Katedra Informatiky
Fakulta Matematiky, Fyziky a Informatiky
Univerzita Komenského, Bratislava

Algoritmus Quadratic Sieve

(Bakalárska práca)

Marek Košta

Vedúci: RNDr. Jaroslav Guričan, CSc.

Bratislava, 2009

Čestne prehlasujem, že som túto bakalársku prácu vypracoval samostatne s použitím citovaných zdrojov.

.....

Touto cestou chcem poďakovať môjmu vedúcemu RNDr. Jaroslavovi Guričanovi, CSc. za ochotu, čas, cenné rady a poznámky pri písaní práce. Tiež chcem poďakovať mojej rodine a priateľom za podporu počas celého štúdia.

Abstrakt

Práca pojednáva o algoritme na hľadanie netriviálneho deliteľa k vstupnému celému číslu n. Algoritmus je známy pod názvom Quadratic Sieve, autorom hlavnej myšlienky je Carl Pomerance. Popisujeme základnú ideu preosievania, ktorá prispieva k efektivite algoritmu. Pojednávame o úspešnosti algoritmu, nakoľko algoritmus sa dá chápať ako pravdepodobnostný a heuristický. Podávame argumenty k zložitosti algoritmu, ktoré podporujú očakávanie subexponenciálneho času behu. Z hľadiska realizácie algoritmu spomíname metódy na riešenie každej fázy. V závere spomíname rôzne varianty a vylepšenia algoritmu.

Kľúčové slová:
Quadratic Sieve, faktorizácia celých čísel, kongruencia štvorcov, prvočíslo, konečné pole, binárna matica

Obsah

Kapitola 1

Úvod

Dôležitosť a význam faktorizácie celých čísiel ako problému netreba nijako zvlášť predstavovať ani prízvukovať. Má veľký teoretický a v modernej dobe najmä praktický význam. Teoretický význam spočíva hlavne v myšlienke „čo ešte ide“, teda kde ležia hranice medzi problémami riešiteľnými efektívne a medzi problémami, ktoré nie sme schopní s nám doteraz známymi prostriedkami uspokojivo riešiť. Z toho praktického hľadiska stačí spomenúť informačnú bezpečnosť, pre ktorú má problém faktorizácie kritický význam. Žiarivým príkladom je šifrovacia schéma RSA, ktorej bezpečnosť stojí na tomto probléme. Ak by sme boli schopní efektívne faktorizovať aj veľké čísla, potom pohľad na informačnú bezpečnosť by sa razantne zmenil a techniky ktorých používanie je dnes samozrejmosťou a istou zárukou kvality by neboli použiteľné.

Ak sa pozrieme na súčasný stav faktorizačných algoritmov v popredí sú dva takzvané General-purpose algoritmy a to sú Quadratic Sieve a General Number Field Sieve. Algoritmus General Number Field Sieve je akýmsi vylepšením algoritmu Quadratic Sieve. V súčasnej dobe je to najlepší známy faktorizačný algoritmus.

General-purpose znamená, že čas behu algoritmu nezávisí na špeciálnom

tvare čísla n, ktoré chceme faktorizovať, ale iba na jeho veľkosti. Špeciálnym tvarom môže byť napríklad počet prvočíselných deliteľov n. Ďalej zaujímavým(a význačným) je tiež predpoklad, že n má v prvočíselnom rozklade prvočísla s mocninou vždy aspoň dva. Iným príkladom môže byť faktorizovanie tzv. Mersenneových čísel, respektíve problém rozhodovania, či je Mersenneovo číslo prvočíslo. Mersenneovo číslo je definované ako $M_n = 2^n - 1$. Keďže ale predpokladáme nejaký špeciálny tvar, problém faktorizácie v „jednoduchej“ forme sa môže zmeniť z ťažkého na jednoduchší alebo sa môžu použiť techniky vo všeobecnosti neefektívne alebo vôbec nepoužiteľné. General-purpose algoritmy žiadne takéto predpoklady na vstupné n pri postupoch alebo výpočtoch nepoužívaju a tým pádom ani nevyžadujú. Teda ich čas behu a pravdepodobnosť úspechu(ak hovoríme o pravdepodobnostných algoritmoch) v nijakej razantnej miere nezáleží na špeciálnych predpokladoch, hoci za niektorých predpokladov môže byť ľubovoľný z týchto parametrov(alebo dokonca aj oba) kolísať, lenže iba do tej miery do akej to povoľujú garancie, odhady a dokázané tvrdenia. Hlavným parametrom od ktorého sa všetky vlastnosti algoritmu a tým aj jeho efektívnosť odvíja je preto *jedine* veľkosť vstupného čísla n. Toto je podstata pojmu General-purpose.

V tejto práci sa venujeme popisu hlavných častí a myšlienok algoritmu Quadratic Sieve.

Kapitola 2

Hlavné myšlienky algoritmu

Pre úplnosť treba definovať problém, ktorý sa algoritmus Quadratic Sieve vôbec snaží riešiť. Nebudeme uvažovať o probléme faktorizácie v klasickom slova zmysle, to jest je dané vstupné celé číslo n a výstupom má byť rozklad

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} \tag{2.1}$$

kde p_i sú prvočísla, ktoré sú navzájom rôzne. Toto je úplný prvočíselný rozklad čísla n. V tejto práci je problém faktorizácie ponímaný ako „jednoduchšia“ verzia klasického problému a to tak, že vstupom je n a výstupom je ľubovoľný netriviálny deliteľ n. Samozrejme, pomocou hľadania netriviálneho deliteľa sme schopní klasický problém buď úplne vyriešiť, alebo jeho riešenie rozdeliť na podproblémy podľa nájdených netriviálnych deliteľov čísla n.

V tejto kapitole nebudeme uvádzať všetky jednoduché pojmy známe už zo strednej školy, resp. fundamentálne pojmy z elementárnej teórie čísel. V celej kapitole znamená obvykle n vstupné číslo, teda také pre ktoré chceme nájsť netriviálneho deliteľa, p, q sú obvykle prvočísla. O n vždy predpokladáme, že je nepárne. Tiež budeme používať označenie z (2.1), lebo na základe fundamentálnej vety aritmetiky vieme, že pre zložené n rozklad v takom tvare existuje. Napriek tomu pre úplnosť a jednoznačnosť nejaké pojmy definujeme.

Definícia 2.1 *Hovoríme, že číslo x je kvadratickým zvyškom(rezíduom) modulo n ak existuje také a, že $a^2 \equiv x \bmod n$. Ak také a neexistuje, číslo x nazývame nerezíduum.*

Definícia 2.2 *Nech $B \geq 2$. Číslo x sa nazýva B-hladkým (anglicky B-smooth) ak každý jeho prvočíselný deliteľ je nanajvýš B.*

Ďalej budeme používať zaužívané označenie $\gcd(a, b)$[1], ktorým sa označuje najväčší spoločný deliteľ čísel a a b.

2.1 Kongruencie štvorcov

Ako už názov algoritmu (Quadratic) napovedá, bude využívať takzvanú kongruenciu štvorcov, teda kongruenciu

$$x^2 \equiv y^2 \bmod n \tag{2.2}$$

Lebo ak máme k dispozícií čísla x a y ktoré spĺňajú kongruenciu (2.2) platí $n \mid (x-y)(x+y)$. Potom výpočtom najväčšieho spoločného deliteľa $\gcd(x-y, n)$, alebo $\gcd(x+y, n)$ máme veľkú pravdepodobnosť, že tento bude netriviálnym deliteľom čísla n. Je samozrejmé, že ak $x \equiv \pm y$ tak nám výpočet gcd nič nepovie, lebo gcd bude v tomto prípade buď n, alebo 1.

Vidíme, že ak vieme nájsť dvojicu x a y zo vzťahu (2.2) pričom $x \not\equiv \pm y$ tak potom vieme aj efektívne faktorizovať. Kľúčovou otázkou teda je, ako hľadať táketo dvojice.

S ideou faktorizovať pomocou (2.2) prišiel už v roku 1920 Maurice Kraitchik.

[1] z anglického greatest common divisor

2.2 Prvočíselná báza

Definícia 2.3 *V ďalšom budeme prvočíselnou bázou nazývať vzostupne usporiadanú množinu prvočísel* p_1, p_2 $\ldots p_b$.

Nech $f(x)$ je nejaký vhodne zvolený polynóm. Predstavme si, že máme k dispozícií množiny M_1, a M_2 také, že $|M_1| = |M_2| = m$ pričom $x_i \bmod n \in M_1$ a $f(x_i) \bmod n \in M_2$. Teda máme k sebe prislúchajúce čísla x_i a $f(x_i) \bmod n$ rozdelené do dvoch množín, pričom čísla $f(x_i) \bmod n$ sa dajú rozložiť nad prvočíselnou bázou. V algoritme sa používa $f(x)$ spravidla druhého stupňa. Odtiaľ je aj v názve slovo Quadratic. Základný algoritmus používa $f(x) = x^2 \bmod n$. Prvočíslo p_b, respektíve jeho rozumné horné ohraničenie z predošlej definície budeme označovať B. Teda všetky čísla z množiny M_2 sú B-hladké. To znamená, že

$$f(x_i) \bmod n = p_1^{\beta_1} p_2^{\beta_2} \ldots p_b^{\beta_b} \tag{2.3}$$

Ak máme pevne danú prvočíselnú bázu, môžeme teda čísla z množiny M_2 reprezentovať ako vektor exponentov. Presnejšie číslu $f(x_i) \in M_2$ priradíme vektor $(\beta_1, \ldots, \beta_b)$ z rovnosti (2.3).

