Groups

- A group \((\mathbb{G}, \star)\) consists of a group \(\mathbb{G}\) together with an operation \(\star\) with the following properties:
  - **Closure**: If \(g, h \in \mathbb{G}\), then \(g \star h \in \mathbb{G}\).
  - **Associativity**: For all \(g, h, k \in \mathbb{G}\), \(g \star (h \star k) = (g \star h) \star k\).
  - **Identity**: There exists an (unique) element \(e \in \mathbb{G}\) such that for all \(g \in \mathbb{G}\), \(e \star g = g = g \star e\).
  - **Inverse**: For every element \(g \in \mathbb{G}\), there exists an (unique) element \(h \in \mathbb{G}\) where \(g \star h = e = h \star g\).

- A group \((\mathbb{G}, \star)\) is **commutative** (or abelian) if for all \(g, h \in \mathbb{G}\), \(g \star h = h \star g\).

- **Notation**: Unless otherwise noted, we will denote the group operation by ‘·’ (i.e., multiplicative notation). If \(g, h \in \mathbb{G}\), we write \(gh\) to denote \(g \cdot h\). For a group element \(g \in \mathbb{G}\), we write \(g^0\) and 1 to denote the identity element. For a positive integer \(k\), we write \(g^k\) to denote the inverse of \(g\). We write \(g^k\) to denote
  \[g^k := g \cdot g \cdots g.\]
  \[\underbrace{g \cdot g \cdots g}_{k \text{ copies}}\]
  For a negative integer \(k\), we write \(g^{-k}\) to denote \((g^k)^{-1}\).

- A group \(\mathbb{G}\) is **cyclic** if there exists a generator \(g\) such that \(\mathbb{G} = \{g^0, \ldots, g^{\mid \mathbb{G} \mid - 1}\}\).

- For an element \(g \in \mathbb{G}\), we write \(\langle g \rangle := \{g^0, g^1, \ldots, g^{\mid \mathbb{G} \mid - 1}\}\) to denote the **subgroup generated by** \(g\). The **order** \(\text{ord}(g)\) of \(g\) in \(\mathbb{G}\) is the size of the subgroup generated by \(g\): \(\text{ord}(g) := \mid \langle g \rangle \mid\). The order of the group \(\mathbb{G}\) is the size of the group: \(\text{ord}(\mathbb{G}) = \mid \mathbb{G} \mid\).

- **Lagrange’s theorem**: For a group \(\mathbb{G}\) and any element \(g \in \mathbb{G}\), the order of \(g\) divides the order of the group: \(\text{ord}(g) \mid \mid \mathbb{G} \mid\).

- If \(\mathbb{G}\) is a group of prime order, then \(\mathbb{G} = \langle g \rangle\) for every \(g \neq 1\) (i.e., every non-identity element of a prime-order group is a generator).

The Groups \(\mathbb{Z}_n\) and \(\mathbb{Z}_n^*\)

- We write \(\mathbb{Z}_n\) to denote the group of integers \(\mathbb{Z}_n := \{0, 1, \ldots, n - 1\}\) under addition modulo \(n\).

- We write \(\mathbb{Z}_n^*\) to denote the group of integers \(\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n : (\exists y \in \mathbb{Z}_n : xy = 1 \mod n)\}\) under multiplication modulo \(n\).

- **Bezout’s identity**: For all integers \(x, y \in \mathbb{Z}\), there exists integers \(s, t \in \mathbb{Z}\) such that \(xs + yt = \gcd(x, y)\).
  - Given \(x, y\), computing \(s, t\) can be computed in time \(O(\log |x| \cdot \log |y|)\) using the extended Euclidean algorithm.
An element $x \in \mathbb{Z}_n$ is invertible if and only if $\gcd(x, n) = 1$. This gives an equivalent characterization of $\mathbb{Z}_n^*$: $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}$. Computing an inverse of $x \in \mathbb{Z}_n^*$ can be done efficiently via the extended Euclidean algorithm.

For prime $p$, the group $\mathbb{Z}_p^* = \{1, 2, \ldots, p - 1\}$. The order of $\mathbb{Z}_p^*$ is $\left| \mathbb{Z}_p^* \right| = p - 1$. In particular $\mathbb{Z}_p^*$ is not a group of prime order (whenever $p > 3$). Computing the order of an element $g \in \mathbb{Z}_p^*$ is efficient if the factorization of the group order (i.e., $p - 1$) is known.

For a positive integer $n$, Euler’s phi function (also called Euler’s totient function) is defined to be the number of integers $1 \leq x \leq n$ where $\gcd(x, n) = 1$. In particular, $\varphi(n)$ is the order of $\mathbb{Z}_n^*$.

\[ \varphi(n) = n \cdot \prod_{i \in \mathbb{Z}} \left( 1 - \frac{1}{p_i} \right) = \prod_{i \in \mathbb{Z}} p_i^{k_i - 1}(p_i - 1). \]

Special cases of Lagrange’s theorem:

- **Fermat’s theorem**: For prime $p$ and $x \in \mathbb{Z}_p^*$, $x^{p-1} = 1 \pmod{p}$.
- **Euler’s theorem**: For a positive integer $n$ and $x \in \mathbb{Z}_n^*$, $x^{\varphi(n)} = 1 \pmod{n}$.

**Operations over Groups**

- Let $n$ be a positive integer. Take any $x, y \in \mathbb{Z}_n$. The following operations can be performed efficiently (i.e., in time $\text{poly}(\log n)$):
  - Sampling a random element $r \leftarrow \mathbb{Z}_n$.
  - Basic arithmetic operations: $x + y \pmod{n}$, $x - y \pmod{n}$, $xy \pmod{n}$, $x^{-1} \pmod{n}$. These operations suffice to solve linear systems.
  - Exponentiation: Computing $x^k \pmod{n}$ can be done in $\text{poly}(\log n, \log k)$ time using repeated squaring.

- Suppose $N = pq$ where $p, q$ are two large primes. Let $x \in \mathbb{Z}_n$. Then, the following problems are believed to be hard:
  - Finding the prime factors of $N$. This is equivalent to the problem of computing $\varphi(N)$.
  - Computing an $e^{th}$ root of $x$ where $\gcd(N, e) = 1$ (i.e., a value $y$ such that $x^e = y \pmod{N}$).

- Let $\mathbb{G}$ be a group of prime order $p$ with generator $g$. We often consider the following computational problems over $\mathbb{G}$:
  - **Discrete logarithm**: Given $(g, h)$ where $h = g^x$ and $x \leftarrow \mathbb{Z}_p$, compute $x$.
  - **Computational Diffie-Hellman (CDH)**: Given $(g, g^x, g^y)$ where $x, y \leftarrow \mathbb{Z}_p$, compute $g^{xy}$.
  - **Decisional Diffie-Hellman (DDH)**: Distinguish between $(g, g^x, g^y, g^{xy})$ and $(g, g^x, g^y, g^r)$ where $x, y, r \leftarrow \mathbb{Z}_p$. 

2