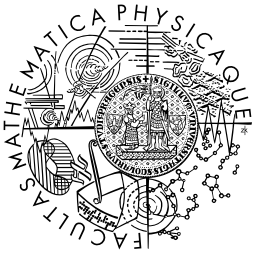


MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

DIPLOMOVÁ PRÁCE

Lukáš Langer

Analýza algoritmu SQUFOF

Katedra algebry

Vedoucí diplomové práce: Mgr. et Mgr. Jan Žemlička, Ph.D.

Studijní program: Matematika

Studijní obor: Matematické metody informační bezpečnosti

Praha 2016

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: Analýza algoritmu SQUFOF

Autor: Lukáš Langer

Katedra: Katedra algebry

Vedoucí diplomové práce: Mgr. et Mgr. Jan Žemlička, Ph.D., katedra algebry

Abstrakt: Tato práce se zabývá sesbíráním faktů a vypracováním celistvé analýzy algoritmu SQUFOF. Po krátkém historickém úvodu popisuje, jak spolu souvisí binární kvadratické formy reprezentující číslo N, rozvoj čísla $\sqrt{N}$ řetězovými zlomky, ideály v okruhu $\mathbb{Z}(\sqrt{N})$ a svazy v $\mathbb{Q}(\sqrt{N})$. Tato práce dále nabízí nástroje, jak mezi těmito strukturami plynule přecházet a nakonec s jejich pomocí ukazuje, jak algoritmus SQUFOF funguje.

Klíčová slova: SQUFOF čtverec forma faktorizace

Title: Analysis of SQUFOF algorithm

Author: Lukáš Langer

Department: Department of algebra

Supervisor: Mgr. et Mgr. Jan Žemlička, Ph.D., department of algebra

Abstract: This thesis deals with collecting facts and making the complete analysis of SQUFOF algorithm. In the beginning you can find a short hystorical review and then it continues with desribing how the binary quadratic forms, which represents the number N, continued fractions of $\sqrt{N}$, ideals in the ring $\mathbb{Z}(\sqrt{N})$ and lattices in $\mathbb{Q}(\sqrt{N})$ are related. This thesis offers the tools usable to switch between these structures and finally it uses these tools to show, how the algorithm SQUFOF works.

Keywords: SQUFOF square form factorization

Mé poděkování patří Mgr. et Mgr. Janu Žemličkovi, Ph.D. za odborné vedení, trpělivost a ochotu, kterou mi v průběhu zpracování diplomové práce věnoval.

Obsah

1. Úvod

1.1 Představení

SQUFOF (SQUare FOrm Factorization) je faktorizační algoritmus, jehož základy byly položeny v roce 1975 Danielem Shanksem v práci "Analysis and Improvement of the Continued Fraction Method of Factorization"[Sha75a].

Dnešní počítačová algebra disponuje různými faktorizačními algoritmy, které se liší svoji efektivitou v závislosti na délce vstupujícího přirozeného čísla. V současnosti je pro čísla větší než 10^{120} jasným favoritem číselné síto (NFS, number field sieve), pro čísla o velikosti mezi 10^{50} a 10^{120} podává nejlepší výsledky kvadratické síto (QS, quadratic sieve). Tyto hranice se neustále posunují - jsou totiž závislé jak na výpočetní síle aktuálně dostupného hardwaru, tak na objevech na poli matematiky a různých nových algoritmech, či optimalizacích těch starých.

Na 32 bitové architektuře počítačů je pro čísla z rozsahu $10^{10} - 10^{18}$ jasnou jedničkou právě algoritmus SQUFOF. Pro čísla z daného rozsahu má v podstatě ideální vlastnosti - je to rychlý algoritmus, má velmi nízké paměťové nároky a v neposlední řadě je implementačně nenáročný. I díky těmto skutečnostem je SQUFOF součástí mnoha implementací QS a NFS a těší se velké oblibě i u programovatelných kalkulaček, pro které je důležitá, ona výše zmíněná, nízká hardwarová náročnost.

Tato práce má převážně kompilační charakter a dává si za cíl shromáždit na jednom místě všechny potřebné poznatky pro vybudování teorie, která stojí za algoritmem SQUFOF a popsat, jak a proč algoritmus SQUFOF funguje. Základním zdrojem byly práce [GSSW07] a [McM04], z které bylo převzato základní členění sekce Matematický podklad. Nad rámec kompilace z těchto a dalších zdrojů bylo třeba některé koncepty lépe dodefinovat, přidat některá tvrzení, ilustrovat použití získaných matematických nástrojů na příkladech, či dokázat několik faktů, které si autoři odborného článku mohli dovolit uvést bez komentáře.

1.2 Historie

V 70. letech 20. století vyvinuli pánové Morrison a Brillhart jednoduchý a velice intuitivní faktorizační algoritmus [MB75], který je postaven na užití řetězových zlomků.

Kompletní algoritmus je o něco komplikovanější, ale následující popis bude pro naše potřeby plně postačovat.

Pokud vztah

$$x^2 \equiv y^2 \pmod{N}$$

má řešení ve tvaru

$$x \not\equiv \pm y \pmod{N}$$

pak platí, že NSD($x - y$,N) nám dává netriviální faktor N. Tato myšlenka je poměrně prostá a elegantní. Bohužel, není úplně zřejmé, jak efektivně vybírat hodnoty x a ani jak k nim nějak efektivně dopočítávat hodnoty y. Tento algoritmus je ve své ryzí verzi pro velká N poměrně hodně výpočetně náročný.

První praktičtější verze tohoto algoritmu byla pojmenována po Pierre de Fermatovi - Fermatův algoritmus. Tento algoritmus prochází pouze $x > \sqrt{N}$ a hledá, kdy výsledek $x^2 \pmod{N}$ bude čtverec. Toto zúžení prostoru, ve kterém hledáme x, efektivitě algoritmu pomohlo. Nicméně výsledek stále nebyl úplně uspokojivý. Čísla, se kterými algoritmus pracoval, velmi rychle rostla, což kladlo vysoké nároky jak na výpočetní výkon, tak na potřebnou paměť. Předností tohoto algoritmu je rychlost, se kterou najde rozklad, pokud jsou oba faktory podobně veliké. Poznamenejme, že vlastnosti tohoto algoritmu nám dnes dávají některé požadavky pro volbu prvočíselného páru při generování RSA klíče.

Výhodným nástrojem, který nám umožní dále zdokonalit implementaci původní myšlenky, se ukázala býti teorie řetězových zlomků. Pokud platí $0 < Q_i < 2\sqrt{N}$, pak jsou šance na nalezení čtverce výrazně navýšeny, což se velice příznivě odráží na efektivitě celého algoritmu. Dále využijeme další fakt z teorie řetězových zlomků, a sice $A_{i-1}^2 - B_{i-1}^2 N = (-1)^i Q_i$. Odsud platí $A_{i-1}^2 \equiv (-1)^i Q_i \pmod{N}$. Pokud pro nějaké i je Q_{2i} čtverec, pak máme řešení $x^2 \equiv y^2 \pmod{N}$ a jediné, co nám zbývá k dosažení cíle, je zjistit, zda nám NSD($x+y, N$) nebo NSD($x-y, N$) dává netriviální faktor N. Bohužel, v rozvoji řetězových zlomků se mnoho čtverců nevyskytuje. Tento pro nás poněkud nepříjemný fakt přivedl pány Morrisona a Brillharta [MB75] k myšlence násobení již známých rovností mezi sebou.

Příklad 1. Pro $N = 3127$ získáme pomocí rozvoje řetězovými zlomky $148^2 \equiv 15 \pmod{N}$ a $678^2 \equiv 15 \pmod{N}$. Z těchto výsledků dostaneme $(148.678)^2 \equiv 15.15 = 15^2 \pmod{N}$. Odsud získáme $280^2 \equiv 15^2 \pmod{N}$ a $NSD(280+15,3127)$ nám dává rozklad $3127 = 53.59$.

Tento algoritmus má však také několik nedostatků. Jedním z nich je fakt, že počítá s prvky A_i, které jsou modulo N stejné velikosti jako N, což není příliš praktické. Mnohé jiné algoritmy si vystačí s aritmetikou s čísly velikosti přibližně $\sqrt{N}$. Další nepříjemností je fakt, že ani po získání řešení rovnice $x^2 \equiv y^2 \pmod{N}$, což samo o sobě obvykle představuje nezanedbatelné množství výpočtů, nám získané řešení nemusí dávat netriviální faktor.

Příklad 2. V rozvoji řetězovými zlomky čísla $\sqrt{1777}$ získáme $Q_{14} = 16 = 4^2$ a $A_{13} = 26884229$, tedy $26886229^2 \equiv 4^2$ $(mod\ 1777)$. Naneštěstí ale $26884229 \equiv -4$ $(mod\ 1777)$, tudíž faktor čísla 1777 nedostáváme.

Ačkoliv pro počítač není problém pustit algoritmus vícekrát s tím, že několikrát neuspěje, Daniel Shanks se pokusil porozumět dané problematice hlouběji. Objevil několik velice zajímavých algoritmů pro faktorizaci, založených na teorii kvadratických forem a pochopení vnitřní struktury třídových grup [Sha75b].

Nejprve se mu podařilo vymyslet vylepšení Morrison-Brillhartova algoritmu. Zjednodušeně řečeno, ku získávání vhodných dvojic (x,y) využil místo uchovávání prvků A_i, skládání kvadratických forem a následně pro dopočítání faktoru využil vnitřní strukturu třídových grup.

Za jeho další úspěch na tomto poli můžeme považovat systém pravidel, který dokázal poměrně přesně odhadovat, zda nám daný čtverec pomůže získat netriviální faktor. Tato pravidla se mu podařila sestrojit na základě poznatků z jeho výzkumu na poli vnitřní struktury třídových grup. Bohužel, v praxi nám tato pravidla příliš času neušetří, protože je díky nim celý algoritmus výrazně komplikovanější než původní verze Morrison-Brillhartova algoritmu.

Na vývoji však pokračovali i objevitelé původního Morrison-Brillhartova algoritmu. Výzvou se jim mělo stát číslo $2^{60}+2^{30}-1$. Toto číslo bylo podle Fermatova testu prvočíselnosti číslem složeným, avšak jeho faktory byly neznámé. Morrison-Brillhartův algoritmus jim na tomto čísle selhal 114x. Frustrace a zklamání je však přivedla na geniální myšlenku. Zkusit, jak se algoritmus zachová, když číslo N přenásobí nějakou malou konstantou. Algoritmus, poněkud nečekaně, slavil úspěch hned při prvním pokusu. Odpověděl tedy sice na otázku, jaká je hodnota onoho hledaného faktoru, nicméně zároveň nastolil otázku, jak je možné, že tolikrát selhal a že přenásobení malou konstntou může mít takový vliv na jeho průběh.

Nalézt odpověď na tuto otázku jim měl pomoci Shanks, kterého nabídka analýzy tohoto poněkud nečekaného chování algoritmu zaujala. Naneštěstí (zpětně hodnoceno však naštěstí), měl Shanks k dispozici pouze kalkulačku HP-65, do jejíž paměti se celý původní algoritmus nevešel. Proto upustil od konceptu kombinování rovnic aby získal čtverec a namísto toho procházel cyklem forem, dokud nenašel čtvercovou formu. Tento kód byl výrazně kratší a navíc výrazně rychlejší než původní verze.

1.3 Motivační popis algoritmu

Nyní si rámcově, a zatím poněkud vágně, popíšeme, jak algoritmus SQUFOF pracuje. Jelikož v tento moment nemáme zadefinovánu spoustu pojmů a nemáme dokázánu žádnou větu, která by nám zaručila, že algoritmus opravdu funguje, berte prosím tento popis jako motivaci k následujícím kapitolám. Podrobný popis algoritmu následně najdete v sekci 3, nicméně jeho části budou vysvětlovány v průběhu celé práce.

Algoritmus na začátku dostane číslo N. Prvním krokem je vždy test, jestli číslo N není náhodou čtverec. Dále si algoritmus zvolí hlavní kvadratickou formu [2.2], která bude mít diskriminant právě $4N$. Odpověď na otázku "proč má být diskriminant právě $4N$?"si ukážeme v 2.2. Prozatím si vystačíme s tím, že se zmíněnou konstantou 4 pro nás bude mít diskriminant žádoucí vlastnosti. Při hledání hlavní formy využijeme řetězových zlomků [viz. 2.1]. Dále aplikujeme fakt, že binární kvadratické formy tvoří cykly forem se stejným diskriminantem [Definice 14], které mohou být generovány pomocí redukčního operátoru ρ a operátoru jemu inverzního ρ^{-1}. Počítání vedlejší formy je v jazyce kvadratických forem ne zcela intuitivní a elegantní. Proto v tomto místě využijeme skutečnost, že existuje přímočará korespondence mezi kvadratickými formami, řetězovými zlomky, ideály a mřížemi. Každá z těchto korespondencí nám nabídne různé výhody. Některé nám pomohou pouze s důkazy správnosti algoritmu, jiné nám zajistí velice snadné a elegantní počítání vedlejších forem v cyklu. Krása algoritmu SQUFOF mimo jiné pramení i z toho, že nám při průchodu cyklem stačí uchovávat pouze koeficienty u poslední navštívené kvadratické formy, což má zásadní pozitivní vliv na paměťovou náročnost celého algoritmu.

Algoritmus rekurzivním výpočtem prochází cyklus forem a hledá formu, která by byla čtvercová. Pro naše motivační účely postačí zjednodušený pohled na čtvercovou formu. Kvadratická forma F je čtvercová, pokud existuje kvadratická forma G taková, že $F = G \circ G = G^2$, kde $\circ$ značí operaci skládání forem a tedy G^2 chápeme jako symbolický zápis pro "mocninu"v jazyce skládání forem. Dále si také ukážeme, že tyto formy budou v námi zvoleném cyklu právě 2 a budou tvořit středy symetrie. To znamená, že ostatní formy kolem nich budou v nějakém slova smyslu symetrické. Co to přesně znamená si ukážeme napříč všemi sekcemi.

Ve chvíli, kdy nalezneme střed symetrie, dává nám lemma 18 vztah, pomocí kterého z koeficientů středu symetrie dokážeme získat netriviální faktor diskriminantu, tedy $4N$.

2. Matematický podklad

2.1 Periodické řetězové zlomky

Jeden z klíčových nástrojů, který budeme pro popis algoritmu SQUFOF využívat je vyjádření $\sqrt{N}$ za pomocí rozvoje řetězovými zlomky. Toto vyjádření je počítáno rekurzivně a má pro nás mnohé výhodné vlastnosti. Tato kapitola si nedává za cíl precizně nadefinovat a popsat teorii řetězových zlomků, kterou se zabývá nespočet jiných publikací, nýbrž shrnout poznatky potřebné pro vybudování teorie na které stojí nejoblíbenější implementace SQUFOF. Poznamenejme, že pro nás bude mít zvláštní význam rozvoj druhé odmocniny bezčtvercového N, který budeme potřebovat pro popis algoritmu SQUFOF.

$$x_0 = \sqrt{N}, b_0 = \lfloor x_0 \rfloor \tag{2.1}$$

$$\forall i \geq 1 \quad x_i = \frac{1}{x_{i-1} - b_{i-1}}, b_i = \lfloor x_i \rfloor \tag{2.2}$$

$$\sqrt{N} = b_0 + \frac{1}{b_1 + \frac{1}{b_2 + \ldots}} \tag{2.3}$$

Všimněme si, že vyjádřením x_{i-1} z rovnice 2.2 dostaneme $x_{i-1} = b_{i-1} + \frac{1}{x_i}$. Iterativním dosazením tohoto výrazu do sebe sama dostaneme rovnici 2.3. Než budeme pokračovat v budování teorie, uveďme krátký příklad.