Popíšme bližšie takúto reprezentáciu čísel pomocou vektorov exponentov. Táto reprezentácia má zjavnú výhodu, čo sa týka násobenia čísel. Ak totiž máme dve čísla c, $d \in M_2$ reprezentované ako exponent vektor s b súradnicami, tak vektor exponentov súčinu cd je iba súčet týchto vektorov po zložkách. Toto je zjavné z toho, že c aj d sa dajú rozložiť *úplne* nad prvočíselnou bázou, presnejšie kvôli *rovnosti* (2.3). Tiež je hneď vidno, že ak máme číslo c a jeho exponent vektor je tvaru $(2c_1, 2c_2, \ldots, 2c_b)$, teda každá súradnica je párna, vieme c ľahko odmocniť. Odmocninou je číslo, ktorého exponent vektor je $(c_1, \ldots, c_b)$.

Zámerom teraz je nájsť takú podmnožinu čísel z množiny M_2, že ich súčin bude štvorcom. Označme si túto množinu ako M_2' a k nej prislúchajúcu

podmnožinu množiny M_1 ako M_1'. V reči exponent vektorov to znamená, že chceme nájsť takú podmnožinu čísel reprezentovaných ako exponent vektory že súčet týchto vektorov po zložkách nám dá vektor, ktorý bude mať všetky súradnice párne. Keďže náš polynóm je $x^2 \bmod n$, tak budeme mať kongruenciu $x^2 \equiv y^2 \bmod n$ kde

$$\begin{aligned} x &= \left(\prod_{o \in M_1'} o \right) \bmod n \\ y^2 &= \left(\prod_{o \in M_2'} o \right) \bmod n \end{aligned}$$

z voľby M_2' vyplýva, že vieme vypočítať aj y ako predelenie každej súradnice exponent vektora čísla y^2 dvomi. Samozrejme nič nám nezaručuje, že pre y ktoré takto dopočítame platí $x \not\equiv \pm y$. Tento fakt je obvykle ignorovaný, neskôr uvedieme argumenty prečo.

Odpovieme teraz na otázku, ako nájsť podmnožinu M_2'. Ak si zapíšeme exponent vektory $f(x_i)$ z množiny M_2 do riadkov matice $\mathbf{M}$ rozmerov $m \times b$, potom nás zaujíma, ktoré riadky spolu treba sčítať aby sme dostali vektor iba s párnymi súradnicami. Teda si stačí uvedenú maticu predstaviť modulo 2. Takto dostaneme maticu nad poľom $\mathbb{Z}_2$. V ďalšom pre nás $\mathbf{M}$ bude znamenať maticu s exponent vektormi modulo 2. Formálne teraz treba vyriešiť sústavu lineárnych rovníc

$$\mathbf{M}^{\mathrm{T}}.\mathbf{Z}^{\mathrm{T}} = \mathbf{0} \tag{2.4}$$

pričom $\mathbf{Z} = (z_1, \ldots, z_m)$ sú neznáme. Teraz z lineárnej algebry vieme, že ak chceme mať zaručenú existenciu netriviálneho riešenia tejto sústavy rovníc, tak musí mať matica $\mathbf{M}$ viacej riadkov ako stĺpcov. Toto je postačujúca podmienka pre existenciu netriviálneho riešenia. Takúto sústavu vyriešime a dostaneme netriviálny vektor $(z_1, \ldots, z_m)$, kde $z_i \in \{0,\ 1\}$. Máme teda

$$M_1' = \{x_i \in M_1 \mid z_i = 1\}$$

$$M_2' \;=\; \{f(x_i) \in M_2 \mid z_i = 1\}$$

a keďže riešenie je netriviálne sú M_2' a k nej prislúchajúca M_1' neprázdne.

Zároveň sme aj odpovedali na otázku koľko dvojíc treba do množín M_1 a M_2 nazbierať, aby sme vedeli v nej určite nájsť kongruenciu štvorcov. Presnejšie aby sme mali netriviálne riešenie vzťahu (2.4). Z uvedeného vidno, že tento počet prvkov je aspoň $b + 1$.

Uveďme pre ozrejmenie príklad realizácie vyššie popísaných ideí na malých číslach. Majme dané $n = 103 * 73 = 7519$. Zvoľme veľkosť faktor bázy 4, teda v nej budeme mať prvočísla 2, 3, 5 a 7. Skúšajme rozkladať nad touto bázou čísla z intervalu $[\lceil\sqrt{n}\rceil; \lfloor\sqrt{2n}\rfloor]$ Neskôr pri preosievaní uvidíme prečo takáto voľba intervalu, ale už teraz môžeme upozorniť na to, že výhodou je platnosť $x^2 \bmod n = x^2 - n$ pre $x \in [\lceil\sqrt{n}\rceil; \lfloor\sqrt{2n}\rfloor]$. V tomto konkrétnom prípade teda postupným rozkladom čísel $x^2 - n$, $x \in [86; 122]$ nad našou faktor bázou dostaneme:

$$\begin{aligned}
87^2 &\equiv 50 \bmod n = 2^1 3^0 5^2 7^0 \\
88^2 &\equiv 225 \bmod n = 2^0 3^2 5^2 7^0 \\
92^2 &\equiv 945 \bmod n = 2^0 3^3 5^1 7^1 \\
97^2 &\equiv 1890 \bmod n = 2^1 3^3 5^1 7^1 \\
111^2 &\equiv 4802 \bmod n = 2^1 3^0 5^0 7^4
\end{aligned}$$

V súlade s označením zavedeným vo vzťahu (2.4) je teda

$$\mathbf{M} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

čo sú vektory exponentov modulo 2 zapísané v riadkoch matice. Pripomíname, že sme skončili hneď ako sme našli viac dvojíc ako je počet prvkov

faktor bázy, teda máme zaručenú existenciu netriviálneho riešenia systému. Ostatné čísla z intervalu $[86; 122]$ sa nedajú úplne rozložiť nad faktor bázou. Opäť v súlade s označením v (2.4) máme

$$\mathbf{M}^{\mathrm{T}}(z_1, z_2, z_3, z_4, z_5)^{\mathrm{T}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Báza riešení tohto systému je $(0, 1, 0, 0, 0)\,; (1, 0, 1, 1, 0)\,; (1, 0, 0, 0, 1)$. Ak vezmeme napríklad posledný vektor, tak vieme, že vynásobením prvej a piatej dvojice dostaneme štvorce na oboch stranách(lebo $(1, 0, 0, 0, 1)$ je riešením). Konkrétne teda máme

$$\begin{aligned} 87^2 111^2 &\equiv (2^1 3^0 5^2 7^0) * (2^1 3^0 5^0 7^4) \bmod n \\ (87 * 111)^2 &\equiv (2^2 3^0 5^2 7^4) \bmod n \\ x^2 &\equiv y^2 \bmod n \\ x &\equiv 87 * 111 \bmod n = 2138 \\ y &\equiv 2^1 3^0 5^1 7^2 \bmod n = 490 \\ (x - y)(x + y) &\equiv 0 \bmod n \\ (2138 - 490)(2138 + 490) &\equiv 0 \bmod n \end{aligned}$$

Výpočet $\gcd(x - y, n) = \gcd(1648, 7519)$ nám dá 103, teda netriviálneho deliteľa n. Iba upozornime, že sme kvôli demonštrácií toho, že sa pomocou riešenia systému (2.4) dá „namiešať“ kongruencia štvorcov úmyselne prehliadli, že už z kongruencie $88^2 \equiv 225 \equiv 15^2 \bmod n$ sme schopní výpočtom $\gcd(88 - 15, n)$ dostať faktorizáciu n. Tiež upozorňujeme, že v praxi sa nehľadá báza všetkých riešení systému, ako sme to urobili my pomocou štandradných metód lineárnej algebry. Ak sú totiž rozmery matice *veľké*, môže to

byť extrémne výpočtovo náročné. Preto v praxi hľadáme iba niekoľko netriviálnych riešení, povedzme dve alebo tri. V najhoršom prípade sa nám môže stať, že žiadne z nájdených riešení nevedie k netriviálnemu deliteľovi, potom treba algoritmus buď opakovať celý, alebo sa snažiť nájsť ďalšie netriviálne riešenie. V našom prípade je jedným takýmto nepriaznivým prípadom riešenie $(1, 0, 1, 1, 0)$. Preto ak by sme vynásobili prvú, tretiu a štvrtú rovnosť dostaneme iba $(87 * 92 * 97)^2 \equiv (2^1 3^3 5^2 7^1)^2 \bmod n$, teda $1931^2 \equiv 1931^2 \bmod n$. Toto evidentne nemá žiadnu výpovednú hodnotu o deliteľoch čísla n. Pravdepodobnosti úspechu sa budeme neskôr osobitne venovať.

2.3 Preosievanie

Zaoberajme sa teraz tým, ako efektívne hľadať množiny M_1 a M_2, teda aby sme vôbec mali dáta na to, aby sme mohli prikročiť k riešeniu (2.4).

Jednoduchým spôsobom ako získavať páry do množín M_1 a M_2 je vziať nejaký interval, alebo náhodne brať jednotlivé čísla dosádzať ich do polynómu $f(x)$ a predeľovaním zistiť, či sa dá $f(x)$ úplne rozložiť nad našou prvočíselnou bázou, teda či je B-hladké. Tento postup je však časovo veľmi náročný, lebo zahŕňa veľa operácií delenia.

