Počítačová algebra: Cvičení 4

21. listopadu 2022

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 příkaz v Sagi 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 pomocí funkce z předchozího příkladu naprogramujte funkci na rychlé počítání IDFT v $GF(257)$. Ověřte její funkčnost na polynomu z předchozího příkladu.

4. Naprogramujte funkci pro rychlé násobení celočíselných polynomů za pomocí FFT pro komplexní polynomy (aproximujte celočíselné polynomy pomocí komplexních čísel). Sledujte, jak se výsledky mění se změnou přesnosti komplexních čísel.

   (Nápověda: *ComplexField(prec=n)* vytvoří těleso komplexních čísel s danou přesností).

5. Za pomocí předchozí úlohy implementujte algoritmus na rychlé násobení polynomů nad $\mathbb{Q}$.

6. Pro zvolená přirozená čísla k a n najděte prvočíslo p takové, že $p > n$ a $2^k \mid p - 1$.

7. Implementujte rychlé násobení polynomů modulární metodou.

8. Pokud jste v předchozích případech naprogramovali FFT rekurzivně, zkuste si ho naprogramovat i iterativním způsobem.