Introduction to

Cryptography

Lecture 12–14

Chair for Foundations of Software Reliability and Theoretical Computer Science
Technische Universität München

2018/12/12, 15:31

1 Lecture 12-14 – Group theory

1 Lecture 12-14 – Group theory

- As soon as we have a PRG, we also have

  PRFs, PRPs, CPA-secure ES, CCA-secure ES, secure MACs

▷ I.e. PRGs suffice for private-key cryptography.

▷ In fact, PRGs are also necessary for private-key cryptography (later).

- Open question: Do PRGs really exist?

▷ We don't know if PRGs (unconditionally) exists.

  At least in the assymptotic setting, one can show that $\mathbf{NP} \neq \mathbf{P}$ if PRGs exist.

  But we know how to build PRGs from a certain class of computational problems called one-way functions.

- Construction of PRGs is based on the existence of problems for which only a negligible fraction of the problem instances might be easy (i.e. in PPT) to solve .

  Such problems are called one-way functions (OWF) (formal definition later).

- Some examples:

▷ For G a PRG, computing x given $G(x)$ needs to be hard not only for some $x \in \{0,1\}^n$ but for almost all except for a negl. fraction.

▷ For G-sCTR with G a PRG, computing the secret key k from known plaintext-ciphertext pairs (m, c) (CPA setting) needs to be hard not only for some $k \in \{0,1\}^n$, but for almost all except a negl. fraction.

▷ For F a PRF, computing the secret key k from a known input-output-pair $(x, F_k(x))$ needs to be hard not only for some $k \in \{0,1\}^n$ but for almost all except a negl. fraction. Analogously for F-MAC.

- For the actual construction of PRGs, OWFs are of particular interest which are themselves not cryptographic problems like e.g. long standing problems from number theory:
  - Integer factorization: Given an integer N

    find the largest prime factor of N.
  - Discrete logarithm: Given a cyclic group $\langle g\rangle = \mathbb{G}$ and $y \in \mathbb{G}$,

    find $x \in \mathbb{Z}$ s.t. $g^x = y$.
  - RSA problem: Given $N \in \mathbb{N}, e \in \mathbb{Z}^*_{\lambda(N)}$ and $y \in \mathbb{Z}^*_N$,

    find $x \in \mathbb{Z}^*_N$ s.t. $x^e \equiv y \pmod N$.
  - Quadratic residues: Given N and $y \in \mathbb{Z}^*_N$,

    compute $x \in \mathbb{Z}^*_N$ with $x^2 \equiv y \pmod N$ if such an x exists.

▷ Hence, first a detour to primes and commutative groups.

- **Definition**:

  Let $a, b, N \in \mathbb{Z}$ with $N > 0$. Then:

  ▷ $\mathbb{Z}_N := \{0, 1, 2, \ldots, N-1\}$.

  ▷ $a|b$ if $\exists k \in \mathbb{Z} : b = k \cdot a$, i.e., if a divides b.

  ▷ $a \bmod N$ is the unique $k \in \mathbb{Z}_N$ s.t. $N|(a-k)$.

  ▷ $\mathsf{gcd}(a, b) := \max\{d \in \mathbb{N} \mid d|a \wedge d|b\}$.

  ▷ $\mathsf{lcm}(a, b) := \min\{m \in \mathbb{N} \mid m > 0 \wedge a|m \wedge b|m\} = \frac{ab}{\mathsf{gcd}(a,b)}$.

  ▷ $\mathbb{Z}_N^* := \{k \in \mathbb{Z}_N \mid \mathsf{gcd}(k, N) = 1\}$.

  ▷ $\varphi(N) := |\mathbb{Z}_N^*|$ (Euler's phi-function)

  ▷ $a \equiv b \pmod{N}$, $a \equiv b \ (N)$, and $a \equiv_N b$ short for
  $a \bmod N = b \bmod N$.

- **Given**: Natural numbers $0 \leq a \leq b$.

  Goal: Compute integers (x, y) s.t. $\text{gcd}(a, b) = xa + yb$.

  Algorithm:

  - If $a = 0$: return $(0, 1)$
  - If $b \mod a = 0$: return $(1, 0)$
  - Recursively compute (x', y') s.t. $\text{gcd}(b \bmod a, a) = x'(b \bmod a) + y'a$.

    Return $(y' - kx', x')$ with $k = \lfloor \frac{b}{a} \rfloor = \frac{b-(b \mod a)}{a}$.

▷ Correctness: Obviously $\text{gcd}(a, b) = \text{gcd}(b \bmod a, a)$.

  Inductively: $\text{gcd}(b \bmod a, a) = x'(b \bmod a) + y'a$

  Check that $\text{gcd}(a, b) = (y' - kx')a + x'b$ using $(b \bmod a) = b - ka$.

- **Remark**: There are at most $2 \log_2 a$ many recursive calls.

- **Example**: recursive calls
  - $a_0 = 27, b_0 = 35$: recursion ($k_0 = 1$).
  - $a_1 = 8, b_1 = 27$: recursion ($k_1 = 3$).
  - $a_2 = 3, b_2 = 8$: recursion ($k_2 = 2$).
  - $a_3 = 2, b_3 = 3$: recursion ($k_3 = 1$).
  - $a_4 = 1, b_4 = 2$: return $(x_4, y_4) = (1, 0)$
  - Final result:

$$\begin{pmatrix} -k_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -k_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -k_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -k_3 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_4 \\ y_4 \end{pmatrix}$$

  - **Ex**: Compute x, y for $a = 23, b = 120$.
  - **Ex**: Let $F_0 := 0$, $F_1 := 1$, $F_{n+2} = F_{n+1} + F_n$ be the sequence of Fibonacci numbers.

    Determine the number of recursive calls for EEA(F_n, F_{n+1}).

- **Definition:** $\mathbb{G} \hat{=} \langle \mathbb{G}, \cdot, 1 \rangle$ is a group if

  1. $\cdot : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$ (closed under $\cdot$).
  2. $\forall a, b, c \in \mathbb{G} \colon a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ($\cdot$ associative).
  3. $\forall a \in \mathbb{G} \colon a \cdot 1 = 1 \cdot a = a$ (1 is neutral).
  4. $\forall a \in \mathbb{G} \exists b \in \mathbb{G} \colon a \cdot b = b \cdot a = 1$ (b inverse of a).