Veľmi efektívny postup, ako hľadať vhodných kandidátov x takých, že $f(x)$ bude B-hladké číslo je pomocou takzvaného preosievania alebo sita, anglicky sieve.

Obvykle túto ideu realizujeme tak, že preosievame nejaký interval prirodzených čísel dĺžky d začínajúc od nejakého čísla o. Preosievanie spočíva v tom, že si do pamäte k číslu x zaznamenávame, či je číslo $f(x)$ deliteľné prvočíslom p_i. Prvým pozorovaním, ktoré má pre nás význam je takýto fakt.

Tvrdenie 2.4 *Nech $g(x)$ je polynóm a p prvočíslo. Ak $g(b) \equiv 0 \bmod p$, potom $g(b + kp) \equiv 0 \bmod p$, kde k je ľubovoľné celé číslo.*

Dôkaz. Nech $g(x) = a_n x^n + \ldots a_1 x + a_0$. Podľa binomickej vety platí, že

$$(b + kp)^n = \sum_{i=0}^{n} \binom{n}{i} b^i \, (kp)^{n-i}$$

teda modulo p sú všetky členy 0 okrem posledného, kedy $i = n$ a tento člen je b^n. Teda

$$\begin{aligned} g(b + kp) &= a_n(b + kp)^n + \ldots + a_1(b + kp) + a_0 \equiv \\ &\equiv a_n b^n + \ldots + a_1 b + a_0 = g(b) \equiv 0 \end{aligned}$$

□

Teda ak vezmeme z intervalu najmenšie také b, že $p \mid f(b)$, potom $p \mid f(b+kp)$ teda vieme a môžeme si zaznačiť, že $p \mid f(b + ip)$ pre každé $b + ip$ z nášho intervalu.

Toto v počítači realizujeme tak, že máme alokované v pamäti celočíselné pole A dĺžky d. Inicializujeme každý jeho prvok na 1. Potom postupne pre každé prvočíslo vo faktor báze nájdeme minimálne b také, že $p \mid f(o + b)$. Lebo na i-tom mieste poľa je uložené: súčin doteraz nájdených prvočíselných deliteľov čísla $f(o + i)$. Ak teda máme takéto b, prenásobíme b-ty prvok prvočislom p a ďalej aj každý p-ty nasledujúci. Toto spravíme pre každé prvočíslo v našej faktor báze.

Po skončení tohto postupu prechádzame pole A a ak platí, že $A[i] = f(o + i)$ našli sme B-hladké číslo $f(o + i)$. Teda pár prvkov $o + i$ a $f(o + i)$ môžeme pridať do našich množín M_1', resp. M_2'.

Uvedený postup nám určite pridal na efektívnosti, ale aj tak je stále dosť „drahý“, lebo intenzívne používame násobenie na všetkých kandidátov, pričom B-hladkých čísel bude z nich len dosť malý počet.

Ďalším problémom je aj to, že sme neopísali, ako efektívne hľadať minimálne b také, že $p \mid f(b)$. Jednoduché metódy v štýle „dosadzuj a skúšaj“ nás tiež budú stáť dosť veľa času, lebo prvočísla v našej faktorbáze sú pre

relevantné n na ktoré chceme algoritmus použiť dosť veľké. Uvedené výpočty sú tiež vykonávané s dosť veľkými číslami. Veľkými preto, lebo nemá zmysel hľadať páry b, $f(b)$ kde $b < \sqrt{n}$ ak uvažujeme avízovaný polynóm $f(x) = x^2 \bmod n$.

Čitateľa, ktorý nie je oboznámený s definíciou takzvaného Legendreovho symbolu, písaného ako $\left(\frac{a}{p}\right)$ odkazujume na definíciu (4.4). V ďalšom totiž toto označenie využijeme.

Interval na ktorom budeme robiť toto preosievanie bude $\lceil\sqrt{n}\rceil$ až $\lfloor\sqrt{2n}\rfloor$. Na tomto intervale je náš polynóm $x^2 \bmod n$ totožný s polynómom $x^2 - n$. Teraz vieme nájsť ľahko minimálne b s uvedenou vlastnosťou. Lebo na tomto intervale máme

$$p \mid f(x) = x^2 - n \quad \Rightarrow \quad \left(\frac{n}{p}\right) = 1$$

lebo ak $p \mid f(x)$ potom $x^2 - n \equiv 0 \bmod p$, teda $x^2 \equiv n \bmod p$, teda n je kvadratický zvyšok modulo p. Vieme že ak $\left(\frac{n}{p}\right) = 1$ tak rovnica $x^2 - n = 0$ má v $\mathbb{Z}_p$ dve riešenia, ktoré sú si navzájom opačné. Na ich nájdenie je uvedený algoritmus v kapitole 4. Teda nájdeme odmocniny z n modulo p pomocou uvedeného algoritmu, presnejšie dve zvyškové triedy. A pre každú takúto triedu b' nájdeme minimálne b z nášho intervalu tak, že $b \equiv b' \bmod p$. Toto je už veľmi jednoduché, lebo platí $i = b' - o \bmod p$, kde i je minimálny index v našom poli s uvednou vlastnosťou. Potom už iba urobíme prenásobenie prvočíslom p podľa predošlého postupu. Z povedaného tiež vyplýva, že do našej faktor bázy berieme iba také prvočísla, pre ktoré platí, že $\left(\frac{n}{p}\right) = 1$.

Tiež treba poznamenať, že preosievanie vo všeobecnosti nerobíme s mocninami prvočísel vo faktor báze. Dôvodov je viacero. Algoritmus pre odmocňovanie vo všeobecnosti nefunguje ak pracujeme modulo p^m, kde $m > 1$. Toto by ale nebol problém pre malé prvočísla. Omnoho väčším problémom je, že počet odmocnín z n modulo p^k môže byť až 2^k, teda počet zvyškových tried cez ktoré by sme museli preosievať by razantne narástol a tak by sa nám mohlo stať, že týmto preosievaním nič neušetríme.

Majoritné vylepšenie vďaka ktorému sa algoritmus Quadratic Sieve stal najlepším známym algoritmom na faktorizáciu v dobe jeho vymyslenia je myšlienka preosievania pomocou približných logaritmov čísel. Jej jednoduchosť je až prekvapujúca. Všetko sa deje tak ako v bežnom preosievaní ktoré sme popísali. Teda presnejšie nájdeme normálne prvočíselnú bázu, odmocniny z n pre každé prvočíslo aby sme vedeli cez aké zvyškové triedy treba sievovať. Rozdiel je „iba“ v tom, že namiesto násobenia prvkov poľa A uloženého v pamäti k týmto prvkov pripočítavame približné (celočíselné) logaritmy prvočísla ktorým práve preosiavame. Teda ak sievujeme prvočíslom p pripočítame ku každému prvku poľa A na ktorý narazíme $\lg p$, kde ale lg je *veľmi* približný. Pre naše účely stačí zobrať $\lg 2 = 1$, $\lg 3 = 2$, $\lg 5 = 2$, $\lg 7 = 3$. Používame pravidlo, že presný dvojkový logaritmus z p jednoducho zaokrúhlime. Pole A je teraz pre zmenu inicializované na nuly a sievované pomocou týchto veľmi hrubých odhadov. Po zbehnutí sita vyzbieranie prvkov vyzerá jednoducho: Prechádzame A a ak je hodnota $A[i]$ približne $lg(f(o+i))$ uložíme si pár $o + i$ a $f(o + i)$. Približná chyba sa obvykle berie okolo lgB. Celé toto vylepšenie funguje kvôli jednoduchému faktu, že

$$\lg(ab) = \lg(a) + \lg(b)$$

teda ak je číslo x B-hladké, tak jeho logaritmus, ak ho berieme presne je súčet logaritmov takýchto deliteľov. Keďže robíme iba hrubé odhady na $\lg(p)$, tak toto samozrejme neplatí, ale ostáva v platnosti, že ak je x B-hladké tak potom jeho hrubý logaritmus je dosť blízko súčtu približných logaritmov jeho deliteľov. Preto berieme ako kandidátov tie čísla, pre ktoré je súčet logaritmov ich deliteľov dosť blízko k nim. Toto je hlavná myšlienka, na ktorej to celé stojí.

Samozrejme o nazbieraných pároch nemáme nijakú istotu, že $f(o + i)$ je B-hladké. Preto sa o každom presvedčíme jednoduchým delením, či je to skutočne tak. Toto vylepšenie je razantné, lebo sa nemusíme spomaľovať pre-

deľovaním veľkého množstva čísel, ktoré sa k tomu aby boli B-hladké ani neblížia, resp. k veľkému množstvu násobení pri preosievaní. Takto realizované preosievanie používa iba sčítanie a to naozaj *malých* čísel, lebo pracujeme s približnými logaritmami. Takto odstánime zjavných nekandidátov, teda čísla ktoré nie sú zjavne B-hladké, lebo ich logaritmus je príliš „ďaleko“.

Ďalším vylepšením je, keď vôbec nepreosievame malými prvočíslami, napr. nepreosievame nikdy číslami 2, 3, 5, ani 7, ale treba o niečo zvýšiť toleranciu, že kedy číslo $f(o+i)$ berieme ako kandidáta na to, aby bol B-hladkým. Preosievanie malými číslami trvá najdlhšie, teda na preosievaní ušetríme. Na druhej strane sa nám možno zvýši počet zlých kandidátov. Preto je hodnota tolerancie, alebo koľkými prvými prvočíslami nebudeme preosievať prenechaná na experimentovanie.

