CS 346 Cryptography (Fall 2021) David Zuckerman

# Mathematical Background

## Functions

- A function $f : A \to B$ is *injective* if $f$ is one-to-one, i.e. $f(x) = f(y)$ implies $x = y$.
- A function $f : A \to B$ is *surjective* if $f$ is onto, i.e. for all $y \in B$ there exists $x \in A$ such that $f(x) = y$.
- A function $f$ is *bijective* if $f$ is both injective and surjective.

## Probability

- Probability and events:
  1. A *probability distribution* on a finite set $S$ is an assignment of probabilities $\Pr[x]$ to each element $x \in S$, where $\sum_{x \in S} \Pr[x] = 1$. The *uniform distribution* is the probability distribution where $\Pr[x] = 1/|S|$ for all $x \in S$.
  2. An *event* $T$ is a subset of $S$. We have $\Pr[T] = \sum_{x \in T} \Pr[x]$, but often this probability can be computed more directly.
  3. For any events $A, B$,
  $$\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B].$$
  4. *Union bound*: for any events $A_1, A_2, \ldots A_n$,
  $$\Pr[A_1 \cup A_2 \cup \ldots \cup A_n] \leq \Pr[A_1] + \Pr[A_2] + \ldots + \Pr[A_n].$$
  5. For *independent* events $A_1, A_2, \ldots A_n$,
  $$\Pr[A_1 \cap A_2 \cap \ldots \cap A_n] = \Pr[A_1] \cdot \Pr[A_2] \cdot \ldots \cdot \Pr[A_n].$$

- Conditional probability:

  1. The *conditional probability* of $A$ given $B$, denoted $\Pr[A|B]$, is the probability that $A$ occurs given that $B$ occurs. It satisfies

  $$\Pr[A|B] = \Pr[A \cap B] / \Pr[B].$$

  2. *Bayes' Law*:

  $$\Pr[A|B] = \frac{\Pr[A]\Pr[B|A]}{\Pr[B]}.$$

- Random variables:

  1. A *random variable* is a function on a probability space.
  2. Random variables $X_1, X_2, \ldots, X_n$ are *independent* if and only if for all $x_1, \ldots, x_n$, we have

  $$\Pr[(X_1 = x_1) \wedge (X_2 = x_2) \wedge \ldots \wedge (X_n = x_n)] = \prod_{i=1}^{n} \Pr[X_i = x_i].$$

- Expectation:

  1. The *expectation* of a random variable $X$ with range $S$ is

  $$\mathbb{E}[X] = \sum_{x \in S} x \cdot \Pr[X = x].$$

  2. Expectation is linear: for constants $a, b$ and random variables $X, Y$ we have

  $$\mathbb{E}[aX + bY] = a\,\mathbb{E}[X] + b\,\mathbb{E}[Y].$$

- Statistical distance:

  The *statistical distance* (or total variation distance) between probability distributions $P$ and $Q$ defined on the same space $S$ is

  $$\|P - Q\| = \max_{T \subseteq S} |P(T) - Q(T)| = \frac{1}{2} \sum_{s \in S} |P(s) - Q(s)|.$$

**Number Theory**

- $\mathbb{Z}$ denotes the set of integers, and $\mathbb{Z}^+$ denotes the set of positive integers.
- For $d \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$:
  1. $d|a$ means there exists an integer $c$ such that $a = dc$.
  2. $d|a$ and $d|b$ implies $d|(a+b)$ and $d|(a-b)$.
  3. $d|a$ implies $d|ab$.
  4. The common divisors of $a$ and $b$ are all positive integers that divide both $a$ and $b$. $\gcd(a, b)$ is the greatest (largest) common divisor of $a$ and $b$.
- For $a, b, c, d, m \in \mathbb{Z}$, $m \geq 2$:
  1. $a \equiv b \mod m$ means $m|(a-b)$.
  2. $a \bmod m$ is the unique $b \in \{0, 1, \ldots, m-1\}$ such that $a \equiv b \mod m$.
  3. $a \equiv c \mod m$ and $b \equiv d \mod m$ imply both

$$\begin{aligned} a+b &\equiv c+d \mod m \\ a \cdot b &\equiv c \cdot d \mod m. \end{aligned}$$

     Therefore $((a \bmod m)(b \bmod m)) \bmod m = (ab) \bmod m$.
- For $m \in \mathbb{Z}$, $m \geq 2$:
  1. $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ where the operations $+$, $-$, and $\cdot$ are performed mod $m$.
  2. $\mathbb{Z}_m^* = \{x \in \mathbb{Z}_m : \gcd(x, m) = 1\}$.
- For $a, b, c, m \in \mathbb{Z}$, $m \geq 2$:
  1. If $\gcd(a, m) = 1$, then $ab \equiv ac \mod m$ implies $b \equiv c \mod m$.
  2. If $\gcd(a, m) = 1$, then there is a unique solution $x \in \mathbb{Z}_m^*$ to $ax \equiv b \mod m$.
  3. For $a \in \mathbb{Z}_m^*$, the *multiplicative inverse of* $a$, denoted $a^{-1}$, is the unique element in $\mathbb{Z}_m^*$ such that $a \cdot a^{-1} \equiv 1 \mod m$. Division $b/a$ in $\mathbb{Z}_m$ means $b \cdot a^{-1}$.