1. [**Testování maticového násobení (15 bodů)**] Mějme tři matice $A, B, C \in \mathbb{R}^{n \times n}$ a chceme v kvadratickém čase rozhodnout, jestli $AB = C$. Použijeme následující algoritmus:

   - vybereme uniformně náhodný vektor $x \in \{0,1\}^n$
   - ověříme, že $Cx = A(Bx)$
   - opakujeme několikrát

   (a) Určete pravděpodobnost, že jediný test (bez opakování) odhalí nerovnost (za podmínky $AB \neq C$).

   (b) Kolikrát musíme opakovat, když chceme chybu menší, než ε?

   (c) O jaký typ algoritmu jde? (ZPP, BPP, RP, coRP, ...)

2. [**Coupling (15 bodů)**] Uvažme následující míchání karet:

   - Vybereme dvě karty uniformně náhodně (když K je množina karet, vybereme $(x, y) \in K \times K$)
   - Prohodíme karty x, y (pokud $x = y$ nic se nestane)

   (a) Ukažte, že předchozí je ekvivalentní vybrání karty $x \in K$ a pozice $i \in [|K|]$ a prohození karty x s kartou na pozici i.

   (b) Uvažte coupling, kde výběr karty a pozice je v obou Markovovských procesech stejný. Nechť X_t je počet karet, jejichž pozice se v těch Markovovských liší. Ukažte, že X_t je nerostoucí (jako funkce t).

   (c) Ukažte, že
   $$\Pr[X_{t+1} \leq X_t - 1 \mid X_t > 0] \geq \left(\frac{X_t}{|K|}\right)^2$$

   (d) Zdůvodněte, že střední hodnota počtu kroků t, než $X_t = 0$, je $\mathcal{O}(|K|^2)$ nezávisle na počátečním stavu těch dvou řetězců.

3. **Marné samplování (15 bodů)** Mějme DNF formuli, která má n proměnných a $\alpha(n)$ splňujících ohodnocení (pro nějaký polynom α). Ukažte, že po $2^{n/2}$ nezávislých uniformně náhodných samplech je pravděpodobnost nalezení jediného splňujícího ohodnocení exponenciálně malá.