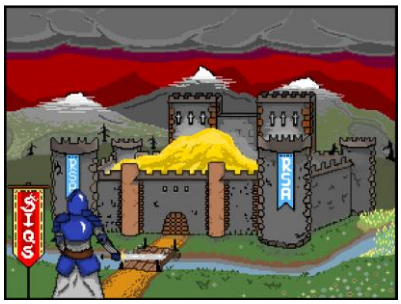
Excel@FIT

ID práce: 60

Paralelní faktorizace celých čísel metodou SIQS

Bc. Dominik Breitenbacher



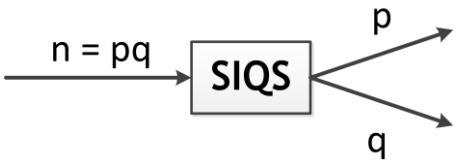
Motivace

Práce se zabývá rozkladem složeného čísla na jeho faktory. Za tímto účelem byla vybrána faktorizační metoda zvaná SIQS. SIQS je považována za nejrychlejší metodu k faktorizaci čísel do 100 dekadických číslic.

Cílem této práce je také ukázat, jak jednoduše lze v mnoha případech využít paralelizace kódu a dále také, jak díky podrobné analýze kódu lze dosáhnout poměrně velkého urychlení. Představenou metodikou se podařilo implementaci urychlit až 99-krát.

Faktorizace

- Faktorizace je proces, při kterém se snažíme zpětně nalézt faktory složeného čísla



- Nelze efektivně řešit v konečném čase
- Na problému faktorizace je založena šifra RSA
- Faktorizace RSA-1024 je dnes nezvládnutelné

SIQS – Self-Initialization Quadratic Sieve

SIQS je nejrychlejší metodou pro faktorizování čísel do 100 dekadických číslic a obecně je metoda druhou nejrychlejší z doposud objevených. Problémem této metody je ale její poměrně velká náročnost na pochopení, což může odradit případné zájemce o tuto metodu.

Jedním z cílů této práce tak je metodu SIQS přiblížit a vysvětlit všem zájemcům o faktorizace. Za tímto účelem je tvořen dokument, který metodu SIQS popisuje a také problémy, s nimiž se může zájemce setkat při implementaci a tyto problémy jsou zde zároveň řešeny.

Profilace a optimalizace

Implementace probíhala ve dvou fázích. V první fázi byl naimplementován kompletní a funkční algoritmus, zatím bez přihlédnutí k požadavkům na rychlost (referenční verze).

Optimalizace na rychlost byla druhou fází řešení celého zadání. Metodika iteračního provádění se ukázala jako velmi účinná a je použitelná obecně, nejenom v této úloze.

Optimalizace spočívala v důsledné paralelizaci všude tam, kde to bylo možné z podstaty algoritmu, v jednotlivých iteracích pak docházelo ke změnám datových typů za jiné, vhodnější (mapy na vektory, bool na uint64 apod.).

⊞ SieveValues	731.829s
⊞ FastGaussian	644.813s
⊞ _gmpn_divrem_1	592.906s
⊞ log	334.865s
⊞ DeleteDuplicants$c	308.109s
⊞ _gmpz_powm	253.242s
⊞ std::operator<<<s	223.865s

Obrázek: Ukázka výsledku profilování SIQS

Po doposud všech provedených optimalizacích bylo dosaženo 99-násobného urychlení u faktorizace čísla s 60 dekadickými číslicemi (197 bitů).

Po poslední optimalizaci byl proveden pokus o faktorizování čísla o 100 dekadických číslicích (332 bitů). Faktorizování tohoto čísla bylo úspěšné a trvalo 2 dny 16 hodin a 13 minut.

Budoucí práce

Vývoj na implementaci SIQS nebyl ukončen. Je zde stále mnoho nápadů, jak implementaci dále urychlit. S postupem času tak budou jednotlivé myšlenky do implementace zapracovány.