm 6, \pm 12, \dots\}$; $[1]_6 = \{\dots, -11, -5, 1, 7, 13, \dots\}$; ...

Residue Class

THEOREM: Let $n \in \mathbb{Z}^+, a, b \in \mathbb{Z}$. Then

$$[a]_n \cap [b]_n = \emptyset \text{ or } [a]_n = [b]_n.$$

- $[a]_n \cap [b]_n = \emptyset$: done
- $[a]_n \cap [b]_n \neq \emptyset$
  - $\exists c \in [a]_n \cap [b]_n$
  - $c \equiv a \pmod{n}, c \equiv b \pmod{n}$
  - $a \equiv b \pmod{n}$ transitive
  - $\exists t \in \mathbb{Z}$ such that $a = b + nt$ mod 显式化
  - $[a]_n = \{a + nx : x \in \mathbb{Z}\} = \{b + nt + nx : x \in \mathbb{Z}\} = [b]_n$

推论

COROLLARY: $[a]_n = [b]_n$ iff $a \equiv b \pmod{n}$.

COROLLARY: $\{[0]_n, [1]_n, \dots, [n-1]_n\}$ is a partition of $\mathbb{Z}$.

- $[a]_n \cap [b]_n = \emptyset$ for all $a, b \in \{0, 1, \dots, n-1\}$
- $\mathbb{Z} = [0]_n \cup [1]_n \cup \cdots \cup [n-1]_n$

Read

CRT Map

THEOREM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ and $\gcd(n_i, n_j) = 1$ for all $i \neq j$. Let $n = n_1 \cdots n_k$. The **CRT map** $\theta([x]_n) = ([x]_{n_1}, \ldots, [x]_{n_k})$ is a well-defined bijection from $\mathbb{Z}_n$ to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

- ***θ* is bijective**: it suffices to show that θ is injective //why?
  - $\theta([x]_n) = \theta([y]_n)$
  - $([x]_{n_1}, \ldots, [x]_{n_k}) = ([y]_{n_1}, \ldots, [y]_{n_k})$
  - $[x]_{n_i} = [y]_{n_i}$ for every $i \in [k]$
  - $n_i | (x - y)$ for every $i \in [k]$
  - $n | (x - y)$
  - $[x]_n = [y]_n$

bij: $a = b \iff f(a) = f(b)$

CRT Map

THEOREM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ and $\gcd(n_i, n_j) = 1$ for all $i \neq j$. Let $n = n_1 \cdots n_k$. The CRT map $\theta([x]_n) = ([x]_{n_1}, \ldots, [x]_{n_k})$ is a well-defined bijection from $\mathbb{Z}_n^*$ to $\mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$.

- **θ is well-defined**:
  - show that $\theta([x]_n) \in \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$ for every $[x]_n \in \mathbb{Z}_n^*$
    - $[x]_n \in \mathbb{Z}_n^*$
    - $\gcd(x, n) = 1$
    - $\gcd(x, n_i) = 1$ for every $i \in [k]$
    - $[x]_{n_i} \in \mathbb{Z}_{n_i}^*$ for every $i \in [k]$
  - show that $[x]_n = [y]_n \Rightarrow \theta([x]_n) = \theta([y]_n)$
    - see the previous theorem
- **θ is injective**: see the previous theorem

CRT Map

THEOREM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ and $\gcd(n_i, n_j) = 1$ for all $i \neq j$. Let $n = n_1 \cdots n_k$. The CRT map $\theta([x]_n) = ([x]_{n_1}, \ldots, [x]_{n_k})$ is a well-defined bijection from $\mathbb{Z}_n^*$ to $\mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$.

