Jméno							
Úloha	1	2	3	4	5	6	Celkem
Body							

Teorie čísel a RSA, písemka 1 (předtermín)

22. května 2019
90 minut

1. (5 bodů) Definuj dobrou aproximaci reálného čísla ξ.

2. (3+3 body)

   a) Popiš všechny prvočinitele v $\mathbb{Z}[i]$.

   b) Zformuluj větu o tom, která prvočísla v $\mathbb{Z}$ jsou tvaru $a^2 + b^2$.

3. (10 bodů) Buď n přirozené číslo. Urči, kterému reálnému číslu se rovná periodický řetězový zlomek $[\overline{n, 2}]$.

4. (3+7 bodů)

   a) Definuj silné pseudoprvočíslo v bázi a.

   b) Najdi všechna $0 \leq a \leq 20$ taková, že 21 je silné pseudoprvočíslo v bázi a.

5. (2+8 bodů) Buď p liché prvočíslo.

   a) Zformuluj vzorec udávající hodnotu $\left(\frac{2}{p}\right)$.

   b) Dokaž tento vzorec v případě $p \equiv 1 \pmod 4$.

6. (15 bodů) Buď n přirozené číslo. Dokaž, že existuje aspoň jedno prvočíslo $p \equiv 1 \pmod n$.

Informace

V úlohách 1., 2. není potřeba nic dokazovat. V početních příkladech 3., 4. můžeš používat tvrzení z přednášky (a cvičení), pokud je zformuluješ. V důkazech 5., 6. můžeš používat všechna předcházející tvrzení z přednášky, pokud je zformuluješ. („Tvrzení“ samozřejmě zahrnují i lemmata, věty, atd.)

Pokud si něčím nejsi jistý, radši se zeptej!

Maximálně jde získat 56 bodů, z toho na 1, 2, resp. 3 bude určitě stačit 48, 39, resp. 30 bodů, možná i méně: přesné hranice určím podle obtížnosti písemky.