Své výpočty pište podrobně a srozumitelně včetně potřebných zdůvodnění.

1. Definujte pojem „Carmichaelovo číslo“.

2. Formulujte Mazurovu větu.

3. V projektivní rovině nad konečným tělesem $\mathbb{F}_q$ o q prvcích je rovnicí $x^3 + 5xz^2 + 2z^3 - y^2z = 0$ dána křivka. Napište, pro která přirozená čísla q existuje těleso o q prvcích, a určete, pro která q je uvedená křivka singulární.

4. Je dáno prvočíslo $p = 2017$. Pomocí kvadratického zákona reciprocity rozhodněte, zda je číslo 12345 kvadratický zbytek nebo nezbytek modulo p (ověřovat, že p je opravdu prvočíslo, nemusíte).

5. Nalezněte alespoň sedm dobrých aproximací čísla $\sqrt{47}$.

6. Sestrojte těleso L o 49 prvcích a určete, kolik v tělese L má polynom $g = x^3 + 3$ kořenů.

7. (a) Weierstrassovou rovnicí
$$y^2 = x^3 + 2x - 1$$
je dána eliptická křivka $\mathcal{E}_1$ nad tělesem o 5 prvcích. Nalezněte generátor eliptické křivky (jde-li o cyklickou grupu), resp. systém nezávislých generátorů (není-li to grupa cyklická), a všechny body eliptické křivky $\mathcal{E}_1$ pomocí tohoto generátoru, resp. těchto generátorů, vyjádřete.

   (b) Pro přirozená čísla $n = 2$, $n = 3$ a $n = 4$ určete, kolik bodů má eliptická křivka $\mathcal{E}_n$ určená Weierstrassovou rovnicí
$$y^2 = x^3 + 2x - 1$$
nad tělesem o 5^n prvcích, a pokuste se rozhodnout o její cykličnosti.