Problem diskretnega logaritma, zgoščevalne funkcije

1. Naj bo p praštevilo in α generator grupe $\mathbb{Z}_p^*$.
   (a) Recimo, da znamo faktorizirati $p-1$. Kako lahko hitro preverimo, ali je dani element $\mathbb{Z}_p^*$ generator grupe $\mathbb{Z}_p^*$? Preverite, da je 2 generator grupe $\mathbb{Z}_{181}^*$.
   (b) Kolikšen je red elementa α^i za $i \in \{1, 2, \ldots, p-1\}$? Kolikšen je red elementa 2^{10} v grupi $\mathbb{Z}_{181}^*$? Poiščite vse elemente reda 10 v grupi $\mathbb{Z}_{181}^*$.
   (c) Kolikšna je verjetnost, da je naključno izbran element grupe $\mathbb{Z}_p^*$ generator te grupe? Kolikšna je ta verjetnost za $p = 181$?
   (d) Recimo, da znamo faktorizirati $p-1$. Sestavite hiter algoritem, ki poišče generator grupe $\mathbb{Z}_p^*$.

2. Naj bo p praštevilo in α, γ generatorja grupe $\mathbb{Z}_p^*$. Recimo, da znamo učinkovito računati diskretne logaritme za bazo α. Pokažite, da lahko potem učinkovito računamo diskretne logaritme tudi za bazo γ.

3. Poiščite vse rešitve enačb
   (a) $7x \equiv 3 \pmod{25}$,
   (b) $5x \equiv 3 \pmod{25}$,
   (c) $5x \equiv 15 \pmod{25}$.

4. Naj bo $n \geq 2$ naravno število. Kompresijsko funkcijo $h : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ definiramo takole:
   $$h : (x, y) \mapsto ax + by \bmod n.$$
   Poiščite trk (za poljubna $a, b \in \mathbb{Z}_n$).