Příklad 3. Vyjádřeme pomocí řetězových zlomků číslo $\sqrt{33}$

$x_0 = \sqrt{33}, b_0 = 5$ $\qquad \sqrt{33} = 5 + \frac{1}{x_1}$

$x_1 = \frac{1}{\sqrt{33}-5} = \frac{\sqrt{33}+5}{8} = 1 + \frac{\sqrt{33}-3}{8}$ $\qquad \sqrt{33} = 5 + \frac{1}{1+\frac{1}{x_2}}$

$x_2 = \frac{8}{\sqrt{33}-3} = \frac{8(\sqrt{33}+3)}{24} = \frac{\sqrt{33}+3}{3} = 2 + \frac{\sqrt{33}-3}{3}$ $\qquad \sqrt{33} = 5 + \frac{1}{1+\frac{1}{2+\frac{1}{x_3}}}$

$x_3 = \frac{3}{\sqrt{33}-3} = \frac{3(\sqrt{33}+3)}{24} = \frac{\sqrt{33}+3}{8} = 1 + \frac{\sqrt{33}-5}{8}$ $\qquad \sqrt{33} = 5 + \frac{1}{1+\frac{1}{2+\frac{1}{1+\frac{1}{x_4}}}}$

$x_4 = \frac{8}{\sqrt{335}} = \frac{8(\sqrt{33}+5)}{8} = \frac{\sqrt{33}+5}{1} = 10 + \frac{\sqrt{33}-5}{1}$ $\qquad \sqrt{33} = 5 + \frac{1}{1+\frac{1}{2+\frac{1}{1+\frac{1}{10+\frac{1}{x_5}}}}}$

$x_5 = \frac{1}{\sqrt{33}-5} = x_1$

Jelikož $x_5 = x_1$, je patrné, že sekvence x_1,x_2,x_3,x_4 se bude opakovat do nekonečna. Pokud nekonečný řetězový zlomek v kterémkoliv místě ořízneme, získáme nějakou racionální aproximaci čísla $\sqrt{33}$. Protože zápis řetězového zlomku není příliš praktický, budeme dále používat pouze zjednodušený zápis [5,1,2,1,10,1,...], tedy seznam koeficientů $[b_0,b_1,b_2,\ldots]$. V případě, že chceme označit periodu, použijeme zápis $[5,\overline{1,2,1,10}]$.

Předpokládejme, že N je liché, bezčtvercové přirozené číslo. Zaveďme si značení

$$x_0 = \frac{\sqrt{N} + P_{-1}}{Q_0} \tag{2.4}$$

kde jsou celá čísla P_{-1} a Q_0 vybrána tak, aby platilo

$$P_{-1}^2 \equiv N(mod\ Q_0),\ 0 < P_{-1} < \sqrt{N}, |\sqrt{N} - Q_0| < P_{-1} \tag{2.5}$$

Takovéto volby můžeme docílit vícero způsoby. Jedním z nich je zvolení si $x_0 = \sqrt{N} + \lfloor\sqrt{N}\rfloor$ a $Q_0 = 1$. Dalším validním způsobem může být $x_0 = \frac{\sqrt{N}+P_{-1}}{2}$, kde $P_{-1} = \lfloor\sqrt{N}\rfloor$, nebo $\lfloor\sqrt{N}\rfloor - 1$ tak, aby P_{-1} bylo liché.

i-tý člen x_i a b_i vyjádříme rekurentními vztahy

$$x_i = \begin{cases} \sqrt{N} & \text{pro } i = 0 \\ 1/(x_{i-1} - b_{i-1}) & \text{pro } i \geq 1 \end{cases} \tag{2.6}$$

$$b_i = \begin{cases} \lfloor\sqrt{N}\rfloor & \text{pro } i = 0 \\ \left\lfloor \frac{b_0+P_{i-1}}{Q_i} \right\rfloor & \text{pro } i > 0 \end{cases} \tag{2.7}$$

Ve zbytku práce budeme pro P_i a Q_i uvažovat následující rekurentní vztahy

$$P_i = \begin{cases} 0 & \text{pro } i = -1 \\ \lfloor\sqrt{N}\rfloor & \text{pro } i = 0 \\ b_iQ_i - P_{i-1} & \text{pro } i \geq 1 \end{cases} \tag{2.8}$$

$$Q_i = \begin{cases} 1 & \text{pro } i = 0 \\ N - P_0^2 & \text{pro } i = 1 \\ Q_{i-2} + (P_{i-2} - P_{i-1})b_{i-1} & \text{pro } i \geq 2 \end{cases} \tag{2.9}$$

Definujme si vztah pro x_i vyjádřené pomocí Q_i, P_i, Q_{i+1}, $P_{i+1} \in \mathbb{Z}$:

$$x_{i+1} = \frac{Q_i}{\sqrt{N} - P_i} = \frac{\sqrt{N} + P_i}{Q_{i+1}} = b_{i+1} + \frac{\sqrt{N} - P_{i+1}}{Q_{i+1}} \text{ pro } i \geq 0 \tag{2.10}$$

Věta 1 nám dává některé známé základní vlastnosti řetězových zlomků. Krom toho nám nabízí způsob, jak počítat koeficienty Q_i, P_i, b_i. Dílčí tvrzení, která jsou obsažena v této větě, ve své práci [Rie85] zformuloval Hans Rieser

Věta 1. *V rozvoji řetězovými zlomky x_0 takovém, kde P_i, Q_i jsou definována vztahy 2.8 a 2.9 a tedy splňují podmínky 2.5, je každé $x_i = \frac{\sqrt{N}+P_{i-1}}{Q_i}$, a platí:*

a) $N = P_i^2 + Q_iQ_{i+1}$

b) $P_i = b_iQ_i - P_{i-1}$

c) $b_i = \lfloor\frac{\sqrt{N}+P_{i-1}}{Q_i}\rfloor \geq 1$

d) $0 < P_i < \sqrt{N}$

e) $|\sqrt{N} - Q_i| < P_{i-1}$

f) Q_i *je celé číslo*

g) $Q_{i+1} = Q_{i-1} + b_i(P_{i-1} - P_i)$

h) tato posloupnost je od nějakého bodu periodická

Důkaz.

a) Z 2.10 využijeme $\frac{Q_i}{\sqrt{N}-P_i} = \frac{\sqrt{N}+P_i}{Q_{i+1}}$. Vyjádříme si N a přímo dostáváme $N = P_i^2 + Q_iQ_{i+1}$

b) Vezmeme pravou rovnost z 2.10 a převedeme celý pravý člen na společného jmenovatele. $\frac{\sqrt{N}+P_i}{Q_{i+1}} = \frac{\sqrt{N}+b_{i+1}Q_{i+1}-P_{i+1}}{Q_{i+1}}$. Odsud vyjádříme $P_{i-1} = b_{i+1}Q_{i+1} - P_i$

c) pro $i = 0$ máme z předpokladu $|\sqrt{N} - Q_0| < P_{-1}$, proto

$$Q_0 < \sqrt{N} + P_{-1}$$

a tedy

$$b_0 = \left\lfloor \frac{\sqrt{N} + P_{-1}}{Q_0} \right\rfloor \geq 1$$

Pro $i > 0$ platí $b_{i-1} = \lfloor x_{i-1} \rfloor$.Z definice dolní celé části máme nerovnost $x_{i-1} - 1 < b_{i-1} \leq x_{i-1}$. Pokud $b_{i-1} = x_{i-1}$, pak řetězový zlomek $[b_0,b_1,\ldots,b_{i-1}]$ je racionální a je roven $x_0 = \frac{\sqrt{N}+P_{-1}}{Q_0}$. Jenže x_0 je pro nečtvercová N iracionální. Z odhadu $x_{i-1} - 1 < b_{i-1} < x_{i-1}$ dostaneme $0 < x_{i-1} - b_{i-1} < 1$. Z toho přímo plyne $x_i = \frac{1}{x_{i-1}-b_{i-1}} > 1$, tudíž $b_i = \lfloor x_i \rfloor \geq 1$. Všimněme si, že mezi $\lfloor\sqrt{N}\rfloor + P_{i-1}$ a $\sqrt{N} + P_{i-1}$ není žádné celé číslo a tedy platí rovnost $\left\lfloor \frac{\sqrt{N}+P_{-1}}{Q_0} \right\rfloor = \left\lfloor \frac{\lfloor\sqrt{N}\rfloor+P_{-1}}{Q_0} \right\rfloor$.

d) e) Tvrzení $|\sqrt{N} - Q_i| < P_{i-1}$ a $0 < P_{i-1} < \sqrt{N}$ dokážeme indukcí.
Případ $i = 1$:
$P_0 = \lfloor\sqrt{N}\rfloor$ nebo $P_0 = \lfloor\sqrt{N}\rfloor - 1$, tedy $0 < P_0 < \sqrt{N}$ platí z definice.
Z podmínky 2.5 máme pro x_0 nerovnost $|\sqrt{N} - Q_0| < P_{-1}$.
Indukční předpoklad: Předpokládejme $|\sqrt{N} - Q_i| < P_{i-1}$ a $0 < P_{i-1} < \sqrt{N}$.
Poznamenejme, že tyto předpoklady vyžadují aby $0 < Q_i < 2\sqrt{N}$. Z (c) víme, že platí $0 < x_i - b_i < 1$, což znamená, že $0 < \frac{\sqrt{N}-P_i}{Q_i} < 1$. Pokud $Q_i > 0$, pak $0 < \sqrt{N} - P_i < Q_i$. Z levé strany přímo plyne, že $P_i < \sqrt{N}$.
Nyní nám mohou nastat 2 případy: buď $Q_i \leq \sqrt{N}$ nebo $Q_i > \sqrt{N}$.
Případ 1: Pokud $Q_i \leq \sqrt{N}$, pak $\sqrt{N} - P_i < Q_i < \sqrt{N}$, tedy $P_i > 0$.
Případ 2: Pokud $Q_i > \sqrt{N}$, pak z (b) víme, že $P_i = b_iQ_i - P_{i-1} > b_i\sqrt{N} - \sqrt{N} = (b_{i-1})\sqrt{N} \geq 0$.
Nerovnost $0 < P_i < \sqrt{N}$ tedy platí.
Pro $x_{i+1} > 1$ je skutečnost, že $Q_{i+1} < \sqrt{N} + P_i$, triviální. Odsud ukažme, že $|\sqrt{N} - Q_{i+1}| < P_i$ se redukuje na $Q_{i+1} > \sqrt{N} - P_i$. Pokud $1 = \frac{N-P^2}{Q_iQ_{i+1}} = \frac{\sqrt{N}+P_i}{Q_i}\frac{\sqrt{N}-P_i}{Q_{i+1}}$, což je ekvivalentní ukázání faktu:

$$\frac{\sqrt{N}+P_i}{Q_i} > 1 \tag{2.11}$$

Předpokládejme opak, tedy že $Q_i \geq \sqrt{N}+P_i$. Pak

$$b_i(\sqrt{N}+P_i \leq b_iQ_i - P_i = P_{i-1} < \sqrt{N}$$

$$b_i\sqrt{N} + P_i(b_i-1) < \sqrt{N}$$

$$\sqrt{N}(b_i-1) + P_i(b_i-1) < 0$$

$$(b_i-1)(\sqrt{N}+P_i) < 0)$$

Protože ale $\sqrt{N}$ a P_i jsou kladná, musí platit $b_i < 1$, což je spor s Větou 1 (c). Tudíž je nerovnost 2.11 dokázána.

f) Skutečnost, že $N = P_i^2 + Q_iQ_{i+1}$ vyžaduje, aby platilo $Q_{i+1} = \frac{N-P_i^2}{Q_i}$. Abychom ukázali, že $\forall i$ je Q_i celé číslo a že $Q_i|N-P_i^2$, budeme postupovat indukcí.
Pro $i = 0$:
Z definice je Q_0 celé číslo a platí, že $P_{-1}^2 \equiv N(mod\ Q_0)$. Jelikož $P_0 = P_{-1}$, pak také $P_0^2 \equiv N(mod\ Q_0)$. Proto $Q_0|N-P_0^2$.
Indukce: Předpokládejme že pro nějaké i je Q_i celé číslo a $Q_i|(N-P_i^2)$. Pak pokud $N = P_i^2 + Q_iQ_{i+1}$, pak zřejmě $Q_{i+1} = \frac{N-P_i^2}{Q_i}$. Pokud tedy $Q_i|(N-P_i^2)$, pak je Q_{i+1} celé číslo. Tedy $Q_i = \frac{N-P_i^2}{Q_{i+1}}$, tudíž pokud Q_i je celé číslo, $Q_{i+1}|(N-P_i^2)$, tedy $P_i^2 \equiv N(mod\ Q_{i+1})$. Pokud platí $P_{i+1} = b_{i+1}Q_{i+1} - P_i$, pak $P_{i+1} \equiv P_i(mod\ Q_{i+1})$. Proto $P_{i+1}^2 \equiv N(mod\ Q_{i+1})$ a tedy $Q_{i+1}|(N-P_{i+1}^2)$, čímž je indukce kompletní.

g) Vyjádříme si z rovnice (b) člen b_i, čímž získáme $\frac{P_{i-1}+P_i}{Q_i} = b_i$. Přenásobením $(P_{i-1}-P_i)$ získáme

$$\frac{P_{i-1}^2 - P_i^2}{Q_i} = b_i(P_{i-1}-P_i)$$

Po přeuspořádání a přidání $\frac{N}{Q_i}$ k obou stranám rovnice dostáváme:

$$\frac{N-P_i^2}{Q_i} = \frac{N-P_{i-1}^2}{Q_i} + b_i(P_{i-1}-P_i)$$

A po použití rovnosti (a) získáváme přímo tvrzení (g)

$$Q_{i+1} = Q_{i-1} + b_i(P_{i-1}-P_i)$$

h) Pokud každé x_i a tedy celá posloupnost která ho následuje je definována dvěma celými čísly P_{i-1} a Q_i, která jsou omezena výrazy $0 < Q_i < 2\sqrt{N}$ a $0 < P_i < \sqrt{N}$, pak těchto čísel x_i je pouze konečně mnoho. Proto pro nějaké celé číslo π a celé číslo k platí, že $\forall i \geq k : x_i = x_{i+\pi}$

□

Poznámka. Zafixujme si pro zbytek kapitoly značení pro x_i, Q_i, P_i a b_i.

Pro efektivitu algoritmu SQUFOF je důležitý fakt, že každé x_i lze zapsat ve tvaru $\frac{\sqrt{N}-P_{i-1}}{Q_i}$.
Z rovnic (b) a (g) pak plyne jedna ze stěžejních pozitivních vlastností algoritmu SQUFOF, a sice, že všechny výpočty probíhají s celými čísly menšími než $2\sqrt{N}$.

Pro nás podstatná aplikace řetězových zlomků bude racionální aproximace odmocniny.

$$\sqrt{N} = b_0 + \frac{1}{b_1 + \frac{1}{b_2 + \ldots}}$$

Ať už ořízneme tento nekonečný řetězový rozvoj v kterémkoliv bodě, výsledkem bude racionální aproximace $\sqrt{N}$. Je patrné, že abychom získali aproximaci s přesností, kterou vyžadujeme, budeme muset zjednodušit pravou spodní stranu výrazu nekonečného řetězového zlomku. V které bodě b_o to máme udělat nám říká následující věta.