- **θ is surjective:** Let $([b_1]_{n_1}, \ldots, [b_k]_{n_k}) \in \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$. Preimage?
  - Solve the system $x \equiv b_i \pmod{n_i}$, $1 \leq i \leq k$
  - Due to CRT, there is a solution b
  - $b \equiv b_i \pmod{n_i}$ for all $i \in [k]$
  - $\gcd(b, n_i) = 1$ for all $i \in [k]$
    - Otherwise, $\gcd(b_i, n_i) > 1$, contradiction.
  - $\gcd(b, n_1 n_2 \cdots n_k) = 1$
  - $\theta([b]_n) = ([b]_{n_1}, \ldots, [b]_{n_k})$
    $= ([b_1]_{n_1}, \ldots, [b_k]_{n_k})$
  - $[b]_n$ is a preimage of $([b_1]_{n_1}, \ldots, [b_k]_{n_k})$

Euler's Phi Function

THEOREM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ be pairwise relatively prime. Let $n = n_1 \cdots n_k$. Then $\phi(n) = \phi(n_1) \cdots \phi(n_k)$.

- $\theta: \mathbb{Z}_n^* \to \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$ is bijective
- $\phi(n) = \phi(n_1) \times \cdots \times \phi(n_k)$

COROLLARY: If $n = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes $p_1, \ldots, p_k$ and integers $e_1, \ldots, e_k \geq 1$, then $\phi(n) = n(1 - p_1^{-1}) \cdots \left(1 - p_k^{-1}\right)$.

- $\phi(n) = \phi\left(p_1^{e_1}\right) \cdots \phi\left(p_k^{e_k}\right)$
  $= n(1 - p_1^{-1}) \cdots \left(1 - p_k^{-1}\right)$

EXAMPLE: $\phi(10) = \phi(2)\phi(5) = 4; n = 10; n_1 = 2, n_2 = 5$

- $\theta: \mathbb{Z}_n^* \to \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$
  - $1 \mapsto (1,1); 3 \mapsto (1,3); 7 \mapsto (1,2); 9 \mapsto (1,4)$

Euler's Phi Function

QUESTION: How many elements are there in $\mathbb{Z}_n^*$?

- $|\mathbb{Z}_n^*|$ is the number of integers $a \in [n]$ such that $\gcd(a, n) = 1$

DEFINITION: (Euler's Phi Function) $\phi(n) = |\mathbb{Z}_n^*|, \forall n \in \mathbb{Z}^+$

- $\phi(n)$ is the number of integers $a \in [n]$ such that $\gcd(a, n) = 1$

THEOREM: Let p be a prime. Then $\forall e \in \mathbb{Z}^+, \phi(p^e) = p^{e-1}(p-1)$.

- Let $x \in [p^e]$.
- $\gcd(x, p^e) \neq 1$ iff $p|x$

  iff $x = p, 2p, \ldots, p^{e-1} \cdot p$

  - $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$

EXAMPLE: $\phi(3^2) = 3(3-1) = 6$

- $\mathbb{Z}_9^* = \{1,2,\cancel{3},4,5,\cancel{6},7,8,\cancel{9}\}$

EXAMPLE: $\phi(p) = p - 1$

- $\mathbb{Z}_p^* = \{1,2, \ldots, p-1\}$

Euler's Phi Function

QUESTION: Formula of $\phi(n)$ for general integer n?

THEOREM: If $n = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes $p_1, \ldots, p_k$ and integers $e_1, \ldots, e_k \geq 1$, then $\phi(n) = \phi(p_1^{e_1}) \cdots \phi(p_k^{e_k})$.

Hence, $\phi(n) = n(1 - p_1^{-1}) \cdots (1 - p_k^{-1})$.

- There are many proofs. We will see in the future.

COROLLARY: If $n = pq$ for two different primes p and q, then $\phi(n) = (p-1)(q-1)$.

EXAMPLE: $\phi(10) = (2-1)(5-1) = 4; n = 10; p = 2, q = 5$

- $\mathbb{Z}_{10}^* = \{1, \cancel{2}, 3, \cancel{4}, \cancel{5}, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}\}$

$\mathbb{Z}_n$

DEFINITION: Let n be any positive integer. We define $\mathbb{Z}_n$ to be set of all residue classes modulo n.

- $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$
  - $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$;
- $\mathbb{Z}_n = \{[1]_n, [2]_n, \dots, [n]_n\}$
  - $\mathbb{Z}_n = \{1, 2, \dots, n\}$

cover all residue possibility

$(0, 1, \dots, n-1)$

$= [0]_n$

EXAMPLE: Two representations of the set $\mathbb{Z}_6$

- $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$
  $= \{0, 1, 2, 3, 4, 5\}$
- $\mathbb{Z}_6 = \{[-3]_6, [-2]_6, [-1]_6, [0]_6, [1]_6, [2]_6\}$
  $= \{-3, -2, -1, 0, 1, 2\}$

有0.