  $|\mathbb{G}|$ is called the order of $\mathbb{G}$; $\mathbb{G}$ is finite if $|\mathbb{G}| < \infty$.

  $\mathbb{G}$ is commutative if $\forall a, b \colon a \cdot b = b \cdot a$ holds in addition.

- ▷ **Remark**: For commutative groups the group operation is also often written additively $(+, 0)$. We will use the multiplicative notation $(\cdot)$ most of the time, and simply write ab for $a \cdot b$, and $\mathbb{G}$ for $\langle \mathbb{G}, \cdot, 1 \rangle$.

- **Remark/Lemma**: Sometimes only $\forall a \in \mathbb{G} \colon a1 = a$ (right neutral) and $\forall a \in \mathbb{G} \exists b \in \mathbb{G} \colon ab = 1$ (right inverse) are required. One can show that every right neutral/inverse is also left neutral/inverse.

- **Lemma**: Neutral element and inverse are unique in a group.

▷ Proof:

Assume $ab = 1 = ac$. Then $b = b1 = b(ac) = (ba)c = c$.

Assume $a1' = a$ for all $a \in \mathbb{G}$. Then $1 = 1 \cdot 1' = 1'$.

- **Definition**: From now on a^{-1} denotes the unique inverse of a in $\mathbb{G}$.
  (For additively written groups: $-a$.)

- **Corollary**: In every group
  - $(a^{-1})^{-1} = a$
  - $(ab)^{-1} = b^{-1}a^{-1}$
  - The unique solution of $ax = b$ ($xa = b$) is $x = a^{-1}b$ ($x = ba^{-1}$).

▷ Proof:

$a^{-1}a = 1 = a^{-1}(a^{-1})^{-1}$ resp. $ab(ab)^{-1} = 1 = ab(b^{-1}a^{-1}$

$x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}b$; analogously for $xa = b$.

- **Definition**: Let $\langle \mathbb{G}, \cdot, 1 \rangle$ be a group.
  For $a \in \mathbb{G}$ and $k \in \mathbb{Z}$ define (inductively)

$$a^k := \begin{cases} 1 & \text{if } k = 0 \\ a \cdot a^{k-1} & \text{if } k > 0 \\ (a^{-1}) \cdot a^{k+1} & \text{if } k < 0 \end{cases}$$

  and $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$
  $\mathrm{ord}(a) := |\langle a \rangle|$ is called the order of a (in $\mathbb{G}$).
  $\mathbb{G}$ is cyclic if there is some generator $g \in \mathbb{G}$ s.t. $\langle g \rangle = \mathbb{G}$.

▷ **Remark**: a^k simply means "apply the group operation to k copies of a" if $k \geq 0$ resp. "apply the group operation to k copies of a^{-1}" if $k < 0$, which is written as exponentation when using the multiplicative notation.

▷ Hence: $a^k a^l = a^{k+l} = a^l a^k$ and $(a^k)^{-1} = a^{-k} = (a^{-1})^k$.

▷ **Remark**: Note that in the additive notation (i.e. $a + b$ instead of $a \cdot b$) exponentation becomes multiplication so that $\langle a \rangle = \{ka \mid k \in \mathbb{Z}\}$.

- **Definition**: Let $\langle \mathbb{G}, \cdot, 1 \rangle$ be a group.

  A (nonempty) subset $\mathbb{H} \subseteq \mathbb{G}$ is a subgroup of $\mathbb{G}$ (short: $\mathbb{H} \leq \mathbb{G}$)

  if $\langle \mathbb{H}, \cdot, 1 \rangle$ is itself a group.

▷ Note that a subgroup $\mathbb{H}$ always "inherits" the group operation and the neutral element from its "surrounding" group:

  - Let 1_H be neutral in H.

    Then in G: $1_H = 1_H \cdot 1 = 1_H \cdot (1_H \cdot 1_H^{-1}) = 1_H \cdot 1_H^{-1} = 1$.
  - Hence, assume $ab = 1$ for $a, b \in H$.

    Then also $ab = 1$ in G, and thus $b = a^{-1}$ and $a = b^{-1}$.

- **Lemma**: $\mathbb{H} \leq \mathbb{G}$ iff $ab^{-1} \in \mathbb{H}$ for any $a, b \in \mathbb{H}$.

▷ Proof:

  If $\mathbb{H} \leq \mathbb{G}$, then trivially $ab^{-1} \in \mathbb{H}$ for any $a, b \in \mathbb{H}$.

  Assume that $ab^{-1} \in \mathbb{H}$ for any $a, b \in \mathbb{H}$.

  Then also $1 = aa^{-1} \in \mathbb{H}$, thus also $b^{-1} = 1b^{-1} \in \mathbb{H}$ and $ab = a(b^{-1})^{-1} \in \mathbb{H}$.

- **Lemma**: Let $\mathbb{G}$ be a group.

  Then $\langle a \rangle$ is a cyclic subgroup of $\mathbb{G}$ for any $a \in \mathbb{G}$.

▷ Proof:

We only need to check that $cd^{-1} \in \langle a \rangle$ for any $c, d \in \langle a \rangle$.

Note that $(a^k)^{-1} = a^{-k}$ because of uniqueness of the inverse.

As $c, d \in \langle a \rangle$, we find $m, n \in \mathbb{Z}$ s.t. $c = a^m$ and $d = a^n$.

Thus $c^{-1}d = (a^m)^{-1}a^n = a^{-m}a^n = a^{-m+n} \in \langle a \rangle$.

Simply use $aa^{-1} = a^{-1}a = 1$ to reduce the term until $|-m+n|$ copies of a (if $-m+n \geq 0$) resp. a^{-1} remain.

▷ **Corollary**: Every cyclic group is commutative.

- **Lemma**: If $\mathbb{H} \leq \mathbb{G} = \langle g \rangle$, then $\mathbb{H}$ is cyclic, too.

