Groups

Lukas Helminger

Mathematical Background of Cryptography – WT 2019/20

SCIENCE
PASSION
TECHNOLOGY

Outline

Congruences

Groups
- Subgroups
- Quotient Groups
- Homomorphisms

Cyclic Groups
- Discrete Logarithm Problem
- Zero-Knowledge

Lagrange's Theorem
- RSA

Finitely Generated Abelian Groups

Literature

The slides are based on the following books

- **Algebra of Cryptologists**, Alko R. Meijer
- **An Introduction to Mathematical Cryptography**, Hoffstein, Jeffrey, Pipher, Jill, Silverman, J.H.
- **Algebra**, Gisbert Wüstholz

Congruences

Congruences 1

Let $a, n \in \mathbb{N}$ be integers. The set of all multiples of n is denoted by $n\mathbb{Z} := \{kn : k \in \mathbb{Z}\} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$, in analogy define

$$a + n\mathbb{Z} := \{\ldots, a - 2n, a - n, a, a + n, a + 2n, \ldots\}.$$

The set of congruence or residue classes modulo n is then defined as follows

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}.$$

The fact that two congruence classes $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$ are the same is often denoted by

$$a \equiv b \mod n,$$

which is itself defined as $n \mid a - b$, i.e. $\exists k \in \mathbb{Z} : nk = a - b$.

Congruences 2

We can equip $\mathbb{Z}_n$ with two operations induced by the operations on $\mathbb{Z}$

$$\begin{aligned} +_{\mathbb{Z}_n} : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (a + n\mathbb{Z}, b + n\mathbb{Z}) &\longmapsto (a +_{\mathbb{Z}} b) + n\mathbb{Z}, \\ \cdot_{\mathbb{Z}_n} : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (a + n\mathbb{Z}, b + n\mathbb{Z}) &\longmapsto (a \cdot_{\mathbb{Z}} b) + n\mathbb{Z}. \end{aligned}$$

The set of all residue classes modulo n with an inverse w.r.t. to $\cdot_{\mathbb{Z}_n}$ are denoted by

$$\mathbb{Z}_n^* := \{a + n\mathbb{Z} \mid \exists b + n\mathbb{Z} \in \mathbb{Z}_n : a + n\mathbb{Z} \cdot_{\mathbb{Z}_n} b + n\mathbb{Z} = 1 + n\mathbb{Z}\} = \{a + n\mathbb{Z} \mid \gcd(a, n) = 1\}.$$

Notation: By $\bar{a} \in \mathbb{Z}_n$, we actually mean $a + n\mathbb{Z}$.

Groups

Group

Definition (Monoid, Group)

A monoid is a set M together with a binary operation $* : M \times M \to M$, such that the following is satisfied:

- $\forall a, b, c \in M : a * (b * c) = (a * b) * c$ (associative).
- $\exists e \in M \forall a \in M : e * a = a * e = a$ (identity element).

A group is a monoid $\{G, *\}$ such that

$$\forall a \in G \exists a' \in G : a * a' = a' * a = e \quad \text{(inverses).}$$

We call G commutative/abelian if $a * b = b * a$ for all $a, b \in G$.

Groups: Examples

- $\{\mathbb{Z}, +\}$ is an abelian group
- $\{\mathbb{Z}, \cdot\}$ is an abelian monoid.
- $\{\mathbb{Z}_n, +\}$ and $\{\mathbb{Z}_n^*, \cdot\}$ are abelian groups.
  In particular, $\{\mathbb{Z}_2, +\} = \{\{\bar{0}, \bar{1}\}, +\}$ is an abelian group.
- The set of $n \times n$ matrices with rational entries and nonzero determinate forms a non-abelian group under matrix multiplication.

Immediate Consequences

For $a \in \{G, *\}$, define

$$a^n := \underbrace{a * \cdots * a}_{n \text{ times}}, \quad \text{if } n > 0,$$

$a^0 = e$ and $a^n = (a^{-1})^n$ if $n < 0$.

- The identity element is unique.
- The inverse element is unique.
- $a * b = a * c \Rightarrow b = c$. (cancellation law)
- $(a * b)^{-1} = b^{-1} * a^{-1}$.
- $(a * b)^n = a^n * b^n$.

Subgroups

Definition (Subgroup)

Let $\{G, *\}$ be a group and let $H \subset G$ be a non-empty subset of G such that

- $\forall a, b \in H : a * b \in H$ (closed under $*$)
- $\forall a \in H : a^{-1} \in H$ (closed under taking inverses)

Then H is called a subgroup of G.

Example: Consider $\{\mathbb{Z}_6, +\} = \{\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}, +\}$.

