Jméno								
Úloha	1	2	3	4	5	6	7	Celkem
Body								

Teorie čísel a RSA, písemka 1 (předtermín)

24. května 2018

90 minut

1. (5 bodů) Popiš všechny podgrupy v $\mathbb{Z}_n(+)$. Kolik má $\mathbb{Z}_n(+)$ generátorů? (Stačí správné odpovědi bez důkazů.)

2. (15 bodů) Buď p liché prvočíslo a $r \geq 2$. Dokaž, že $\mathbb{Z}_{p^r}^*$ je cyklická grupa (můžeš bez důkazu používat tvrzení z předchozích sekcí včetně toho, že $\mathbb{Z}_p^*$ je cyklická).

3. (3+7 bodů)

   a) Definuj silné pseudoprvočíslo v bázi a.

   b) Najdi všechna a taková, že 15 je silné pseudoprvočíslo v bázi a.

4. (5 bodů) Definuj charakter χ modulo n a Gaussův součet pro charakter χ.

5. (10 bodů) Pro která prvočísla p existuje $a \in \mathbb{Z}$ takové, že $p|a^2 + 7$? Obecně zformuluj vzorce, které přitom používáš.

6. (3+7 bodů)

   a) Definuj n-tý cyklotomický polynom.

   b) Spočti n-tý cyklotomický polynom pro $1 \leq n \leq 6$ a pro $n = 12$. Rozlož $x^{12} - 1$ na součin ireducibilních polynomů. (Můžeš používat všechna tvrzení z přednášky včetně toho, že cyklotomické polynomy jsou ireducibilní.)

7. (3+7 bodů)

   a) Definuj dobrou aproximaci čísla $\theta \in \mathbb{R}$.

   b) Buď θ iracionální číslo a $\frac{p}{q}$ dobrá aproximace θ. Dokaž, že

$$\left|\frac{p}{q} - \theta\right| < \frac{1}{q^2}.$$

Informace

Úlohy nejsou popořadě podle obtížnosti. V početních příkladech 3., 5., 6. můžeš používat tvrzení z přednášky (a cvičení), pokud je zformuluješ. V důkazech 2., 7. můžeš používat tvrzení z dřívějších sekcí z přednášky. („Tvrzení“ samozřejmě zahrnují i lemmata, věty, atd.) Pokud si něčím nejsi jistý, radši se zeptej!

Maximálně jde získat 65 bodů, z toho na 1, 2, resp. 3 bude určitě stačit 55, 45, resp. 33 bodů, možná i méně: přesné hranice určím podle obtížnosti písemky.