2.4 Pravdepodobnosť úspechu

Predpokladajme, že sa nám hore popísaným postupom podarilo nájsť nejakú kongruenciu štvorcov $x^2 \equiv y^2 \bmod n$. S akou pravdepodobnosťou povedie výpočet $\gcd(x-y, n)$ k netriviálnej faktorizácií n? V ďalšom budeme predpokladať, že algoritmus nám vráti každú kongruenciu s rovnakou pravdepodobnosťou. Toto nebudeme dokazovať, ale takýto predpoklad je na mieste, lebo riešenie matice, a hľadanie prvkov do matice sú síce deterministické postupy, ale môžeme spraviť napríklad premiešanie riadkov a podobne. Tiež voľba B nám v tom akú kongruenciu dostaneme ako výsledok mieša karty. A ako sme sa zmienili, práve najdôležitejší parameter algoritmu ktorým je číslo B je podstatným miestom, kde môže pomôcť aj experimentovanie či skúsenosť. Práve pre tieto dôvody, nie je predpoklad odtrhnutý od reality.

Budeme sa snažiť ukázať, že je to nezanedbateľne veľká pravdepodobnosť, teda aspoň $\frac{1}{2}$. Najprv ukážeme, že ak máme netriviálnu kongruenciu štvorcov, povedie výpočet gcd k faktorizácií. Nech teda $n > x > y > 0$ a $x^2 \equiv y^2 \bmod n$

potom $n \mid (x-y)(x+y)$. Ak ale navyše predpokladáme, že $x \not\equiv \pm y \bmod n$ potom platí $n > \gcd(x-y, n) > 1$. Lebo ak by platilo, že $\gcd(x-y, n) = 1$, potom $n \mid (x+y)$. Z predpokladov, ale vidno, že $2n > x+y \neq n$, teda máme spor. Teda platí $\gcd(x-y, n) > 1$. Z predpokladov tiež vidno, že $n > x-y$, teda triviálne platí aj $n > \gcd(x-y, n)$.

Otázkou teraz ostáva, koľko je netriviálnych kongruencií v pomere ku všetkým kongruenciám $x^2 \equiv y^2 \bmod n$? Definujme si pre každý kvadratický zvyšok k nemu prislúchajúcu množinu odmocnín. Teda pre a, ktoré je kvadratický zvyšok $\bmod n$ je množina odmocnín $O_a = \{x \mid x^2 \equiv a \bmod n\}$, kde berieme iba $0 \leq x < n$. Z definície je tiež hneď vidno, že O_a má párny počet prvkov (pre nenulové a), lebo pre každé x je aj $n-x$ odmocninou z $a \bmod n$. Je zrejmé, že ak $x^2 \equiv y^2 \bmod n$, tak potom $x, y \in O_a$ pre nejaké a. Aká je pravdepodobnosť, že náhodne zvolená kongruencia štvorcov z jednej pevne danej množiny O_a povedie k faktorizácii n? Toto závisí od veľkosti množiny O_a, označme si toto číslo ako s_a. Ak má O_a aspoň 4 prvky, potom je pravdepodobnosť aspoň $\frac{1}{2}$. Toto je preto, lebo všetkých usporiadaných dvojíc prvkov z množiny O_a je s_a^2, toto sú v skutočnosti všetky kongruencie prislúchajúce k O_a. Ďalej všetkých usporiadaných dvojíc takých, kde sa nejedná o opačné prvky alebo rovnaké prvky je $s_a(s_a-2)$, toto sú v skutočnosti všetky netriviálne kongruencie prislúchajúce k O_a. Ak toto dáme do pomeru, dostaneme pravdepodobnosť výberu netriviálnej kongruencie

$$P = \frac{s_a^2 - 2s_a}{s_a^2} = 1 - \frac{2}{s_a}$$

teda ak s_a je 4, tak $P = \frac{1}{2}$ a ak je s_a väčšie, pravdepodobnosť rýchlo rastie k 1.

Ak má O_a iba 2 prvky, tak sú navzájom opačné, teda pravdepodobnosť je bohužiaľ pre takéto a nulová, čo sedí aj s naším vyjadrením pre P. V ďalšom sa pokúsime načrtnúť, že takýchto a je, teda presnejšie by malo byť málo.

Ak je n tzv. square-free, teda že nie je deliteľné žiadnym štvorcom, alebo

ekvivalentne je súčinom rôznych prvočísel tak môžeme použiť nasledujúcu úvahu. Nech teda $n = p_1 \dots p_k$. Podľa Čínskej zvyškovej vety vieme, že $\mathbb{Z}_n$ je izomorfné so $\mathbb{Z}_{p_1} \times \dots \times \mathbb{Z}_{p_k}$, teda, že čísla zo $\mathbb{Z}_n$ môžeme chápať ako usporiadané k-tice (vektory) pričom i-tá súradnica je zo $\mathbb{Z}_{p_i}$. Otázka teraz znie, kedy má číslo zo $\mathbb{Z}_n$ iba dve odmocniny v $\mathbb{Z}_n$? Toto je práve vtedy, keď a má vo vektorovom vyjadrení práve jednu súradnicu nenulovú. Je zrejmé, že ak má byť a kvadratický zvyšok $\bmod n$, musí byť a kvadratický zvyšok $\bmod p_i$ pre všetky i. Teda každý kvadratický zvyšok a má na všetkých súradniciach iba kvadratické zvyšky modulo to-ktoré prvočíslo. Presnejšie $a = (a_1, \dots, a_k)$, kde $a_i = a \bmod p_i$ a a_i je kvadratický zvyšok modulo p_i. Všetky vektory, ktoré majú túto vlastnosť sú práve všetky kvadratické zvyšky $\bmod n$. Teraz pre každú nenulovú súradnicu, teda pre každé a_i existujú v $\mathbb{Z}_{p_i}$ práve dve odmocniny, označme ich b_{i_1} a b_{i_2}, jedna odmocina existuje iba vtedy, ak a_i je nula. Tiež podľa Čínskej zvyškovej vety vieme, že odmocniny z a sú všetky vektory $(b_1, \dots, b_k)$, kde b_i je jedna z odmocnín a_i modulo p_i. Z povedaného už vyplýva, že ak má mať a iba dve odmocniny, tak musí naozaj vyzerať tak, že má všetky okrem jednej súradnice nulové. Teraz už vieme vyjadriť presnú pravdepodobnosť, že kvadratický zvyšok $a \bmod n$ má práve dve odmocniny. Presnejšie uvedieme pomer počtu „zlých“ kvadratických zvyškov k počtu všetkých kvadratických zvyškov $\bmod n$. Zlé sú preto, lebo ak zoberieme kongruenciu z O_a, kde a je zlý zvyšok, tak nemusíme nájsť faktorizáciu n. Nemusíme, lebo existujú príklady, kedy aj takáto „zlá“ kongruencia povedie k faktorizácií. Ako príklad poslúži „zlý“ kvadratický zvyšok 10 mod 15, ktorý má iba dve odmocniny a to $x = 10$ a $y = 5$, ale $\gcd(x-y, n) = \gcd(5, 15) = 5$, čo je netriviálny faktor. Pri dobrých zvyškoch, platia úvahy a vyjadrenia vyššie. Spomínaná pravdepodobnosť výskytu „zlých“ kvadratických zvyškov je teda

$$P = \frac{\sum_{i=1}^{k} \frac{p_i - 1}{2}}{\prod_{i=1}^{k} \frac{p_i - 1}{2}}$$

pričom môžeme predpokladať, že n má iba delitele väčšie ako k. Tento predpoklad je únosný pre k rádovo 10^5, možno aj viac, lebo iba aplikujeme jednoduché delenie prvočíslami menšími alebo rovnými ako k. Z tohto vyplýva, že súčin v menovateli je pre zložené číslo aspoň 10^{10}, zatiaľ čo čitateľ je iba rádovo 10^5. Toto platí ak je n súčinom dvoch veľkých prvočísel. Je evidentné že ak je $k > 2$ potom je podiel ešte omnoho menší. Treba poznamenať, že tieto úvahy sú platné v podstate pre ľubovoľné k, lebo naším cieľom bolo ukázať, že pravdepodobnosť úspechu je aspoň $\frac{1}{2}$. Z povedaného vidno, že sme túto hranicu schopní aj ďaleko prekročiť.

Čo ale čísla, ktoré nie sú square-free? Tu môžu nastať dve možnosti. Buď je číslo n v tvare a^m, kde a aj m sú celé čísla, alebo v prvočíselnom rozklade n vystupujú dve rôzne prvočísla s exponentami navzájom rôznymi, z ktorých jeden je aspoň dva. V druhom prípade ak v prvočíselnom rozklade n existujú aspoň dve rôzne prvočísla, ktorých mocnina je aspoň dva, potom je „zlých“ prípadov nula, lebo nula má v $\mathbb{Z}_{p^i}$, $i > 1$ aspoň dve odmocniny. Ak je ale n v tvare $q^i p$, kde $i > 1$ potom zlé štvorce sú také čísla x mod n pre ktoré platí $x \equiv 0 \bmod p$ a x má v $\mathbb{Z}_{q^i}$ práve dve odmocniny. V tomto prípade je očakávanie že pravdepodobnosť úspechu dosť veľká, lebo máme predpoklad, že delitele n sú väčšie ako k.

