Discrete Mathematics
Lecture 6

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

Summary of Lecture 5

Public-key encryption: $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}) + \mathcal{M}, |\mathcal{M}| > 1$

- **Correctness**: $\mathbf{Dec}\big(sk, \mathbf{Enc}(pk, m)\big) = m$ for any pk, sk, m
- **Security**: if sk is not known, it's difficult to learn m from pk, c

Plain RSA: $N = pq$, $\mathcal{M} = \{m: 0 \le m < N, \gcd(m, N) = 1\}$

- $pk = (N, e), sk = (N, d)$; $\gcd\big(e, \phi(N)\big) = 1$; $de \equiv 1 \pmod{\phi(N)}$
- $c = m^e \bmod N$
- $m = c^d \bmod N$

Implementation Issues: $p, q, N, \phi(N), m, c$ are all large

- Given n, how to choose n-bit primes p, q
- Given $\big(e, \phi(N)\big)$, how to compute d
- Given pk, m, how to compute c

Euclidean Algorithm (EA)

ALGORITHM: compute $\gcd(a, b)$

- **Input**: a, b $(a \geq b > 0)$
- **Output**: $d = \gcd(a, b)$
  - $r_0 = a; r_1 = b;$
  - $r_0 = r_1 q_1 + r_2 \;\; (0 < r_2 < r_1)$
  - $\vdots$
  - $r_{i-1} = r_i q_i + r_{i+1} \;\; (0 < r_{i+1} < r_i)$
  - $\vdots$
  - $r_{k-2} = r_{k-1} q_{k-1} + r_k \; (0 < r_k < r_{k-1})$
  - $r_{k-1} = r_k q_k$
  - output r_k

$a = 12345, b = 123$		
i	r_i	q_i
0	12345	
1	123	100
2	45	2
3	33	1
4	12	2
5	9	1
6	3	3
7	0	

Correctness: $d = \gcd(r_0, r_1) = \cdots = \gcd(r_{k-1}, r_k) = r_k$

Extended Euclidean Algorithm (EEA)

ALGORITHM: compute $d = \gcd(a, b)$, s, t such that $as + bt = d$

- **Input**: a, b $(a \geq b > 0)$
- **Output**: $d = \gcd(a, b)$, integers s, t such that $d = as + bt$
  - $r_0 = a; r_1 = b;$ $\begin{pmatrix} s_0 \\ t_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \begin{pmatrix} s_1 \\ t_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix};$
  - $r_0 = r_1 q_1 + r_2$ $(0 < r_2 < r_1);$ $\begin{pmatrix} s_2 \\ t_2 \end{pmatrix} = \begin{pmatrix} s_0 \\ t_0 \end{pmatrix} - q_1 \begin{pmatrix} s_1 \\ t_1 \end{pmatrix}$
  - $\vdots$
  - $r_{i-1} = r_i q_i + r_{i+1}$ $(0 < r_{i+1} < r_i);$ $\begin{pmatrix} s_{i+1} \\ t_{i+1} \end{pmatrix} = \begin{pmatrix} s_{i-1} \\ t_{i-1} \end{pmatrix} - q_i \begin{pmatrix} s_i \\ t_i \end{pmatrix}$
  - $\vdots$
  - $r_{k-2} = r_{k-1} q_{k-1} + r_k$ $(0 < r_k < r_{k-1});$ $\begin{pmatrix} s_k \\ t_k \end{pmatrix} = \begin{pmatrix} s_{k-2} \\ t_{k-2} \end{pmatrix} - q_{k-1} \begin{pmatrix} s_{k-1} \\ t_{k-1} \end{pmatrix}$
  - $r_{k-1} = r_k q_k$
  - output r_k, s_k, t_k

EEA

Correctness: We have that $r_i = as_i + bt_i$ for $i = 0,1,2,\ldots,k$

- $r_0 = a = (a,b)\binom{s_0}{t_0}$; $r_1 = b = (a,b)\binom{s_1}{t_1}$;
- $r_2 = r_0 - q_1 r_1 = (a,b)\binom{s_0}{t_0} - q_1 \cdot (a,b)\binom{s_1}{t_1} = (a,b)\binom{s_2}{t_2}$;
- $\vdots$
- $r_k = r_{k-2} - q_{k-1} r_{k-1} = (a,b)\binom{s_{k-2}}{t_{k-2}} - q_{k-1} \cdot (a,b)\binom{s_{k-1}}{t_{k-1}} = (a,b)\binom{s_k}{t_k}$

EXAMPLE: Execution of the EEA on input $a = 12345, b = 123$

i	r_i	q_i	s_i	t_i
0	12345		1	0
1	123	100	0	1
2	45	2	1	−100
3	33	1	−2	201
4	12	2	3	−301
5	9	1	−8	803
6	3	3	11	−1104
7	0			

$12345 \times 11 + 123 \times (-1104) = 3$

Complexity

THEOREM: Let $\alpha = \frac{1}{2}(1+\sqrt{5})$. Then $k \leq \ln b / \ln \alpha + 1$ in EA.

