

Písemka z Teorie čísel a RSA (22. května 2008)

1. příklad (5 bodů)

Najdi nějaký primitivní prvek modulo 29.

2. příklad (5 bodů)

Vyřeš kongruenci $x^{21} \equiv -1 \pmod{29}$.

3. příklad (5 bodů)

Rozlož číslo $84 + 98i$ na součin prvočinitelů v $\mathbb{Z}[i]$.

4. příklad (5 bodů)

Najdi všechna celočíselná řešení rovnice $4x^2 + 9 = y^3$.

5. příklad (5 bodů)

Definuj silné pseudoprvočíslo v bázi a . Najdi všechna $a \in \mathbb{Z}$ taková, že 35 je silné pseudoprvočíslo v bázi a .

6. příklad (5 bodů)

Urči, kolik má kongruence $x^2 \equiv 149 \pmod{211}$ celočíselných řešení takových, že $0 \leq x < 211$.

7. příklad (5 bodů)

Urči počet všech charakterů modulo 15.

8. příklad (5 bodů)

Buď χ kvadratický charakter modulo 5. Spočti hodnotu $(g(\chi))^2$, kde $g(\chi)$ je Gaussův součet příslušný charakteru χ .

9. příklad (5 bodů)

Vyjádři číslo $\sqrt{5}$ ve tvaru řetězového zlomku.

10. příklad (5 bodů)

Kolika nulami končí číslo $\binom{77}{42}$?

K získání zápočtu je potřeba aspoň 35 bodů. Přeji hodně štěstí a příjemnou zábavu při řešení.