▷ Proof: Let $\mathbb{H} \leq \langle g \rangle$. ($\mathbb{H} \neq \emptyset$.)
Then $\emptyset \neq \mathbb{H} = \{g^k \mid k \in E\}$ for suitable exponents $E \subseteq \mathbb{Z}$.
Then there is a least $m \in \mathbb{N} \setminus \{0\}$ s.t. $g^m \in \mathbb{H}$ (as $a, a^{-1} \in \mathbb{H}$).
Hence $\langle g^m \rangle \leq \mathbb{H}$. Pick any $a \in \mathbb{H}$.
Then there is some $k \in \mathbb{Z}$ s.t. $a = g^k$.
If $k < 0$, switch to a^{-1}, s.t. $k > 0$.
Then also $a \cdot (g^m)^{-\lfloor k/m \rfloor} = g^{k \bmod m} \in \mathbb{H}$.
By choice of m, we must have $k \bmod m = 0$ and thus $a = 1$ – contradiction.

▷ **Corollary**: If $\mathbb{H} \leq \langle a \rangle \leq \mathbb{G}$, then $\mathbb{H}$ is cyclic.

- As we will see later (Chinese remainder theorem), we can decompose large groups into the so called direct product of two or more smaller groups.
- **Definition**:

  Let $\langle \mathbb{G}_1, \cdot_1, 1_1 \rangle, \langle \mathbb{G}_2, \cdot_2, 1_2 \rangle$ be two groups.

  Their direct product $\langle \mathbb{G}_1 \times \mathbb{G}_2, \cdot, 1 \rangle$ is defined by:

  Carrier: $\mathbb{G}_1 \times \mathbb{G}_2 := \{(a_1, a_2) \mid a_1 \in \mathbb{G}_1, a_2 \in \mathbb{G}_2\}$.

  Group operation: $(a_1, a_2) \cdot (b_1, b_2) := (a_1 \cdot_1 b_1, a_2 \cdot_2 a_2)$

  Neutral element: $1 := (1_1, 1_2)$
- **Lemma**: The direct product is again a group.

▷ Proof: Obvious – we simply compute in both groups in parallel.

- $\mathbb{Z} \hat{=} \langle \mathbb{Z}, +, 0 \rangle$

▷ Infinite.

▷ Group operation: canonical addition.

▷ Cyclic: generated by $1, -1$.

- **Reminder**:

  For additive groups (group operation denoted by $+$), the inverse is denote by $-a$,

  and $\langle a \rangle$ becomes:

$$\ldots, \underbrace{(-a) + (-a) + (-a)}_{3 \cdot (-a)}, (-a) + (-a), (-a), 0, a, a + a, a + a + a, \ldots$$

▷ Here: $\langle 2 \rangle = \{2k \mid k \in \mathbb{Z}\} = 2\mathbb{Z}$.

- Let $N > 2$ be a natural number.
- $\mathbb{Z}_N \hat{=} \langle \mathbb{Z}_N, +_N, 0 \rangle$

▷ Group operation: canonical addition on $\mathbb{Z}$ modulo N,
i.e. $a +_N b := (a + b) \bmod N$.
(We simply write $+$ for $+_N$ if not misleading.)

▷ Inverse: $-a = N - a$ in $\mathbb{Z}_N$.

▷ Cyclic: $\langle g \rangle = \mathbb{Z}_N$ iff $\text{gcd}(g, N) = 1$. (later)

▷ **Ex**: Compute $\langle 4 \rangle$ in $\mathbb{Z}_7$.

▷ **Ex**: Compute $\langle 4 \rangle$ in $\mathbb{Z}_6$.

▷ **Ex**: Compute $\langle (1, 1) \rangle$ in $\mathbb{Z}_4 \times \mathbb{Z}_6$.

▷ $Z_M \times \mathbb{Z}_N$ is cyclic iff $\text{gcd}(M, N) = 1$.

- Let $N > 1$ be a natural number.
- $\mathbb{Z}_N^* \hat{=} \langle \{a \in \mathbb{Z}_N \mid \mathsf{gcd}(a, N) = 1\}, \cdot_N, 1\rangle$.

▷ Group operation: canonical multiplication on $\mathbb{Z}$ modulo N,
i.e. $a \cdot_N b := (a \cdot b) \bmod N$.
(We simply write $\cdot$ for $\cdot_N$ if not misleading.)

▷ Inverse: As $\mathsf{gcd}(a, N) = 1$ there are x, y s.t. $1 = xa + yN$,
hence $a^{-1} = (x \bmod N)$ in $\mathbb{Z}_N^*$.

▷ **Theorem**: (w/o proof)
$\mathbb{Z}_N^*$ is cyclic iff $N \in \{2, 4, p^r, 2p^r\}$ for $p > 2$ prime and $r > 0$.

▷ **Ex**: Compute $\langle 4\rangle$ and $\langle 5\rangle$ in $\mathbb{Z}_7^*$.

▷ **Ex**: Compute $\langle 5\rangle$ in $\mathbb{Z}_6^*$.

▷ **Ex**: Compute $\langle 3\rangle$ in $\mathbb{Z}_8^*$.

- Let $N > 1$ be a natural number.
- The equivalence class of $a \in \mathbb{Z}$ w.r.t. $\equiv_N$ is denoted by $[a]_N := \{a + zN \mid z \in \mathbb{Z}\}$ and called the residue class of $a \in \mathbb{Z}$ modulo N,
- Set $\mathbb{Z}/N\mathbb{Z} := \{[a]_N \mid a \in \mathbb{Z}\}$, $(\mathbb{Z}/N\mathbb{Z})^* := \{[a]_N \mid a \in \mathbb{Z}, \gcd(a, N) = 1\}$
- Define $[a]_N + [b]_N := [a + b]_N$ and $[a]_N \cdot [b]_N := [a \cdot b]_N$.
- **Reminder**: Then
  - $\mathbb{Z}/N\mathbb{Z} = \{[a]_N \mid a \in \mathbb{Z}_N\}$ and $(\mathbb{Z}/N\mathbb{Z})^* = \{[a]_N \mid a \in \mathbb{Z}_N^*\}$.
  - $[a +_N b]_N = [a + b]_N$ and $[a \cdot_N b]_N = [a \cdot b]_N$
    ($\equiv_N$ is a congruence)

  $\mathbb{Z}_N$ and $\mathbb{Z}/N\mathbb{Z}$ resp. $\mathbb{Z}_N^*$ and $(\mathbb{Z}/N\mathbb{Z})^*$ are the "same" (isomorphic).

