1 Kongruence

- Nechť $[k]_0 := \{0, ..., k-1\}$. Pro $m, n \in \mathbb{N}$ máme funkci

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

splňující

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

- F vyhodnocujeme tím, že se podíváme do tabulky hodnot, ale neznámá pětina hodnot je špatně.

1. Popiště jednoduchý algoritmus, který $\forall z \in [n]_0$ vrátí korektní $F(z)$ s pravděpodobností aspoň $1/2$.
2. Spustíme algoritmus třikrát. S jakou pravděpodobností můžeme pak určit $F(z)$?

2 Variance

Nechť X je variance diskrétní náhodné proměnné s hodnotami v $[0, 1]$. Ukažte, že $\mathrm{Var}[X] \leq 1/4$.

3 Hashování

Pro p prvočíslo a $n \leq p$, máme rodiny hashovacích funkcí

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

kde

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

1. Ukažte, že $\mathcal{H}_{a,b}$ je 2-univerzální.
2. Ukažte, že $\mathcal{H}_a$ není.
3. Ukažte, že $\mathcal{H}_a$ je skoro 2-univerzální ve smyslu

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