V prvom prípade sme pre niektoré prípady kde a je prvočíslo a m malé (menšie ako 10) výpočtom overili, že „zlých“ kongruencií je drvivá väčšina. Ďalej sme pre niektoré a zložené a m malé overili, že situácia je priaznivá, teda že „dobrých“ je rádovo viac. Čo ale keď je n v tvare p^m, kde p môže byť veľké? Potom (ako sa nám spravidla stávalo pri malých prípadoch) môže byť pravdepodobnosť úspechu mizivo malá. Toto je síce nepriaznivé ale riešenie tohto problému nie je zložité. Stačí pre vstupné n predpokladať, že nie je v tvare a^m, lebo toto nie je algoritmicky náročné overiť. Tohto problému pre vstupné n vieme vyriešiť pomocou Newtonovej iterácie. Presnejšie vieme vyratáť i-tu odmocninu s celočíselnou presnosťou, teda $t = \lfloor \sqrt{n} \rfloor$ a zistiť,

či $t^i = n$. Toto stačí postupne skúšať pre i od $\lfloor \ln n \rfloor$ do 2. Lebo ak $a^i = n$, potom $i \ln a = \ln n$ a keďže a je aspoň 3 potom platí, že $i < \ln n$. Teda o vstupnom n budeme kvôli týmto faktom predpokladať, že preň vykonávame algoritmus, iba ak je nepárne a nie je v tvare a^m.

Kapitola 3

Zložitosť algoritmu

Základným cieľom pri konštrukcií algoritmu Quadratic Sieve bolo to, aby algoritmus bežal v subexponenciálnom (a presnejšie aj v polynomiálnom) čase. Pritom nie zakaždým sa nám musí podariť netriviálneho deliteľa, ale chceme mať šancu úspechu aspoň $\frac{1}{2}$. Cieľom tejto kapitoly je vyjadriť sa k jednotlivým častiam algoritmu z hľadiska zložitosti. Na úvod je treba hneď povedať že väčšina analýz bude robených nie celkom rigorózne ale hlavne pomocou istých odhadov. Toto ale nie je žiaden razantný problém, lebo algoritmus má byť heuristický a pravdepodobnostný.

Pre úplnosť uveďme

Definícia 3.1 *Prvočíselná funkcia $\pi(x)$ je definovaná takto*

$$\pi(x) = \Big|\{p \mid p \text{ je prvočíslo} \wedge \mathrm{p} \leq \mathrm{x}\}\Big|$$

teda $\pi(x)$ je počet prvočísel menších alebo rovných ako x.

Výsledok bez ktorého by sa tažko formulovali akékoľvek odhady obsahujúce prvočísla známy pod názvom prvočíselná veta vyzerá takto.

Veta 3.2 (Prvočíselná Veta) *Pre prvočíselnú funkciu $\pi(x)$ platí*

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$$

toto tvrdenie sa tiež niekedy zapisuje ako

$$\pi(x) \sim \frac{x}{\ln x}$$

Tvrdenie prvočíselnej vety nám teda dáva odhad na počet prvočísel v intervale $[1; n]$, keď n je „veľké“. Uvidíme, že v ďalšom ho hojne využijeme.

3.1 Zložitosť preosievania

Majme ako v sekcii 2.3 v pamäti pole A veľkosti d. Koľko asi aritmetických operácií musíme vykonať, aby sme z neho vybrali B-hladké čísla? Ak by sme zvolili naivný prístup jednoduchého delenia pre každé číslo z A, dostávame rádovo $\pi(B)d$ operácií, presnejšie delení. Teda pre konkrétne číslo, ktoré je reprezentované v poli A zistenie, či je B-hladké nás stojí rádovo $\pi(B)$ operácií.

3.2 Voľba B v závislosti od n

Z popisu v kapitole 2 je evidentné, že čas behu nám ovplyvní hlavne voľba B, lebo od tohto závisí, akú veľkú maticu budeme mať, alebo ako dlho nám bude trvať, kým vôbec nájdeme dosť párov do tejto matice. Lebo ak bude B príliš malé, tak sa nám nepodarí nájsť dosť B-hladkých čísel a ak bude veľké tak budeme musieť nájsť veľa B-hladkých čísel (aby sme mali zaručenú existenciu netriviálneho riešenia matice), čoho následkom môže byť enormne veľká matica exponent vektorov mod 2, ktorú budeme musieť riešiť. Hlavná otázka preto je: Ako voliť B?

Na to aby sme mohli na túto otázku odpovedať potrebujeme isté výsledky z analytickej teórie čísel, ktoré ale iba uvedieme, lebo ich dôkaz je zložitým problémom sám o sebe.

Definícia 3.3 *Funkciu ψ definujeme ako*

$$\psi(x, y) = |\{1 \leq n \leq x \mid n \text{ je } y-\text{hladké } \}|$$

Teda $\psi(x, y)$ nám hovorí koľko je v intervale $[1, x]$ y-hladkých čísel.

Tento výsledok sa dá nájsť v [CP01, str. 45]

Veta 3.4 *Pre funkciu $\psi(x, y)$ platí*

$$\psi\left(x, x^{\frac{1}{u}}\right) = xu^{-u+o(u)}$$

Teda ak vyberáme náhodné číslo z intervalu $[1, x]$ pravdepodobnosť, že bude $x^{\frac{1}{u}}$-hladké je $u^{-u+o(u)}$. Toto je rádovo u^{-u}.

Ak zvolíme $B = n^{\frac{1}{u}}$, potom $u = \frac{\ln x}{\ln B}$. A „pravdepodobnosť“, že $x^2 \bmod n$ bude B-hladké číslo je pri tomto označení rádovo u^{-u}.

Tu si treba uvedomiť, že chyby ktorej sa pri odhade vedome dopúšťame je to, že *nevieme* či veta 3.4 platí aj pre špeciálnu podmnožinu $[1, n]$, konkrétne pre množinu čísel $x^2 \bmod n$.

Ďalším problémom je to, že veľkosť čísel $x^2 \bmod n$, sme zhoda ohraničili n, čo je síce správne, ale nie presné. Naše čísla x, ktorými sa pri preosievaní zaoberáme a zisťujeme, či $x^2 \bmod n$ je B-hladké sú čísla $\lceil\sqrt{n}\rceil \leq x \leq \lfloor\sqrt{2n}\rfloor$. Ako sme už poznamenali pri opise algoritmu, na tomto intervale je $x^2 \bmod n = x^2 - n$. A teda ak $\sqrt{n} < x < \sqrt{n} + n^{\epsilon}$, kde $\epsilon > 0$ je malé, tak

$$x^2 - n < \left(\sqrt{n} + n^{\epsilon}\right)^2 - n = 2\sqrt{n}n^{\epsilon} + n^{2\epsilon}$$

teda $x^2 - n$ je zhora ohraničené zhruba $n^{\frac{1}{2}+\epsilon}$. Preto môžeme hrubý odhad zhora na čísla stanoviť na rádovo $n^{\frac{1}{2}}$. Teda naše očakávanie, že $x^2 - n$ bude

B-hladké bude u^{-u}, kde $u = \frac{1}{2}\ln n/\ln B$. Iba sme dosadili za n do predošlého odhadu u číslo $n^{\frac{1}{2}}$.

Teraz sme už stanovili istý odhad na pravdepodobnosť, že pre nejaké číslo x bude $n - x^2$ B-hladké. Aby sme mohli odhadnúť ako voliť B aby sme minimalizovali čas behu, treba načrtnúť odhad pre čas behu vzhľadom na B a n.

Ako dlho(koľko operácií) musíme v priemere vykonať aby sme o nejakom čísle x zistili, že je $x^2 - n$ je B-hladké? Ak použijeme iba obyčajné delenie, tak odpoveď je $\pi(B)$ delení. Ak ale použijeme techniku preosievania na interval dĺžky d dostávame na jedno číslo iba rádovo $\ln\ln B$ operácií. Argumenty prečo je to tak sú nasledovné:
Predpokladajme, že máme dané B. Ako sme popísali, do prvočíselnej bázy vyberáme prvočísla p menšie ako B s vlastnosťou $\left(\frac{n}{p}\right) = 1$, takýchto je približne $\frac{1}{2}\pi(B)$, lebo pravdepodobnosť, že n je kvadratický zvyšok modulo p je práve $\frac{1}{2}$. Pre každé takéto p máme dve zvyškové triedy, cez ktoré preosievame. Pre jednoduchosť teda predpokladajme, že vezmeme odhad na to, koľko času nám to bude trvať, ako keby sme preosievali všetkými $\pi(B)$ prvočíslami a iba cez jednu zvyškovú triedu. Lebo takýto odhad je intuitívne jednoduchý(namiesto 2 zvyškových tried cez polovicu prvočísel ako keby sme preosievali cez jednu zvyškovú triedu) a pri dosť veľkých B aj dosť presný. Teda čas behu takéhoto sita na intervale dĺžky d je

$$\sum_{p \leq B} \frac{d}{p} = d \ln\ln B$$

čo platí vďaka odhadu, že rad prevrátených hodnôt prvočísel menších ako t má súčet asi $\ln\ln t$. Ak zoberieme priemer, že na interval dĺžky d treba $d\ln\ln B$ operácií, tak na jedno číslo treba približne $\ln\ln B$ operácií.