▷ Most of the time, it is easier to compute in $\mathbb{Z}/N\mathbb{Z}$ and only reduce the result to $\mathbb{Z}_N$ at the very end.

▷ **Ex**: $994 \cdot 995 \cdot 996 \equiv_{997} (-3) \cdot (-2) \cdot (-1) = -6 \equiv_{997} 991$

▷ We won't distinguish between $\mathbb{Z}_N$ and $\mathbb{Z}/N\mathbb{Z}$ resp. $\mathbb{Z}_N^*$ and $(\mathbb{Z}/N\mathbb{Z})^*$ in the following.

- Let $N > 1$ be a natural number.
- $\mathbb{QR}_N \hat{=} \langle \{x^2 \bmod N \mid x \in \mathbb{Z}_N^*\}, \cdot, 1\rangle$

▷ Subgroup of $\mathbb{Z}_N^*$.

▷ In general not cyclic. Cyclic if $\mathbb{Z}_N^*$ is cyclic.

▷ **Ex**: Compute $\langle 4 \rangle$ in $\mathbb{QR}_7$.

▷ **Ex**: Compute $\mathbb{QR}_6$, $\mathbb{QR}_8$, $\mathbb{QR}_{85}$.

- We are only interested in finite commutative groups in this lecture.
- For these, many things can be shown more easily than in the general setting.
- Let $\mathbb{G}$ be finite and commutative.

▷ Obviously, the map $f_a\colon \mathbb{G} \to \mathbb{G}\colon x \mapsto ax$ is bijective for any $a \in \mathbb{G}$.

▷ Hence: $\mathbb{G} = \{f_a(x) \mid x \in \mathbb{G}\}$ and

$$c := \prod_{x\in\mathbb{G}} x = \prod_{x\in\mathbb{G}} f_a(x) = \prod_{x\in\mathbb{G}} ax = a^{|\mathbb{G}|} \prod_{x\in\mathbb{G}} x = a^{|\mathbb{G}|} c$$

▷ **Lemma**: For $\mathbb{G}$ a finite commutative group: $\forall a \in \mathbb{G}\colon a^{|\mathbb{G}|} = 1$.

▷ **Corollary**: $\forall a \in \mathbb{G}\colon a^{|\langle a\rangle|} = 1$.

▷ **Remark**: The results is also valid for non-commutative finite groups (see Lagrange's theorem)

- **Lemma**: Let
  - $\mathbb{G}$ be a finite group and
  - λ any positive natural number s.t. $\forall a \in \mathbb{G}\colon a^{\lambda} = 1$.
  - ▷ For instance, choose $\lambda = |\mathbb{G}|$ (if $\mathbb{G}$ is commutative).

  Then $\forall a \in G$:
  1. $a^{\lambda-1} = a^{-1}$.
  2. $\langle a \rangle = \{a^0, a^1, \ldots, a^{\lambda-1}\} = \{a^k \mid k \in \mathbb{Z}_\lambda\}$ and $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}_{|\langle a \rangle|}\}$
  3. $a^k = a^{k \bmod \lambda}$ and $a^k = a^{k \bmod |\langle a \rangle|}$ for all $k \in \mathbb{Z}$
  4. $\lambda \bmod |\langle a \rangle| = 0$ i.e. $|\langle a \rangle| \mid \lambda$
  5. If $\lambda \geq |\mathbb{G}|$ is prime, then $\mathbb{G}$ is cyclic.
- **Ex**: Compute 7^{1023} and 7^{-1} in $\mathbb{Z}_{11}^*$.

- Proof:
  1. $a^{\lambda-1}a = a^{\lambda} = 1$ by assumption on λ so $a^{-1} = a^{\lambda-1}$.
  2. As $a^{-1} = a^{\lambda-1}$ also $a^{-k} = a^{k(\lambda-1)}$ so it suffices to only consider nonnegative powers of a, i.e. $\langle a \rangle = \{a^k \mid k \in \mathbb{N}_0\}$.

     Using $a^{\lambda} = 1$ any product/term of k copies of a is reduced to a product of $k \bmod \lambda$ copies.

     In particular, this is true for $\lambda = |\langle a \rangle|$ as $\langle a \rangle$ is itself a group.
  3. See (2) – recall that $-k \equiv_{\lambda} (\lambda - 1)k$.
  4. As $1 = a^{\lambda} = a^{\lambda \bmod |\langle a \rangle|}$.
  5. If λ is prime, then either $|\langle a \rangle| = 1$ (i.e. $a = 1$) or $|\langle a \rangle| = \lambda \geq |\mathbb{G}|$, i.e. $\langle a \rangle = \mathbb{G}$. (Note: we may have $\lambda < |\mathbb{G}|$, e.g. $\langle \mathbb{Z}_8^*, \cdot, 1 \rangle$.)

- **Definition**: The exponent $\lambda_{\mathbb{G}}$ of a group $\mathbb{G}$ is the smallest positive integer λ s.t. $\forall a \in \mathbb{G}\colon a^\lambda = 1$.
  If $\mathbb{G} = \mathbb{Z}_N^*$, then $\lambda(N) := \lambda_{\mathbb{Z}_N^*}$ is called Carmichael function.

▷ **Corollary**: $\lambda_{\mathbb{G}} = \mathrm{lcm}\{\mathrm{ord}(a) \mid a \in \mathbb{G}\}$ and $\lambda_{\mathbb{G}} \mid |\mathbb{G}|$

▷ **Remark**: If $\mathbb{G}$ is cyclic, then obviously $\lambda_{\mathbb{G}} = |\mathbb{G}|$;
in particular, if $\mathbb{G}$ is finite, then $|\langle a \rangle| = \lambda_{\langle a \rangle}$ for any $a \in \mathbb{G}$.
One can show: if $\mathbb{G}$ is finite and commutative and $\lambda_{\mathbb{G}} = |\mathbb{G}|$, then $\mathbb{G}$ is cyclic.

▷ **Ex**: Compute the exponent of (1) $\mathbb{Z}_6$, (2) $\mathbb{Z}_8^*$, (3) $\mathbb{Z}_{10} \times \mathbb{Z}_6$.

