

Počítačová algebra: (Půl)cvičení 4

11. listopadu 2021

1. Najděte primitivní prvek (generátor multiplikativní grupy) v $\mathbb{Z}_{1009}$. Je 158 primitivní prvek v $\mathbb{Z}_{1009}$? Jaký je řád prvku 2 v $\mathbb{Z}_{1009}^*$? Kolik primitivních prvků $\mathbb{Z}_{1009}$ obsahuje?
(Obecně pozor, jestli řády/generátory Sage počítá pro sčítací nebo multiplikativní grupu.)
2. Naprogramujte rychlou Fourierovu transformaci (FFT) pro polynomy nad $GF(257)$. Spočtěte modulární reprezentaci polynomu $7x^7 + 14x^2 + 5$.
(Využijte faktu, že $257 = 2^8 + 1$. Pro zjednodušení můžete předpokládat, že na vstupu máte polynom stupně o jedna menší než mocnina 2. Jak byste postupovali v případě polynomu obecného stupně menšího než 256?)
3. Za pomoci funkce z předchozího příkladu naprogramujte funkci na rychlé počítání IDFT v $GF(257)$. Ověřte její funkčnost na polynomu z předchozího příkladu.
4. Pokud jste v příkladu 2. naprogramovali *FFT* rekurzivně, zkuste si naprogramovat iterativní metodu (časové i paměťové nevýhody rekurze jsme již probírali).