Na odhad pre čas už iba stačí vedieť koľko B-hladkých čísel budeme potrebovať. Ako sme už spomenuli vo faktor báze budeme mať K prvočísel, kde K je niečo okolo $\frac{1}{2}\pi(B)$. Na to aby sme si boli istí, že v maticovom

kroku nájdeme netriviálnu závislosť potrebujeme nazbierať aspoň $K+1$ B-hladkých čísel. Ak je pravdepodobnosť nájdenia B-hladkého čísla u^{-u}, potom predpokladaný počet pokusov na to, aby sme jedno takéto našli je u^u. Teda predpokladaný počet hodnôt x, ktoré budeme musieť otestovať, či je $x^2 - n$ B-hladké na to aby sme našli aspoň $K+1$ B-hladkých je asi $(u^u)(K-1)$.

Odhad na čas v závisloti od B teda je počet hodnôt x, ktoré budeme musieť skúsiť krát čas, ktorý strávime pri jednej hodnote x, formálnejšie

$$T(B) = u^u(K+1)\ln\ln B, \text{ kde } u = \frac{\ln n}{2\ln B}$$

Cieľom je teraz nájsť B v závislosti od n, tak aby bola funkcia $T(B)$ minimálna. Podľa prvočíselnej vety je K rádovo odhliadnuc od konštanty $B/\ln B$. Teda máme odhad

$$T(B) = \left(\frac{\ln n}{2\ln B}\right)^{\frac{\ln n}{2\ln B}} \left(\frac{B}{\ln B}\right)(\ln\ln B)$$

namiesto tohto budeme odhadovať $S(B)$, kde $S(B) = u\ln u + lnB$. Nie je ťažké nahliadnuť, že

$$\lim_{B\to\infty} \frac{\ln T(B)}{S(B)} = 1$$

tento fakt sa označuje aj ako $\ln T(B) \sim S(B)$ a pre nás znamená, že nám stačí ak budeme pracovať s $S(B)$ a z tohto vyjadríme, ako má vyzerať B aby $S(B)$ bolo minimálne. Toto dosiahneme použitím nie zložitého diferenciálneho počtu a to tak, že zderivujeme $S(B)$ podľa B a toto položíme rovné nule. Máme teda

$$\begin{aligned} S(B)' &= (u\ln u + \ln B)' = \left(\frac{\ln n}{2\ln B}\ln\left(\frac{\ln n}{2\ln B}\right) + \ln B\right)' \\ &= \frac{1}{B} + \left(\frac{\ln n\ln\ln n}{2\ln B} - \frac{\ln n\ln(2\ln B)}{2\ln B}\right)' \\ &= \frac{1}{B} - \frac{\ln n\ln\ln n}{2B\ln^2 B} - \ln n\left(\frac{1}{2B\ln^2 B} - \frac{\ln(2\ln B)}{2B\ln^2 B}\right) \end{aligned}$$

$$\begin{aligned} &= \frac{1}{B} - \frac{\ln n \ln\ln n}{2B\ln^2 B} - \frac{\ln n}{2B\ln^2 B} + \frac{\ln n \ln(2\ln B)}{2B\ln^2 B} \\ &= \frac{1}{B} - \frac{\ln n}{2B\ln^2 B}(\ln\ln n + 1 - \ln 2 - \ln\ln B) \\ 0 &= 2\ln^2 B + (\ln\ln B)\ln n + \ln n \ln 2 - \ln n \end{aligned}$$

Vidíme, že $f(B) := S(B)'$ je spojitá, hoci nás zaujíma iba asymptoticky a na prirodzených číslach. Spojitosť nám ale dovolí odhadnúť, kedy $f(\ln B) = 0$. Priamym dosadením za $\ln B$ sa môžeme presvedčiť, že ak $\ln B$ je $\sqrt{\ln n}$ tak

$$\begin{aligned} f(\ln B) &= f\left(\sqrt{\ln n}\right) \\ &= 2\ln n - \ln n \ln\ln n + \frac{1}{2}\ln n \ln\ln n + \ln n \ln 2 - \ln n \\ &= \ln n(1 + \ln 2) - \frac{1}{2}\ln n \ln\ln n \\ &< 0 \end{aligned}$$

pričom nerovnosť platí pre všetky n väčšie od nejakého N_1. Podobne

$$\begin{aligned} f(\ln B) &= f\left(\sqrt{\ln n \ln\ln n}\right) \\ &= \ln n \ln\ln n + \frac{1}{2}\ln n \ln(\ln n \ln\ln n) + \ln n(\ln 2 - 1) \\ &= \frac{3}{2}\ln n \ln\ln n + \ln n \ln\ln\ln n + \ln n(\ln 2 - 1) \\ &> 0 \end{aligned}$$

opäť nie je ťažké nahliadnuť, že existuje také N_2, že pre všetky $n > N_2$ uvedená nerovnosť platí. Vďaka spojitosti funkcie f a ukázaným nerovnostiam teraz vieme, že pre všetky $n > \max(N_1, N_2)$ platí

$$\begin{aligned} \sqrt{\ln n} &< \ln B &< \sqrt{\ln n \ln\ln n} \\ \frac{1}{2}\ln\ln n &< \ln\ln B &< \frac{1}{2}\ln\ln n + \frac{1}{2}\ln\ln\ln n \end{aligned}$$

a keďže

$$\lim_{n\to\infty} \frac{\frac{1}{2}\ln\ln\ln n}{\frac{1}{2}\ln\ln n} = 0$$

tak vidíme, že platí

$$\ln \ln B \sim \frac{1}{2} \ln \ln n \tag{3.1}$$

Z tohto faktu ďalej odvodíme odhad pre $S(B)$ aj $T(B)$. Konkrétne platí

$$\ln B \approx \frac{1}{2} \sqrt{\ln n \ln \ln n} \tag{3.2}$$

uvedieme, prečo sme zámerne nepoužili symbol $\sim$. Ak totiž podľa odhadu (3.1) nahradíme funkciu $\ln B$ funkciou $\sqrt{\ln n}$, čo podľa tohto odhadu očakávame, tak dostaneme

$$\lim_{n \to \infty} \frac{\sqrt{\ln n}}{\frac{1}{2}\sqrt{\ln n \ln \ln n}} = \lim_{n \to \infty} \frac{2}{\sqrt{\ln \ln n}} = 0 \tag{3.3}$$

takže by za spomínaného predpokladu $\ln B = \sqrt{\ln n}$ fakt $\ln B \sim \frac{1}{2}\sqrt{\ln n \ln \ln n}$ *neplatil*. Ak si ale uvedomíme, že funkcia $\sqrt{\ln \ln n}$ rastie *veľmi* pomaly(hoci do nekonečna a toto nám „kazí“ limitu), tak vidíme, že pre isté čísla je daná limita skoro jedna. Presnejšie ak je n z intervalu približne $[5.1{*}10^{23}; 9.3{*}10^{225}]$ tak je funkcia $\sqrt{\ln \ln n}$ blízka dvom, lebo pre začiatočný bod je jej hodnota približne 2 a pre koncový bod tohto intervalu je jej hodnota približne 2,5. Preto pre „rozumné“ hodnoty n, (teda asi do 10^{100}) nás oprávňujú použiť odhad (3.2). Treba tiež poznamenať, že Quadratic Sieve sa neodporúča používať pre čísla väčšie ako práve 10^{100}, dôvodom môže byť aj to, že odhad do tejto hranice je ešte, ako sme uviedli, presný, ale ďalej je stále nepresnejší. Z odhadu 3.2 ďalej odvodíme

$$\begin{aligned} u &\approx \sqrt{\ln n / \ln \ln n} \\ S(B) &\approx \sqrt{\ln n \ln \ln n} \end{aligned}$$

toto sa dá nahliadnuť, ak v definícií u dosadíme za $\ln B$ aproximáciu tohto výrazu podľa odhadu (3.2). Keďže platí fakt $S(B) \sim \ln T(B)$, opäť dosadením odhadu získame fakt, že čas behu bude veľmi blízko k $\exp(\sqrt{\ln n \ln \ln n})$ Teda

sumárne dostávame ako voliť približne B a aký bude čas

$$\begin{aligned} B &= e^{\frac{1}{2}\sqrt{\ln n \ln\ln n}} \\ T(B) &= e^{\sqrt{\ln n \ln\ln n}} \end{aligned}$$

kde rovnosti platia, respektíve sú dostatočne presným odhadom pre „rozumné“ n.

3.3 Zložitosť maticového kroku

Jedným z hlavných úskalí je po fáze preosiania nájsť lineárnu závislosť medzi exponent vektormi v matici veľkosti asi $b \times (b + c)$, kde b je počet prvočísel vo faktor báze a c je nejaká malá konštanta, avšak aspoň 1. Gaussovou elimináciou sa táto úloha dá zvládnuť v čase $O(b^3)$, čo je pre dostatočne malé b, povedzme okolo 5000 ešte únosné. Pre veľké n, ak je b rádovo v miliónoch je čas $O(b^3)$ neúnosný. Existujú však omnoho zložitejšie a lepšie algoritmy na riešenie tohto problému, ktoré dosahujú heuristickú zložitosť rádovo $b^{2+o(1)}$. Asi najlepšia z týchto metód je Lanczosova metóda. Opäť, keďže zložitosť týchto algoritmov, ich vylepšení a pod. je vhodná ako samostatná téma nijako bližšie sa im nevenujeme. Preto odkazujeme čitateľa na [CP01, str. 233], kde nájde mnoho odkazov na vedecké články pojednávajúce o tejto problematike.

