1. Ukažte, že dokonce i systém $\{h_a(x) = ((ax) \bmod p) \bmod m; a \in [1,p], m \leq p, p \text{ je prvočíslo}\}$, tedy bez aditivního členu, je universální. Bude to platit, když povolíme $a = 0$?

2. Uvažme systém hashovacích funkcí $\{h_{a,b}(x) = ((ax+b) \bmod p) \bmod m; a,b \in [p], m \leq p, p \text{ je prvočíslo}\}$. Ukažte, že není 3-nezávislý.

3. Ukažte, že tabulkové hashování je 3-nezávislé.

4. Mějme hodnoty $m < n$. Ukažte, že $\{0, m \bmod n, 2m \bmod n, 3m \bmod n, \ldots, (n-1)m \bmod n\} = [n]$, pokud m je nesoudělné s n.

5. Ukažte *randomizovanou redukci* ze SATu na UniqueSAT.

   UniqueSAT je problém rozhodnout, zda formule v CNF má právě jedno splňující ohodnocení či nikoliv.

   Randomizovaná redukce je polynomiální algoritmus, který z formule φ (v roli instance SATu) vyprodukuje formuli φ' (v roli instance UniqueSATu) takovou, že

   $$\varphi \in \mathsf{SAT} \Rightarrow \Pr[\varphi' \in \mathsf{UniqueSAT}] \geq \frac{1}{100000n} \qquad \text{a}$$

   $$\varphi \notin \mathsf{SAT} \Rightarrow \Pr[\varphi' \in \mathsf{UniqueSAT}] = 0.$$

   Nápověda. Nechť $S \subseteq \mathbb{Z}_2^n$ je množina splňujících ohodnocení pro φ. Zvolme k takové, že $2^{k-2} \leq |S| \leq 2^{k-1}$. Zvolíme náhodnou hashovací funkci z 2-universální rodiny $\mathbb{A}x + \vec{b}$, kde $A \in \mathbb{Z}_2^{n,k}, b \in \mathbb{Z}_2^k$. Teď to jen dopočítat.