Univerzita Karlova
Přírodovědecká fakulta

Základy programování

#18 Rozklad čísla na součin prvočísel

David Šklíba 3. ročník BGEKA Jablonec nad Nisou 2021

Zadání:

Ze standartního vstupu přečtěte číslo c. Vyjádřete ho jako součin prvočísel ve tvaru: $c = p_1 * p_2 * \ldots * p_n$ a výsledek vytiskněte.

Pojem prvočíslo

Prvočíslo je přirozené číslo dělitelné číslem jedna a sebou samým. Samotné číslo jedna prvočíslem není, tudíž nejnižším prvočíslem je číslo 2, které je zároveň jediným sudým prvočíslem. Každé přirozené číslo N > 1 lze rozložit na součin prvočísel.

Algoritmy prvočíselného rozkladu

Faktorizace dělením („Hrubá síla“)

Tento algoritmus vychází z již předdefinované množiny prvočísel. Číslo, jehož rozklad se má provést je postupně děleno jednotlivými prvočísly. Nejprve je tedy číslo děleno prvočíslem dva, a to do té doby, než vznikne dělením výsledek se zbytkem. V tom případě, se přistoupí k dělení prvočíslem tři. Rozklad čísla končí v momentě, kdy je výsledek rovný jedné.

Pollardův rho algoritmus

Při vytvoření posloupnosti podle vztahu: $x_i \equiv x_i^2 + 1 \pmod{N}$, kde x_0 je zvolené přirozené číslo a N číslo rozkládané se v posloupnosti objeví cykličnost. Společní dělitelé rozdílů dvojic hodnot v posloupnosti a čísla N poté odhalí prvočíselný rozklad.

Pollardův p - 1 algoritmus

Algoritmus vychází z formulace Malé Fermatovy věty, ze které pro nalezení největšího společného dělitele vyplývá následující vztah: $D(a^{B!} - 1, N) > 1$, kde $a > 0$ je přirozené číslo nesoudělné s rozkládaným číslem N. Zvyšováním hodnoty B algoritmus pravděpodobně nalezne netriviálního dělitele čísla N.

Eulerova metoda

Tento algoritmus je využitelný v případě možnosti rozkladu čísla N na součet dvou čtvercových čísel. Využitím největšího společného dělitele jsou vypočteny konstanty k, l, m, n, skrze které dojde k rozložení čísla N na prvočísla podle vzorce: $N = [(k/2)^2 + (n/2)^2] \cdot (m^2 + l^2)$.

(Šuster 2018)

Zvolený algoritmus

Pro prvočíselný rozklad byl využit princip faktorizace dělením, ovšem s jedním rozdílem. Využitím tzv. „hrubé síly“ se na začátku algoritmu objevuje vytvoření datové struktury obsahující konečnou množinu prvočísel. Ta je však nekonečná, a proto program sám po inkrementaci dělitele rozliší, zdali se jedná o prvočíslo.

Struktura programu

Program nejprve ošetří validitu vstupní číselné hodnoty N. Vzhledem k omezení množiny čísel, která mohou být rozložena na součin prvočísel, program proběhne pouze pro hodnoty ležící v množině přirozených čísel, pro které platí: N > 1. Při zadání jiné hodnoty program skončí chybovou hláškou.

V další fázi program vytvoří 4 lokální proměnné. Při nacházení prvočíselných dělitelů hodnoty N dochází v hlavní části k postupnému zmenšování této vstupní hodnoty. Jakmile je podíl hodnoty N a daného prvočísla roven jedné, program vypíše součin prvočísel a skončí. V případě, že je vstupní hodnota N prvočíslo, program jej rozpozná a tuto informaci namísto prvočíselného rozkladu vypíše.

Popis vstupních a výstupních dat

Vzhledem k základní větě aritmetiky, která udává, že každé přirozené číslo větší než 1 lze jednoznačně rozložit na součin prvočísel, jsou vstupní data omezena právě na tuto množinu. Výstup je zobrazen v terminálu a nikam se neukládá.

Problematická místa a možnosti vylepšení

Problém zvoleného algoritmu tkví v jeho zvyšující se výpočetní náročnosti s rostoucí vstupní hodnotou. V případě, že se v součinu prvočísel objevuje vysoká hodnota prvočísla, program toto číslo hledá dlouze, protože nedělí proměnnou n pouze prvočísly. Výpočetní náročnost by mohla poklesnout ústupem od dynamického vyhledávání prvočísel za pomoci inkrementace. Použitím Eratosthenova síta by mohla vzniknout množina prvočísel, která jsou menší nebo rovna vstupní hodnotě. Program by tak provedl méně výpočetních úkonů.

Seznam literatury:

Šuster Z. (2018): Některé metody pro prvočíselné rozklady. Diplomová práce. Katedra matematiky, fyziky a technické výchovy, FPe ZČU, Plzeň.