Kapitola 4

Realizovateľnosť častí algoritmu

V tejto kapitole uvedieme niekoľko algoritmov, ktoré sú nevyhnutné pre realizáciu celého algoritmu Quadratic Sieve. Ako sme mali možnosť vidieť z popisu tohto faktorizačného algoritmu je to spojenie rôznych metód algebry. Objasnenie hlavných z nich je cieľom tejto kapitoly.

4.1 Niekoľko faktov z teórie konečných polí

Kvôli výkladu algoritmov v ďalšom texte sformulujeme a dokážeme v tejto sekcii niekoľko výsledkov. Rozsiahlejšie poznatky a aplikácie teórie konečných polí sú napríklad v knihe [LN94].

Iba poznamenáme, že každé konečné pole má $q = p^n$ prkov, kde p je prvočíslo a n je prirodzené číslo väčšie ako nula. Pritom vzhľadom na izomorfizmus existuje pre každé q iba jedno takéto pole. Budovanie takýchto polí, kde $n > 1$ sa deje pomocou algebraických rozšírení. Tiež vieme, že rozšírenie konečného poľa $\mathbb{F}$ s q prvkami na pole $\mathbb{F}'$ sa dá chápať ako konečnorozmerný vektorový priestor nad poľom $\mathbb{F}$. Tiež je dôležitá aj takáto skutočnosť.

Tvrdenie 4.1 *V poli* $\mathbb{F}$ *s* $q = p^n$ *prvkami platí*

$$(\forall a, b \in \mathbb{F})\ \ (a+b)^q = a^q + p^q$$

Pravidlá počítania v jednom konkrétnom type poľa sformulujeme, lebo budú pre nás dôležité neskôr.

Tvrdenie 4.2 *Nech* $f(x) = x^2 - t \in \mathbb{Z}_p[x]$. *Nech* $f(x)$ *nemá korene v* $\mathbb{Z}_p$, *teda je ireducibilný. Teda množina*

$$\mathbb{F} = \left\{a + b\alpha \mid a, b \in \mathbb{Z}_p \ \wedge\ \alpha^2 = t\right\}$$

je vzhľadom na násobenie a sčítanie vykonávané ako

$$\begin{aligned}(a;b) + (c;d) &= (a + b\alpha) + (c + d\alpha) = (a + c; b + d)\\ (a;b) * (c;d) &= (ac + ad\alpha + bc\alpha + bd\alpha^2) = (ac + bdt; ad + bc)\end{aligned}$$

poľom.

Ďalší aj sám o sebe zaujímavý fakt uvedieme pre úplnosť aj s dôkazom.

Veta 4.3 *Multiplikatívna grupa konečného poľa je cyklická.*

Dôkaz. Vieme, že každé konečné pole má $q = p^n$ prvkov, kde p je prvočíslo. Môžeme predpokladať, že $q \geq 3$, lebo pre $q = 2$ je multiplikatívna grupa iba jednoprvková. Nech $h = q - 1$ je počet prvkov multiplikatívnej grupy $\mathbb{F}_q$ a nech $h = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$ je prvočíselný rozklad. Pre každé i, $1 \leq i \leq m$ má polynóm $x^{h/p_i} - 1$ najviac h/p_i koreňov v $\mathbb{F}_q$. Teda pre každé i existuje prvok a_i, taký, že nie je koreňom takéhoto i-tého polynómu. Označme $b_i = a_i^{h/p_i^{r_i}}$. Určite platí, že $b_i^{p_i^{r_i}} = a_i^h = 1$, lebo rád prvku delí počet prvkov grupy. Kvôli tomuto je rád b_i deliteľom $p_i^{r_i}$. Ukážeme že tento rád je práve $p_i^{r_i}$. Sporom predpokladajme, že je menší, potom platí, že

$$b_i^{p_i^{s_i}} = 1 = b_i^{p_i^{r_i - 1}} = a_i^{h/p_i} \neq 1$$

a toto je spor. V uvedenom je $s_i < r_i$ a druhá rovnosť platí práve kvôli tomu, že potom $p_i^{s_i} \mid p_i^{r_i-1}$. Ukážeme teraz, že $b = b_1 \dots b_m$ má rád h. Opäť pre spor predpokladajme, že rád b je vlastným deliteľom h. Potom tento rád delí aspoň jedno z m čísel h/p_i pre $1 \leq i \leq m$. Nech je to bez ujmy na všeobecnosti h/p_1. Potom platí

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \dots b_m^{h/p_1} \tag{4.1}$$

Ak $2 \leq i \leq m$ potom $p_i^{r_i} \mid h/p_1$ a preto $b_i^{h/p_1} = 1$. Teda $b_1^{h/p_1} = 1$, kvôli tomu, že všetky ostatné členy v rovnosti (4.1) sú rovné jednej. Ale ako sme ukázali rád b_1 je $p_1^{r_1}$. Teda $p_1^{r_1} \mid h/p_1$, čo nie je možné, lebo $h = p_1^{s_1}.p_2^{r_2} \dots p_m^{r_m}$, kde $s_1 < r_1$. Kvôli tomuto sporu je rád prvku b rovný h a teda je generátorom celej multiplikatívnej grupy.

□

4.2 Odmocňovanie

V inicializačnej fáze Quadratic Sievu potrebujeme riešiť problémy:

- zistiť, či n je kvadratický zvyšok modulo p
- ak je pridať p do faktor bázy a nájsť odmocninu z n modulo p

Hoci prvočísla sú malé a tieto problémy sú pomerne efektívne riešiteľné úplným prebraním všetkých možností existujú veľmi efektívne metódy dobre fungujúce aj pre väčšie p. Navyše pri faktorizácií čísel s veľkosťou okolo 100 cifier v desiatkovej sústave môže mať faktor báza rádovo milióny „malých“ prvočísel. Teda dôležitosť riešenia týchto problémov je z hľadiska celého algoritmu veľmi veľká.

Definícia 4.4 *Pre nepárne prvočíslo p je Legendreov symbol, označovaný*

ako $\left(\frac{a}{p}\right)$*, definovaný*

$$\left(\frac{a}{b}\right) = \begin{cases} 0 & \Leftrightarrow \quad a \equiv 0 \bmod p \\ 1 & \Leftrightarrow \quad a \text{ je kvadratický zvyšok modulo } p \\ -1 & \Leftrightarrow \quad a \text{ nie je kvadratický zvyšok modulo } p \end{cases}$$

Teda Legendreov symbol nám hovorí o tom, či je číslo „odmocniteľné“, presnejšie povedané či je kvadratický zvyšok, alebo nie. Definícia sama o sebe nemá žiadny praktický význam. Pre nás má z výpočtového hľadiska význam najmä takzvané Eulerovo kritérium.

Veta 4.5 (Eulerovo kritérium) *Ak p je nepárne prvočíslo a a ľubovoľné celé číslo platí*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$$

Dôkaz. Nech $\left(\frac{a}{p}\right) = 0$, potom $a^{\frac{p-1}{2}} = 0$ lebo $\frac{p-1}{2} > 1$ a $a \equiv 0 \bmod p$. Naopak, ak $a^{\frac{p-1}{2}} \equiv 0 \bmod p$, potom aj $a \equiv 0 \bmod p$, lebo $\mathbb{Z}_p$ je pole. Týmto sme vyriešili triviálny prípad, keď $p \mid a$. V ďalšom teda, môžeme predpokladať, že $(a, p) = 1$. Ak sú teda a a p nesúdeliteľné, potom výraz $b := a^{\frac{p-1}{2}}$ môže nadobudnúť buď hodnotu 1, alebo $-1 \bmod p$. Lebo $b^2 \equiv 1 \bmod p$ a vieme, že jednotka má v $\mathbb{Z}_p$, iba dve druhé odmocniny a to 1 a -1. Ak teda ukážeme, že pre naše a platí

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \bmod p \tag{4.2}$$

bude dôkaz vety skončený. Nech teda $\left(\frac{a}{p}\right) = 1$, potom z definície máme, že existuje x s vlastnosťou $x^2 \equiv a \bmod p$. Potom máme

$$a^{\frac{p-1}{2}} \equiv x^{2\left(\frac{p-1}{2}\right)} \equiv x^{p-1} \equiv 1 \bmod p$$

Nech teda $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. Vieme, že multiplikatívna grupa $\mathbb{Z}_p$ je cyklická, teda môžeme písať $g^x \equiv a \bmod p$, pre nejaké x a g – generátor tejto grupy. Z uvedeného vyplýva, že

$$g^{\frac{x(p-1)}{2}} \equiv 1 \bmod p$$

keďže ale g je generátor, jeho rád je $p-1$ a teda platí, že $(p-1) \mid \frac{x(p-1)}{2}$. Z čoho vidno, že $\frac{x}{2}$ je celé číslo, lebo $\frac{x(p-1)}{2}$ bolo celé číslo. Teda x je párne číslo. Toto teda znamená, že $g^{2y} \equiv a \bmod p$, pre nejaké y a teda $(g^y)^2 \equiv a \bmod p$. Teda a je kvadratický zvyšok a podľa definície $\left(\frac{a}{p}\right) = 1$, čo bolo treba dokázať.

□

Teraz už teda máme algoritmus, ktorým hravo zistíme, či je číslo a kvadratický zvyšok. Uvedený postup z vety 4.5 vyžaduje logaritmický počet násobení modulo p. Ďalej si ukážeme, ako nájsť odmocninu z a, ak vieme, že a je kvadratický zvyšok.

