

Písemka z Teorie čísel a RSA (18. května 2009)

1. příklad (5 bodů)

V závislosti na přirozených číslech k, l urči $\text{NSD}(3k^2 - 3kl, k^2 + l^2)$.

2. příklad (5 bodů)

Rozlož číslo $540 + 30i$ na součin prvočinitelů v $\mathbb{Z}[i]$. Nezapomeň zdůvodnit, že jde skutečně o prvočinitele.

3. příklad (5 bodů)

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. příklad (5 bodů)

Definuj silné a slabé pseudoprvočíslo v bázi a . Najdi všechna $a \in \mathbb{Z}$ taková, že 55 je silné, respektive slabé pseudoprvočíslo v bázi a .

5. příklad (5 bodů)

Urči, kolik má kongruence $x^2 \equiv 181 \pmod{237}$ celočíselných řešení takových, že $0 \leq x < 237$.

6. příklad (5 bodů)

Popiš všechny charaktery modulo 13. Popiš ty z nich, které mají řád 6.

7. příklad (5 bodů)

Definuj Euklidovský obor. Dokaž, že $\mathbb{Z}[\sqrt{-2}]$ je Euklidovský. Dokaž, že jeho invertibilní prvky jsou pouze 1 a -1.

8. příklad (5 bodů)

Najdi všechna celočíselná řešení rovnice $x^2 + 2 = y^3$.

9. příklad (5 bodů)

Najdi všechna celočíselná řešení rovnice $x^2 - 6y^2 = 1$. Najdi aspoň dvě řešení rovnice $x^2 - 6y^2 = 10$ v přirozených číslech.

10. příklad (5 bodů)

Vyjádři číslo $\sqrt{8}$ ve tvaru řetězového zlomku. Popiš všechny dobré aproximace tohoto čísla.

Při řešení každého z příkladů můžeš předpokládat, že platí tvrzení předcházejících úloh, i pokud jsi je nedokázal.

K získání zápočtu je potřeba aspoň 32 bodů. Přeji hodně štěstí a příjemnou zábavu při řešení.