> Q: diff?

一种简写法

$\mathbb{Z}_n$

DEFINITION: Let $n \in \mathbb{Z}^+$. For all $[a]_n, [b]_n \in \mathbb{Z}_n$, define

- **addition**: $[a]_n + [b]_n = [a+b]_n$
- **subtraction**: $[a]_n - [b]_n = [a-b]_n$
- **multiplication**: $[a]_n \cdot [b]_n = [a \cdot b]_n$

residue class operation

Well-defined? If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$a \pm b \equiv a' \pm b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.

- Hence, $[a]_n \pm [b]_n = [a']_n \pm [b']_n$; $[a]_n \cdot [b]_n = [a']_n \cdot [b']_n$
  - $a \equiv a' \pmod{n} \Rightarrow n|(a-a') \Rightarrow \exists x$ such that $a - a' = nx$
  - $b \equiv b' \pmod{n} \Rightarrow n|(b-b') \Rightarrow \exists y$ such that $b - b' = ny$
    - $(a+b) - (a'+b') = nx + ny$
    - $(a-b) - (a'-b') = nx - ny$
    - $ab - a'b' = a(b-b') + b'(a-a') = any + b'nx$

(mod n)相关证明：结果n因子化

$\mathbb{Z}_n^*$

DEFINITION: Let $n \in \mathbb{Z}^+$ and $[a]_n \in \mathbb{Z}_n$. $[s]_n \in \mathbb{Z}_n$ is called an **inverse** of $[a]_n$ if $[a]_n[s]_n = [1]_n$.

- **division**: If $[a]_n\,[s]_n = [1]_n$, define $\frac{[b]_n}{[a]_n} = [b]_n \cdot [s]_n$

THEOREM: Let $n \in \mathbb{Z}^+$. $[a]_n \in \mathbb{Z}_n$ has an inverse iff $\gcd(a, n) = 1$.

- Only if: $\exists\, s$ s.t. $[a]_n[s]_n \equiv [1]_n$; $\exists\, t, as - 1 = nt$; $\gcd(a, n) = 1$
- If: $\exists\, s, t$ s.t. $as + nt = 1$; $as \equiv 1 \pmod{n}$

DEFINITION: Let $n \in \mathbb{Z}^+$. Define $\mathbb{Z}_n^* = \{[a]_n \in \mathbb{Z}_n : \gcd(a, n) = 1\}$

- If n is prime, then $\mathbb{Z}_n^* = \{1, 2, \ldots, n-1\}$
- If n is composite, then $\mathbb{Z}_n^* \subset \mathbb{Z}_n$

EXAMPLE: $\mathbb{Z}_5^* = \{1,2,3,4\}$; $\mathbb{Z}_6^* = \{1,5\}$; $\mathbb{Z}_8^* = \{1,3,5,7\}$

Group

DEFINITION: Let $\star$ be a binary operation on G. The pair $(G,\star)$ is called an **group** if the following are satisfied:

- **Closure**: $\forall a, b \in G, a \star b \in G$
- **Associative**: $\forall a, b, c \in G, a \star (b \star c) = (a \star b) \star c$
- **Identity**: $\exists e \in G, \forall a \in \mathbb{G}, a \star e = e \star a = a$
- **Inverse**: $\forall a \in \mathbb{G}, \exists b \in G, a \star b = b \star a = e$

阿贝尔群

DEFINITION: A group is said to be an **Abelian group** if it additionally satisfies the following property:

- **Commutative**: $\forall a, b \in G, a \star b = b \star a$
  - An Abelian group is also called a **commutative group**.

better

EXAMPLE: $(\mathbb{Z}, +), (n\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q}^*, \times), (\{\pm 1\}, \times)$

Group $\mathbb{Z}_n$

$\{Z_n, +\}$.

THEOREM: $\mathbb{Z}_n$ is an Abelian group for any $n \in \mathbb{Z}^+$.