- **Lemma**: Let $\mathbb{G}$ be finite and commutative, and $k \in \mathbb{Z}$.
  Set $g_e \colon \mathbb{G} \to \mathbb{G} \colon x \mapsto x^k$. Then:
  1. $g_k(x) := x^k$ is a permutation on $\mathbb{G}$ iff $\gcd(k, \lambda_{\mathbb{G}}) = 1$.
  2. If g_k is a permutation, there are $e, d \in \mathbb{Z}_{\lambda_{\mathbb{G}}^*}$ s.t. $g_k = g_e$ and $g_k^{-1} = g_d$.
  3. $|\{g_k \mid k \in \mathbb{Z} \text{ s.t. } g_k \text{ is bijective}\}| = \left|\mathbb{Z}_{\lambda_{\mathbb{G}}}^*\right|$

▷ This is the algebraic essence of RSA:
e is the encryption exponent, d is the decryption exponent.
In order to compute g_e, one has to know e and how to compute in $\mathbb{G}$.
Necessary requirement: "Computing d from e and $\mathbb{G}$ has to be hard."

▷ **Ex**: Show that if $e \in \mathbb{Z}_{|\mathbb{G}|}^*$, then g_e is also a permutation on $\mathbb{G}$.
But there might be an $e' \in \mathbb{Z}_{|\mathbb{G}|}^*$ with $e \neq e'$ and yet $g_e = g_{e'}$.

▷ **Proof**:

1. As $\mathbb{G}$ is finite, g_e is bijective iff it is injective.
   We have: $g_e(x) = g_e(y)$
   iff $(xy^{-1})^e = 1$ (as $\mathbb{G}$ is commutative)
   iff $e \bmod \left|\langle xy^{-1}\rangle\right| = 0$
   iff $\mathsf{gcd}(e, \lambda_{\mathbb{G}}) \geq \left|\langle xy^{-1}\rangle\right|$
   As $\left|\langle xy^{-1}\rangle\right| = 1$ iff $x = y$, the claim follows.
2. Pick $e := (k \bmod \lambda_{\mathbb{G}})$ and $d \in \mathbb{Z}^*_{\lambda_{\mathbb{G}}}$ s.t. $ed \equiv_{\lambda_{\mathbb{G}}} 1$
3. We have:
   $\forall x \in \mathbb{G}\colon g_k(x) = g_k(x)$ iff $\forall x \in \mathbb{G}\colon x^{k-l} = 1$ iff $\lambda_{\mathbb{G}} \mid k - l$ iff $k \equiv_{\lambda_{\mathbb{G}}} l$

- Often we know that a group is cyclic, e.g. as its order is a prime.

▷ But we still need to find some generator.

▷ Idea: use again rejection sampling

  - Choose a group element $a \overset{u}{\in} \mathbb{G}$ uniformaly at random.

  ▷ For $\mathbb{G} = \mathbb{Z}_N^*$, you can also use rejection sampling here:

  Choose $a \overset{u}{\in} \mathbb{Z}_N$ and reject it if $\mathsf{gcd}(a, N) > 1$.

  - Test if a is a generator.

▷ This works quite well if

(1) we hit a generator with high prob. (enough generators) and

(2) we can efficiently test if a is a generator.

▷ First: How to test if a is generator.

▷ Then: How many generators has a cyclic group?

- **Lemma**: Let $\mathbb{G}$ be a finite group of order M.
  Then: $\langle a \rangle = \mathbb{G}$ iff $a^{M/p} \neq 1$ for every prime $p \mid M$.
- Proof:
- ▷ ($\Rightarrow$) Assume $\langle a \rangle = \mathbb{G}$. Then $\mathsf{ord}(a) = M = \min\{k > 0 \mid a^k = 1\}$.
- ▷ ($\Leftarrow$) Assume $\langle a \rangle \neq \mathbb{G}$, i.e. $\mathsf{ord}(a) < M$.
  - ▷ As $\mathsf{ord}(a) \mid M$, there is a $m > 1$ s.t. $M = m \cdot \mathsf{ord}(a)$.
  - ▷ Choose any $p|m$ s.t. $m = m'p$. Then: $a^{M/p} = a^{m' \cdot \mathsf{ord}(a)} = 1$.
- **Remark**: There are at most $\log_2 M$ distinct primes p with $p \mid M$.
- **Remark**: When the prime factors of M are unknown, no efficient generator test is known.
- ▷ **Corollary**: $\langle a \rangle = \mathbb{Z}_N$ iff $\mathsf{gcd}(a, N) = 1$.
- ▷ Proof: The generator test becomes "$\langle a \rangle \neq \mathbb{Z}_N$ iff $\mathsf{gcd}(a, N) > 1$".

- First question: How many generators has $\mathbb{Z}_N$?

▷ As just seen: $\langle a \rangle = \mathbb{Z}_N$ iff $\gcd(a, N) = 1$.

▷ So $\mathbb{Z}_N^*$ is exactly the set of all generators of $\mathbb{Z}_N$ (!).

▷ Euler's φ-function: $\varphi(N) := |\mathbb{Z}_N^*|$.

- **Lemma**:
  $\varphi(p^r) = p^{r-1}(p-1)$ for any prime p and $r > 0$.
  $\varphi(MN) = \varphi(M) \cdot \varphi(N)$ if $\gcd(M, N) = 1$.

- Proof:

▷ First claim: $\gcd(a, p^r) > 1$ iff $a = p \cdot s$ with $s \in \mathbb{Z}_{p^{r-1}}$.

▷ Second claim follows from the Chinese remainder theorem (later).

- **Ex**: Compute $\varphi(57)$.

- **Ex**: How many generators has $\mathbb{Z}_{100}$?

- **Ex**: Let $N = pq$ for $p \neq q$ distinct odd primes.

  Show: Given N and $\varphi(N)$, we can compute p, q efficiently.

  That is: if factoring N is hard, then so is computing $\varphi(N)$.

▷ So, in general computing $\varphi(N)$ is infeasible for large N if we do not know a factorization of N.

- Second question: How many generators has a finite cyclic group $\langle g \rangle = \mathbb{G}$?

