Písemka z Teorie čísel a RSA, 17. května 2007

1. příklad (5 bodů)
Najdi (nějaký) primitivní prvek modulo 17.

2. příklad (5 bodů)
Najdi všechna řešení kongruence $x^4 \equiv 1 \pmod{17}$.

3. příklad (7 bodů)
Definuj prvočinitele v (obecném) oboru integrity. Rozlož $21-12i$ v $\mathbb{Z}[i]$ na součin prvočinitelů.

4. příklad (7 bodů)
Uvažujme okruh $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2}, a, b \in \mathbb{Z}\}$ s normou definovanou $N(a + b\sqrt{-2}) = a^2 + 2b^2$. Dokaž, že tato norma je euklidovská (to, že jde o normu, dokazovat nemusíš).

5. příklad (7 bodů)
Najdi všechna celočíselná řešení rovnice $x^3 = y^2 + 2$ (můžeš předpokládat, že platí tvrzení 4. příkladu, i pokud jsi je nedokázal).

6. příklad (5 bodů)
Vyjádři $\sqrt{\frac{1}{2}}$ ve tvaru řetězového zlomku.

7. příklad (5 bodů)
Urči, kolik má kongruence $x^2 \equiv 43 \pmod{83}$ řešení.

8. příklad (5 bodů)
Urči všechna reálná čísla, která jdou vyjádřit řetězovým zlomkem tvaru $[k, 2, \ldots]$ ($k \in \mathbb{Z}$; místo $\ldots$ je vždy libovolná (konečná nebo nekonečná, ale neprázdná) posloupnost přirozených čísel).

K získání zápočtu je potřeba aspoň 25 bodů. Přeji hodně štěstí a hodně zábavy při řešení.