Tvrzení 2. *Definujme si posloupnosti A_i a B_i rekurentními vztahy:*

$$A_{-1} = 1,\ A_0 = b_0,\ A_i = b_i A_{i-1} + A_{i-2},\ i > 0$$

$$B_{-1} = 0,\ B_0 = 1,\ B_i = b_i B_{i-1} + B_{i-2},\ i > 0$$

Pak pro $i \geq 0$ platí $[b_0,b_1,\ldots,b_i] = \frac{A_i}{B_i}$.

Důkaz. Postupujme indukcí.
Pro $i = 1$: $\frac{A_1}{B_1} = b_0 + \frac{1}{b_1} = \frac{b_1 B_0 + 1}{b_1}$, což znamená, že $A_1 = b_1 B_0 + 1 = b_1 A_0 + A_{-1}$ a $B_1 = b_1 = b_1 B_0 + B_{-1}$ a tedy rekurzivní formule pro $i = 1$ platí.

Dále předpokládejme, že tvrzení platí pro i a ukažme, že platí i pro $i + 1$.
Podle definice řetězového rozvoje bude stačit nahradit b_i výrazem $b_i + \frac{1}{b_{i+1}}$.

$$\frac{A_{i+1}}{B_{i+1}} = \frac{\left(b_i + \frac{1}{b_{i+1}}\right) A_{i-1} + A_{i-2}}{\left(b_i + \frac{1}{b_{i+1}}\right) B_{i-1} + B_{i-2}} = \frac{b_i A_{i-1} + A_{i-2} + \frac{A_{i-1}}{b_{i+1}}}{b_i A_{i-1} + B_{i-2} + \frac{B_{i-1}}{b_{i+1}}} = \frac{A_i + \frac{A_{i-1}}{b_{i+1}}}{B_i + \frac{B_{i-1}}{b_{i+1}}} =$$

$$= \frac{b_{i+1} A_i + A_{i+1}}{b_{i+1} B_i + B_{i+1}}$$

což odpovídá rekurentní definici A_i a B_i a tedy tvrzení platí.

□

Věta 3. *Mějme posloupnosti A_i a B_i z minulého tvrzení. Pak platí:*

$$A_{i-1}B_i - A_iB_{i-1} = (-1)^i$$

Důkaz. Použijeme indukci. $A_{-1}B_0 - A_0B_{-1} = 1.1 - b_0.0 = 1$ a tedy rovnost pro $i = 0$ platí. Předpokládejme, že platí pro i. Pak pro $i + 1$ dostáváme:

$$A_iB_{i+1} - A_{i+1}B_i = A_i(b_{i+1}B_i + B_{i-1}) - (b_{i+1}A_i + A_{i+1})B_i = -(A_{i-1}B_i - A_iB_{i-1}) =$$
$$= -(-1)^i = (-1)^{i+1}$$

□

Věta 4. *Nechť jsou A_i, B_i definovány stejně jako v minulé větě. Q_i, x_i a b_i jsou definovány rovnostmi 2.4 a 2.6. Pak platí:*

$$A_{i-1}^2 - NB_{i-1}^2 = (-1)^iQ_i$$

Důkaz. Vyjdeme ze vztahu $\sqrt{N} = \frac{A_{i-2}+A_{i-1}x_i}{B_{i-2}+B_{i-1}x_i}$ (Jeho odvození lze nalézt v [Rie85]: A8.12 + A8.13). Dosazením $x_i = (\sqrt{N} + P_i)/Q_i$ dostaneme

$$\sqrt{N} = \frac{Q_iA_{i-2} + P_iA_{i-1} + A_{i-1}\sqrt{N}}{Q_iB_{i-2} + P_iB_{i-1} + B_{i-1}\sqrt{N}}$$

což můžeme upravit na tvar

$$(Q_iB_{i-2} + P_iB_{i-1})\sqrt{N} + NB_{i-1} = Q_iA_{i-2} + P_iA_{i-1} + A_{i-1}\sqrt{N}$$

$\sqrt{N}$ je iracionální (v celé kapitole předpokládáme N bezčtvercové) a tedy můžeme získanou rovnici rozdělit na racionální a iracionální část. Tím získáme 2 následující rovnice (druhou jsme vydělili číslem $\sqrt{N}$, které bylo ve všech členech):

$$Q_iA_{i-2} + P_iA_{i-1} = NB_{i-1}$$

$$Q_iB_{i-2} + P_iB_{i-1} = A_{i-1}$$

Z druhé rovnice si vyjádříme P_i:

$$P_i = \frac{A_{i-1} - Q_iB_{i-2}}{B_{i-1}}$$

a dosadíme do první rovnice. Tím získáme

$$(A_{i-2}B_{i-1} - A_{i-1}B_{i-2})Q_i = NB_{i-1}^2A_{i-1}^2$$

A konečně použitím věty 3 dostáváme

$$(-1)^{i-1}Q_i = NB_{i-1}^2 - A_{i-1}^2$$

□

Poznamenejme, že poslední rovnost věty nám dává $A_{i-1}^2 \equiv (-1)^iQ_i \ (modN)$. Jmenovatele $\{Q_i\}$ budeme nadále označovat jako pseudo-čtverce.

Příklad 4. Demonstrujme si užití předcházející věty na příkladu rozvoje $\sqrt{177}$:

$$\begin{aligned}
x_0 &= \frac{\sqrt{177}+13}{1} = 26 + \frac{\sqrt{177}-13}{1} \\
x_1 &= \frac{1}{\sqrt{177}-13} = \frac{\sqrt{177}+13}{8} = 3 + \frac{\sqrt{177}-11}{8} \\
x_2 &= \frac{8}{\sqrt{177}-11} = \frac{\sqrt{177}+11}{7} = 3 + \frac{\sqrt{177}-10}{7} \\
x_3 &= \frac{7}{\sqrt{177}-10} = \frac{\sqrt{177}+10}{11} = 2 + \frac{\sqrt{177}-12}{11} \\
x_4 &= \frac{11}{\sqrt{177}-12} = \frac{\sqrt{177}+12}{3} = 8 + \frac{\sqrt{177}-12}{3} \\
x_5 &= \frac{3}{\sqrt{177}-12} = \frac{\sqrt{177}+12}{11} = 2 + \frac{\sqrt{177}-10}{11} \\
x_6 &= \frac{11}{\sqrt{177}-10} = \frac{\sqrt{177}+10}{7} = 3 + \frac{\sqrt{177}-11}{7} \\
x_7 &= \frac{7}{\sqrt{177}-11} = \frac{\sqrt{177}+11}{8} = 3 + \frac{\sqrt{177}-13}{8}
\end{aligned}$$

$b_0 = 26$, protože potřebujeme u členu za odmocninou mít mínus. Dále počítáme podle pravidel uvedených výše. Nakonec když chceme vyjádřit $\sqrt{177}$ musíme od b_0 znovu 13 odečíst.

Výše popsané aproximace můžeme vyjádřit tabulkou, kterou dovedeme dopočítat rekurzivně:

i	-1	0	1	2	3	4	5	6	7
b_i		13	3	3	2	8	2	3	3
A_i	1	13	40	133	306	2581	5468	18985	62423
B_i	0	1	3	10	23	194	411	1427	4692

Tabulku vyplňujeme zleva doprava. Podíl $\frac{A_n}{B_n}$ nazveme n-tý konvergent. Tento název plyne z faktu, že $\lim_{n\to\infty} \frac{A_n}{B_n} = \sqrt{N}$. Z posledního sloupečku tabulky tedy dostáváme aproximaci $\sqrt{177} \approx 62423/4692$

Protože jsou řetězové zlomky aproximující $\sqrt{N}$ od jistého bodu periodické, je smysluplné uvážit, že pokud jsme se dostali už do periodické části, pak výrazy, které právě hledáme, mohou vycházet z výrazů, které jsme v rekurzi potkali dříve. Příklad 4 nám ukázal, jak může být rekurzivní výraz obrácen, tak že $\{Q_i\}$ a $\{b_i\}$ jsou kolem x_4 symetrické (za x_4 se opakují koeficienty, které se již objevily, ale v opačném pořadí).

Lemma 5 nám ukazuje, jak lze každé b_i počítat dvěma různými způsoby.

Lemma 5.

$$\left\lfloor \frac{\sqrt{N}+P_i}{Q_i} \right\rfloor = \left\lfloor \frac{\sqrt{N}+P_{i-1}}{Q_i} \right\rfloor = b_i$$

Důkaz. Druhá část rovnice, $\left\lfloor \frac{\sqrt{N}+P_{i-1}}{Q_i} \right\rfloor = b_i$ plyne z definice b_i.
Věta 1 (e) implikuje $Q_i > \sqrt{N} - P_{i-1}$. Proto platí:

$$\left\lfloor \frac{\sqrt{N}+P_i}{Q_i} \right\rfloor = \left\lfloor \frac{\sqrt{N}+b_iQ_i-P_{i-1}}{Q_i} \right\rfloor = b_i + \left\lfloor \frac{\sqrt{N}-P_{i-1}}{Q_i} \right\rfloor = b_i$$

□

Po přečtení příkladu 4, je přirozené očekávat, že mechanismus získání opačného směru dopočítávání koeficientů v rozvoji bude přesně stejný jako standardní přístup, až na to, že čitatel se mění první. Všimněme si, že stejné změny můžeme dosáhnout i pouhou změnou znaménka P_{i-1}.

Dále budeme pro počítání opačného směru v cyklu uvažovat celá čísla c_i a y_i, které tvoří posloupnost definovanou stejně jako b_i a x_i, akorát budou použity jiné 0. členy.

Lemma 6. *Nechť jsou čísla b_i, P_i, Q_i jako ve větě 1, $i \geq 0$. Nechť $y_0 = \frac{\sqrt{N}+P_{i+1}}{Q_{i+1}}$ a $c_0 = \lfloor y_0 \rfloor$. Dále induktivně definujme $y_j = \frac{1}{y_{j-1}-c_{j-1}}$ a $c_j = \lfloor x_{i-j+1} \rfloor$. Pak $c_0 = b_{i+1}$ a $y_j = \frac{\sqrt{N}+P_{i-j+1}}{Q_{i-j+1}}$, $j \geq 0$*

Důkaz. Z 2.11 a Lemma 5, $c_0 = \lfloor y_0 \rfloor = \lfloor \frac{\sqrt{N}+P_{i+1}}{Q_{i+1}} \rfloor = b_{i+1}$. Provedem důkaz matematickou indukcí. Stačí nám dokázat, že lemma platí pro $j = 1$. Použijeme větu 1

$$y_1 = \frac{1}{y_0 - c_0} = \frac{1}{\frac{\sqrt{N}+P_{i+1}}{Q_{i+1}-b_{i+1}} - b_{i+1}} = \frac{1}{\frac{\sqrt{N}+P_{i+1}-b_{i+1}Q_{i+1}}{Q_{i+1}}} = \frac{1}{\frac{\sqrt{N}-P_i}{Q_{i+1}}} = \frac{\mathbb{N}+P_i}{\frac{N-P_i^2}{Q_{i+1}}} =$$

$$= \frac{\sqrt{N}+P_i}{Q_i}$$

□

Toto nám ukazuje důležitou vlastnost řetězových zlomků, a sice fakt, že směr posloupnosti pseudo-čtverců a reziduí lze změnit pouze malou úpravou a použitím stejného rekurzivního mechanismu.

Za použití lemma 6, může být x_3 použito, např. k nalezení x_2 a x_1. Pokračováním tohoto procesu získáme výrazy předcházející x_0 a označíme si je jako x_{-1},$x_{-2}, \ldots$. Podobně definujme Q_{-1} a P_{-1}.

A můžeme si dodefinovat x_{-j}, P_{-j}, Q_{-j} pro $j > 0$:

$$x_{-j} = \frac{1}{x_{1-j} - c_{1-j}} = \frac{\sqrt{N}+P_{1-j}}{Q_{1-j}}$$

$$P_0 = P_0' = \lfloor \sqrt{N} \rfloor, \quad Q_0 = Q_0' = 1, \quad c_j = \lfloor x_{-j} \rfloor$$
$$P_{-j} = P_j' = c_j Q_j' - Q_{j+1}'$$
$$Q_{-j} = Q_j' = Q_{j+2}' + (P_{j+2}' - P_{j+1}')c_j$$

Jelikož y_0 splňuje 2.5 a je použita stejná rekurzivní formule, pak je jasné, že věta 1 platí stejně i na záporných indexech.

Příklad 5. $x_3 = \frac{\sqrt{177}+12}{11}$ a $P_3 = 12$. Nechť tedy $y_0 = \frac{\sqrt{177}+12}{11}$. Pak:

$$
\begin{aligned}
y_0 &= \tfrac{\sqrt{177}+12}{11} = 2 + \tfrac{\sqrt{177}-10}{11} \\
y_1 &= \tfrac{11}{\sqrt{177}-10} = \tfrac{\sqrt{177}+10}{7} = 3 + \tfrac{\sqrt{177}-11}{7} \\
y_2 &= \tfrac{7}{\sqrt{177}-11} = \tfrac{\sqrt{177}+11}{8} = 3 + \tfrac{\sqrt{177}-13}{8} \\
y_3 &= \tfrac{8}{\sqrt{177}-13} = \tfrac{\sqrt{177}+13}{1} = 26 + \tfrac{\sqrt{177}-13}{1} \\
y_4 &= \tfrac{1}{\sqrt{177}-13} = \tfrac{\sqrt{177}+13}{8} = 3 + \tfrac{\sqrt{177}-11}{8} \\
y_5 &= \tfrac{8}{\sqrt{177}-11} = \tfrac{\sqrt{177}+11}{7} = 3 + \tfrac{\sqrt{177}-10}{7}
\end{aligned}
$$

Pak stejně tak, jako z y_2 získáme $x_1 = \frac{\sqrt{177}+13}{8}$, získáme z y_4 výraz pro $x_{-1} = \frac{\sqrt{177}+13}{8}$ a z y_5 dostáváme $x_{-2} = \frac{\sqrt{177}+11}{7}$.

Kombinací periodicity a reverzibility můžeme posílit větu 1 (h).

Lemma 7. *Existuje přirozené číslo π, takové, že pro všechna celá i, $x_i = x_{i+\pi}$.*

Důkaz. Z věty 1 (h) víme, že existují k a π taková, že $\forall i \geq k$, $x_i = x_{i+\pi}$. To v podstatě znamená, že naším cílem je ukázat, že neexistuje žádná dolní mez pro k. Předpokládejme pro spor, že nějaká taková dolní mez pro k existuje. Nechť pak π a k jsou nejmenší možná celá čísla, pro která věta 1 (e) platí. Pak platí, že $x_k = x_{k+\pi}$. Díky lemma 6 víme, že platí $x_{k-1} = x_{k+\pi-1}$, což znamená, že $k-1$ také splňuje podmínku, což je ale spor s minimalitou voleného k. Proto tedy pro $\forall i$ $x_i = x_{i+1}$.

□

π bude všude dále v této práci značit periodu.

Pro faktorizaci budou velice důležité symetrie, které se vyskytují ve vyjádření $\sqrt{N}$, tak jako v příkladě 4 v bodech x_0 a x_5. Pokud je počáteční podmínka kolem nějakého bodu stejná na obě strany, pak je kolem tohoto bodu symetrická celá posloupnost. Přesněji to popisuje lemma 8.