- **Closure**: $[a]_n + [b]_n \in \mathbb{Z}_n$
  - $[a]_n + [b]_n = [a + b]_n \in \mathbb{Z}_n$
- **Associative**: $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$
  - $$([a]_n + [b]_n) + [c]_n = [a + b]_n + [c]_n = [(a + b) + c]_n$$
    $$= [a + (b + c)]_n = [a]_n + [b + c]_n$$
    $$= [a]_n + ([b]_n + [c]_n)$$
- **Identity**: $[a]_n + [0]_n = [0]_n + [a]_n = [a]_n$
  - $[a]_n + [0]_n = [a + 0]_n = [0 + a]_n = [0]_n + [a]_n$
- **Inverse**: $[a]_n + [-a]_n = [-a]_n + [a]_n = [0]_n$
  - $[a]_n + [-a]_n = [a + (-a)]_n = [0]_n$
- **Commutative**: $[a]_n + [b]_n = [b]_n + [a]_n$
  - $[a]_n + [b]_n = [a + b]_n = [b + a]_n = [b]_n + [a]_n$

Group $\mathbb{Z}_n^*$

THEOREM: $\mathbb{Z}_n^*$ is an Abelian group for any integer $n > 1$.

- **Closure**: $\forall\, [a]_n, [b]_n \in \mathbb{Z}_n^*, [a]_n \cdot [b]_n = [ab]_n \in \mathbb{Z}_n^*$
- **Associative**:$\forall [a]_n, [b]_n, [c]_n \in \mathbb{Z}_n^*, [a]_n \cdot ([b]_n \cdot [c]_n) = [abc]_n = ([a]_n \cdot [b]_n) \cdot [c]_n$
- **Identity element**: $\exists [1]_n \in \mathbb{Z}_n^*, \forall [a]_n \in \mathbb{Z}_n^*, [a]_n \cdot [1]_n = [1]_n \cdot [a]_n = [a]_n$
- **Inverse**: $\forall [a]_n \in \mathbb{Z}_n^*, \exists [s]_n \in \mathbb{Z}_n^*$ such that $[a]_n \cdot [s]_n = [s]_n \cdot [a]_n = [1]_n$
- **Commutative**: $\forall [a]_n, [b]_n \in \mathbb{Z}_n^*, [a]_n \cdot [b]_n = [ab]_n = [ba]_n = [b]_n \cdot [a]_n$

REMARK: we are interested in two types of Abelian groups

- **Additive Group**: binary operation +; identity 0
  - Example: $(\mathbb{Z}, +), (n\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Z}_n, +)$
- **Multiplicative Group**: binary operation ·; identity 1 //$(\mathbb{Z}_n^*, \cdot)$
  - Example: $(\mathbb{Q}^*, \times), (\{\pm 1\}, \times), (\mathbb{Z}_n^*, \cdot)$

Order

DEFINITION: The **order** of a group G is the cardinality of G.

- $|\mathbb{Z}_n| = n, |\mathbb{Z}_p^*| = p - 1, |\mathbb{Z}| = \infty$

DEFINITION: when $|G| < \infty$, $\forall a \in G$, the **order** of a is defined as the least integer $l > 0$ s.t. $a^l = 1$ ($la = 0$ for additive group)

EXAMPLE: Determine the orders of all elements of $\mathbb{Z}_7^*$

- $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$
- $o(1) = 1, o(2) = 3, o(3) = 6, o(4) = 3, o(5) = 6, o(6) = 2$

EXAMPLE: Determine the orders of all elements of $\mathbb{Z}_6$

- $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$
- $o(0) = 1, o(1) = o(5) = 6, o(2) = o(4) = 3, o(3) = 2$

Order of $a \in \mathbb{Z}_{11}^*$

Target:

a	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	$o(a)$
1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1	10
3	3	9	5	4	1	3	9	5	4	1	5
4	4	5	9	3	1	4	5	9	3	1	5
5	5	3	4	9	1	5	3	4	9	1	5
6	6	3	7	9	10	5	8	4	2	1	10
7	7	5	2	3	10	4	6	9	8	1	10
8	8	9	6	4	10	3	2	5	7	1	10
9	9	4	3	5	1	9	4	3	5	1	5
10	10	1	10	1	10	1	10	1	10	1	2

- $a^{10} = 1$ for every $a \in \mathbb{Z}_{11}^*$; $o(a) | 10$ for every $a \in \mathbb{Z}_{11}^*$

① $a^{n-1} = 1$ $\quad a \in \mathbb{Z}_n^*$ $\quad$ ② $o(a) \mid n-1$

Euler's Theorem

multi !

