Zápočtový program

Jakub Šošovička

August 2024

1 Úvod

Program obsahuje dva algoritmy na rozkladanie prvočísel a to Eulerov algoritmus a Fermatov algoritmus. Program dostane na vstupe číslo a rozkladá ho postupne obomi algoritmami.

2 Fermatov algoritmus

2.1 Algoritmus

Princíp Fermatovho algoritmu je vyjadriť číslo na vstupe ako rozdiel dvoch druhých mocnín. Pokiaľ totiž $n = a^2 - b^2$, tak $n = (a - b)(a + b)$. Tým sme našli netriviálneho deliteľa čísla n (pokiaľ $a - b \neq 1$). Rekurzívne potom môžeme rozložiť aj jeho delitele a proces opakovať kým nedostaneme prvočísla.

2.2 Program

Program najskôr skontroluje prvých $\sqrt[3]{n}$ čísel, či nedelia číslo na vstupe. Tento krok zrýchli program pokiaľ je vstupom "náhodné" číslo a keďže časová zložitosť algoritmu je $\sqrt{n}$, tak program veľmi nespomaluje. Následne program hľadá spomínané vyjadrenie čísla n ako rozdiel dvoch štvorcov $n = a^2 - b^2$. To robí funkcia *Find_Squares*. Tá hľadá číslo a vo vyjadrení smerom od odmocniny z n vyššie. K nemu dopočíta b. Pokiaľ sa hodnota $a - b$ začne zmenšovať o menej ako 1, tak sa menšie hodnoty $a - b$ overia triviálne. Pokiaľ program nájde v nejakom momente netriviálneho deliteľa d, rekurzívne sa zavolá na čísla d a $\frac{n}{d}$. Pokiaľ deliteľa nenájde, tak je n nutne prvočíslo. Rekurzívne na konci dostaneme zoznam s prvočíselnými deliteľmi. Funkcia *fact* potom tento zoznam premení na string. Napríklad pri rozklade čísla 24 dostaneme zoznam, v ktorom bude 3-krát číslo 2 a raz číslo 3. Ten program premení na string 2^3 * 3.

2.3 Príklad

Pre vstup $n = 1641643 = 1009 \cdot 1627$ by vyzeral nasledovne. Program by najskôr overil delitele do $\sqrt[3]{n} < 1009$, teda deliteľa by nenašiel. Ďalej by hľadal rozklad $n = a^2 - b^2$. Keďže $\sqrt{n} = 1281.3$, program začne na $a = 1282$. Program neskôr nájde rozklad pre $a = 1318, b = 309$, teda delitele sú $a - b = 1009, a + b = 1627$.

Pre prvočíselný vstup $n = 10007$ by sa hľadanie rozdielu štvorcov skončilo skôr. Opäť by program začal na $a = 101$. Program v každom kroku dopočíta b zo vzťahu $b^2 = a^2 - n$. Pre $a = 116$ dostaneme $b = 58.73$, teda $a - b = 57.27$. Pre $a = 117$ dostávame $b = 60.68$, teda $a - b = 56.32$. Rozdiely sa zmenšili o menej ako 1, a preto program overí zvyšné hodnoty deliteľov od $d = 56$ nižšie triviálnym algoritmom.

2.4 Funkčnosť programu

Program rozloží každé prirodzené číslo. Pokiaľ je číslo párne, vydelí ho dvomi. Pokiaľ je číslo nepárne, potom nutne musí mať rozklad tvaru $n = pq$ pre nepárne p, q (nie nutne prvočísla). Potom $n = \left(\frac{p+q}{2} - \frac{p-q}{2}\right)\left(\frac{p+q}{2} + \frac{p-q}{2}\right)$. Pri hľadaní rozkladu hodnota $a - b$ klesá, keďže $(a - b)(a + b) = n$ je konštantné a s rastúcim a rastie aj b, teda aj $a + b$. Preto program nemôže "preskočiť"žiadneho deliteľa pri hľadaní rozdielu štvorcov. Napriek tomu, že je tento algoritmus rýchlejší ako triviálne overovanie deliteľov po odmocninu, časová zložitosť je $\sqrt{n}$. V porovnaní s ostatnými rozkladacími algoritmami, algoritmus najlepšie funguje, ak je n súčinom dvoch prvočísel, ktoré sú "blízko pri odmocnine".

3 Eulerov algoritmus

3.1 Algoritmus

Princíp Eulerovho algoritmu spočíva vo vyjadrení čísla ako súčet dvoch štvorcov dvoma spôsobmi. Teda $n = a^2 + b^2 = c^2 + d^2$. Potom nech $k = gcd(a - c, b - d), m = gcd(a + c, b + d)$, kde $gcd(x, y)$ značí najväčšieho spoločného deliteľa čísel x, y. Potom je dokázané, že nutne:

$$n = \left(\frac{k^2 + m^2}{4}\right)\left(\left(\frac{a-c}{k}\right)^2 + \left(\frac{a+c}{m}\right)^2\right)$$

.

3.2 Program

Program najskôr skontroluje zvyšok po delení 4. Ak je číslo párne, vydelí ho dvomi a pokračuje rekurzívne ďalej. Ak má zvyšok 3, určite sa nebude dať zapísať ako súčet dvoch štvorcov, keďže štvorce môžu mať zvyšky iba 0 alebo

1 modulo 4. Teda program vráti číslo na vstupe. Pokiaľ má číslo zvyšok 1 po delení 4, program hľadá jeho vyjadrenie ako súčet dvoch štvorcov. Pokiaľ nájde dve také vyjadrenia, spočíta z nich vyššie spomínaný rozklad. Funkcia *fact* na záver rovnako prevedie zoznam čísel na string v tvare rozkladu.

3.3 Príklad

Vyskúšame program na vstupe $n = 1000009 = 1000^2 + 3^2 = 972^2 + 235^2$. Program nájde tieto dve vyjadrenia ako súčet dvoch druhých mocnín. Z nich dopočíta $k = gcd(a-c, b-d) = 4, m = gcd(a+c, b+d) = 34$. Z toho dopočíta rozklad $n = \left(\frac{4^2+34^2}{4}\right)\left(\left(\frac{28}{4}\right)^2 + \left(\frac{1972}{34}\right)^2\right) = 293 \cdot 3413$.

3.4 Funkčnosť programu

Program nenájde rozklad pre všetky n, napríklad ak n dáva zvyšok 3 modulo 4. Je známe, že číslo, ktoré je súčinom dvoch čísel, ktoré sa obe dajú vyjadriť ako súčet dvoch štvorcov, sa dá vyjadriť ako súčet dvoch štvorcov dvoma spôsobmi, teda ho program rozloží (nájde netriviálneho deliteľa). Túto vlastnosť spĺňajú všetky prvočísla tvaru $4k + 1$. Program teda nájde deliteľa napríklad vždy vtedy, keď číslo na vstupe obsahuje v rozklade iba prvočísla tvaru $4k + 1$. Avšak napríklad číslo $n = pq$, kde p, q sú prvočísla tvaru $4k + 3$ rozložiť nevie aj napriek tomu, že n dáva zvyšok 1 po delení 4. Program najlepšie funguje (v porovnaní s ostatnými rozkladacími algoritmami) pre vstupy $n = pq$, kde p, q sú prvočísla tvaru $4k + 1$.