Veta 4.6 *Nech p je prvočíslo. Majme čísla a a t s vlastnosťami: $\left(\frac{a}{p}\right) = 1$, $\left(\frac{t^2-a}{p}\right) = -1$. Potom pre*

$$x := \left(t + \sqrt{t^2 - a}\right)^{\frac{p+1}{2}}$$

platí $x^2 \equiv a \bmod p$. Pričom aritmetika pri výpočte prvku x sa realizuje nad poľom $\mathbb{F}_{p^2}$ a prvok x je z poľa $\mathbb{Z}_p$, teda x je v tvare $x + 0\alpha$.

Dôkaz. Keďže $t^2 - a$ nie je kvadratický zvyšok, vyplýva z toho, že polynóm $h(x) = x^2 - (t^2 - a)$ nemá koreň v $\mathbb{Z}_p$. Teda rozšírením $\mathbb{Z}_p$ o algebraický prvok α, kde $h(\alpha) = 0$, teda $\alpha^2 = t^2 - a$ dostávame pole $\mathbb{Z}_p[\alpha]$. Tu nám tvrdenie 4.2 dáva návod ako v takomto poli počítať. Najprv ukážeme, že x vypočítané popísaným spôsobom má uvedené vlastnosti

$$\begin{aligned}
x^2 &= (t+\alpha)^{\frac{2(p+1)}{2}} = (t+\alpha)^p (t+\alpha) = \\
&= (t^p + \alpha^p)(t+\alpha) = (t+\alpha^p)(t+\alpha) = \\
&= t^2 + \alpha t + \alpha^p t + \alpha^{p+1} = t^2 + \alpha t + \alpha^{2d+1} t + \alpha^{2d+2} = \\
&= t^2 + \alpha t - \alpha t - \alpha^2 = t^2 + -(t^2 - a) = \\
&= a
\end{aligned}$$

kde $d = (p-1)/2$. Keďže $\alpha^2 = t^2 - a$ je nerezíduum, tak podľa vety 4.5 platí $\alpha^{2d} = -1$.

□

Práve dokázaná veta nám hneď dáva elegantný algoritmus na výpočet odmocniny z kvadratického zvyšku modulo p. Stačí nájsť t, tak aby platili predpoklady vety. Na toto neexistuje žiadny deterministický algoritmus, ktorý by bežal v rozumnom čase[1]. Riešením je jednoduchý a priamočiary randomizovaný algoritmus skúšania náhodných prvkov t a overenia či $\left(\frac{t^2-a}{p}\right) = -1$. Pre každé náhodne volené t máme šancu $\frac{1}{2}$ že táto rovnosť platí. Po nájdení t vypočítame na logaritmický počet násobení $\frac{p+1}{2}$-tú mocninu prvku $(t; 1)$ podľa tvrdenia 4.2.

[1] o tomto probléme pozri [CP01, str. 95]

Kapitola 5

Záver

Cieľom tejto práce bolo urobiť zrozumiteľný výklad myšlienok a postupov algoritmu Quadratic Sieve. Od prvotného zámeru venovať sa implementácií tohto algoritmu sme upustili kvôli dvom veciam. Prvá je, že literatúra o tomto algoritme, teda vedecké články a knihy na základe týchto článkov, nie sú učebnice, sú písané odborníkmi pre odborníkov. Nejaký súhrn faktov z teórie polí a príbuzných odborov, ktoré sa priamo dotýkajú algoritmu sme nenašli. Preto sme sa rozhodli hlbšie venovať ideám, ich pochopeniu a ich súhrnnému výkladu. V neposledom rade sa snažíme uviesť dosť odkazov na materiály z ktorých sme čerpali, lebo tieto obsahujú mnohé iné samo o sebe zaujímavé témy, ktoré priamo či nepriamo súvisia s preberaným algoritmom. Druhým dôvodom je existencia implementácií v rámci rôznych programátorských knižníc, ktoré obsahujú algoritmus, alebo niektorý jeho variant. Spomenieme napríklad program Msieve, alebo knižnicu FactInt k veľmi zaujímavému softvéru GAP. Práve pre tieto dôvody ostala práca hlavne v teoretickej rovine, hoci mnohé myšlienky a postupy boli naimplementované pri tvorbe práce kvôli lepšiemu pochopeniu problematiky.

Ďalej by sme chceli poznamenať, že algoritmus popísaný v tejto práci, ako sme azda už aj spomenuli je základný. Základný v tom zmysle, že používa

„iba“ ideu preosievania intervalu. Existujú ďalšie vylepšenia, v ktorých sa narába s inými polynómami. Konkrétne neberie sa polynóm $x^2 \bmod n$, ale iné spravidla kvadratické polynómy. Tento variant sa nazýva Multiple Polynomial Quadratic Sieve. Tiež existujú „drobné“ vylepšenia ohľadom toho, aký interval preosievať.

My sme vo výklade spomínali dôvody pre, ktoré sa nepreosieva mocninami prvočísel vo faktor báze. Niektoré varianty algoritmu preosievajú aj s mocninami prvočísel vo faktor báze. Jednoduché zamyslenie nahovára, že ak vezmeme fixné k a budeme preosievať mocninami až do k-tej, pričom nehľadáme všetky odmocniny z n modulo p^k, ale povedzme iba dve tak by to asymptoticky nemalo poškodiť zložitosť. Prínos je zrejmý: zväčšenie šance objavenia B-hladkých čísel, ktoré majú v rozklade prvočísla s väčšími mocninami. Hlbšiu analýzu týmto smerom sme ani nerobili a ani nevideli robenú.

Ďalej, ako sme už spomenuli, maticový krok je miestom, ktoré je témou samo o sebe, teda sú k dispozícií rôzne vylepšenia, teórie a odhady, lebo ako sme videli tak matica s ktorou sa narába je iba binárna a navyše aj dosť riedka v zmysle výskytu jednotkových prvkov. Tomu ako efektívne využiť túto špecifickosť o sa venujú samostatné vedecké články.

Tiež existujú experimenty uberajúce sa smerom k „voľnej“ faktor báze, teda že povolíme isté výnimky pri zbieraní dát pre maticovú fázu v tom zmysle, že nežiadame aby $f(x) \bmod n$ bolo rozložiteľné úplne nad faktor bázou, ale mohlo mať aj jedno alebo dve väčšie prvočísla vo svojom rozklade.

Uviesť treba aj to, že algoritmus Quadratic Sieve a najmä spomínaný variant s rôznymi polynómami je veľmi dobre paralelizovateľný, presnejšie fáza zberu dát pre maticovú fázu je veľmi dobre paralelizovateľná. Maticový krok je „veľká neprijemná nutnosť“ sama o sebe.

Ďalej čo sa týka zložitosti by sme chceli obhájiť nie úplnú exaktnosť pri jej analýze. Pri začiatkoch myšlienok algoritmu sa takáto analýza vôbec nerobila, na pevno sa zvolila nejaká veľkosť faktor bázy, povedzme tri až päť tisíc

a toto sa skúšalo pre vtedy nefaktorizované čísla. Viacej sa dá nájsť v článku Carla Pomeranca. S analýzou ktorú sme uviedli aj my sa prišlo až neskôr. Zrejme táto bola výsledkom snahy podporiť úspechy algoritmu serióznymi tvrdeniami z teórie čísel, hoci sa to tak na prvý pohľad nemusí javiť.
Odkazy na všetky uvedené témy sa dajú nájsť v použitej literatúre.

Ďalší rozvoj práce má veľa smerov. Dalo by sa ísť hlbšie do teórie, konkrétne do algebraickej teórie čísel. Po preštudovaní a pochopení by mohla vzniknúť podobná práca o algoritme General Number Field Sieve. Toto je akási priama nadstavba Quadratic Sievu. Faktorizácia je zaujímavá oblasť sama o sebe, čize v týchto inštanciách by nadstavbou mohli byť aj iné zaujímavé témy a algoritmy z tejto oblasti, postavené aj na odlišných ideách ako Quadratic Sieve. Tiež by mohlo byť zaujímavé venovať čas podrobnej implementácií algoritmu, alebo štúdiu praktických vylepšení aritmetiky, výpočtu a podobne. Tiež by bolo možné venovať sa štúdiu zdrojového kódu už existujúcich implementácií. Možností na ďalší rozvoj je ozaj neúrekom. Preto je možné pokračovať týmto smerom ďalej v diplomovej práci.

Literatúra

[CLR89] Thomas Cormen, Charles Leiserson, and Ronald Rivest. *Introduction to Algorithms*. MIT Press, 1989.

[CP01] Richard Crandall and Carl Pomerance. *Prime Numbers a Computational Perspective*. Springer-Verlag, 2001.

[DH] J. A. Davis and D. B. Holdridge. Factorization of large integers on a massively parallel computer.

[DH83] J. A. Davis and D. B. Holdridge. Factorization using the quadratic sieve algorithm. 1983.

[EW05] Graham Everest and Thomas Ward. *An Introduction to Number Theory*. Springer-Verlag, 2005.

[KGGS02] Tibor Katriňák, Martin Gavalec, Eva Gedeonová, and Jaroslav Smítal. *Algebra a Teoretická Aritmetika*. Univerzita Komenského, 2002.

[LN94] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, 1994.

[Pom84] Carl Pomerance. The quadratic sieve factoring algorithm. 1984.

[Pom96] Carl Pomerance. A tale of two sieves. *Notices of the AMS*, 43(12):1473–1485, 1996.