- $\{\bar{0}\}$ is a subgroup.
- $\{\bar{0}, \bar{1}, \bar{2}\}$ is not a subgroup.
- $\{\bar{0}, \bar{2}, \bar{4}\}$ is a subgroup.

Quotient Groups

Notation: Let $\{G, \cdot\}$ be an abelian group, $g \in G$ and let M be a non-empty set, then $gM := \{gm : m \in M\}$.

Definition (Quotient group)

Let $\{G, \cdot\}$ be an abelian group and let $H \subset G$ be a subgroup of G. The quotient group $\{G/H, \circ\}$ is defined as follows $G/H := \{gH : g \in G\}$, with the operation

$$\begin{aligned} \circ : G/H \times G/H &\longrightarrow G/H \\ (gH, g'H) &\longmapsto (gg')H. \end{aligned}$$

This abstract construction is quite familiar. Consider $G = \{\mathbb{Z}, +\}$ and for some $n \in \mathbb{N}$ the subgroup $H := n\mathbb{Z} \subset \mathbb{Z}$. Then the corresponding quotient group is $G/H = \mathbb{Z}/n\mathbb{Z}$, with the operation

$$(a + n\mathbb{Z}, b + n\mathbb{Z}) \longmapsto (a + b) + n\mathbb{Z}.$$

Direct Sum

Definition (Direct sum)

The direct sum of a set of abelian groups $\{G_i\}_{i=1}^m$ is a group G defined as follows. As a set G is the cartesian product $G_1 \times \cdots \times G_m = \{a_1, \ldots, a_m : a_i \in G_i\}$. The group operations given two elements $(a_1, \ldots, a_m), (b_1, \ldots, b_m) \in G$ is the component-wise addition

$$(a_1, \ldots, a_m) + (b_1, \ldots, b_m) := (a_1 + b_1, \ldots, a_m + b_m).$$

Example: The Klein four-group

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{1})\}.$$

Homomorphisms 1

Definition (Homomorphism)

A map $\phi : G \to G'$ between two groups is called (group) homomorphism if

$$\phi(gh) = \phi(g)\phi(h) \quad \forall g, h \in G.$$

The kernel and the image of ϕ are defined as the following sets

$$\ker \phi := \{g \in G : \phi(g) = e\} \qquad \operatorname{im} \phi := \{\phi(g) : g \in G\}.$$

We call ϕ an isomorphism if in addition ϕ is bijective.

Homomorphisms 2

Proposition

Let $\phi : G \to G'$ be a group homomorphism, then the kernel $\ker \phi \subset G$ and the image $\operatorname{im} \phi \subset G'$ are subgroups. Further, ϕ is injective if and only if $\ker \phi = \{e\}$.

Examples:

- $\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, for the case that $\gcd(m, n) = 1$.
- $\mathbb{Z}/p^2\mathbb{Z} \ncong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Cyclic Groups

Order

Definition (Order)

Let G be a group and let $a \in G$. The order of g, denoted by $\operatorname{ord}(g)$ is the smallest positive integer n such that $g^n = e$, if there is no such n, then g has infinite order. The order (exponent) of the group G is its cardinality and denoted by $|G|$ or $\#G$.

Examples:

- Take the group $(\mathbb{Z}_{30}^*, \cdot)$, and the residue class $\overline{7} := 7 + 30\mathbb{Z}$. We get that $\operatorname{ord}(\overline{7}) = 4$, because

$$7^1 \equiv 7 \pmod{30}, \quad 7^2 \equiv 19 \pmod{30}, \quad 7^3 \equiv 13 \pmod{30}, \quad 7^4 \equiv 1 \pmod{30}.$$

- Let $n = pq$ with p, q primes. Consider the order of the group $\mathbb{Z}_n^*$:

$$\#\{a + n\mathbb{Z} \mid \gcd(a, n) = 1\} = \phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1).$$

Cyclic Group

Definition (Cyclic group)

A group G (and implicitly a subgroup) is called cyclic if

$$\exists g \in G : \langle g \rangle := \{g^n \mid n \in \mathbb{N}\} = G.$$

Note, for $a \in G$, the subgroup $\langle a \rangle$ is the smallest possible subgroup of G which contains the element a, and is often referred to as the subgroup generated by a.

Proposition

Every finite cyclic group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$ and every cyclic group with infinitely many elements is isomorphic to the integers $\mathbb{Z}$.

Generators of cyclic groups

Proposition

Let $G = \langle g \rangle$ be a finite cyclic group. Then g^r is a generator of G if $r \neq 0$ and $\gcd(r, \mathrm{ord}(g)) = 1$. In particular, the number of generators of G is $\phi(\#G)$.