Lemma 8. *Nechť $x_0 = \frac{\sqrt{N}-P_{-1}}{Q_0}$ splňuje podmínku 2.5 tak, že $Q_0 | 2P_{-1}$. Pak posloupnost pseudo-čtverců je symetrická kolem Q_0, takže pro $\forall i$ platí $Q_i = Q_{-i}$.*

Důkaz. Všimněme si, že platí $0 < \sqrt{N} - P_0 < Q_0$ s $P_0 = b_0 Q_0 - P_{-1}$, takže

$$0 < \sqrt{N} - b_0 Q_0 + P_{-1} < Q_0.$$

Aby byla splněna nerovnost, připadá v úvahu pouze kladné (celé) b_0. Pokud $0 < \sqrt{N} - P_{-1} < Q_0$, pak $b_0 = 2P_{-1}/Q_0$ splňuje nerovnost a tedy $P_0 = P_{-1}$. Nechť $y_{-1} = \frac{\sqrt{N}+P_1}{Q_1}$. Pak podle lemma 6, $y_0 = \frac{\sqrt{N}+P_0}{Q_0} = \frac{\sqrt{N}+P_{-1}}{Q_0} = x_0$.

Proto posloupnost pseudo-čtverců bude symetrická podle Q_0, pokud jsou výrazy pro spočítání prvních členů na obě strany stejné. A proto platí $Q_i = Q_{-i}$.

□

Existence středu symetrie nám dovolí dokázat, že existuje i další střed symetrie a že nám později tyto středy symetrie poskytnou výbornou službu při hledání faktorizace N.

Poznámka. Tyto 2 fakty byly objeveny v opačném pořadí. Bylo zřejmé, že nejednoznačné formy, které splňující tyto podmínky, nám poskytnou faktorizaci, ale až později bylo objeveno, že tyto formy vytváří středy symetrie. Poprvé to bylo zmíněno Gaussem [Gau66] a poprvé tento fakt aplikoval Shanks [Sha75b].

Věta 9. *Nechť $s = \lfloor \frac{\pi}{2} \rfloor$, kde π je perioda popsaná v lemma 7. Pokud π je sudé, platí $\forall i Q_{s+i} = Q_{s-i}$, ale $Q_s \neq Q_0$ a $Q_s | 2N$. Pokud je π liché, pak pro všechna i platí $Q_{s+i+1} = Q_{s-i}$ a buď je $NSD(Q_s,N)$ netriviální faktor N, nebo je -1 kvadratické reziduum N.*

Důkaz. Případ 1: Pokud je π sudé, $\pi = 2s$. Pak z lemmat 7 a 8 máme: $Q_{s+i} = Q_{-s-i} = Q_{2s-s-i} = Q_{s-i}$. Pokud $Q_{s+1} = \frac{N-P_s^2}{Q_s}$ a $Q_{s-1} = \frac{N-P_{s-1}^2}{Q_s}$, získáváme $P_s^2 = P_{s-1}^2$, což pro $P_i > 0$ implikuje $P_s = P_{s-1}$.

Nyní $Q_s = \frac{P_s + P_{s-1}}{b_s} = \frac{2P_s}{b_s}$ a tedy $Q_s | 2P_s$.

Předpokládejme, že $Q_0 = Q_s$. Pokud Q_s je sudé, pak $P_0 \equiv P_s \equiv 1 \ (mod\ 2)$ a pokud Q_s je liché, pak $Q_s | P_s$. Důležité je, že v obou případech existuje jednoznačné celé číslo z intervalu $(\sqrt{N} - Q_0, \sqrt{N})$, které tyto podmínky splňuje, a tedy $P_s = P_0$. Proto $x_s = \frac{\sqrt{N}+P_0}{Q_0} = x_0$, což je spor s volbou π, jako nejmenšího možného celého čísla takového, že $\forall i Q_i = Q_{i+\pi}$. Proto $Q_s \neq Q_0$.

Nyní $N = P_s^2 + Q_s Q_{s+1}$ a tedy je zjevné, že pokud Q_s je liché, pak $Q_s | P_s$, a tedy $Q_s | N$. Opačně, pokud Q_s je sudé, pak $(Q_s/2) P_s$ a tedy $(Q_s/2) | N$. V obou případech $Q_s | 2N$.

Případ 2: Pokud je π liché, $\pi = 2s + 1$. Pak z lemmat 7 a 8 máme $Q_{s+i+1} = Q_{-s-i-1} = Q_{2s+1-s-i-1} = Q_{s-i}$.

Speciálně $Q_s = Q_{s+1}$ a tedy $N = P_s^2 + Q_s Q_{s+1} = P_s^2 + Q_s^2$ a tedy $P_{s+1}^2 \equiv -Q_s^2 \ (mod\ N)$. Pokud je $NSD(Q_s,N) > 1$, pak se jedná o netriviální faktor čísla N a důkaz je hotov. Proto předpokládejme, že čísla Q_s a N jsou nesoudělná.Pak $Q_s^{-1} \ (mod N)$ existuje. Pak $(Q_s^{-1})^2 P_{s+1}^2 \equiv -1 \ (mod\ N)$. Pak $Q_s^{-1} P_{s+1}$ je odmocnina z -1 modulo N.

□

Poslední důležitá skutečnost z teorie řetězových zlomků, která bude pro faktorizaci velmi podstatná, je níže popsaná ekvivalence. Tuto ekvivalenci budeme v následujících kapitolách dále rozvíjet a na konci našeho studia teorie nám dá matematický aparát, který umožní přesunovat se mezi níže definovanou množinou $\mathbb{T}$, prostorem kvadratických forem, ideály či mřížemi. Každá z těchto struktur pro nás má nějaké užitečné vlastnosti. Některé struktury a vlastnosti budou praktické spíš pro získání důkazu správnosti celého algoritmu SQUFOF, jiné budou ryze praktické a mlčky užívané přímo v implementaci algoritmu.

Definujme si množinu $\mathbb{T}$ jako množinu všech čísel ve tvaru $\frac{\sqrt{N}+P_i}{Q_i}$ (v $\sqrt{N}$ je fixováno N jehož rozklad hledáme, x_i, P_i a Q_i jako v 2.6 - 2.9) takových, že:

$$P_i^2 \equiv N \ (mod\ Q_i) \tag{2.12}$$

Dále definujme

$$\mathbb{T}^* = \{x_i = \frac{\sqrt{N} + P_i}{Q_i} \in \mathbb{T} : 0 < P_i < \sqrt{N},\ |\sqrt{N} - Q_i| < P_i \ \ i \in \mathbb{Z}\}.$$

Prvek $x_i \in \mathbb{T}$ nazveme *redukovaným*, pokud $x_i \in \mathbb{T}^*$. Pro x,$y \in \mathbb{T}^*$ platí, že x je ekvivalentní s y, pokud se oba společně vyskytují v rozvoji řetězového zlomku. Je zřejmé, že se jedná o ekvivalenci na $\mathbb{T}^*$. Rozšíření této ekvivalence na všechny prvky $\mathbb{T}$ vyžaduje lemma které nám popíše vztah mezi prvky z $\mathbb{T} - \mathbb{T}^*$ a prvky z $\mathbb{T}^*$.

Lemma 10. *Nechť $x_0 \in \mathbb{T} - \mathbb{T}^*$. x_0 můžeme redukovat za (iterativního) použití rovnosti*

$$x_{i+1} = \frac{1}{x_i - b_i},\ b_i = \lfloor x_i - 1/2 \rfloor,\ i \geq 0 \tag{2.13}$$

tak, aby platilo $|Q_i| < 2\sqrt{N}$ pro nějaké i. Následným (vícenásobným) užitím rovnosti 2.2 dostaneme $x_k \in \mathbb{T}^*$, pro nějaké $k > 0$.

Důkaz. Volba b_i nám dává $\left|\frac{\sqrt{N}-P_i^2}{Q_i}\right| < \frac{1}{2}$ po prvním kroku a tedy $|P_i| < \frac{1}{2}|Q_i| + \sqrt{N}$. Proto

$$\begin{aligned} |Q_{i+1}| &= \left|\frac{N - P_i^2}{Q_i}\right| \\ &\left|\frac{\sqrt{N} - P_i}{Q_i}\right| |\sqrt{N} + P_i| \\ &< \frac{1}{2}(2\sqrt{N} + \frac{1}{2}|Q_i|) \\ &= \sqrt{N} + \frac{1}{4}|Q_i| \end{aligned}$$

a tedy Q_i bude klesat, dokud $|Q_i| > \frac{4}{3}\sqrt{N}$. Pokud $|Q_r| < 2\sqrt{N}$, vrátíme se zpět k standardnímu zápisu pro b_r. Jsou celkem 3 možnosti, jaké Q_r je:
Případ 1: $0 < Q_r < \sqrt{N}$. V tomto případě je zřejmé, že x_{i+1} bude redukované.
Případ 2: $\sqrt{N} < Q_r < 2\sqrt{N}$. V tomto případě, pokud $P_r > 0$, pak x_{r+1} je redukované. Jinak $|P_r| < \sqrt{N}$ a tedy x_{r+1} nám spadne do případu 1.
Případ 3: $-2\sqrt{N} < Q_r < 0$. Pak $\sqrt{N} < P_r < \sqrt{N}+|Q_r|$ dává $Q_{r+1} < 2\sqrt{N}+|Q_r|$. Pokud $Q_{r+1} < 2\sqrt{N}$, pak spadneme do případu 1 nebo 2. Pokud $2\sqrt{N} < Q_{r+1} < 2\sqrt{N} + |Q_r|$, pak nám volba b_r dává $\sqrt{N} + P_r > Q_{r+1}$, tedy $0 < P_{r+1} < \sqrt{N}$ a konečně x_{r+2} nám spadne do případu 1.

□

Ilustrujme si to na příkladu:

Příklad 6.

$$\begin{aligned} x_0 &= \tfrac{\sqrt{403}+267}{-134} = -2 + \tfrac{\sqrt{403}-1}{-134} \\ x_1 &= \tfrac{-134}{\sqrt{403}-1} = \tfrac{\sqrt{403}+1}{-3} = -8 + \tfrac{\sqrt{403}-23}{-3} \\ x_2 &= \tfrac{-3}{\sqrt{403}-23} = \tfrac{\sqrt{403}+23}{42} = 1 + \tfrac{\sqrt{403}-19}{42} \\ x_3 &= \tfrac{42}{\sqrt{403}-19} = \tfrac{\sqrt{403}+19}{1} = -39 + \tfrac{\sqrt{403}-20}{1} \end{aligned}$$

Lemma 10 definuje zobrazení $\mathfrak{R} : \mathbb{T} \to \mathbb{T}^*$. Toto zobrazení není jednoznačné, nicméně pokud pro $X \in \mathbb{T}$ máme $\mathfrak{R}(X) = x_1 \in \mathbb{T}^*$ a $\mathfrak{R}(X) = x_1 \in \mathbb{T}^*$, pak x_1 je ekvivalentní s x_2. Prvky $\mathbb{T}^*$ se tímto zobrazením zobrazují samy na sebe. Dva prvky jsou pak ekvivalentní, pokud prvky z $\mathbb{T}^*$, na které je možné je převést, jsou ekvivalentní. Je patrné, že se stále jedná o relaci ekvivalence. To celé můžeme ekvivalentně popsat tvrzením, že dvě čísla x a y jsou ekvivalentní právě tehdy, když pro jejich řetězový rozvoj od jistých indexů Δ_x a Δ_y platí, že $x_i = y_j$ pro $\forall x > \Delta_x$ a $\forall y > \Delta_y$. Tuto skutečnost můžeme popsat o něco uchopitelněji tak, že po určitém počtu výrazů mají identické cykly. V 2.2 si zadefinujeme relaci ekvivalence na kvadratických formách a následně dokážeme, že mezi těmito ekvivalencemi existuje korespondence, které budeme následně využívat.

2.2 Binární kvadratické formy

Algoritmus SQUFOF získal své jméno od kvadratických forem a tedy se dá očekávat, že kvadratické formy budou pro popis tohoto algoritmu stěžejní. Postupně si ukážeme, že možná ještě větší váhu, než-li samotné kvadratické formy, mají pro algoritmus vztahy mezi kvadratickými formami a řetězovými zlomky, ideály a svazy. Formy samotné jsou ale i tak pro celý algoritmus kriticky důležité a proto se jim budeme v této kapitole poměrně intenzivně věnovat.

V této kapitole si tedy zadefinujeme, co to binární kvadratická forma je, povíme si něco o jejich vlastnostech, ukážeme si, že kvadratické formy tvoří cykly, že 2 formy si mohou být ekvivalentní a ukážeme, že ekvivalence forem toho má spoustu společného s ekvivalencí řetězových zlomků, a že mezi těmito dvěma zobrazeními existuje korespondence.

Definice 1 (Binární kvadratická forma)**.** *$f(x,y) = ax^2+bxy+cy^2$, kde konstanty $a, b, c \in \mathbb{Z}$, nazveme binární kvadratickou formou v proměnných $x, y \in \mathbb{Z}$.*

Definice 2 (Diskriminant)**.** *Diskriminant kvadratické formy f je definován jako $b^2 - 4ac$.*
Diskriminant Δ nazveme fundamentálním, pokud buď Δ je lichý a bezčtvercový, nebo pokud Δ je sudý a platí, že $\Delta/4$ je bezčtvercový a zároveň $\Delta/4 \equiv 2$ nebo 3 (mod 4).

Často budeme psát pouze $f = (a,b,c)$. V případě, že c lze dopočítat ze známého diskriminantu formy f, pak můžeme použít značení $f = (a,b,*)$. Značení $f = (a,*,*)$ používáme, pokud jsou konstanty b a c buď neznámé, nebo nepodstatné. Dále poznamenejme, že pokud Δ je diskriminant formy f, pak $\Delta \equiv 0$ nebo 1 mod 4 a $b \equiv \Delta \bmod 2$.

Analogicky k definici primitivního polynomu zadefinujeme primitivní formu.

Definice 3 (Primitivní forma)**.** *Formu f nazveme primitivní, pokud $NSD(a,b,c) = 1$*

Definice 4 (Reprezentace)**.** *O formě f řekneme, že reprezentuje $m \in \mathbb{Z}$, pokud existují $x_0,y_0 \in \mathbb{Z}$ takové, že $f(x_0,y_0) = ax_0^2 + bx_0y_0 + cy_0^2 = m$. Reprezentaci nazveme primitivní, pokud $NSD(x_0,y_0) = 1$*

Jiný pohled nám kvadratické formy popisuje jako množinu všech čísel, kterou dokážeme konkrétní formou reprezentovat. Tento pohled na formy nám umožní vyslovit názornou definici ekvivalence kvadratických forem.

Definice 5 (Ekvivalence forem)**.** *Dvě kvadratické formy jsou ekvivalentní právě tehdy, když reprezentují stejnou množinu celých čísel.*

Je patrné, že pokud je jedna forma transformována na jinou formu substitucí

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \; ad - bc \pm 1$$

pak, pokud je tato matice invertibilní, jsou obě formy ekvivalentní. Následuje jiná definice ekvivalence forem, která je výrazně techničtější a naznačuje, jak s ekvivalencí budeme moci zacházet.

Definice 6 (Ekvivalence forem)**.** *O formách f_1 a f_2 řekneme, že jsou vlastně ekvivalentní právě tehdy, když existují $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$, $\alpha\delta - \beta\gamma = 1$ takové, že platí $f_1(x,y) = f_2(\alpha x + \beta y, \gamma x + \delta y)$. Skutečnost, že jsou formy f_1 a f_2 vlastně ekvivalentní, zapisujeme jako $f_1 \sim f_2$.*
Pokud platí, že $\alpha\delta - \beta\gamma = -1$, pak říkáme, že f_1 a f_2 jsou nevlastně ekvivalentní.

Poznámka. V této práci budeme používat v naprosté většině případů vlastní ekvivalenci a proto pokud u ekvivalence nebude napsáno explicitně "nevlastní", předpokládáme, že se jedná o vlastní a tento přívlastek neuvádíme.