▷ Let $M = |\mathbb{G}|$. Then $\mathbb{G}$ is isomorphic to $\mathbb{Z}_M$ by means of $h\colon Z_M \to \mathbb{G}\colon k \mapsto g^k$.

  - **Remark**: Isomorphic groups $\mathbb{G}_1 \cong \mathbb{G}_2$ are "the same" w.r.t. the group properties.

    From a computational point of view, computing in $\mathbb{G}_1$ (e.g. $\mathbb{Z}_M$) can still be much easier than in $\mathbb{G}_2$.

    See the discrete logarithm problem later.

▷ So:

Lemma: A cyclic group $\mathbb{G}$ has exactly $\varphi(|\mathbb{G}|)$ many generators.

- **Ex**: How many generators has $\mathbb{Z}_{85}^*$?
- **Ex**: Is 7 a generator of $\mathbb{Z}_{54}^*$? What is the prob. that $a \overset{u}{\in} \mathbb{Z}_{54}^*$ is a generator?

- Second question:

  How many generators has a finite cyclic group $\langle g \rangle = \mathbb{G}$?

▷ **Definition**: Let $\langle \mathbb{G}_1, \cdot_1, 1_1 \rangle$, $\langle \mathbb{G}_2, \cdot_2, 1_2 \rangle$ be two groups.

A map $h \colon \mathbb{G}_1 \to \mathbb{G}_2$ is a homomorphism if it respects the group operations i.e.

$$h(a \cdot_1 b) = h(a) \cdot_2 h(b)$$

If h is a homorphism and bijective, then it is called an isomorphism, and $\mathbb{G}_1$ and $\mathbb{G}_2$ are called ismorphic (short: $\mathbb{G}_1 \cong \mathbb{G}_2$).

- **Lemma**: If $h\colon \mathbb{G}_1 \to \mathbb{G}_2$ is a homomorphism, then
  1. $h(1_1) = 1_2$
  2. $h(a^{-1}) = h(a)^{-1}$
  3. $h(\mathbb{G}_1) \leq \mathbb{G}_2$.

▷ Proof:

$$\begin{array}{rcl}
1_2 = h(1_1) \cdot_2 h(1_1)^{-1} & = & h(1_1 \cdot_1 1_1) \cdot_2 h(1_1)^{-1} \\
& = & h(1_1) \cdot_2 h(1_1) \cdot_2 h(1_1)^{-1} = h(1_1) \\
h(a)^{-1} = h(a)^{-1} \cdot_2 1_2 & = & h(a)^{-1} \cdot_2 h(a \cdot_1 a^{-1}) \\
& = & h(a)^{-1} \cdot_2 h(a) \cdot_2 h(a^{-1}) = h(a^{-1}) \\
h(a) \cdot_2 h(b)^{-1} & = & h(a \cdot_1 b^{-1}) \in \mathbb{H}
\end{array}$$

- **Lemma**: If $h\colon \mathbb{G}_1 \to \mathbb{G}_2$ is an isomorphism, then
  1. Also the inverse map $h^{-1}\colon \mathbb{G}_2 \to \mathbb{G}_1$ is an isomorphism.
  2. $\langle g \rangle = \mathbb{G}_1$ iff $\langle h(g) \rangle = \mathbb{G}_2$.
  3. Both groups have the same number of generators.

▷ Proof:
  1. $h^{-1}(h(a) \cdot_2 h(b)) = h^{-1}(h(a \cdot_1 b)) = a \cdot_1 b = h^{-1}(h(a)) \cdot_2 h^{-1}(h(b))$
  2. If $\langle g \rangle = \mathbb{G}_1$, then $\langle h(g) \rangle = h(\langle g \rangle) = h(\mathbb{G}_1) = \mathbb{G}_2$, and analogously for h^{-1}.
  3. Follows from (3).

- **Lemma**: Let $\mathbb{G} = \langle g \rangle$ be a finite cyclic group.

  Then $\mathbb{G}$ is isomorphic to $\langle \mathbb{Z}_N, +, 0 \rangle$ for $N = |\mathbb{G}|$ via

$$h\colon \mathbb{Z}_N \to \mathbb{G}\colon k \mapsto g^k$$

- **Lemma**: Let $\mathbb{G} = \langle g \rangle$ be a finite cyclic group.
  Then $\mathbb{G}$ is isomorphic to $\langle \mathbb{Z}_N, +, 0 \rangle$ for $N = |\mathbb{G}|$ via

$$h \colon \mathbb{Z}_N \to \mathbb{G} \colon k \mapsto g^k$$

▷ Proof: $N = \lambda_{\mathbb{G}} = \min\{\lambda > 0 \colon g^\lambda = 1\}$.

▷ **Corollary**:
  A finite cyclic group $\mathbb{G}$ has exactly $\varphi(|\mathbb{G}|)$ many generators.

- **Ex**: How many generators has $\mathbb{Z}_{85}^*$?
- **Ex**: Is 7 a generator of $\mathbb{Z}_{54}^*$? What is the prob. that $a \overset{u}{\in} \mathbb{Z}_{54}^*$ is a generator?

- **Theorem**: Let M, N be coprime, i.e. $\mathsf{gcd}(M, N) = 1$.
  Then (i) $\mathbb{Z}_{MN} \cong \mathbb{Z}_M \times \mathbb{Z}_N$ and (ii) $\mathbb{Z}^*_{MN} \cong \mathbb{Z}^*_M \times \mathbb{Z}^*_N$.
  by means of $h\colon \mathbb{Z}_{MN} \to \mathbb{Z}_M \times \mathbb{Z}_N : a \mapsto (a \bmod M, a \bmod N)$.
  For $\alpha, \beta \in \mathbb{Z}$ s.t. $1 = \alpha M + \beta N$:
  $h^{-1}(u, v) = (u\beta N + v\alpha M) \bmod MN$.
- **Remark**: α, β can be computed using the extended Euclidean algorithm.
- CRT short for "chinese remainder theorem".

- Proof:
- **Ex**: Show
  - $(a \bmod MN) \mod M = a \bmod M$.

