1 Congruence

- Let $[k]_0 := \{0, ..., k-1\}$. For $m, n \in \mathbb{N}$ we have the function

$$F : [n]_0 \to [m]_0$$

with the property

$$\forall x, y \in [n]_0 : \; F((x+y) \mod n) = (F(x) + F(y)) \mod m.$$

- We evaluate F by looking up values in a table, but an unkown fifth of the values is wrong.

1. Describe a simple algorithm, which returns the correct $F(z)$ with probability at least $1/2$ for any $z \in [n]_0$.
2. Let us run this algorithm three times. With what probability can we now determine $F(z)$?

2 Variance

Let X be a discrete random variable with values constrained to $[0, 1]$. Show that $\mathrm{Var}[X] \leq 1/4$.

3 Hashing

For p prime and $n \leq p$, we have the hash function families

$$\mathcal{H}_{a,b} := \{h_{a,b} |\; a, b \in [p-1]\} \text{ and } \mathcal{H}_a := \{h_a |\; a \in [p-1]\},$$

where

$$h_{a,b}(x) = ((ax + b) \mod p) \mod n \text{ and } h_a(x) = (ax \mod p) \mod n.$$

1. Show that $\mathcal{H}_{a,b}$ is 2-universal.
2. Show that $\mathcal{H}_a$ is not.
3. Show that $\mathcal{H}_a$ is almost 2-universal, meaning

$$\forall x, y \in [n]_0,\; x \neq y : \; P[h_a(x) = h_a(y))] \leq 2/n.$$