University of Michigan–Ann Arbor

Department of Electrical Engineering and Computer Science

EECS 475 **Introduction to Cryptography**, Winter 2023

Lecture 20: Elementary number theory: Abelian groups, cyclic groups, Diffie-Hellman key exchange Intro

March 22, 2023

Lecturer: Mahdi Cheraghchi

Scribe: Yi-Wen Tseng

1 Number Thoery

2 Group Thoery

2.1 Abelian Group

Definition: $(G, \circ)$ where $\circ$ is a binary operation such that $\circ : G \times G \to G$ (we denote $\circ(g, h)$ as $g \cdot h$) is a group if:

1. **Identity**: $\exists e \in G$ such that $\forall g \in G$: $e \circ g = g \circ e = g$
2. **Inverse**: $\forall g \in G$, $\exists g^{-1} (or - g)$ such that $g \circ g^{-1} = e$
3. **Associativity**: $\forall g_1, g_2, g_3 \in G$: $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$
4. **Commutativity (Abelian Group)**: $\forall g, h \in G$, $g \circ h = h \circ g$

Example: $(\mathbb{Z}_n, \ + \pmod{\text{N}})$ is an Abelian Group

1. **Identity**: $a + 0 \pmod{\text{N}} = 0 + a \pmod{\text{N}} = a \bmod \text{N}$
2. **Inverse**: $a + (-a) \pmod{\text{N}} = 0 \pmod{\text{N}}$
3. **Associativity**: $(a + b) + c \pmod{\text{N}} = a + (b + c) \pmod{\text{N}}$
4. **Commutativity**: $a + b \pmod{\text{N}} = b + a \pmod{\text{N}}$

Example: $(\mathbb{Z}_n^*, \ \cdot \pmod{\text{N}})$ is an Abelian Group

1. **Identity**: $a \cdot 1 \pmod{\text{N}} = 1 \cdot a \pmod{\text{N}} = a \bmod \text{N}$
2. **Inverse**: $a \cdot (a^{-1}) \pmod{\text{N}} = 1 \pmod{\text{N}} \to$ a and a^{-1} are coprime.
3. **Associativity**: $(a \cdot b) \cdot c \pmod{\text{N}} = a \cdot (b \cdot c) \pmod{\text{N}}$

4. **Commutativity**: $a \cdot b$ (mod N) = $b \cdot a$ (mod N)

*Note: If $a, b \in \mathbb{Z}_n^*$, we never get $a \cdot b = 0$ (mod N). We have numbers in the group as always.

Notation: $|G|$: group order.

- $(\mathbb{Z}_n, +)$ has order N
- $(\mathbb{Z}_p^*, \cdot)$ (where p stands for prime) has order p-1 (from 1 to $p-1$).

Theorem: G is a group and $m = |G|$. $\forall g \in G$, $g^m = \underbrace{(((g \circ g) \circ g) \circ g)}_{\text{m times}} = 1$

Proof: For simplicity assume G is abelian. Suppose $G = \{g_1, g_2, g_3, g_4, g_5, \dots\}$ and let $g \in G$ arbitrary. Because $g \cdot g_i = g \cdot g_j \Rightarrow g_i = g_j$ (multiply by g^{-1}), the set $\{g \cdot g_i : i \in \{1, \dots, m\}\}$ covers all elements of G exactly once.

$$g_1 \cdot g_2 \cdot g_3 \cdots g_m = (g \cdot g_1) \cdot (g \cdot g_2) \cdot (g \cdot g_3) \cdot \cdots \cdot (g \cdot g_m)$$

$$g_1 \cdot g_2 \cdot g_3 \cdots g_m = g^m \cdot (g_1 \cdot g_2 \cdot g_3 \cdots g_m)$$

$$1 = g^m$$

Corollary: Fermat's Little Theorem: $\forall$ prime p, $gcd(a, p) = 1$ and $a^{p-1} = 1$ (mod p)

More General Theorem: Euler's Theorem:

$$\varphi(N) = |\{a \text{ such that } 1 \leq a \leq N, gcd(a, N) = 1\}|, |\mathbb{Z}_n^*| = \varphi(N)$$

$$\text{If } gcd(g, N) = 1 \implies g^{\varphi(N)} = 1 \text{ (mod N)}$$

Corollary: $m = |G|$, $\forall g \in G$, $\forall x \in \mathbb{Z}$. Because $g^m = 1$, $g^x = g^{x \bmod m}$.

Corollary: $m = |G| > 1$, $e \in \mathbb{Z}$, $gcd(e, m) = 1$. Define $d = e^{-1}$ (mod m). Define function $f_e : G \to G$ as $f_e(g) = g^e$. Then, f_e is a bijection whose inverse is f_d.

Proof:

$$f_d(f_e(g)) = f_d(g^e) = (g^e)^d = g^{e \cdot d} = g^{e \cdot d \text{ (mod m)}} = g^1 = g$$

2.2 Cyclic Group

Definition: G is cyclic if $\exists g \in G$ such that

$$\{g^0 = 1, g^1, g^2, g^3, \ldots, g^{m-1}\} = G$$

(we say g generates G)

Non-example

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$$

$$\text{power of } 1 = \{1\}$$

$$\text{power of } 3 = \{1, 3, 3^2 = 1, 3, \ldots\}$$

$$\text{power of } 5 = \{1, 5, 5^2 = 1, 5, \ldots\}$$

$$\text{power of } 7 = \{1, 7, 49 = 1, 7, \ldots\}$$

Example: $\mathbb{Z}_p^*$ for prime p

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

$$\text{power of } 3 = \{1, 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1\} \Rightarrow \text{ 3 generates } \mathbb{Z}_7^*$$

$$\text{power of } 2 = \{1, 2, 2^2 = 4, 2^3 = 1, \ldots\} \Rightarrow \text{ 2 does not generates } \mathbb{Z}_7^*$$

$G' \subseteq G$ is a subgroup if $(G', \cdot)$ is a group. When g does not generate G, it generates a subgroup.
Lagrange's Theorem: If $G' \subseteq G$ is a subgroup then,

$$|G'| \Big| |G|$$

Fast Exponentiation: Suppose we have an element g. Want to compute g^M.

Naive method: $g^M = \underbrace{g \cdot g \cdot g \cdots g}_{\text{M times}} = \underbrace{(((g \cdot g) \cdot g) \cdot g) \cdots}_{\text{M times}}$

Observe:

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis

natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.