

Domácí úlohy: Číselné algoritmy

2024/25

Domácí úkoly budou zadány celkem čtyři, k získání zápočtu bude třeba získat aspoň 25 bodů z celkových 40 bodů.

1. DOMÁCÍ ÚKOL

Odevzdejte do 3. dubna, 12:30

1.1. Použijeme-li pro nalezení ireducibilního faktoru Fermatova čísla F_{12} první verzi Pollardovy (p-1)-metody (s testem největšího společného dělitele v každém kroku for-cyklu pro prvočísla $p_i \geq 2$) s hodnotou $B = 2^{14}$, objasněte, v kterém kroku for-cyklu lze nejpozději očekávat jeho opuštění, víte-li, že F_{12} má prvočíselný faktor $7 \cdot 2^{14} + 1$. Vysvětlete, proč za náhodnou hodnotu a nemůžete zvolit 2.

5 bodů

1.2. Pro prvočísla p, q určete periodu a preperiodu posloupnosti $\{s_n\}_{n \geq 0} \in \mathbb{Z}_p$ určené vztahem $s_n = s_{n-1}^q$ v závislosti na řádu $o_{\mathbb{Z}_p^*}(s_0)$, kde pro $s_0 \in \mathbb{Z}_p^*$.

5 bodů

2. DOMÁCÍ ÚKOL

Odevzdejte do 24. dubna, 12:30

2.1. Pomocí Tonelli-Shanksova algoritmu najděte všechna řešení rovnice $x^2 + 37 = 8x$ v tělese $\mathbb{F}_{89}$ (pokud příklad nebudete počítat ručně, ilustруйте průběh algoritmu vypsány mi mezivýsledky).

5 bodů

2.2. Existuje-li, najděte nějaké řešení kongruence $x^2 \equiv 58 \pmod{27 \cdot 121}$.

5 bodů

3. DOMÁCÍ ÚKOL

Odevzdejte do 22. května, 12:30

3.1. Víte-li, že $\mathbb{Z}_{2^e}^* = \{(2^e - 1)^i \cdot 5^j \mid i \in \mathbb{Z}_2, j \in \mathbb{Z}_{2^{e-2}}\}$, popište všechny čtverce z $\mathbb{Z}_{2^e}^*$. Kolik jich je?

3 body

3.2. Pomocí Algoritmu 16 najděte řetězový rozvoj čísla $\sqrt{71}$.

3 body

3.3. Nechť V je prostor všech řešení a U podprostor všech špatných řešení pro systém hladkých relací (x_i, y_i) , $i \leq k$ vzhledem k bázi B faktorizace přirozeného čísla N a platí, že $\gcd(y_i, N) = 1$ pro všechna $i \leq k$. Určete pravděpodobnost, že uniformně náhodně zvolené řešení není špatné, víte-li, že $\dim_{\mathbb{F}_2}(V) - \dim_{\mathbb{F}_2}(U) = 4$ a své tvrzení vysvětlete.

4 body

4. DOMÁCÍ ÚKOL

Odevzdejte do 30. června nebo do zkoušky

4.1. Pomocí Pohlig-Hellmanovy redukce rozhodněte, zda existuje řešení

$$2^x \equiv 3 \pmod{25 \cdot 1331}$$

a pokud ano řešení najděte.

4 body

4.2. Pomocí algoritmu Baby-Steps, Giant Steps vyřešte kongruence

$$2^x \equiv 3 \pmod{983} \quad \text{a} \quad 3^x \equiv 2 \pmod{983}.$$

6 bodů