THEOREM: Let G be a multiplicative Abelian group of order m. Then for any $a \in G$, $a^m = 1$.

- $G = \{a_1, \ldots, a_m\}$
  - If $i \neq j$, then $aa_i \neq aa_j$.
    - $aa_1 \cdot aa_2 \cdots aa_m = a_1 a_2 \cdots a_m \Rightarrow a^m = 1$

Euler's Theorem: Let $n > 1$ and $\alpha \in \mathbb{Z}_n^*$. Then $\alpha^{\phi(n)} = 1$.

- $\alpha^{\phi(n)}, 1$ are both residue classes modulo n
- Proof: a corollary of the previous theorem for $G = \mathbb{Z}_n^*$

Fermat's Little Theorem: If p is a prime and $\alpha \in \mathbb{Z}_p$. Then $\alpha^p = \alpha$.

Euler's Theorem

THEOREM (Euler) Let $n \geq 1$ and $a \in \mathbb{Z}_n^*$. Then $a^{\phi(n)} = 1$.

- $a^{\phi(n)}, 1$ are both residue classes modulo n
- Suppose that $a = [a]_n$ for $a \in \mathbb{Z}$. Then $a^{\phi(n)} = 1$ is $([a]_n)^{\phi(n)} = [1]_n$
- How to prove?
  - Consider the map $f\colon \mathbb{Z}_n^* \to \mathbb{Z}_n^* \quad [x]_n \mapsto [a]_n \cdot [x]_n$
  - We show that f is injective 単射
    - $f([x]_n) = f([y]_n)$
    - $[a]_n \cdot [x]_n = [a]_n \cdot [y]_n$
    - $[ax]_n = [ay]_n$
    - $n | a(x - y)$
    - $n | (x - y)$, this is because $\gcd(n, a) = 1$
      - $[x]_n = [y]_n$

Fermat's Little Theorem

EXAMPLE: Understand Euler's theorem with $\mathbb{Z}_{10}^* = \{1,3,7,9\}$.

- $n = 10, \phi(n) = 4,$
- $1^4 \equiv 1 \pmod{10} \Rightarrow ([1]_{10})^4 = [1]_{10}$
- $3^4 = 81 \equiv 1 \pmod{10} \Rightarrow ([3]_{10})^4 = [1]_{10}$
- $7^4 = 2401 \equiv 1 \pmod{10} \Rightarrow ([7]_{10})^4 = [1]_{10}$
- $9^4 = 6561 \equiv 1 \pmod{10} \Rightarrow ([9]_{10})^4 = [1]_{10}$
  - Consider the map $f\colon \mathbb{Z}_{10}^* \to \mathbb{Z}_{10}^* \quad [x]_n \mapsto [9]_n \cdot [x]_n$
  - $f([1]_{10}) = [9]_{10} \cdot [1]_{10} = [9]_{10}; f([3]_{10}) = [7]_{10}; f([7]_{10}) = [3]_{10}, f([9]_{10}) = [1]_{10}$
  - f is injective
  - $f([1]_{10})f([3]_{10})f([7]_{10})f([9]_{10}) = [9]_{10}[7]_{10}[3]_{10}[1]_{10}$

Fermat's Little Theorem: If p is a prime and $\alpha \in \mathbb{Z}_p$.

Then $\alpha^p = \alpha$.