Další možný pohled na kvadratické formy je skrze modulární grupy.

Definice 7 (Modulární grupa)**.** *Modulární grupa je projektivní speciální lineární grupa $PSL_2(\mathbb{Z})$ matic 2×2 s celočíselnými koeficienty a s determinantem rovným ± 1. Grupovou operací je násobení matic.*

Nechť $\Gamma = PSL_2(\mathbb{Z})$ je modulární grupa a definujme akci grupy Γ na množině binárních kvadratických forem výrazem

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot f(x,y) = f(\alpha x + \beta y, \gamma x + \delta y).$$

Pak $f_1 \sim f_2$ právě tehdy, když f_1 a f_2 jsou ekvivalentní modulo akci grupy Γ.

Poznámka. Poznamenejme, že platí rovnost $(a,b+2na,a+nb+c) \sim (a,b,c)$ pro všechna $n \in \mathbb{Z}$, při použití matice $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

Počet tříd forem s diskriminantem Δ budeme značit jako $h^+(\Delta)$ a nebo pouze h^+. Lze dokázat, že $h^+(\Delta)$ je konečný.

Definice 8. *Formy se záporným diskriminantem nazýváme definitní, zatímco formy s diskriminantem kladným nazýváme indefinitní.*

Definice 9 (Nejednoznačná forma)**.** *Nejednoznačná forma je taková, která je nevlastně ekvivalentní sama se sebou. Tzn. po přenásobení nějakou maticí s determinantem -1 se zobrazí sama na sebe.*

Příklad 7. $F(x,y) = -14x^2 + 10xy + 5y^2$ je transformována na sebe sama pomocí substituce:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$$

tedy forma $(-14,10,5)$ je nejednoznačná.

Definice 10. *Forma (k,kn,c) se nazývá nejednoznačná (k, n, $c \in \mathbb{Z}$).*
alternativně: Forma (a,b,c) se nazývá nejednoznačná, pokud $a \mid b$.

Lemma 11. *Nejednoznačné formy ve tvaru (k,kn,c) s diskriminantem Δ existují pro každé $k \mid \Delta$.*

Důkaz. Plyne přímo z definice diskriminantu $\Delta = (kn)^2 - 4\dot{k}\dot{c} = k\dot{(}k - 4c)$, tedy $k \mid \Delta$.

□

Pro porozumění algoritmu SQUFOF budeme potřebovat pouze formy indefinitní. Nyní bude třeba nadefinovat si vlastnosti indefinitních forem, operace na nich a jejich možné vzájemné vztahy. Dalším důležitým bodem pro nás bude organizace a reprezentace kvadratických forem ekvivalentních nějaké dané formě. Protože každá forma má nekonečně mnoho ekvivalentních forem, potřebujeme náš výběr zúžit. K tomu nám pomůže následující definice:

Definice 11. *Kvadratická forma $ax^2 + bxy + cy^2$, s kladným diskriminantem $\Delta = b^2 - 4ac$ je redukovaná právě tehdy, pokud:*

$$0 < b < \sqrt{\Delta} \tag{2.14}$$

$$|\sqrt{\Delta} - 2|a|| < b \tag{2.15}$$

Poznamenejme, že $\Delta = b^2 - 4ac$ a 2.14 vyžadují, aby $ac < 0$, tedy aby koeficienty a a c měly opačná znaménka.

Pro vysvětlení Gaussova popisu uspořádání forem budeme potřebovat ještě jednu z jeho definic:

Definice 12. *Dvě formy $F(x,y) = ax^2 + bxy + cy^2$ a $F'(x,y) = a'x^2 + b'xy + c'y^2$ s diskriminantem Δ jsou sousední, pokud $c = a'$*

Následující definice nám ukáže, jak lze s redukovanými formami pracovat a jak vůbec najít k libovolné formě redukovanou formu jí ekvivalentní.

Definice 13 (Standardní redukční operátor)**.** *Pro každou indefinitní formu $f = (a,b,c)$ s $ac \neq 0$ definujeme standardní redukční operátor*

$$\rho(a,b,c) = \Big(c, r(-b,c), \frac{r(-b,c)^2 - \Delta}{4c}\Big)$$

kde $r(-b,c)$ je definováno jako jednoznačné celé číslo r takové, že $r + b \equiv 0 \ mod \ 2c$ a

$$-|c| < r \leq |c| \qquad pokud \ \sqrt{\Delta} < |c|$$
$$\sqrt{\Delta} - 2|c| < r < \sqrt{\Delta} \qquad pokud \ |c| < \sqrt{\Delta}$$

$\rho(f)$ nazveme redukcí f a výsledek n aplikací ρ zapíšeme jako $\rho^n(f)$. Formy f a $\rho(f)$ jsou ekvivalentní.

Bude se nám hodit zadefinovat si i inverzní redukční operátor a to jako

$$\rho^{-1}(a,b,c) = \Big(\frac{r(-b,a)^2 - \Delta, r(-b,a), a}{4c}\Big),$$

kde $r(-b,a)$ je definováno stejně jako v definici ρ.

Všimněme si, že forma $\rho(f)$ splňuje podmínky z definice sousední formy. Platí tedy, že všechny formy vzniklé aplikací redukčního operátoru na f jsou s f sousední a z definice redukčního operátoru platí, že jsou ekvivalentní. Z toho mimojiné plyne, že každá forma je sousední a ekvivalentní nějaké redukované formě.

Protože následující lemmata jsou uvedena pouze pro utvoření lepší představy a nejsou pro samotný popis algoritmu důležitá, nebudou v této práci dokázána.

Lemma 12. *Rovnost $\rho(\rho^{-1}(f)) = \rho^{-1}(\rho(f)) = f$ platí právě tehdy, když je forma f redukovaná.*

Lemma 13. *Forma f je redukovaná $\Leftrightarrow$ forma $\rho(f)$ je redukovaná $\Leftrightarrow$ forma $\rho^{-1}(f)$ je redukovaná.*

Pro každou formu existuje jednoznačná redukovaná sousední forma jak zleva, tak zprava, a jedná se právě o formy $\rho(a,b,c)$ a $\rho^{-1}(a,b,c)$.

Opusťme nyní redukční operátor a vraťme se zpět k naší otázce uspořádání forem. Nyní máme konečně zadefinováno vše, co potřebujeme k tomu, abychom mohli zadefinovat cyklus forem.

Definice 14 (Cykly)**.** *Cyklem kvadratických forem generovaným formou F nazveme množinu všech redukovaných forem, které jsou formě F ekvivalentní. Tyto formy jsou si navzájem formami sousedními.*
Definujme dále délku cyklu (periodu) π tak, že $\pi \in \mathbb{N}$ je nejmenší číslo takové, že pro všechna F_i $(i = 1, \ldots, \pi)$ z cyklu platí, že $\rho^{\pi}(F_i) = F_i$ a zároveň $(\rho^{-1})^{\pi}(F_i) = F_i$

Věta 14. *[Gau66] Pokud jsou redukované formy F,F' vlastně ekvivalentní, pak se forma F nachází v cyklu generovaném F' a forma F' se nachází v cyklu generovaném F.*

Kompletní důkaz této věty nabízí Gauss ve své publikaci [Gau66] jako důkaz k Větě 193. Jelikož se jedná o poměrně dlouhý důkaz spíše technického ražení, dovolíme si jeho plné znění v této práci vynechat a nabídneme pouze jeho ideu.

Poznámka (Idea důkazu). Gauss v důkazu uvažuje na obě strany nekonečnou posloupnost forem sousedních k formě F. Jelikož jsou všechny formy sousední zároveň formami ekvivalentními, tak pro každou takovou formu f_s ($s \in \mathbb{Z}$ značí pozici v posloupnosti) existuje čtveřice koeficientů $(\alpha_s,\beta_s,\gamma_s,\delta_s)$ taková, že platí $F(x,y) = f_s(\alpha_s x + \beta_s y, \gamma_s x + \delta_s y)$ a zároveň $\alpha_s\delta_s - \beta_s\gamma_s = 1$. Podobně z předpokladu, že F,F' jsou vlastně ekvivalentní, dostáváme podmínku, že musí existovat čtveřice koeficientů $(\mathfrak{A},\mathfrak{B},\mathfrak{C},\mathfrak{D})$ taková, že $F(x,y) = F'(\mathfrak{A}x + \mathfrak{B}y, \mathfrak{C}x + \mathfrak{D}y)$.

Celý důkaz je pak rozbor všech případů, jak mohou koeficienty vypadat, aby splnily výše uvedené podmínky a několik dalších, které plynou ze substituce. V každém z těchto jednotlivých případů se ukáže, že $(\mathfrak{A},\mathfrak{B},\mathfrak{C},\mathfrak{D}) = (\alpha_s,\beta_s,\gamma_s,\delta_s)$ pro nějaké konkrétní s. Z toho získáme identitu formy F' a formy f_s, která je formou sousední s F a tedy F' leží v cyklu generovaném F. Situace je pro F a F' symetrická a tedy není nutné celý důkaz opakovat pro posloupnost sousedních forem F'.

Podobnost pojmů jako je cyklus či ekvivalence u forem se stejnými pojmy v kontextu řetězových zlomků není vůbec náhodná. Nyní se zaměříme na korespondenci, která by tyto 2 koncepty dokázala propojit. Zadefinujeme zobrazení, které nám ukáže korespondenci mezi kvadratickými formami a prvky $\mathbb{T}$ a ukážeme, že toto zobrazení zároveň potvrzuje i korespondenci mezi redukovanými kvadratickými formami a prvky $\mathbb{T}^*$.

Definice 15 (Zobrazení $\Phi_{\mathbb{T},\mathbb{F}}$)**.** *Definujme si zobrazení z* $\mathbb{T}$ *do* $\mathbb{F}$*:*

$$\Phi_{\mathbb{T},\mathbb{F}} : \mathbb{T} \to \mathbb{F}$$

$$\frac{\sqrt{N} - P_i}{Q_i} \to Q_i(-1)^i x^2 + 2P_i xy + Q_{i+1}(-1)^{i+1} y^2 \tag{2.16}$$

Lemma 15. *Inverzní zobrazení nechť je definováno:*

$$\Phi_{\mathbb{F},\mathbb{T}} : \mathbb{F} \to \mathbb{T}$$

$$ax^2 + bxy + cy^2 \to x_i = \frac{\sqrt{\Delta/4} - b/2}{|a|} \in \mathbb{T} \tag{2.17}$$

kde diskriminant kvadratické formy je roven Δ*, což je prvek* $\mathbb{T}$*.*

Důkaz. Dosazením:

$$\Phi_{\mathbb{F},\mathbb{T}}(\Phi_{\mathbb{T},\mathbb{F}}(x_i)) = \Phi_{\mathbb{F},\mathbb{T}}(\Phi_{\mathbb{T},\mathbb{F}}(\frac{\sqrt{N} - P_i}{Q_i})) =$$

$$= \Phi_{\mathbb{F},\mathbb{T}}(Q_i(-1)^i x^2 + 2P_i xy + Q_{i+1}(-1)^{i+1} y^2) =$$

$$= \frac{\sqrt{(4P_i^2 - 4Q_iQ_{i+1}(-1)^i(-1)^{i+1})/4} - (2P_i)/2}{Q_i} =$$

$$= \frac{\sqrt{(P_i^2 + Q_iQ_{i+1})} - P_i}{Q_i} \overset{\text{z věty 1(a)}}{=} \frac{\sqrt{N} - P_i}{Q_i}$$

Tedy platí, že $\Phi_{\mathbb{F},\mathbb{T}}$ je inverzní zobrazení k $\Phi_{\mathbb{T},\mathbb{F}}$.

□

Poznamenejme, že z $\Delta = b^2 - 4ac$ plyne, že $4a|\Delta - b^2$ a tedy x_i opravdu náleží do $\mathbb{T}$.

Na konci sekce o řetězových zlomcích jsme definovali ekvivalenci na $\mathbb{T}$ a naznačili, že koresponduje s ekvivalencí na binárních kvadratických formách. Následující věta toto formalizuje:

Věta 16. *Zobrazení* $\Phi_{\mathbb{T},\mathbb{F}}$ *zobrazuje třídy ekvivalence na* $\mathbb{T}$ *na třídy ekvivalence na* $\mathbb{F}$*. To znamená, že* $x_i, x_j \in \mathbb{T}$ *odpovídají* $F_i = \Phi_{\mathbb{T},\mathbb{F}}(x_i), F_j = \Phi_{\mathbb{T},\mathbb{F}}(x_j) \in \mathbb{F}$*, respektive* $x_i \sim x_j$ *právě tehdy, když* $F_i \sim F_j$*.*

Důkaz. Nechť $x_i \sim x_j$. Protože x_i a x_j musí být ve stejném rozvoji řetězovými zlomky, předpokládejme, bez újmy na obecnosti, že $j = i + 1$. Jiné případy lze snadno na tento případ převést.
Kvadratická forma odpovídající x_i je pak dána v (2.16). Pak substituce

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & (-1)^i b_{i+1} \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix}$$

zobrazuje F_i na

$$Q_{i+1}(-1)^{i+1}x^2 + 2P_{i+1}xy + Q_{i+2}(-1)^{i+2}y^2$$

Všimněme si, že matice má determinant roven 1 a tedy ekvivalence je vlastní. Abychom dokázali opačný směr, tedy že x_i, která jsou (v kontextu $\Phi_{\mathbb{F},\mathbb{Q}}$) obrazy ekvivalentních kvadratických forem, jsou si ekvivalentní (podle věty 14). Všimněme si, že poslední koeficient kvadratické formy odpovídající x_i, tedy výraz $Q_{i+1}(-1)^{i+1}$, je zároveň prvním členem kvadratické formy odpovídající x_{i+1}. To znamená, že tyto 2 formy jsou sousední a proto jsou z definice cyklu ekvivalentní. □

Abychom mohli s kvadratickými formami pracovat, potřebujeme na nich zavést nějaké operace. Základní operací pro kvadratické formy je skládání forem.

Tomuto tématu se Gauss věnuje v otázce 236 práce [Gau66]. Tam nabízí velice univerzální definici pro skládání. Skládané formy spolu vynásobí a výsledek poté za pomocí různých substitucí upraví na jinou, jednodušší, binární kvadratickou formu. Bohužel tento obecný algoritmus je v tomto případě velice komplikovaný a navíc umožňuje volbu konstanty tak, že výsledkem skládání může být kterákoliv kvadratická forma z výsledné třídy ekvivalence.

Shanks a Buell nebyli spokojeni s faktem, že při takto definovaném skládání forem není výsledek předvídatelný. Vytvořili proto výrazně zjednodušenou variantu algoritmu skládání forem, která nedovolí libovolně vybírat žádnou konstantu a tedy složení dvou forem bude mít vždy stejný výsledek.

Pro skládání forem budeme dále používat symbol $\circ$.