- $k = 1$: $k \leq \ln b / \ln \alpha + 1$
- $k > 1$: we show that $r_{k-i} \geq \alpha^i$ for $i = 0, 1, \dots, k-1$
    - $i = 0$: $r_k \geq 1 = \alpha^0$
    - $i = 1$: $r_{k-1} > r_k \Rightarrow r_{k-1} \geq r_k + 1 \geq 2 \geq \alpha^1$
    - Suppose that $r_{k-i} \geq \alpha^i$ for $i \leq j$
        - $$\begin{aligned} r_{k-(j+1)} &= r_{k-j} q_{k-j} + r_{k-(j-1)} \\ &\geq \alpha^j + \alpha^{j-1} \\ &= \alpha^{j-1}(\alpha+1) \\ &= \alpha^{j+1} \end{aligned}$$
- $b = r_1 \geq \alpha^{k-1} \Rightarrow k \leq \ln b / \ln \alpha + 1$

Complexity of EA and EEA: $\boxed{O(\ell(a)\ell(b))}$ bit operations

Prime Number Theorem

DEFINITION: For $x \in \mathbb{R}^+$, $\pi(x) = \sum_{p \leq x} 1$: # of primes $\leq x$

THEOREM: $\lim\limits_{x \to \infty} \pi(x)/(x/\ln x) = 1$

- Conjectured by Legendre and Gauss
- Chebyshev: if the limit exists, then it is equal to 1
- Rosser and Schoenfeld:
  - $\pi(x) > \frac{x}{\ln x}(1 + \frac{1}{2 \ln x})$ when $x \geq 59$
  - $\pi(x) < \frac{x}{\ln x}(1 + \frac{3}{2 \ln x})$ when $x > 1$

NOTATION: $\mathbb{P}$- the set of all primes; $\mathbb{P}_n = \{p \in \mathbb{P}: 2^{n-1} \leq p < 2^n\}$.

THEOREM: $|\mathbb{P}_n| \geq \frac{2^n}{n \ln 2}\left(\frac{1}{2} + O\left(\frac{1}{n}\right)\right)$ when $n \to \infty$.

Number of n-bit Primes

EXAMPLE: The number of n-bit primes for $n \in \{10, \ldots, 25\}$.

n	$\lvert\mathbb{P}_n\rvert$	$2^{n-1}/n \ln 2$	n	$\lvert\mathbb{P}_n\rvert$	$2^{n-1}/n \ln 2$
10	75	73.8	18	10749	10505.4
11	137	134.3	19	20390	19904.9
12	255	246.2	20	38635	37819.4
13	464	454.6	21	73586	72036.9
14	872	844.2	22	140336	137525.0
15	1612	1575.8	23	268216	263091.4
16	3030	2954.6	24	513708	504258.5
17	5709	5561.7	25	985818	968176.3

Prime Number Generation

RSA选p,q时在范围内随机选

Basic Idea: randomly choose n-bit integers until a prime found.

- The number of n-bit integers is 2^{n-1}
- $|\mathbb{P}_n| \geq \frac{2^n}{n \ln 2}\left(\frac{1}{2} + O\left(\frac{1}{n}\right)\right)$ when $n \to \infty$
- The probability that a prime is chosen in every trial is equal to

$$\alpha_n = \frac{1}{n \ln 2}\left(1 + O\left(\frac{1}{n}\right)\right), n \to \infty$$

- In $\alpha_n^{-1} = \frac{n \ln 2}{1+O\left(\frac{1}{n}\right)} \leq 2n \ln 2$ trials, we get a prime.

Efficient Algorithms: An algorithm is considered as efficient if its (expected) running time is a polynomial in the bit length of its input. //a.k.a. (expected) polynomial-time algorithm

EXAMPLE: Choosing an n-bit prime can be done efficiently.