  Conclude:
  - $((a+b) \bmod MN) \bmod M = (a+b) \bmod M$ and
  - $((ab) \bmod MN) \bmod M = ab \bmod M$.
- **Ex**: Show
  - $(a+b) \bmod M = ((a \bmod M) + (b \bmod M)) \bmod M$ and
  - $ab \bmod M = ((a \bmod M)(b \bmod M)) \bmod M$.

  Conclude:
  - $h(a+b) = h(a) + h(b)$ and $h(ab) = h(a)h(b)$.
- **Ex**: Check that h^{-1} (as defined in the theoem) is the inverse map of h.
- **Ex**: Show $h(\mathbb{Z}_{MN}^*) = \mathbb{Z}_M^* \times \mathbb{Z}_N^*$

- **Corollary**:

  Let $N = \prod_{i=1}^{r} p_i^{e_i}$ be a prime factorization of N.

  Then: $\mathbb{Z}_N^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \mathbb{Z}_{p_2^{e_2}}^* \times \ldots \times \mathbb{Z}_{p_r^{e_r}}^*$.

  Thus $\varphi(N) = \prod_{i=1}^{r} \varphi(p_i^{e_i}) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1)$.

- **Remark**: The CRT allows us to compute within $\mathbb{Z}_M \times \mathbb{Z}_N$ instead of $\mathbb{Z}_{MN}$, i.e. we may compute with smaller numbers.

  This can be used to speed-up the decryption of RSA-based PKES (later).

▷ **Ex**: Let $p = 13, q = 19$ and $N = pq = 247$.

Compute 197^{200} in $\mathbb{Z}_N^*$ using the CRT.

- **Reminder**:
  $\lambda_{\mathbb{G}}$ is the least positive integer λ s.t. $\forall a \in \mathbb{G}$: $a^\lambda = 1$.
  For $\mathbb{G} = \mathbb{Z}_N^*$: $\lambda(N) := \lambda_{\mathbb{Z}_N^*}$ (Carmichael function).

▷ By the CRT: If $N = \prod_{i=1}^r p_i^{e_i}$ (prime factorization),
then $\mathbb{Z}_N^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \mathbb{Z}_{p_2^{e_2}}^* \times \ldots \times \mathbb{Z}_{p_r^{e_r}}^*$.
Hence: $\lambda(N) = \mathsf{lcm}(\lambda(p_1^{e_1}), \ldots, \lambda(p_r^{e_r}))$.

▷ Recall: $\mathbb{Z}_N^*$ is cyclic iff $N \in \{2, 4, p^r, 2p^r\}$ ($p > 2$ prime,$r > 0$).
Hence: $\lambda(p^r) = \varphi(p^r)$ if p is a odd prime.

▷ What about $\mathbb{Z}_{2^k}^*$?
One can show: $\mathbb{Z}_{2^k}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$ for $k > 2$.

▷ Hence: $\lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(2^k) = 2^{k-2}$ for $k > 2$.

▷ 2 is the "oddest" prime.

- Recall: $\mathbb{QR}_N := \{x^2 \bmod N \mid x \in \mathbb{Z}_N^*\}$ is the set of quadratic residues modulo N.

  $\mathbb{QR}_p$ will be important later for the Elgamal PKES.

- **Lemma**: $\mathbb{QR}_N \leq \mathbb{Z}_N^*$.

▷ Proof: $1 \in \mathbb{QR}_N$ and it is closed under multiplication.

- **Corollary**: $\mathbb{QR}_p$ is cyclic for any prime p.

- **Ex**: $\mathbb{QR}_N$ can be cyclic although $\mathbb{Z}_N^*$ is acyclic (e.g. $N = 15$).

- **Remark**: Let $N = \prod_{i=1}^{r} p_i^{e_i}$ be a prime factorization of N. From the CRT it follows:

  $x^2 \equiv y \pmod{N}$ iff $\forall i \in [r]$: $x^2 \equiv y \pmod{p_i^{e_i}}$.

  That is: $\mathbb{QR}_N \cong \mathbb{QR}_{p_1^{e_1}} \times \ldots \times \mathbb{QR}_{p_r^{e_r}}$.

▷ **Ex**: Modulo a composite $N = pq$ (both prime), every $y \in \mathbb{QR}_N$ has at least four square roots. Hence: $|\mathbb{QR}_N| \leq \varphi(N)/4$.

- **Lemma**: Let $p > 2$ be prime.

  Then every $y \in \mathbb{QR}_p$ has exactly two square roots modulo p.

▷ Proof: **Ex**

  Hint: recall that $u^2 - v^2 = (u+v)(u-v)$.

▷ **Corollary**: $x^{\frac{p-1}{2}} \equiv_p \pm 1$ for p prime and $\left|\mathbb{QR}_p\right| = (p-1)/2$.

- **Remark**: Let p be prime with $p \equiv 3 \pmod{4})$ (e.g. a safe prime).

  Then: $(x^2)^{\frac{p+1}{4}} \equiv_p x^{\frac{p+1}{2}} \equiv_p x^{\frac{p-1}{2}} \cdot x \equiv_p \pm x$.

  Computing a square root of x^2 in the case $p \equiv 1 \pmod{4}$ is more difficult, see e.g. here.

- **Definition**: Let $p > 2$ be prime.
  $\left(\frac{x}{p}\right) := x^{\frac{p-1}{2}} \bmod p$ is the Legendre symbol modulo p.
- **Lemma**: Let $p > 2$ be prime, and $y \in \mathbb{Z}_p^*$. Then:
  $\left(\frac{y}{p}\right) = -1$ iff $y \in \mathbb{Z}_p^* \setminus \mathbb{QR}_p$, and $\left(\frac{y}{p}\right) = 1$ iff $y \in \mathbb{QR}_p$.
- Proof: **Ex**
  Hint: Let $\langle g \rangle = \mathbb{Z}_p^*$ and show that $g^{\frac{p-1}{2}} \equiv_p -1$.

- **Note**: Let p be prime.
  Then $\mathbb{Z}_p^*$ has $\varphi(\varphi(p))$ many generators.
  While computing $\varphi(p) = p - 1$ is trivial,
  computing $\varphi(\varphi(p)) = \varphi(p-1)$ requires a factorization of $p - 1$.
  One possible solution: Use safe primes.
- **Definition**: A prime $p > 5$ is safe iff $p = 2q + 1$ with q prime.
  (q is called a Sophie-Germain prime.)