Definice 16. *Nechť $F_1 = (a_1,b_1,c_1)$ a $F_2 = (a_2,b_2,c_2)$ jsou primitivní formy s diskriminanty d_1 a d_2, takovými, že $d_1 = \Delta n_1^2$ a $d_2 = \Delta n_2^2$ pro $n_1,n_2,\Delta \in \mathbb{Z}$ a $\Delta = NSD(d_1,d_2)$. Nechť*

$$m = gcd(a_1n_2,a_2n_1,\frac{b_1n_2 + b_2n_1}{2}).$$

Pak soustava kongruencí

$$\begin{aligned} mn_1B &\equiv mb_1 \quad (mod\ 2a_1) \\ mn_2B &\equiv mb_2 \quad (mod\ 2a_2) \\ m(b_1n_2 + b_2n_1)B &\equiv m(b_1b_2 + \Delta n_1n_2) \quad (mod\ 4a_1a_2) \end{aligned}$$

je řešitelná a dává nám celé číslo B (konvence nám říká, že bereme takové B, které splňuje všechny podmínky a má nejmenší absolutní hodnotu). Pak skládání forem F_1 a F_2 je definováno jako:

$$F_1 \circ F_2 = (\frac{a_1 a_2}{m^2}, B, \frac{(B^2 - \Delta)m^2}{4a_1 a_2})$$

s diskriminantem Δ [Bue89].

Nyní nás čeká zodpovězení otázky, jaký je vztah skládání k ekvivalenci forem.

Věta 17. *Pokud $F_1 \sim F_2$, pak $F \circ F_1 \sim F \circ F_2$.*

Tato věta je důsledkem vět 237, 238 a 239, které ve svém díle [Gau66] publikoval Gauss. Tyto 3 věty popisují rozklad formy, vlastnosti těchto rozkladů a vlastnosti forem s rozkladem ekvivalentní. Všechny jsou spíše technického ražení a jejich důkazy pracují s posloupnostmi sousedních forem a hledají koeficienty $(\alpha, \beta, \gamma, \delta)$ které určují vlastní ekvivalenci. V této práci si je pro jejich rozsah dovolíme vynechat.

Z této věty nám plyne, že skládání forem se chová vzhledem k ekvivalenci velice přirozeně. Udělejme si nyní malé shrnutí faktů o třídách ekvivalence kvadratických forem. Věta 17 nám říká, že skládání má na třídách ekvivalence kvadratických forem požadované vlastnosti, aby mohlo být grupovou operací, a že je jedno, kterou formu použijeme pro reprezentaci dané třídy. Abychom ukázali, že se opravdu jedná o grupu, musíme ještě dokázat, že pro každou kvadratickou formu existuje vzhledem ke skládání inverz. To ukážeme v lemma 19. Tím budeme mít splněny všechny podmínky, abychom mohli o množině tříd ekvivalence kvadratických forem a o skládání forem říci, že tvoří grupu.

Definice 17 (Třídová grupa)**.** *Třídovou grupou budeme nazývat grupu tvořenou třídami ekvivalence kvadratických forem společně s operací skládání.*

Význam nejednoznačných forem pro faktorizaci již byl naznačen. Z výše ukázaných skutečností je patrné, že pokud je jedna forma v třídě ekvivalence nejednoznačná, pak celá třída ekvivalence je nejednoznačná.

Následující lemma nám popisuje vlastnosti takových cyklů a naznačuje důvod, proč nás tyto třídy budou tolik zajímat. Dovedeme-li totiž najít v této třídě střed symetrie, dostáváme netriviální faktor determinantu. Tento fakt v praxi znamená, že můžeme převést problém hledání faktoru čísla N na problém hledání jednoho ze dvou středů symetrie v třídě ekvivalence kvadratických forem s diskriminantem N.

Lemma 18. *Nejednoznačná třída ekvivalence (třída tvořená nejednoznačnými formami) obsahuje právě 2 středy symetrie. Těmi je pár redukovaných sousedních forem (c,b,a) a (a,b,c), které jsou v cyklu navzájem formami opačnými. Nechť a je jejich společný člen. Pak buď a nebo $a/2$ dělí diskriminant.*

Důkaz. Nechť A je nejednoznačná třída ekvivalence a nechť $F = ax^2+bxy+cy^2 \in A$. Nechť $F' = cx^2 + bxy + ay^2$. Pak pokud $F \in A$, existuje substituce s determinantem -1, která zobrazí F samo na sebe. Jelikož zřejmá substituce, které by

v F zaměnila x za y má determinant také -1, součin těchto dvou substitučních matic dává vlastní substitucí a transformuje F v F'. Proto $F' \in A$.
Označme si nyní F jako F_0 a F' jako F_j pro nějaké j. Pak F_1 musí být opačná forma k formě F_{j-1} a tak dále. Pokud je j sudé, pak by měla forma $F_{j/2}$ být sama sobě opačná. Nicméně, z definice redukované formy plyne, že musí každá z opačných forem mít jiné znaménko, což je spor. Proto platí, že j musí být liché a pak $F_{\frac{j-1}{2}}$ je forma opačná formě $F_{\frac{j+1}{2}}$.
Zde si všimněme, že pokud se u posledního koeficientu formy mění znaménka, pak perioda musí být sudá.
Použitím stejného argumentu jako ve větě 9 lze ukázat, že musí existovat ještě jeden střed symetrie s vlastností, že $\forall i Q_{s+i} = Q_{s-i}$, ale toto Q_s není stejné, jako společný člen u prvního středu symetrie. Dvě kvadratické formy obsahující Q_s jakožto poslední koeficient pak splňují naše kriteria.

Fakt, že buď a, nebo $\frac{a}{2}$ dělí diskriminant byl pro diskriminant ve tvaru $4N$ dokázán v důkazu věty 9. Je pouze nutné uvědomit si, že díky definici funkce $\Phi_{\mathbb{F},\mathbb{T}}$ si odpovídají a a $(-)Q_s$ z důkazu 9 (vzhledem k tomu, že nás zajímají dělitelnosti, tak znaménko můžeme zanedbat). Pak dokázaný výrok pro π sudé: $Q_s \mid 2N$ přímo implikuje, že $\frac{a}{2} \mid 4N =$ diskriminant. A pro π liché máme dokázáno, že $NSD(Q_s,N)$ je faktor N a tedy $a \mid N \Rightarrow a \mid 4N$. □

Všimněme si, že věta 9 popisuje 2 různé typy středů symetrie. Nicméně druhý případ ve větě popsaný není v aplikaci na kvadratické formy pro svá měnící se znaménka zajímavý. Prakticky je sice možné, že výraz bude v jednom středu symetrie pouze záporem výrazu v druhém středu symetrie (tato situace odpovídá rozvoji řetězovými zlomky s lichou periodou, kde se vyskytuje střed symetrie 2. typu), ale takováto symetrie nám obecně nedává žádnou použitelnou informaci, která by mohla vést k faktorizaci N.

Definice 18 (Hlavní forma)**.** *Jednoznačně určená redukovaná forma s diskriminantem* Δ *ve tvaru* $(1,b,c)$ *se nazývá hlavní forma.*

Mezi ostatními cykly pro nás bude mít výsadní postavení cyklus obsahující hlavní formu. Tento nazveme hlavním cyklem. Stojí za to zdůraznit fakt, že počet redukovaných forem v hlavním cyklu je vždy sudý (viz. důkaz lemma 18).

Nyní je ještě třeba popsat, jak nejednoznačné formy zapadají mezi ostatní prvky třídové grupy. Pro práci s třídovou grupou budeme potřebovat inverzy. Nechť 1 reprezentuje hlavní formu. Nechť F^{-1} značí symetrický inverz F, $(a,b,c)^{-1} = (c,b,a)$.

Lemma 19. $F \circ F^{-1} \sim 1$

Důkaz. Nechť $F = ax^2 + bxy + cy^2$. Pak $F^{-1} = cx^2 + bxy + ay^2$. Nechť G je další forma sousední k F^{-1}, tedy $G = ax^2 + b'xy + c'y^2$, kde $a|(b+b')$ z korespondence s řetězovými zlomky. Složme $F \circ G$, s $n_1 = n_2 = 1$ a $m = a$. Dostáváme $F \circ G$, kde první koeficient je roven 1. Tedy $F \circ G \sim 1$ a zároveň $F^{-1} \sim G$ a tedy $F \circ F^{-1} \sim 1$
□

Poznamenejme, že toto implikuje, že druhá mocnina středu symetrie je 1. Věta 20 pravděpodobně byla Shanksovi známa, protože SQUFOF na ní závisí, nicméně nezdá se, že by ji kdekoliv explicitně vyjádřil. Využiji proto formulaci kterou použil Stephen McMath v [McM04].

Věta 20. *Třída ekvivalence má v třídové grupě řád* 2 *nebo* 1 $\Leftrightarrow$ *je nejednoznačná*

Důkaz. Nechť A je nejednoznačná třída. Nechť $F \in A$. Pak $F \sim F^{-1}$, a tedy $F \circ F \sim F \circ F^{-1} \sim 1$. Z toho plyne, že $F \circ F$ je v hlavním cyklu a tedy A má v třídové grupě řád 2 nebo 1.

Naopak předpokládejme, že třída A má v třídové grupě řád 2 nebo 1. Nechť $F \in A$. Pak $F \circ F$ je v hlavním cyklu a tedy $F \circ F \sim (F \circ F)^{-1}$. Ze skládání je ale patrné, že $(F \circ F)^{-1} \sim F^{-1} \circ F^{-1}$. To znamená, že $F \circ F \sim F^{-1} \circ F^{-1}$. Protože skládání je v třídové grupě asociativní, můžeme k oběma stranám rovnice přidat F, aniž by to mělo vliv na platnost ekvivalence.

$$(F \circ F) \circ F \sim (F^{-1} \circ F^{-1}) \circ F$$
$$1 \circ F \sim F^{-1} \circ (F^{-1} \circ F)$$
$$F \sim F^{-1}$$

a tedy A je nejednoznačná.

□

Příklad 8. Uvažujme kvadratickou formu $F = (36{,}70, -3)$ s determinantem $4 \cdot 1333$. Porovnejme $(F \circ F) \circ F$ s $F \circ F \circ F$, kde jediný rozdíl je v tom, že první výsledek je redukován již po prvním skládání. $F \circ F = (324, -38, -3)$ a nejbližší sousední forma $(-3{,}68{,}59)$ je redukovaná. $F \circ (-3{,}68{,}59) = (-12{,}70{,}9)$, která je již sama o sobě redukovaná. Nicméně, bez redukování $F \circ F \circ F = F \circ (324, -38, -3) = (729{,}448, -348)$. Pokud tuto formu redukujeme, je první redukovaná forma nalezena po dvou krocích a je to forma $(9{,}56, -61)$.

Odsud je patrné, že hlavní cyklus s operací skládání následovanou redukcí nesplňuje ani podmínky pro asociativní mocnění. Nicméně, pozorování, že 2 výsledky jsou sousední formy a že druhá redukce trvá o jeden krok déle nás nutí prozkoumat problém ještě trochu hlouběji.

Pochopení tohoto vyžaduje něco, co Shanks označil jako vnitřní vzdálenost. Pro $m < n$ a pro $x_m, x_{m+1}, \ldots, x_n \in \mathbb{T}$ (definováno v 2.10), definuje

$$D_{\mathbb{F}}(x_m{,}x_n) = log(\prod_{k=m+1}^{n} x_k) \tag{2.18}$$

Lenstra [Len01] k této definici přidává výraz $\frac{1}{2}log(Q_n/Q_m)$, který výsledek nepatrně zjednoduší, ale důkazy všech vlastností jsou pak mnohem komplikovanější a méně intuitivní. Tuto definici používá ku příkladu Williams v [Wil85].

Protože sousední kvadratické formy tvoří cyklus, musíme pro udržení konzistence měření, uvažovat vnitřní vzdálenost dvou forem vždy modulo vzdálenost

kolem celého hlavního cyklu.

Definice 19 (Regulátor)**.** *Nechť π je perioda hlavního cyklu. Regulátor R třídové grupy je vzdálenost kolem celého hlavního cyklu, která je rovna*

$$R = D_{\mathbb{F}}(F_0,F_\pi) = D(1,F_\pi)$$

Je přirozené vyžadovat, že měření vnitřní vzdálenosti v cyklu musí být nutně prováděno modulo R a $D_{\mathbb{F}}$ je zobrazení dvojic forem na interval $[0,R) \in \mathbb{R}$. Součet dvou vzdáleností musí být samozřejmě také redukován modulo R.

Práce se nyní bude ubírat směrem k analýze konceptu vnitřní vzdálenosti, který nám pomůže s hledáním správných forem a důkazu, že takovou formu doopravdy můžeme pro zadané N najít. Abychom dokázali vnitřní vzdálenost popsat podrobněji, budeme potřebovat další nástroje. K popisu nám poslouží jazyk ideálů a mříží.

Námi využité ideály budou v okruhu $\mathbb{Z}[\sqrt{N}] = \{a + b\sqrt{N} : a,b \in \mathbb{Z}\}$ a mříže budou v $\mathbb{Q}(\sqrt{N}) = \{a + b\sqrt{N} : a,b \in \mathbb{Q}\}$, kde N je bezčtvercové přirozené číslo.

Poznámka. Ideály v $\mathbb{Z}[\sqrt{N}]$ obvykle odpovídají pouze kvadratickým formám s diskriminantem $4N$. Poznamenejme, že pokud $N \equiv 1 \ (mod\ 4)$, pak $\mathbb{Z}[\sqrt{N}]$ není pro $\mathbb{Q}(\sqrt{N})$ okruh celistvých čísel nad $\mathbb{Z}$. Pro $N \equiv 1 \ (mod\ 4)$ je sice analýza ideálů v $\mathbb{Z}[\frac{\sqrt{N}+1}{2}]$ zajímavá, ale v zájmu jednoduchosti algoritmu se jí elegantně vyhneme. Pokud máme kvadratickou formu s diskriminantem ve tvaru $N \equiv 1 \ (mod\ 4)$, pak nežli s ní začneme pracovat, vynásobíme ji konstantou 2, čímž získáme kvadratickou formu s diskriminantem 4N, která odpovídá ideálu v $\mathbb{Z}[\sqrt{N}]$.

2.3 Ideály

Mějme $\xi \in \mathbb{Q}(\sqrt{N})$. Definujme si $\overline{\xi}$ vztahem $\overline{\alpha + \sqrt{\beta}} = \alpha - \sqrt{\beta}$. Toto číslo nazveme vzhledem ke ξ číslem konjugovaným.

Norma čísla $\xi \in \mathbb{Q}(\sqrt{N})$ je $\mathcal{N}(\xi) = \xi\overline{\xi} \in \mathbb{Q}$.

Abychom si zjednodušili zápis, budou dále symboly H, I, J a K ideály, u a v budou prvky ideálů, α a β budou prvky $\mathbb{Z}[\sqrt{N}]$, ξ a ζ budou prvky $\mathbb{Q}(\sqrt{N})$ a $\mathcal{L}$ bude mříž.

Naše definice ideálu je stejná jako v jakémkoliv jiném komutativním okruhu s jednotkou:

Definice 20. *Podmnožina I okruhu R je ideál právě tehdy, když u,$v \in I$, $u \pm v \in I$ a pro $\alpha \in R$, $u \cdot \alpha \in I$, tedy pokud I je uzavřená na sčítání a násobení prvkem z R. Definujme $L(I)$ jako nejmenší kladné celé číslo v I.*

Popis ideálů si vyžádá značení pro svazy generované množinou. Pokud

$$\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{Z}[\sqrt{N}]$$

označme mříž generovanou touto množinou jako

$$[\alpha_1, \alpha_2, \ldots, \alpha_k] = \{\sum_{i=1}^{k} n_i\alpha_i : n_i \in \mathbb{Z}\} \tag{2.19}$$

Všimněme si, že nad $\mathbb{Z}[\sqrt{N}]$ stačí uvažovat generující množinu mříže mohutnosti 2, tedy $[\alpha_1, \alpha_2]$. Důvodem je, že zde nalezneme nejvýše dvouprvkové $\mathbb{Z}$-lineárně nezávislé báze.