- The expected # of trials is $\leq 2n \ln 2$, a polynomial in n (input length)
- Determine if an n-bit integer is prime can be done efficiently

线性同余方程

Linear Congruence Equations

DEFINITION: Let $a, b \in \mathbb{Z}, n \in \mathbb{Z}^+$. A **linear congruence equation** is a congruence of the form $ax \equiv b (\text{mod } n)$, where x is unknown.

THEOREM: Let $n \in \mathbb{Z}^+, a \in \mathbb{Z}$ and $d = \gcd(a, n)$. Then $ax \equiv b (\text{mod } n)$ has a solution if and only if $d|b$.

- $\Rightarrow$: suppose that $ax_0 \equiv b(\text{mod } n)$ for a specific $x_0 \in \mathbb{Z}$
  - $\exists z \in \mathbb{Z}$ such that $ax_0 - b = nz$
  - $b = ax_0 - nz$
  - $d|a, d|n \Rightarrow d|b$
- $\Leftarrow$: suppose that $d|b$ $\exists z \in \mathbb{Z}$ such that $b = dz$
  - $d = \gcd(a, n)$
    - $\exists s, t \in \mathbb{Z}$ such that $as + nt = d$
    - $b = dz = asz + ntz$
    - $a\ (sz) \equiv b\ (\text{mod } n)$
    - sz is a solution

Linear Congruence Equations

THEOREM: Let $n \in \mathbb{Z}^+, a \in \mathbb{Z}, \gcd(a,n) = d,\ t = \left(\frac{a}{d}\right)^{-1} \bmod \frac{n}{d}$.
If $d|b$, then $ax \equiv b \pmod{n}$ iff $x \equiv \frac{b}{d} t \left(\bmod \frac{n}{d}\right)$.

- $t = \left(\frac{a}{d}\right)^{-1} \bmod \frac{n}{d}$ $\quad t \cdot \frac{a}{d} \equiv 1 \left(\bmod \frac{n}{d}\right)$ $\quad \exists s \in \mathbb{Z}$ such that $t \cdot \frac{a}{d} = 1 + s \cdot \frac{n}{d}$

- $ax \equiv b \pmod{n}$
- $\exists z \in \mathbb{Z}$ such that $ax - b = nz$
- $\frac{t}{d}(ax - b) = \frac{t}{d} nz$
- $\left(1 + s \cdot \frac{n}{d}\right) x - t\frac{b}{d} = t\frac{n}{d} z$
- $x \equiv \frac{b}{d} t \left(\bmod \frac{n}{d}\right)$

- $x \equiv \frac{b}{d} t \left(\bmod \frac{n}{d}\right)$
- $\exists z \in \mathbb{Z}$ such that $x - t\frac{b}{d} = \frac{n}{d} z$
- $ax - at\frac{b}{d} = a\frac{n}{d} z$
- $ax - \left(1 + s \cdot \frac{n}{d}\right) b = a \cdot \frac{n}{d} z$
- $ax \equiv b \pmod{n}$

System of Linear Congruences

Sun-Tsu's Question: There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?

- $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 \pmod 7$

DEFINITION: A **system of linear congruences** is a set of linear congruence equations of the form

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \quad\vdots \\ a_k x \equiv b_k \pmod{n_k} \end{cases}.$$

- $x \in \mathbb{Z}$ is a **solution** if it satisfies all k equations.

Chinese Remainder Theorem

THEROEM: Let $n_1, \ldots., n_k \in \mathbb{Z}^+$ be pairwise relatively prime and let $n = n_1 \cdots n_k$. Then for any $b_1, \ldots, b_k \in \mathbb{Z}$, then the system

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \quad\vdots \\ x \equiv b_k \pmod{n_k} \end{cases}$$

always has a solution. Furthermore, if $b \in \mathbb{Z}$ is a solution, then any solution x must satisfy $x \equiv b \pmod{n}$.

- Let $N_i = n/n_i$ for every $i \in [k]$.
  - $\gcd(N_i, n_i) = 1$ for every $i \in [k]$.
  - $\exists\, s_i, t_i, N_i s_i + n_i t_i = 1$.
- Let $b = b_1(N_1 s_1) + \cdots + b_k(N_k s_k)$.
  - Then $b \equiv b_i \pmod{n_i}$ for every $i \in [k]$.