- This is a corollary of Euler's theorem for $n = p$
- By Euler's theorem, $\alpha^{p-1} = 1$
  - $\alpha^p = \alpha$

$p \geq 1 \quad \phi(p) = p-1 \quad \alpha \in \mathbb{Z}_p$

$\alpha \in \mathbb{Z}_n^*$ since p prime

$\alpha^{p-1} = 1 \rightarrow \alpha^p = p$

Subgroup

DEFINITION: Let $(G,\star)$ be an Abelian group. A subset $H \subseteq G$ is called a **subgroup** of G if $(H,\star)$ is also a group. $(H \leq G)$

- Multiplicative: $G = \mathbb{Z}_6^* = \{1,5\}, H = \{1\}$
- Additive: $G = \mathbb{Z}_6 = \{0,1,2,3,4,5\}; H = \{0,2,4\}$

THEOREM: Let $(G,\cdot)$ be an Abelian group. Let $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ be a subset of G, where $g \in G$. Then $\langle g \rangle \leq G$.

- Closure: $g^a \cdot g^b = g^{a+b} \in \langle g \rangle$
- Associative: $g^a \cdot (g^b \cdot g^c) = g^{a+b+c} = (g^a \cdot g^b) \cdot g^c$
- Identity element: $g^0 \cdot g^a = g^a \cdot g^0 = g^a$
- Inverse: $g^a \cdot g^{-a} = g^{-a} \cdot g^a = g^0$
- Communicative: $g^a \cdot g^b = g^{a+b} = g^{b+a} = g^b \cdot g^a$

Cyclic Group

$\langle g \rangle = \{g^k\}$.

DEFINITION: Let $(G,\cdot)$ be an Abelian group. G is said to be **cyclic** if there exists $g \in G$ such that $G = \langle g \rangle$.

- g is called a **generator** of G.

EXAMPLE: $\mathbb{Z}_{10}^* = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\} = \langle [3]_{10} \rangle$

- $g = [3]_{10}$
- $g^0 = [1]_{10}, g^1 = [3]_{10}, g^2 = [9]_{10}, g^3 = [27]_{10} = [7]_{10}$

REMARK: Let G be a finite group and let $g \in G$. Then $\langle g \rangle$ can be computed as $\{g^1, g^2, \dots\}$

Cyclic Group

EXAMPLE: $\mathbb{Z}_p^*$ is a cyclic group and $G = \langle g \rangle$ is a cyclic subgroup.

- p =17976931348623159077293051907890247336179769789423065727343008115773267580550096313270847732240753602112011387987139335765878976881441662249284743063947412437776789342486548527630221960124609411945308295208500576883815068234246288147391311054082723716335051068458629823994724593847971630483535632962422799885 9
  - p is a prime; $\mathbb{Z}_p^* = \langle 2 \rangle$ is a cyclic group of order $p - 1$
- q =89884656743115795386465259539451236680898848947115328636715040578866337902750481566354238661203768010560056939935696678829394884407208311246423715319737062188883946712432742638151109800623047059726541476042502884419075341171231440736956555270413618581675255342293149119973622969239858152417678164812113999429
  - $q = (p - 1)/2$ is a prime
  - $g = 3$
  - $G = \langle g \rangle$ is a subgroup of $\mathbb{Z}_p^*$ of order q

DLOG and CDH

DEFINITION: Let $G = \langle g \rangle$ be a cyclic group of order q with generator g. For every $h \in G$, there exists $x \in \{0,1,\dots,q-1\}$ such that $h = g^x$. The integer x is called the **discrete logarithm of h with respect to g**.

- $x = \log_g h$

DLOG Problem: $G = \langle g \rangle$ is a cyclic group of order q

- **Input**: G and $h = g^x$ for $x \leftarrow \{0,1,\dots,q-1\}$
- **Output**: $f_{\text{DLOG}}(q, G, g; h) = \log_g h$ find x

CDH Problem: computational Diffie-Hellman

- **Input**: $G = \langle g \rangle$ of order q and $A = g^a, B = g^b$ for $a, b \leftarrow \{0,1,\dots,q-1\}$
- **Output**: $f_{\text{CDH}}(q, G, g; A, B) = g^{ab}$

Diffie-Hellman Key Exchange

The Scheme: $G = \langle g \rangle$ is a cyclic group of prime order q

- Alice: $a \leftarrow \mathbb{Z}_q, A = g^a$; send (q, G, g, A) to Bob
- Bob: $b \leftarrow \mathbb{Z}_q, B = g^b$; send B to Alice; output $k = A^b$
- Alice: output $k = B^a$