Následující lemma nám dává nutnou a postačující podmínku pro to, aby množina $\mathbb{Z}[\sqrt{N}]$ byla ideál.

Lemma 21. *Pro Q, s, N, $P \in \mathbb{Z}$, $s \neq 0$, N kladné a bezčtvercové, $[Q, s\sqrt{N} + P]$ je ideál okruhu $\mathbb{Z}[\sqrt{N}]$ právě když $sQ|\mathcal{N}(s\sqrt{N} + P), s|Q$ a $s|P$.*

Důkaz. Předpokládejme, že $I = [Q, s\sqrt{N} + P]$ je ideál v $\mathbb{Z}[\sqrt{N}]$.
Zvolme $\alpha = P - s\sqrt{N}$ a tedy $\mathcal{N}(s\sqrt{N} + P) \in I$. Protože je to celé číslo, $Q|\mathcal{N}(s\sqrt{N} + P)$.
Zvolme $\alpha = \sqrt{N}$ a tedy $Q\sqrt{N} \in I$. Pak $s|Q$ a díky tomu, že $Q|\mathcal{N}(s\sqrt{N} + P)$, dostáváme, že $s|P$.
Proto α mohlo být zvoleno jako: $\alpha = P/s - \sqrt{N}$ tak, že $Q|\mathcal{N}(s\sqrt{N} + P)/s$ a tedy $sQ|\mathcal{N}(s\sqrt{N} + P)$

Naopak, nechť $I = [Q, s\sqrt{N} + P]$ a předpokládejme, že $sQ|\mathcal{N}(s\sqrt{N} + P), s|Q$ a $s|P$. Uzavřenost na sčítání je triviální. Abychom dokázali, že I je uzavřený na násobení prvkem $\mathbb{Z}[\sqrt{N}]$, stačí uvažovat pouze násobení 1 a $\sqrt{N}$, které tvoří $\mathbb{Z}$-volnou bázi $\mathbb{Z}[\sqrt{N}]$. Přenásobení 1 je triviální. Pro $\sqrt{N}$

$$Q\sqrt{N} = \frac{Q}{s}(s\sqrt{N} + P) - \frac{P}{s}Q$$

a Q/s a $-P/s$ jsou celá čísla. Tedy

$$(s\sqrt{N}+P)\sqrt{N} = sN + P\sqrt{N} = \frac{P}{s}(s\sqrt{N}+P) + (\frac{-P^2+s^2N}{sQ})Q$$

a $\frac{P}{s}$ jsou celá čísla $(\frac{-P^2+s^2N}{sQ})$ jsou celá čísla.

□

Pokud $s = 1$, je ideál *primitivní.* protože $s|P$ a $s|Q$, ideály, které nejsou primitivní budou často značeny $(s)|[Q,\sqrt{N}+P]$. Označme $\mathbb{I}$ množinu všech primitivních ideálů.

Ze zápisu ve tvaru $I = [Q,\sqrt{N}+P]$ je zřejmé, že $|Q|$ je nejmenší kladné celé číslo v I. Definujme

$$L(I) = min\{I \cap \mathbb{Z}^+\} \tag{2.20}$$

V tuto chvíli máme vše, co potřebujeme k tomu, abychom definovali závislost mezi kvadratickými formami s diskriminantem $\Delta \equiv 0(mod\ 4)$ a ideály. Definujme zobrazení následovně:

$$\Phi_{\mathbb{F},\mathbb{I}}(Ax^2+Bxy+Cy^2) = [A,\sqrt{(\frac{B}{2})^2 - AC} + \frac{B}{2}] \tag{2.21}$$

$$\Phi_{\mathbb{I},\mathbb{F}}([Q,\sqrt{N}+P]) = Qx^2 + Pxy + \big(\frac{P^2-N}{Q}\big)y^2 \tag{2.22}$$

a definujme *redukovaný ideál* odpovídající redukované kvadratické formě. Poznamenejme, že $\Delta = 4N$.

Příklad 9. Kvadratická forma $(15{,}2\cdot 12, -1)$ odpovídá ideálu $[15,\sqrt{159}+12]$.

Zde se nám však objevuje jeden potenciální problém. Ideály $[15,\sqrt{159}+12]$ a $[-15,\sqrt{159}+12]$ jsou stejné, zatímco jim odpovídající kvadratické formy $(15{,}2\cdot 12, -1)$ a $(-15{,}2\cdot 12{,}1)$ jsou různé.

Je však zřejmé, že záporné znaménko má vliv pouze při skládání a neovlivní výpočet funkce Φ. Proto každá tato forma má v rámci svého cyklu stejnou polohu a tento rozdíl nebude pro naše zkoumání skládání a vnitřní vzdálenosti podstatný.

$\Phi_{\mathbb{T},\mathbb{F}}$ a $\Phi_{\mathbb{F},\mathbb{I}}$ mohou být složeny, čímž získáme

$$\Phi_{\mathbb{T},\mathbb{I}}(\frac{Q}{\sqrt{N}-P}) = [Q,\sqrt{N}-P]$$

a inverzní zobrazení $\Phi_{\mathbb{I},\mathbb{T}}$ je definováno zřejmým způsobem.

Pokud $A = [\alpha_1, \dots \alpha_d]$ a $B = [\beta_1 \dots \beta_d]$, pak je zřejmé, že $A = B$ právě tehdy, když existuje matice M rozměru $d \times d$ a s determinantem ± 1, taková, že:

$$\langle \alpha_i \rangle = M\langle \beta_i \rangle$$

kde $\langle\alpha_i\rangle$ a $\langle\beta_i\rangle$ jsou vektory.

Pro naše potřeby bude nejdůležitější operace na ideálech násobení. To je definováno následovně:

$$[\alpha_i] * [\beta_j] = [\alpha_i\beta_j \mid i,j = 1 \dots d]$$

Příklad 10.

$$I = [4,\sqrt{113}+11] * [16,\sqrt{113}+9] = [64,16\sqrt{113}+176,4\sqrt{133}+36,212+20\sqrt{113}]$$

4. člen je pouze součet 2. a 3. členu, proto nemá pro popis ideálu význam.

Pokračujme v úpravách použitím matice s determinantem 1, která od 2. členu odečte 4× 3. člen

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix}$$

Tím získáváme

$$I = [64,32,4\sqrt{113}+36]$$

Nyní je 1. člen násobek členu 2. a tedy je také zbytečný. Výsledek po zjednodušení je tedy

$$I = [32,4\sqrt{113}+36] = 4[8,\sqrt{113}+9]$$

Poznámka. Pro proces násobení ideálů jsou dobře známa pravidla, která ho výrazně zjednodušují [MvdP95] .

Věta 22. *Nechť* $I = [Q,\sqrt{N}+P]$ *a* $J = [Q',\sqrt{N}+P']$ *jsou ideály* $\mathbb{Z}[\sqrt{N}]$. *Nechť* $C = \frac{N-P^2}{Q}, C' = \frac{N-(P')^2}{Q'}$. *Pokud* $NSD(Q,P,C) = NSD(Q',P',C') = 1$, *pak* $I * J = s[q,\sqrt{N}+p]$, *kde*

$$s = NSD(Q,Q',P+P') \tag{2.23}$$

$$h = NSD(Q,Q',C,C',2) \tag{2.24}$$

$$q = hQQ'/s^2 \tag{2.25}$$

$$p \equiv P \pmod{Q/s} \tag{2.26}$$

$$p \equiv P' \pmod{Q'/s} \tag{2.27}$$

$$(P+P')p \equiv N + PP' \pmod{QQ'/s} \tag{2.28}$$

Důkaz. Uvažujme součin

$$I * J = [QQ',Q\sqrt{N} + QP',Q'\sqrt{N} + Q'P, N + PP' + (P + P')\sqrt{N}] \qquad (2.29)$$

Nejmenší celé číslo v $I * J$ bude nalezeno tak, že budeme hledat nejmenší celé číslo, které vznikne vynásobením jednotlivých členů po dvojicích. Pro usnadnění zápisu si zaveďme značení $\{\dots\}$, které bude odpovídat nejmenšímu společnému násobku.

$$L(I * J) = NSD(QQ',\{Q,Q'\},(P - P'),\frac{\{Q,P + P'\}Q'C'}{P + P'},\frac{\{Q',P + P'\}QC}{P + P'})$$

Nechť $s = NSD(Q,Q',P + P'), h = NSD(Q,Q',C,C',2), w = hQQ'/s$.Nechť $f \neq 2$ je prvočíslo. Nechť a,b,c,d,e,k jsou největší celá čísla taková, aby platilo $f^a|Q$, $f^b|Q'$, $f^c|(P + P')$, $f^d|C$, $f^e|C'$, $f^k|(P - P')$.
Pak $f^{a+b} \| QQ'$, $f^{max(a,b)+k} \| \{Q,Q'\}(P - P')$, $f^{max(a,c)+b+e-c} \| \frac{\{Q,P+P'\}Q'C'}{P+P'}$ a $f^{max(b,c)+a+d-c} \| \frac{\{Q',P+P'\}QC}{P+P'}$.

Následující analýza dokazuje, že pokud se $f \neq 2$, pak maximální exponent u f v $L(I * J)$ je $a + b - min(a,b,c)$, přičemž v případě, že $h = 2$, pak maximální exponent u 2 v $L(I * J)$ je $a + b + 1 - min(a,b,c)$ a pokud $h = 1$, pak je maximální exponent u f v $L(I * J)$ roven znovu $a + b - min(a,b,c)$. Jelikož se nám tímto rozpadá důkaz na několik případů, uveďme si jejich seznam.

1. $a = 0 \ \vee \ b = 0 \ \vee \ c = 0$
2. $a \neq 0 \ \wedge \ b \neq 0 \ \wedge \ c \neq 0$
   - 2.1. $f \neq 2$
     - 2.1.1. $a + d \neq b + e$
       - $f \mid (P - P')$
       - $f \nmid (P - P')$
     - 2.1.2. $a + d = b + e$
       - $f \mid (P - P')$
       - $f \nmid (P - P')$
   - 2.2. $f = 2$
     - 2.2.1. $a + d \neq b + e$
       - $c > 1$,$k > 1$
       - $c > 1$,$k \leq 1$
       - $c = 1$
     - 2.2.2. $a + d = b + e$
       - $c > 1$,$k > 1$
       - $c = 1$
       - $k = 1$

Případ 1) Pokud $a = 0$, pak $max(a,c) + b + e - c = b + e \geq b$, $max(b,c) + a + d - c \geq b$ a $a + b = b$ a tedy maximální exponent pro f v $L(I * J)$ je $b = a + b - min(a,b,c)$. Analogicky platí, že pro $b = 0$ je maximální exponent $a = a + b - min(a,b,c)$.
Předpokládejme $c = 0$. $f^{a+d} \| QC = N - P^2$ a $f^{b+e} \| Q'C' = N - (P')^2$. Výrazy od sebe odečteme a získáme $f^{min(a+d,b+e)} | (P^2 + (P')^2) = (P - P')(P + P')$. Pokud tedy $c = 0$, pak $f^{min(a+d,b+e)} \mid (P - P')$. Proto $f^{max(a,b)+min(a+d,b+e)} \mid \{Q,Q'\}(P - P')$. Nicméně platí $max(a,b) + min(a + d,b + e) \geq max(a,b) + min(a,b) = a + b$. Proto maximální exponent f v $L(I * J)$ je

$$min(a+b,max(a,c)+b+e-c,max(b,c)+a+d-c) = min(a+b,a+b+e,a+b+d) =$$

$$= a + b = a + b - min(a,b,c)$$

Případ 2.1.1) Předpokládejme $c \neq 0$, $f \neq 2$ a $a + d \neq b + e$.
Pak $f^{min(a+d,b+e)} \| (P^2 - (P')^2)) = (P + P')(P - P')$. Pokud $f \mid (P - P')$, pak $f \mid 2P$ a $f \mid 2P'$. Protože $f \neq 2$, platí že $f \mid P, f \mid P'$. Pak ale $a = e = 0$ a tedy $c \leq min(a,b)$. Potom je maximální exponent pro f v $L(I * J)$ roven

$$min(a+b,max(a,b)+min(a,b)-c,max(a,c)+b-c,max(b,c)+a-c) = a+b-c =$$

$$= a + b - min(a,b,c)$$

Pokud $f \nmid (P - P')$, pak $c = min(a + d,b + d)$ a maximální exponent pro f v $L(I * J)$ je

$$min(a + b,max(a,b),max(a,c) + b + e - c,max(b,c) + a + d - c)$$

Pokud $a = min(a,b,c)$, pak platí $min(b,c + b + e - c,max(b,c) + a + d - c) = b = a + b - min(a,b,c)$. Analogicky tvrzení platí pro $b = min(a,b,c)$. Pokud $c = min(a,b,c)$, pak protože platí $c = min(a + d,b + e)$, dostáváme $c = min(a,b)$. Maximální exponent je pak roven

$$min(max(a,b),a + b + e - c,b + a + d - c) = max(a,b) = a + b - min(a,b) =$$

$$= a + b - min(a,b,c)$$

Případ 2.1.2) Předpokládejme $c \neq 0, f \neq 2$, ale $a + d = b + e$. Stejně jako výše, pokud $f \mid (P - P')$, pak $d = e = 0$. V tomto případě tedy také $a = b$. Předpokládejme $c \leq a$. Poznamenejme, že $f^{a-c} \mid (P - P')$ a $max(a,b) + min(a + d,b + e) - c = a + b - c$. Pak je maximální exponent roven

$$min(a + b,max(a,c) + b - c,max(b,c) + a - c) = a + b - c = a + b - min(a,b,c).$$

Nyní předpokládejme $c > a$. Pak pro nějaké k platí $f^k \| (P - P')$. Maximální exponent je pak

$$min(a + b,max(a,b) + k,b,max(b,c) + a - c) = b = a + b - a = a + b - min(a,b,c)$$

Naopak předpokládejme $f \nmid (P - P')$. Pak $c \geq a + d = b + e$ a maximální exponent je

$$min(a + b, max(a,b), max(a,c) + b + e - c,max(b,c) + a + d - c) =$$

$= min(max(a,b),a+d) = max(a,b) = a+b-min(a,b = a+b-min(a,b,c))$

Případ 2.2.1)Nechť $f = 2$. Předpokládejme $a+d \neq b+e$. Pak $2^{min(c,k)} \| 2P$ a $2^{min(c,k)} \| 2P'$, tedy $2^{min(c,k)-1} \| P,P'$. Pokud $c > 1$ a $k > 1$, pak $d = e = 0$ a stejně jako v předešlém případě je největší exponent roven $a+b-min(a,b,c)$.
Předpokládejme $c > 1$, $k \leq 1$. Pak $k = 1$ a $c = min(a+d,b+e) - 1$. Největší exponent je pak

$$min(a+b,max(a,b)+1,max(a,c)+b+e-c,max(b,c)+a+d-c)$$

Pokud $a \leq min(b,c)$ dostáváme $b + min(e,1) = a+b+min(e,1) - min(a,b,c)$. $c+1 \leq a+d \leq c+d$ a tedy $d \geq 1$. Poznamenejme, že pokud $e \geq 1$, pak pak nastává speciální případ $h = 2$. Pokud $e = 0$, dostáváme totéž jako v minulém případě. Případy, kde je $b \leq min(a,c)$ jsou analogické.
Pokud $c \leq min(a,b)$, bude minimální exponent roven $min(max(a,b)+1,a+b+e-c,b+a+d-c)$. Bez újmy na obecnosti předpokládejme, že $a+d > b+e$ a tedy $c = a+d-1 \geq c+d-1$ z čehož plyne $d = 1$ a $a = c$. Exponent je nyní $min(b+1,b+e,b+d) = b + min(1,e,d) = a+b+min(1,e,d) - min(a,b,c)$ Znovu poznamenejme, že pokud $e \geq 1$ a $d \geq 1$, pak je toto speciální případ $h = 2$. Pro ostatní případy je vše stejné jako v minulém případě.

