1. V projektivní rovině nad konečným tělesem $\mathbb{F}_q$ o q prvcích je křivka určená rovnicí $x^5 + y^5 + z^5 = 0$. Napište, pro která přirozená čísla q existuje těleso o q prvcích, a určete, pro která q je uvedená křivka singulární.

2. Pro každé přirozené číslo n určete, kolik bodů má eliptická křivka $\mathcal{E}_n$ určená Weierstrassovou rovnicí $y^2 = x^3 + x$ nad tělesem o 7^n prvcích.

(a) Navíc v případě $n = 1$ nalezněte též generátor eliptické křivky $\mathcal{E}_1$ (jde-li o cyklickou grupu), resp. systém nezávislých generátorů (není-li grupa cyklická), a všechny body eliptické křivky pomocí tohoto generátoru, resp. těchto generátorů, vyjádřete.

(b) Dále v případě $n = 2$ rozhodnete, zda eliptická křivka $\mathcal{E}_2$ je cyklická grupa nebo ne.

3. Popište okruh všech celých čísel v tělese $\mathbb{Q}(\sqrt{-6})$. Dokažte, že tento okruh není okruh s jednoznačným rozkladem. [Návod: nalezněte nějaké dva podstatně odlišné rozklady nějakého čísla na součin ireducibilních prvků.]

4. Sestrojte těleso o 27 prvcích a určete, kolik jeho prvků je takových, že (samotné) generují jeho multiplikativní grupu. Dále alespoň jeden takový prvek explicitně popište.

5. Nalezněte aspoň šest dobrých aproximací čísla $\sqrt{\frac{5}{3}}$.

6. Rozhodněte, zda číslo 2821 je Carmichaelovo.

7. Zformulujte větu, na níž je založen $N - 1$ test Poclingtona a Lehmera.