Alice

Bob

(q, G, g)

$a \leftarrow \mathbb{Z}_q$

$A = g^a$

(q, G, g, A) →

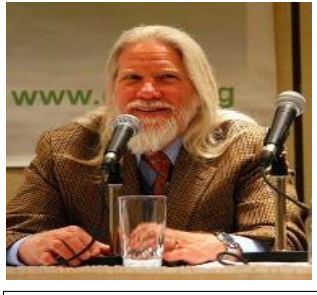
$b \leftarrow \mathbb{Z}_q$

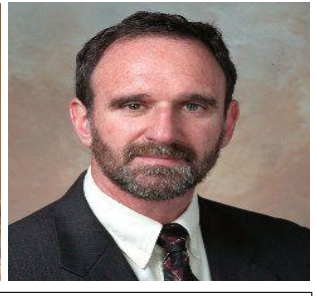
$B = g^b$

← B

output B^a

output A^b





Whitfield Diffie, Martin E. Hellman: New directions in Cryptography, IEEE Trans. Info. Theory, 1976

Turing Award 2015

Correctness: $A^b = g^{ab} = B^a$

Wiretapper: view $= (q, G, g, A, B)$

Security: view $\nrightarrow$ g^{ab}

Diffie-Hellman Key Exchange

Z_{23}

EXAMPLE: $p = 23;\ \mathbb{Z}_p^* = \langle 5 \rangle; G = \langle 2 \rangle, q = |G| = 11, g = 2$

Alice

$a = 3$

$A = g^a = 8$

Bob

(q, G, g, A)

$b = 13$

$B = g^b = 4$

B

$k = 18$

$k = 18$

Adversary: $q = 11, p = 23, g = 2, A = 8, B = 4, k =?$

Primitive Roots

Patrick Corn, Christopher Williams, Pablo A. Barros, and 3 others contributed

Let n be a positive integer. A **primitive root** mod n is an integer g such that every integer relatively prime to n is congruent to a power of g mod n. That is, the integer g is a primitive root (mod n) if for every number a relatively prime to n there is an integer z such that $a \equiv (g^z \pmod n)$.

EXAMPLE

2 is a primitive root mod 5, because for every number a relatively prime to 5, there is an integer z such that $2^z \equiv a$. All the numbers relatively prime to 5 are 1, 2, 3, 4, and each of these (mod 5) is itself (for instance 2 (mod 5) = 2) :

- $2^0 = 1,\ 1 \pmod 5 = 1$, so $2^0 \equiv 1$
- $2^1 = 2,\ 2 \pmod 5 = 2$, so $2^1 \equiv 2$
- $2^3 = 8,\ 8 \pmod 5 = 3$, so $2^3 \equiv 3$
- $2^2 = 4,\ 4 \pmod 5 = 4$, so $2^2 \equiv 4$.

For every integer relatively prime to 5, there is a power of 2 that is congruent.

M : None-secret

M : Secret

p=23 g=5

Cryptographic explanation [edit]

The simplest and the original implementation[2] of the protocol uses the multiplicative group of integers modulo *p*, where *p* is prime, and *g* is a primitive root modulo *p*. These two values are chosen in this way to ensure that the resulting shared secret can take on any value from 1 to *p*–1. Here is an example of the protocol, with non-secret values in blue, and secret values in **red**.

1. Alice and Bob publicly agree to use a modulus $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).
2. Alice chooses a secret integer $a = 4$, then sends Bob $A = g^a \bmod p$
   - $A = 5^4 \bmod 23 = 4$
3. Bob chooses a secret integer $b = 3$, then sends Alice $B = g^b \bmod p$
   - $B = 5^3 \bmod 23 = 10$
4. Alice computes $s = B^a \bmod p$
   - $s = 10^4 \bmod 23 = 18$
5. Bob computes $s = A^b \bmod p$
   - $s = 4^3 \bmod 23 = 18$
6. Alice and Bob now share a secret (the number 18).