- $x \equiv b_i \pmod{n_i}$ for all i

$\Rightarrow x \equiv b \pmod{n_i}$ for all i

$\Rightarrow n_i | (x - b)$ for all i

$\Rightarrow (n_1 n_2 \cdots n_k) | (x - b)$

$\Rightarrow x \equiv b \pmod{n}$

Solution to Sun-Tsu's Question

EXAMPLE: Solve the system $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5}. \\ x \equiv 2 \pmod{7} \end{cases}$

- $n_1 = 3, n_2 = 5, n_3 = 7; \; n = n_1 n_2 n_3 = 105; \; b_1 = 2, b_2 = 3, b_3 = 2$
  - $N_1 = n_2 n_3 = 35, N_2 = n_1 n_3 = 21, N_3 = n_1 n_2 = 15$
  - $12\, n_1 - N_1 = 1; -4 n_2 + N_2 = 1; -2\, n_3 + N_3 = 1$
  - $t_1 = 12, s_1 = -1; t_2 = -4, s_2 = 1; t_3 = -2, s_3 = 1$
- $b = b_1(N_1 s_1) + b_2(N_2 s_2) + b_3(N_3 s_3)$

  $= 2\,(-35) + 3\,(21) + 2(15)$

  $= 23$
- $x \in \mathbb{Z}$ is a solution of the system iff $x \equiv 23 \pmod{105}$
  - Solutions: $[23]_{105}$

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** $\theta([x]_n) = \left([x]_{n_1}, \ldots, [x]_{n_k}\right)$ 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 $i \in [k]$
  - $\theta([x]_n) = \left([x]_{n_1}, \ldots, [x]_{n_k}\right)$
    $= \left([y]_{n_1}, \ldots, [y]_{n_k}\right)$
    $= \theta([y]_n)$

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 $i \in [k]$
  - $n | (x - y)$
  - $[x]_n = [y]_n$

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 $\theta([x]_n) = \left([x]_{n_1}, \ldots, [x]_{n_k}\right)$ 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 $\left([b_1]_{n_1}, \ldots, [b_k]_{n_k}\right) \in \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$. Preimage?
  - Solve the system $x \equiv b_i \pmod{n_i}, \quad 1 \le i \le k$
  - 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.
  - $\gcd(b, n_1 n_2 \cdots n_k) = 1$
  - $$\begin{aligned} \theta([b]_n) &= \left([b]_{n_1}, \ldots, [b]_{n_k}\right) \\ &= \left([b_1]_{n_1}, \ldots, [b_k]_{n_k}\right) \end{aligned}$$
  - $[b]_n$ is a preimage of $\left([b_1]_{n_1}, \ldots, [b_k]_{n_k}\right)$

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 $\phi(n) = \phi(n_1) \cdots \phi(n_k)$.

- $\theta\colon \mathbb{Z}_n^* \to \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$ 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 $\phi(n) = n(1 - p_1^{-1}) \cdots (1 - p_k^{-1})$.

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

  $= n(1 - p_1^{-1}) \cdots (1 - p_k^{-1})$

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

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

Group

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

- **Closure**封闭性: $\forall a, b \in G, a \star b \in G$
- **Associative**结合律: $\forall a, b, c \in G, a \star (b \star c) = (a \star b) \star c$
- **Identity**单位元: $\exists e \in G, \forall a \in \mathbb{G}, a \star e = e \star a = a$
- **Inverse**逆元: $\forall a \in \mathbb{G}, \exists b \in G\ , a \star b = b \star a = e$

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

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

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

Group $\mathbb{Z}_n$

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**: $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$
  - $$\begin{aligned}([a]_n + [b]_n) + [c]_n &= [a+b]_n + [c]_n = [(a+b)+c]_n \\ &= [a+(b+c)]_n = [a]_n + [b+c]_n \\ &= [a]_n + ([b]_n + [c]_n)\end{aligned}$$
- **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 $\cdot$; 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 $a \in \mathbb{Z}_{11}^*$

$\boldsymbol{a}$	$\boldsymbol{a^1}$	$\boldsymbol{a^2}$	$\boldsymbol{a^3}$	$\boldsymbol{a^4}$	$\boldsymbol{a^5}$	$\boldsymbol{a^6}$	$\boldsymbol{a^7}$	$\boldsymbol{a^8}$	$\boldsymbol{a^9}$	$\boldsymbol{a^{10}}$	$\boldsymbol{o(a)}$
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 $a \in \mathbb{Z}_{11}^*$

Euler’s Theorem

THEOREM: Let G be a multiplicative Abelian group of order m.

Then for any $a \in G$, $a^m = 1$.

- $G = \{a_1, \dots, a_m\}$
  - 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 $\alpha^p = \alpha$.