Uživatelská dokumentace

Tento modul napsaný v Pythonu slouží především k rychlému násobení dvou polynomů, jejichž koeficienty jsou přirozená čísla na daném tělese Zp. K tomu je využita Fourierova transformace. Dále umožňuje modul přístup k samotnému algoritmu FFT na konečném tělese, který může uživatel využít podle své vlastní potřeby.

Modul ve výchozím režimu pracuje s tělesem, jenž umožňuje relativně vysoký rozsah koeficientů, je nicméně možné dodat vlastní těleso, pokud splňuje požadavky algoritmu.

Není-li uvedeno jinak, jsou polynomy reprezentovány jako python seznamy koeficientů polynomu, kde i-tý index odpovídá koeficientu i-tého členu. Na indexu 0 se tedy nachází koeficient absolutního členu a například na indexu 2 se nachází koeficient kvadratického členu.

multiply_polynomials

První dva argumenty této funkce jsou povinné a mělo by se jednat o dva polynomy v reprezentaci popsané výše.

Další argumenty nejsou nepovinné a týkají se použitého tělesa, pokud nechce uživatel použít výchozí. Jedná se v tomto pořadí o modulo (tedy prvočíslo, které určuje uživatelem vybrané těleso), generátor, který generuje pro algoritmus vhodné hodnoty, ve kterých je polynom v průběhu FFT vyhodnocen a počet takových hodnot. Počet hodnot musí být vždy mocninou dvojky.

Dále musí uživatel dát při zvolení daného tělesa pozor na to, že jím dodaný generátor musí být schopen vygenerovat dostatek hodnot na to, aby byl výsledný polynom jednoznačně určen.

Výstupem této funkce je polynom vzniklý vynásobením dvou vstupních.

FFT

Tato funkce odpovídá samotné rychlé Fourierově transformaci.

První povinný argument této funkce je polynom, druhý počet hodnot, ve kterých chce uživatel polynom vyhodnotit. Tento počet funkce zaokrouhlí nahoru k nejbližší mocnině dvojky a stejně tak

i doplní do polynomu nuly tak, aby jeho délka odpovídala této mocnině dvojky. Proto platí, že je-li polynom delší, než tato mocnina, funkce spadne.

Funkce vrátí polynom reprezentovaný jako tabulka hodnot polynomu v jednotlivých bodech zvolených algoritmem.

Zbývající volitelné argumenty se opět týkají použitého tělesa a jsou ve stejném pořadí jako v předchozí funkci.

remove_trailing_zeroes

Tato funkce na vstupu obdrží polynom a odstraní z jeho konce přebytečné nuly. V případě, že je celý seznam nulový, jednu nulu v něm ponechá.

Použité těleso

V modulu je použito ve výchozím režimu těleso Zp, pro které platí:

p = 3*2^30 + 1

g = 125

n = 2^30

Kde p je modulo a g je generátor generující n pro FFT vhodných hodnot.

Technická dokumentace

Použil jsem algoritmus pro násobení polynomů na konečném tělese pomocí FFT tak, jak je to popsáno v knize Průvodce labyrintem algoritmů. FFT jsem implementoval iterativně.

Algoritmus dostane dva polynomy a z jejich délek zjistí délku výsledného polynomu. Tu zaokrouhlí nahoru na nejbližší mocninu dvojky a získá tak počet hodnot, které musí do polynomu dosadit.

Dosazení všech těchto do obou polynomů udělá modul pomocí dvou zavolání FFT a získá tak dva seznamy výsledných hodnot. Následně algoritmus po dvou vynásobí složky těchto seznamů a získá seznam hodnot, který určuje jednoznačně výsledný polynom. Ten algoritmus získá pomocí FFT, jen v něm používá místo původního generátoru jeho inverzi.