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

1.1 Division

In last class, we learned that:

$$a = b \text{ (mode N)} \iff N|a - b$$

Assume $a = a'$ (mod N) and $b = b'$ (mod N), then

- $a + b = a' + b'$ (mod N)
- $a - b = a' - b'$ (mod N)
- $a \cdot b = a' \cdot b'$ (mod N)

However, division is not always possible. For instace,

$$3 \cdot 2 = 15 \cdot 2 \text{ (mod 24)}$$

$$\text{But} 3 \neq 15 \text{ (mod 24)}$$

1.2 GCD

Invertability: Given b, it's invertible if $\exists c$ such that $b \cdot c = 1$ (mod N), where b and c are multiplicative inverse.
Lemma: $b \leq 1$, $N > 1$, b is invertible mod N if and only if $gcd(b, N) = 1$
Proof: Assume $b \cdot c = 1$ (mod N)

$$b \cdot c - 1 = N \cdot q$$

$$bc - Nq = 1$$

$$gcd(b, N) = 1$$

becasue we learned that gcd is the smallest positive integer expressible in this way. Also, if $gcd(b, N) = 1$, then $\exists X, Y$ such that $X \cdot b + Y \cdot N = 1$ (mod N) and $X \cdot b = 1$ (mod N)

Corollary: Using Extended Euclidean, we can compute inverse mod N fast.

Uniqueness: If c, c' are both inverse of b, then $c = c'$ (mod N)
Assume $b \cdot c = 1$, then we can write it as $N \mid b \cdot c - 1$. Assume $b \cdot c' = 1$, then we can write it as $N \mid b \cdot c -' 1$.
Then, $N \mid b \cdot (c - c')$. Because $gcd(N, b) = 1$, inverse exists. Thus,

$$N \mid (c - c')$$

$$c = c' \text{ (mod N)}$$

Example: $b = 11, N = 17$

$$(-3) \cdot 11 + 2 \cdot 17 = 1$$

$$-3 \text{ (mod 17)} = 14 \text{ (mod 17)}$$

$$11 \cdot 14 = 1 \text{ (mod 17)}$$

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

1. **Identity**: $a + 0$ (mod N) $= 0 + a$ (mod N) $= a$ mod N
2. **Inverse**: $a + (-a)$ (mod N) = 0 (mod N)
3. **Associativity**: $(a + b) + c$ (mod N) $= a + (b + c)$ (mod N)
4. **Commutativity**: $a + b$ (mod N) $= b + a$ (mod N)

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

1. **Identity**: $a \cdot 1$ (mod N) $= 1 \cdot a$ (mod N) $= a$ mod N
2. **Inverse**: $a \cdot (a^{-1})$ (mod N) = 1 (mod N) $\to$ a and a^{-1} are coprime.
3. **Associativity**: $(a \cdot b) \cdot c$ (mod N) $= a \cdot (b \cdot c)$ (mod 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 $G = \{g_1, g_2, g_3, g_4, g_5, \ldots\}$ 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 $\{g \cdot g_i : i \in \{1, \ldots, m\}\}$ 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:

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

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

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

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

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

(we say g generates G)

Non-example

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$$
$$\text{power of } 1 = \{1\}$$
$$\text{power of } 3 = \{1, 3, 3^2 = 1, 3, \dots\}$$
$$\text{power of } 5 = \{1, 5, 5^2 = 1, 5, \dots\}$$
$$\text{power of } 7 = \{1, 7, 49 = 1, 7, \dots\}$$

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

$$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$
$$\text{power of } 3 = \{1, 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1\} \Rightarrow \text{ 3 generates } \mathbb{Z}_7^*$$
$$\text{power of } 2 = \{1, 2, 2^2 = 4, 2^3 = 1, \dots\} \Rightarrow \text{ 2 does not generates } \mathbb{Z}_7^*$$

$G^{'} \subseteq G$ 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: $g^{2^m} = g^{2^{m-1}} \cdot g^{2^{m-1}} = (g^{2^{m-1}})^2$

If $M = 2^m$,

$$g, g^2, g^4, g^8, g^{16}, \dots$$

How many operations we perform in this case? $T(M)$

$$T(M) = T(\frac{M}{2}) + 1 \Rightarrow T(M) = \log M = M$$

which is efficient
In general, $M = \sum_{i=0}^{l} m_i \cdot 2^i$. We get $g^M = \prod_{i=0}^{l} g^{2^i}$ by applying the trick above for each g^{2^i}. If M is l bits long, there are $O(l^2)$ multiplications altogether.

Corollary: Fast exponentiation allows us to compute inverses very fast because $g^{-1} = g^{|G|-1}$ (since $g^{|G|} = 1$). However, for $\mathbb{Z}_p^*$, we have a faster method: Extended Euclidean.
We now know how to compute g^m from g efficiently. Do we know how to compute m from g^m? Discrete log: $m = ''log''g^m$ is conjectured to be extremely difficult. We use the difficulty in calculating this discrete log on constructing the **Diffie Hellman key exchange** mechanism.