

5. přednáška a cvičení (2009)

Co jsme dělali na přednášce?

Sekci 2.12 ze skript a povídání o tom, jak se testuje, zda je číslo prvočíslo.

Co jsme dělali na cvičení?

Popsali jsme si postup, jak hledat primitivní prvky v $\mathbb{Z}_{p^\alpha}$. Pověděli jsme si, jak funguje Fermatův a Rabin-Millerův test prvočíselnosti, co to je (silné) pseudoprvočíslo v nějaké bázi a čemu říkáme slabá a silná báze. A nezapomněli jsme ani na Carmichaelova čísla.

Příklady

-1. Popiš explicitně izomorfismy $\mathbb{Z}_{49}^* \simeq \mathbb{Z}_6 \times \mathbb{Z}_7 \simeq \mathbb{Z}_{42}$ (a najdi primitivní prvek v $\mathbb{Z}_{49}^*$).

0. Najdi všechny slabé a silné báze pro 49.

1. Najdi všechny slabé a silné báze pro 21.

2. Dokaž, že 561 je Carmichaelovo číslo.

3. Popiš explicitně izomorfismy $\mathbb{Z}_{25}^* \simeq \mathbb{Z}_4 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{20}$ (a najdi primitivní prvek v $\mathbb{Z}_{25}^*$).

4. Najdi všechny slabé a silné báze pro 25.

5. Mějme různá prvočísla p, q . Dokaž, že pq není Carmichaelovo číslo.

6. Popiš $\mathbb{Z}_{40}^*$. Najdi všechny involuce v $\mathbb{Z}_{40}^*$.

7. Najdi všechny slabé a silné báze pro 45.

8. Dokaž, že pokud $(\varphi(N), N - 1) = 2$, pak jediné silné báze pro N jsou ± 1 .

9. Dokaž, že $N = \prod p_i^{\alpha_i}$ je Carmichaelovo číslo, právě když $(p_i - 1)p_i^{\alpha_i - 1} | N - 1$ pro všechna i .

10. Ať $N = 2^a \prod p_i^{\alpha_i}$. Kolik je involucí v $\mathbb{Z}_N^*$?