Jméno							
Úloha	1	2	3	4	5	6	Celkem
Body							

Teorie čísel a RSA, písemka 1 (předtermín)

13. května 2020
90 minut

1. (5 bodů) Definuj Jacobiho symbol a zformuluj zákon kvadratické reciprocity pro Jacobiho symboly.

2. (5 bodů) Pro prvočíslo p (ne nutně liché) a přirozené číslo k popiš strukturu grupy $\mathbb{Z}^*_{p^k}(\cdot)$.

3. (10 bodů) Najdi řetězový zlomek a všechny dobré aproximace čísla $\frac{58}{49}$.

4. (2+8 bodů)

   a) Definuj míjení prvků v grupě $G(\cdot)$.

   b) Najdi všechny prvky grupy $\mathbb{Z}_{30}(+)$, které míjí prvek 4.

5. (10 bodů) Buď p liché prvočíslo. Dokaž, že $p \equiv 1 \pmod 4$, právě když $p = a^2 + b^2$ pro nějaká celá čísla a, b.

6. (10 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 50 bodů, z toho na 1, 2, resp. 3 bude určitě stačit 44, 36, resp. 28 bodů, možná i méně: přesné hranice určím podle obtížnosti písemky.