

Univerzita Karlova
Přírodovědecká fakulta
Úvod do programování



Úloha č. 18
Rozklad čísla na součin prvočísel
Václav Thám 3. ročník B-SGG
Chlum 2022

Zadání:

Ze standardního vstupu přečtete číslo c . Vyjádřete ho jako součin prvočísel ve tvaru:
 $c = p_1 * p_2 * \dots * p_n$ 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 roven jedné.

Pollardův rho algoritmus

Při vytvoření posloupnosti podle vztahu: $x_i \equiv x_{i-1}^2 + 1 \pmod{N}$, 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. Algoritmus funguje na principu toho, že se přirozené číslo zkouší dělit prvočísly, které se zvyšují postupně od 2 pokud, se přirozené číslo po vydělení pořád dá dělit stejným prvočíslem

pouze se navýší exponent. Pokud dělit nejde vytiskne prvočíslo případně s exponentem pokud je tam vícekrát. tento cyklus se opakuje pokud je přirozené číslo větší než 1. Pokud je přirozené číslo zároveň prvočíslo program ho rovnou vytiskne.

Pseudokód

```
import math
```

```
# Funkce, která rozloží vstupní parametr n (přirozené číslo větší než 1) na součin prvočísel  
definování funkce přirozeného čísla na prvočíslo
```

```
# Ověřte, zda je vstupní hodnota správná, pokud není zadána správně, program končí.
```

```
Když přirozené číslo je menší nebo rovno 1
```

```
    program skončí
```

```
Když přirozené číslo není dělitelné 1 beze zbytku
```

```
    program skončí
```

```
program vytiskne jakého čísla provádí rozklad
```

```
vytvoření lokální proměnné m= přirozené číslo
```

```
vytvoření lokální proměnné exponent = 0
```

```
vytvoření lokální proměnné prvočíslo = 2
```

```
# Cyklus prvočíselného rozkladu
```

```
Pokud přirozené číslo je větší než 1
```

```
    # podmínka, zda je n dělitelné prvočíslem. Zjistí, zda existuje stejné prvočíslo  
jednou nebo dvakrát
```

```
    Když přirozené číslo je dělitelné prvočíslem
```

```
        exponent zvětší o 1
```

```
        přirozené číslo = přirozené číslo / prvočíslo
```

```
    # vytiskne hodnoty, pokud je prvočíslo pouze jednou nebo vícekrát
```

```
Jinak
```

```
    Když exponent je roven 1
```

```
        vytiskne program prvočíslo
```

```
    Když exponent je vyšší než 1
```

```
        vytiskne program prvočíslo s platným exponentem
```

```
        prvočíslo zvýší o 1
```

```
        exponent vynuluje
```

```
# Podmínka, pokud je vstupní hodnotou prvočíslo
```

```
Když prvočíslo je rovno proměnné m
```

```
    vytiskne přirozené číslo je zároveň prvočíslo
```

```
Jinak
```

```
    Když je exponent roven 1
```

```
        vytiskne prvočíslo
```

```
    Když je exponent větší než 1
```

```
        vytiskne prvočíslo a exponentvytvoření konstanty přirozené číslo
```

```
Když typ přirozeného čísla se nerovná integer
```

```
    program skončí
```

```
spuštění funkce přirozeného čísla na prvočíslo
```

Dokumentace

Popis programu

Program pomocí faktorizace dělením rozdělí dané číslo n na součin prvočísel, který je vepsán do terminálu.

Funkce rozkládající vstupní parametr n

Funkce `decomp_into_prime_num(n)` nejprve ošetří validitu vstupního parametru 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 funkce vytvoří 4 lokální proměnné. Proměnná `m` zachovává hodnotu vstupního parametru n , proměnná `num` je dílčí hádaný prvočíselný dělitel, proměnná `exp` značí mocninu daného prvočíselného dělitele v rozkladu a proměnná `prime` se stará o navyšování hádaného prvočíselného dělitele. Při nacházení prvočíselných dělitelů hodnoty n dochází v hlavní části k postupnému zmenšování vstupní hodnoty n . 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 místo prvočíselného rozkladu vypíše.

Vstupy a výstupy:

Vzhledem k základní větě aritmetiky, která udává, že každé přirozené číslo větší než 1 lze jednoznačně rozložit na součin prvočísel, jsou vstupní data omezená 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 klesnout 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.