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

Oddevzdejte do 3. dubna, 12:30

1.1. Použijeme-li pro nalezení iredeucibilního 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 nemůže zvolit 2.

(Potěšilo by mě, kdyby někdo zjistil, jak algoritmus dopadne pro $a = 3$, ale součástí úkolu to není.)

5 points

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 points