Both Alice and Bob have arrived at the same values because under mod p,

$$A^b \bmod p = g^{ab} \bmod p = g^{ba} \bmod p = B^a \bmod p$$

More specifically,

$$(g^a \bmod p)^b \bmod p = (g^b \bmod p)^a \bmod p$$

Only a and b are kept secret. All the other values – p, g, g^a mod p, and g^b mod p – are sent in the clear. The strength of the scheme comes from the fact that g^{ab} mod p = g^{ba} mod p take extremely long times to compute by any known algorithm just from the knowledge of p, g, g^a mod p, and g^b mod p. Once Alice and Bob compute the shared secret they can use it as an encryption key, known only to them, for sending messages across the same open communications channel.

Of course, much larger values of a, b, and p would be needed to make this example secure, since there are only 23 possible results of n mod 23. However, if p is a prime of at least 600 digits, then even the fastest modern computers using the fastest known algorithm cannot find a given only g, p and g^a mod p. Such a problem is called the discrete logarithm problem.[3] The computation of g^a mod p is known as modular exponentiation and can be done efficiently even for large numbers. Note that g need not be large at all, and in practice is usually a small integer (like 2, 3, ...).

Secrecy chart [edit]

The chart below depicts who knows what, again with non-secret values in blue, and secret values in **red**. Here Eve is an eavesdropper Bob, but she does not alter the contents of their communications.

- g = public (prime) base, known to Alice, Bob, and Eve. g = 5
- p = public (prime) modulus, known to Alice, Bob, and Eve. p = 23
- a = Alice's private key, known only to Alice. a = **6**
- b = Bob's private key known only to Bob. b = **15**
- A = Alice's public key, known to Alice, Bob, and Eve. $A = g^a \bmod p$ = 8
- B = Bob's public key, known to Alice, Bob, and Eve. $B = g^b \bmod p$ = 19

Alice		Bob		Eve	
Known	**Unknown**	**Known**	**Unknown**	**Known**	**Unknown**
p = 23		p = 23		p = 23	
g = 5		g = 5		g = 5	
a = **6**	b	b = **15**	a		a, b
$A = 5^a \bmod 23$		$B = 5^b \bmod 23$			
$A = 5^6 \bmod 23 = 8$		$B = 5^{15} \bmod 23 = 19$			
B = **19**		A = **8**		A = 8, B = 19	
$s = B^a \bmod 23$		$s = A^b \bmod 23$			
$s = 19^6 \bmod 23 = 2$		$s = 8^{15} \bmod 23 = 2$			s, a, b

find g:

If the multiplicative order of a number r modulo n is equal to Euler Totient Function Φ(n) (note that the Euler Totient Function for a prime n is n-1), then it is a primitive root.

```
1- Euler Totient Function phi = n-1 [Assuming n is prime]
1- Find all prime factors of phi.
2- Calculate all powers to be calculated further
   using (phi/prime-factors) one by one.
3- Check for all numbered for all powers from i=2
   to n-1 i.e. (i^ powers) modulo n.
4- If it is 1 then 'i' is not a primitive root of n.
5- If it is never 1 then return i;.
```

Although there can be multiple primitive roots for a prime number, we are only concerned with the smallest one. If you want to find all the roots, then continue the process till p-1 instead of breaking up by finding the first primitive root.

Security

Algorithms for DLOG, CDH: solving the DLOG problem first

- G: **the group $\mathbb{Z}_p^*$ of order $q = p - 1$**
  - The best known algorithm runs in $\exp\left(O\left(\sqrt{\ln q \ln\ln q}\right)\right)$
  - $|G| = 2^{1024}$ has been used for many years; now not very safe
  - $|G| = 2^{2048}$ is recommended for today's application
- G: **an order q subgroup of $\mathbb{Z}_p^*$, where $p = 2q + 1$ is a safe prime**
  - The best known algorithm runs in $\exp\left(O\left(\sqrt{\ln q \ln\ln q}\right)\right)$
- For specific group G of order q, the best known algorithm runs in
  - $\exp\left(O\left(\sqrt{(\ln q)^{1/3}(\ln\ln q)^{2/3}}\right)\right)$ //multiplicative group $\mathbb{F}_{p^k}^*$
- For specific group G of order q, the best algorithm runs in
  - $O(\sqrt{q})$ // elliptic curves