Example: Take the group $(\mathbb{Z}_{11}, +)$.

From the last proposition we get that this group has $\phi(11) = 10$ generators, i.e. every element besides the neutral element is a generator.

In contrast if we look at the larger group $(\mathbb{Z}_{14}, +)$, we see that this group has only $\phi(14) = 6 \cdot 1 = 6$ generators.

Discrete Logartihm Problem

Definition (Discrete Logarithm Problem (DLP))

Given a finite cyclic group $(G, \cdot)$, a generator $g \in G$, and $a \in G$ arbitrarily, computing $x \in \mathbb{Z}$ such that

$$g^x = a. \quad (1)$$

- For the DLP to be well-defined, it is necessary that $\langle g \rangle = G$.
- Usually, one implicitly looks for the smallest positive x satisfying (1).

Application of DLP: Zero Knowledge Proof

Secret: $x \in \mathbb{Z}$.
Public: Finite cyclic group G with a generator g, and $a = g^x$.

Zero Knowledge Proof:

Alice		Bob
$r \leftarrow \mathbb{Z}$,		
$c \leftarrow g^r$	$\xrightarrow{c}$	
	$\xleftarrow{b}$	$b \in \{0, 1\}$
$y \leftarrow xb + r$	$\xrightarrow{y}$	
		Verify: $g^y = ca^b$

Lagrange’s Theorem

and its applications

Lagrange's Theorem

Lemma

Let G be a finite group. Then every element of G has finite order. Further, if $a \in G$ has order d and if $a^k = e$, then $d \mid k$.

Proposition (Lagrange's Theorem)

Let G be a finite group and let $a \in G$. Then the $\operatorname{ord}(a) \mid \#G$.
More precisely, let $n = \#G$ and let $\operatorname{ord}(a) = d$. Then

$$a^n = e \quad \text{and} \quad d \mid n.$$

Further, let $H \subset G$ be a subgroup then $\#H \mid \#G$.

Applications from Lagrange 1

Corollary (Euler's theorem)

Let $n \in \mathbb{N}$ and $\bar{a} \in \mathbb{Z}_n^*$. Then

$$\bar{a}^{\phi(n)} = \bar{1}.$$

Example: Let $n = pq$ with p, q primes. We choose a public key $\bar{e} \in \mathbb{Z}_n^*$. Further, let $\bar{d} \in \mathbb{Z}_n^*$ be the inverse element of $\bar{e}$ in $\mathbb{Z}_n^*$, i.e.

$$de \equiv 1 \mod \phi(n).$$

Then for all $\bar{a} \in \mathbb{Z}_n^*$, we have:

$$(a^e)^d = a^{1+k\phi(n)} = a \cdot (a^{\phi(n)})^k \equiv a \cdot 1^k \equiv a \mod n.$$

Applications from Lagrange 2

Corollary (Fermat's little theorem)

Let p be prime and $\bar{a} \in \mathbb{Z}_p^*$. Then

$$\bar{a}^{p-1} = \bar{1}.$$

Finitely Generated Abelian Groups

Finitely Generated

Definition (Finitely Generated)

Let $(G, +)$ be an abelian group. We call G finitely generated if there exists a finite set $S = \{s_1, \ldots, s_k\} \subset G$ such that every $a \in G$ can be written as linear combination of elements in S

$$a = n_1 s_1 + \cdots + n_k s_k, \text{ with } n_i \in \mathbb{Z}.$$

We call G finite if $\#G$ is finite.

Example:

- $(\mathbb{Z}, +)$ is finitely generated abelian group with $S = \{1\}$.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ is a finite abelian group.
- Every lattice forms a finitely generated abelian group (more on that later).

Fundamental theorem of finitely generated abelian groups

Theorem (Invariant factor decomposition)

If G is a finitely generated abelian group then

$$G \cong \mathbb{Z}^k \times (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_r\mathbb{Z}),$$

for a unique $k \geq 0$, and some $d_1, \ldots, d_r > 0$ such that $d_i \mid d_{i+1}$ for $i = 1, \ldots r - 1$.

Theorem (Primary decomposition)

If G is a finitely generated abelian group then there are unique $p_1^{n_1}, \ldots, p_s^{n_s} > 1$, where $p_1, \ldots, p_s$ are primes, and a unique $k \geq 0$ such that

$$G \cong \mathbb{Z}^k \times (\mathbb{Z}/p_1^{n_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{n_s}\mathbb{Z}).$$

In both cases: if G is finite $\Rightarrow k = 0$.

Example

Let G be an abelian group of order 100. We want to show that G contains an element of order 10. Further, if there exists no element of order greater than 10, then $G \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.