Písemka z Teorie čísel a RSA, 22. května 2007

1. příklad (5 bodů)
Najdi (nějaký) primitivní prvek modulo 31.

2. příklad (5 bodů)
Najdi všechna řešení kongruence $x^5 \equiv 1 \pmod{31}$.

3. příklad (5 bodů)
Najdi největší společný dělitel čísel $7 + 4i$ a $13i - 1$ v $\mathbb{Z}[i]$.

4. příklad (7 bodů)
Najdi všechna celočíselná řešení rovnice $x^3 = y^2 + 4$ taková, že y je liché.

5. příklad (7 bodů)
Definuj euklidovské zobrazení a euklidovský okruh. Uvažujme okruh $\mathbb{Z}[\omega] = \{a + b\omega, a, b \in \mathbb{Z}\}$, kde $\omega = (-1 + \sqrt{-3})/2$. Dokaž, že tento okruh je euklidovský.

6. příklad (5 bodů)
Vyjádři $\sqrt{8}$ ve tvaru řetězového zlomku.

7. příklad (5 bodů)
Urči, kolik má kongruence $x^2 \equiv 79 \pmod{101}$ řešení.

8. příklad (7 bodů)
Buď p prvočíslo, $a, b \in \mathbb{Z}$, $p \nmid a$. Dokaž, že $\sum_{i=0}^{p-1} \left(\frac{ai+b}{p}\right) = 0$.

K získání zápočtu jsou potřeba aspoň 23 body. Přeji hodně štěstí a zábavy při řešení.