Počítačová algebra

Cvičení 3

Problém 1. Spočtěte pomocí Karacubova triku s tužkou a papírem součin 5661×3641.

Problém 2. Buď m přirozené číslo, $a, b \in \{0, 1, \ldots, m-1\}$. Dokažte, že $a^b \bmod m$ lze spočítat v čase $O(\ell(b)\ell(m)^2)$.

Problém 3. Buďte a, b, m přirozená čísla. Dokažte, že $a^b \bmod m$ lze spočítat v čase $O(\ell(a)\ell(m) + \ell(b)\ell(m)^2)$.

Problém 4. Vymyslete, jak Karacubovo násobení aplikovat na polynomy z $R[x]$, a odhadněte časovou složitost výsledného algoritmu (v jednodušším modelu, kdy jedna operace nad okruhem R stojí jednotku času).

Problém 5. Zformulujte a odhadněte složitost algoritmu Toom-3 ze cvičení 6 za sekcí 4 v učebnici. Tato úloha je složitější; pokud se na ní zaseknete, tak nám buď napište mail, nebo si připravte otázky na příští videopřenos.

Problém 6. Vyřešte ručně pomocí Lagrangeova a Garnerova algoritmu následující problém: Najděte číslo $a \in \{-251, \ldots, 0, \ldots, 252\}$ takové, aby

$$\begin{aligned} a &\equiv 1 \pmod 7 \\ a &\equiv 3 \pmod 8 \\ a &\equiv -1 \pmod 9 \end{aligned}$$

Problém 7. Určete všechny primitivní šesté odmocniny z 1 v $\mathbb{Z}_{31}$.

Problém 8. Dokažte, že pokud v $\mathbb{F}_{p^k}$ existuje primitivní n-tá odmocnina z 1, tak p nedělí n.

Problém 9. Kolik primitivních n-tých odmocnin z 1 obsahuje těleso $\mathbb{C}$?

Problém 10. Spočtěte v $\mathbb{C}$ DFT z následujících polynomů p pro následující hodnoty n a ω:

1. $n = 2$, $p = 3x + 4$, $\omega = -1$
2. $n = 3$, $p = x^2 - x + 1$, $\omega = e^{2\pi i/3}$