- **Ex**: For $p = 2q + 1$ a safe prime, $\Pr_{a \overset{u}{\in} \mathbb{Z}_p^*}\left[\langle a \rangle = \mathbb{Z}_p^*\right] = \frac{1}{2} - \frac{1}{2q}$.
- **Ex**: Let $p = 2q + 1$ be a safe prime and $a \in \mathbb{Z}_p^*$.
  Then $\langle a^2 \rangle = \mathbb{QR}_p$ if $a^2 \not\equiv_p 1$, i.e. $\Pr_{a \overset{u}{\in} \mathbb{Z}_p^*}\left[\langle a^2 \rangle = \mathbb{QR}_p\right] = 1 - \frac{1}{q}$.
- **Ex**: Compute all solutions of $X^2 \equiv_{221} 118$.
- **Ex**: Is 6 a quadratic residue modulo 47?
  If so, compute its square roots.

1 Lecture 12-14 – Group theory

- **Theorem** (w/o proof, see e.g. here):
  Let $\pi(x) = |\{p \leq x \mid p \text{ is prime }\}|$. Then: $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$.
- **Lemma** (w/o proof, see e.g. here): For $x \geq 355991$:

$$\frac{x}{\ln x}\left(1 + \frac{1}{\ln x}\right) < \pi(x) < \frac{x}{\ln x}\left(1 + \frac{1}{\ln x} + \frac{2.51}{(\ln x)^2}\right).$$

- **Ex**: Use above lemma to show that there are at least $0.6\frac{2^n}{n}$ primes in $[2^{n-1}, 2^n - 1]$ ("n-bit primes") if $n \geq 20$.
- **Conjecture**: (Hardy,Littlewood)
  Let $\pi_s(x) = \{p \leq x \mid p \text{ is a Sophie-Germain prime }\}$.
  Then: $\pi_s(x) \approx 1.32\frac{x}{(\ln x)^2}$.

- **Ex**: Let $n \geq 20$.

  As Primes is in $\mathbf{P}$ we can use rejection sampling for generating random primes uniformly distributed in $[2^{n-1}, 2^n - 1]$:

  - Choose $x \overset{u}{\in} \{0,1\}^{n-2}$.
  - Read $1||x||1$ as an odd integer a in $[2^{n-1}, 2^n - 1]$.
  - If a is not a prime, go back to step 1; else return a.

  Show that the prob. that we haven't found a prime within $r := n^2$ rounds is negligible.

  Hint: $(1 - 1/x)^x \leq e^{-x}$ for all $x \geq 1$.

  Ex: If the estimate on the number of Sophie-Germain primes is asympt. correct, we can also generate in this way safe primes (for $r \approx n^3$).

- While the AKS primality test runs in DPT, in practice, the probabilistic Miller-Rabin test is still used more often as it faster, and its prob. to give a false answer is negligible.

▷ It is based on the following results:

(i) $a^M = 1$ for all $a \in \mathbb{G}$ if $\mathbb{G}$ is of finite order M.

(ii) $\mathbb{Z}_N^*$ is a finite group of order $\varphi(N)$.

(iii) $\varphi(N) = N - 1$ iff N is prime.

(iv) For $p > 2$ prime: $x^2 \equiv_p 1$ iff $x \equiv_p \pm 1$.

- **Lemma**: Let $p > 2$ be prime with $p - 1 = 2^t d$ with d odd and $t > 0$. Then $\forall a \in \mathbb{Z}_p^* \forall k = 0, 1, \ldots, t-1\colon a^{2^{k+1}d} \equiv_p 1 \rightarrow a^{2^k d} \equiv_p \pm 1$.

▷ Proof: ± 1 are the only two roots of 1 modulo a prime.

▷ **Corollary**: Let $N - 1 = 2^t d$ with d odd. If there is a k s.t. $a^{2^{k+1}d} \equiv_N 1$ and $a^{2^k d} \not\equiv \pm 1$, then N is not prime.

- Miller-Rabin test (simple version):
  - Assume $N > 2$ is prime.
  - Repeat r times:
    - Choose $a \overset{u}{\in} \mathbb{Z}_N \setminus \{0\}$
    - Check that indeed $\mathsf{gcd}(a, N) = 1$.
    - Check that $a^{N-1} \equiv_N 1$.
    - Check that the lemma holds.

- **Definition**: Input: odd integer $N > 2$ and number of rounds $r > 0$
  If $\sqrt{N} \in \mathbb{N}$, return "composite"; //N is a square
  Compute $t = \max\{k \in \mathbb{N}_0 \colon (N-1) \bmod 2^k = 0\}$
  (*) for $i = 1 \ldots r$:

      choose $a \overset{u}{\in} \{2, \ldots, N-2\}$;
      if $\gcd(a, N) \neq 1$, return "composite"; //$\mathbb{Z}_N^* \neq \{1, 2, \ldots, N-1\}$
      if $a^d \equiv_N \pm 1$, goto (*); //Lemma satisfied, N might be prime
      for $j = 1 \ldots t-1$:
          if $a^{2^j d} \equiv_N 1$, return "composite"; //$a^{2^{j-1} d} \not\equiv_N \pm 1$, but a root of 1
          if $a^{2^j d} \equiv_N -1$, goto (*); //Lemma satisfied, N might be prime
      return "composite";

  return "probably prime";

- Assume N is a odd (non square) composite, i.e. $N \geq 15$.

  Then N passes one round of the test if by chance

  $a \in \mathsf{Bad} := \{a \in \mathbb{Z}_N^* \mid a^d \equiv_N \pm 1 \vee \exists 0 < j < t\colon a^{2^j d} \equiv_N -1\}$.
- **Ex**: Determine Bad for $N = 15$ (use the CRT).
- **Lemma** (see e.g. here): $|\mathsf{Bad}| \leq \frac{1}{4}\varphi(N)$.

▷ **Corollary** An odd composite passes r rounds of the Miller-Rabin test with prob. at most 4^{-r}.

- **Remark**: Use repeated squaring to compute $a^d \pmod N$;

  after that only squaring required.

  The total running time becomes $\mathcal{O}(r(\log_2 N)^3)$.