Předpokládejme $c = 1$. Pak $k \geq 1$. Exponent je

$$min(a+b,max(a,b)+min(a+d,b+e)-1,a+b+e-1,a+b+d-1)$$

Pokud $d = 0$ nebo $e = 0$, pak $h = 1$ a exponent se nám zredukuje na $a+b-1 = a+b-min(a,b,c)$. Jinak $h = 2$ a exponent se rovná $a+b = a+b+1-min(a,b,c)$.
Případ 2.2.2) Konečně předpokládejme, že $c \neq 0$ ale $a+d = b+e$. Pro nějaké k platí, $2^k \| (P-P')$. $c+k \geq a+d$. Pokud $c > 1$ a $k > 1$, pak $d = e = 0$, $a = b$. Exponent je pak roven $min(2a,a+k,max(a,c)+b-c)$. Pokud $c > a$, je to rovno $min(2a,a+k,a) = a = a+b-min(a,b,c)$. Pokud $c \leq a$, exponent je $min(2a,a+k,2a-c) = 2a-c = a+b-min(a,b,c)$.

Dále pokud $c = 1$, pak $k \geq a+d-1$ a exponent je

$$min(a+b,max(a,b)+k,a+b+e-1,b+a+d-1) = min(a+b,a+b+e-1,a+b+d-1).$$

Pokud $e > 0$ a $d > 0$, pak $h = 2$ a exponent je $a+b = a+b+1-min(a,b,c)$. Pokud $e = 0$ nebo $d = 0$, pak $h = 1$ a exponent je $a+b-1 = a+b-min(a,b,c)$.

Pokud $k = 1$, pak $c \geq 1$ a konkrétně $c \geq a+d-1 = b+e-1$. Pokud $c \leq min(a,b)$, pak $d = e = 1$ a tedy $h = 2$, $c = a = b$ a exponent je

$$min(2a,a+1) = a+1 = a+b+1-min(a,b,c).$$

Pokud $a \leq min(b,c)$, pak $d \geq e$ a exponent je

$$min(a+b,b+1,b+e,max(b,c)+a+d-c) = min(b+1,b+e).$$

Pokud $e \geq 1$, pak $d \geq e \geq 1$ a tedy $h = 2$ a v tomto případě je exponent $b+1 = a+b+1-min(a,b,c)$. Pokud $e = 0$, $h = 1$ a v takovém případě je

exponent roven $b = a + b - min(a,b,c)$.

Proto

$$L(I * J) = hQQ'/s$$

a tedy pro $f \neq 2$ je největší exponent $a+b-min(a,b,c)$ a pro $f = 2$ je nejvyšší exponent buď $a+b-min(a,b,c)$ pro $h = 1$, nebo je exponent $a+b+1-min(a,b,c)$ pro $h = 2$. Poznamenejme, že toto je také dělitelné s. Po vydělení s dostáváme $q = hQQ'/s^2$.

Existují celá čísla t,u a v taková, že $tQ+uQ'v(P+P') = s$. Nejprve uvažujme dělitelnost koeficientem s. To je triviální pro všechny výrazy kromě $N + PP'$. Z definice s:

$$\begin{aligned} P + P' &\equiv 0 \pmod{s} \\ -P &\equiv P' \pmod{s} \\ PP' &\equiv -P^2 \pmod{s} \\ N + PP' &\equiv N - P^2 \pmod{s} \end{aligned}$$

a pokud $s \mid Q$ a $Q \mid (N - P^2)$, pak $s \mid N + PP'$.

Lineární kombinace tří posledních prvků s koeficienty t,u a v můžeme popsat jako

$$s\sqrt{N} + tQP' + uQ'P + v(N + PP')$$

a tedy je evidentní, že po vydělení s zůstane primitivní ideál. Díky tomu se jedná o prvek $I * J$ s nejmenším koeficientem u $\sqrt{N}$, přesně $p = t(Q/s)P' + u(Q'/s)P + v(N + PP')/s$ modulo $L(I * J)$. Pak

$$\begin{aligned} p &= t(Q/s)P' + (s - tQ - v(P + P'))P/s + v(N + PP')/s \\ &\equiv P + v(N - P^2)/s \pmod{Q/s} \\ &\equiv P \pmod{Q/s} \end{aligned}$$

protože $Q \mid (N - P^2)$. Analogcky bychom ukázali, že $p \equiv P' \pmod{Q'/s}$.

Abychom dokázali 2.28, uvažujme:

$$\begin{aligned} (P + P')sp &= (P + P')(tQP' + uQ'P) + v(N + PP') \\ &= (P + P')(tQP' + uQ'P) + (P + P')(N + PP')v \\ &= (P + P')(tQP' + uQ'P) + (s - tQ - uQ')(N + PP') \\ &= s(N + PP') + tQ((P')^2 - D) + uQ'(P^2 - N) \\ &\equiv s(N + PP') \pmod{QQ'} \end{aligned}$$

Proto $(P + P')p \equiv N + PP' \pmod{QQ'/s}$

□

Všimněme si, že když $h = 1$ (2.25), můžeme přeformulovat

$$L(I * J) = L(I)L(J)/s^2 \tag{2.30}$$

Tato rovnost se nám ještě bude hodit. Její důkaz plyne z 2.24.

Dále si všimněme, že pro $h = 1$ rovnice popisující součin dvou ideálů odpovídají právě skládání dvou kvadratických forem. Shanks toto popsal v [Sha89]. Proto rovnice ve kterých jde o vzdálenosti a násobení ideálů odpovídají rovnicím, ve kterých figurují vzdálenosti a skládání kvadratických forem.

Případ, kdy $h = 2$ propojuje skládání kvadratických forem s diskriminantem $\equiv 1 \ (mod\ 4)$ s násobením ideálů. Pokud F a G jsou dvě kvadratické formy s diskriminantem $N \equiv 1 \ \ (mod\ 4)$, pak formy $2F$ a $2G$ mají diskriminant $4N$ a odpovídají ideálům I_{2F} a I_{2G} v $\mathbb{Z}[\sqrt{N}]$. Násobení $h = 2$ a $I_{2F} * I_{2G} = I_{2(F*G)}$

Proto, ačkoliv tento případ dále již nebude uvažován, je snadno vidět, že formule pro výpočet vzdálenosti odvozená z ideálů v $\mathbb{Z}[\sqrt{N}]$ bude stále odpovídat skládání kvadratických forem s diskriminantem $\equiv 1 \ (mod\ 4)$.

2.4 Mříže

Mříž je množina všech konečných lineárních kombinací (s celými koeficienty) své generující množiny. Generující množina obsahuje nějakou bázi racionálního vektorového prostoru ve kterém se mříž nachází.

V této kapitole budeme potřebovat vektorový prostor $\mathbb{Q}(\sqrt{N}) \times \mathbb{Q}(\sqrt{N})$. Pokud jsou vektory $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{Q}(\sqrt{N}) \times \mathbb{Q}(\sqrt{N})$, pak

$$[\alpha_1, \alpha_2, \ldots, \alpha_k] = \left\{ \sum_{i=1}^{k} n_i \alpha_i : n_i \in \mathbb{Z} \right\}$$

je mříž. Prvky mříže, tedy v našem případě vektory délky 2, budeme zapisovat $v = \langle v_1, v_2 \rangle$.

Pokud jsou souřadnice prvku mříže ζ a $\overline{\zeta}$, pak se značení mnohdy zjednodušuje a místo $\langle \zeta, \overline{\zeta} \rangle$ píšeme pouze ζ.

Definice 21. *[McM05] Pro vektor $v = \langle v_1, v_2 \rangle$ je normované tělo množina $\mathcal{R}(v)$:*

$$\mathcal{R}(v) = \{\langle x_1, x_2 \rangle : x_1, x_2 \in \mathbb{R}, |x_1| < |v_1|, |x_2| < |v_2|\}$$

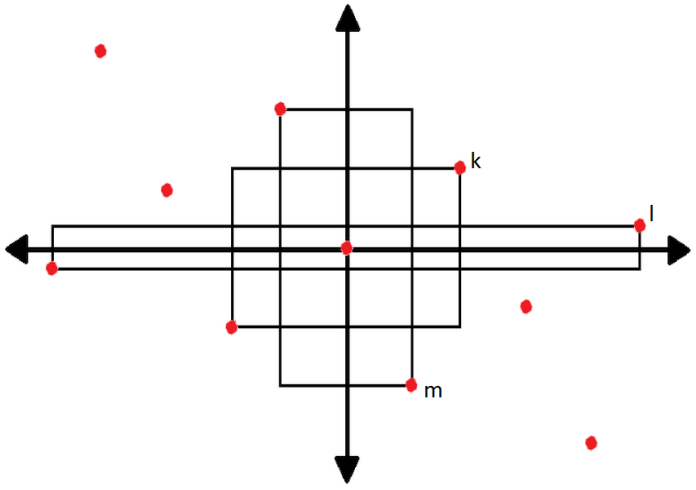
Zde se znovu používá zjednodušení $\mathcal{R}(\xi) = \mathcal{R}(\langle \xi, \overline{\xi} \rangle)$.

Definice 22. *Mějme $\mathcal{L}$ mříž. Číslo ξ (nebo vektor jemu odpovídající) je minimum $\mathcal{L}$, právě tehdy když $\mathcal{R}(\xi) \cap \mathcal{L} = 0$, kde 0 je vektor $\langle 0,0 \rangle$.*

Mříž $\mathcal{L}$ je redukovaná, pokud $1 \in \mathcal{L}$ a 1 je minimum.

Pro náš případ, kdy dimenze mříže je 2, platí, že normované tělo je obdélník v $\mathbb{R}^2$. Poznamenejme, že pro $\xi \in \mathbb{Q}(\sqrt{N})$ má normované tělo $\mathcal{R}(\xi)$ plochu rovnou $4 \cdot |\mathcal{N}(\xi)|$.

Následující obrázek má za úkol přiblížit čtenáři koncept minima mříže. Mříž je množina bodů. Každý z bodů k, l, m je minimem znázorněné mříže. To proto, že v normovaném těle těchto bodů není žádný jiný bod krom počátku $\langle 0,0 \rangle$.



Jelikož tato práce nemá ambice podat obecný náhled do problematiky mříží, budeme se dále zbývat pouze mřížemi, které odpovídají ideálům. Konkrétně definujme pro primitivní ideál $I = [Q,\sqrt{N}+P]$ asociovanou mříž obsahující 1 v $\mathbb{Q}(\sqrt{N})$, jako $\mathcal{L}_I = [1,(\sqrt{N}+P)/Q)]$.
Naopak, pro každou mříž obsahující 1 v $\mathbb{Q}(\sqrt{N})$ existuje asociovaná primitivní mříž (která může, ale nemusí být ideál) v $\mathbb{Z}[\sqrt{N}]$. Rovnost 2.20 definovala funkci L pro ideály. Podobným způsobem, definujeme funkci L i pro mříže $\mathcal{L}$

$$L(\mathcal{L}) = min\{n \in \mathbb{Z}^+ : n\mathcal{L} \subset \mathbb{Z}[\sqrt{N}]\} \tag{2.31}$$

Pak pokud $L(\mathcal{L})\mathcal{L}$ je ideál $\mathbb{Z}[\sqrt{N}]$, jedná se o primitivní ideál asociovaný s mříží $\mathcal{L}$. Poznamenejme, že pokud je ideál I asociovaný s mříží $\mathcal{L}_I$, pak $L(I) = L(\mathcal{L}_I)$. Definujme

$$\Phi_{\mathbb{I},\mathbb{L}}([Q,\sqrt{N}+P]) = [1,(\sqrt{N}+P)/Q]$$

a

$$\Phi_{\mathbb{L},\mathbb{I}}(\mathcal{L}) = L(\mathcal{L})\mathcal{L}$$

Poznamenejme, že pro některé mříže $\mathcal{L}$, $\Phi_{\mathbb{L},\mathbb{I}}(\mathcal{L})$ nemusí být ideál v $\mathbb{Z}[\sqrt{N}]$. Následující lemma nám dává podmínky pro to, abychom získali ideál vhodný pro naši analýzu:

Lemma 23. *Nechť I je primitivní ideál a nechť $\mathcal{L} = \Phi_{\mathbb{I},\mathbb{L}}(I)$. Pokud $\mathcal{L}'$je mříž s bazí $\{1,\xi\}$ a pro nějaké θ platí $\theta\mathcal{L}' = \mathcal{L}$, pak $J = \Phi_{\mathbb{L},\mathbb{I}}(\mathcal{L})$ je primitivní ideál a*

$$(L(I)\theta)J = (L(J))I$$

Důkaz. Nechť $I = [Q,\sqrt{N}+P]$. Pak $\mathcal{L} = [1,(\sqrt{N}+P)/Q]$. Tvrzení, že $\theta\mathcal{L}' = \mathcal{L}$, vyžaduje aby platilo

$$\theta \begin{bmatrix} 1 \\ \xi \end{bmatrix} = T \begin{bmatrix} 1 \\ (\sqrt{N}+P)/Q \end{bmatrix}$$

kde T je matice 2×2 s determinantem ± 1. Přenásobením výrazy $L(I) = L(\mathcal{L}) = Q$ a $L(J) = L(\mathcal{L}')$ získáváme:

$$Q\theta \begin{bmatrix} L(\mathcal{L}') \\ L(\mathcal{L}')\xi \end{bmatrix} = L(\mathcal{L}')T \begin{bmatrix} Q \\ (\sqrt{N}+P) \end{bmatrix}$$

a tedy $(L(I)\theta)J = (L(J))I$. Proto je J ideál a z definice $\Phi_{\mathbb{L},\mathbb{I}}$ je primitivní.

□

Příklad 11. Uvažujme mříž $[1,\sqrt{159}-12]$. $\mathcal{R}(1)$ je čtverec se stranami délky 2 zarovnaný do počátku a z jednoduchého grafu je patrné, že 0 je jediný bod v mříži a zároveň v onom čtverci. Proto je 1 minimum. $\sqrt{159}-12$ je také minimum. $\mathcal{R}(\sqrt{159}+12)$ je užší a vyšší obdélník, také zarovnaný do počátku.

Pokud máme 2 minima, je důležité umět rozhodnout, zda mezi nimi je ještě nějaké jiné minimum. Ve vektorovém zápise, nechť $\langle x_1,y_1\rangle$ a $\langle x_2,y_2\rangle$ jsou minima a platí $|x_1| > |x_2|$ a $|y_1| < |y_2|$, jsou tato dvě minima *sousední*, pokud neexistuje žádné jiné minimum $\langle x_3,y_3\rangle$ takové, že $|x_2| < |x_3| < |x_1|$ a $|y_1| < |y_3| < |y_2|$.
Voronoi objevil metodu (a formuloval větu) pracující se sousedními minimy ([DF64],[Wil85]).

Věta 24. *Nechť $\mathcal{L}$ je mříž s bazí $\{\xi,\zeta\}$, kde $\xi,\zeta \in \mathbb{Q}(\sqrt{N})$ a předpokládejme, že $\zeta > \xi > 0$. Pak ζ a ξ jsou sousední minima $\mathcal{L}$ právě tehdy když $|\overline{\xi}| > |\overline{\zeta}|$ a $\overline{\zeta\xi} < 0$*

Důkaz. Předpokládejme, že ξ a ζ jsou sousední minima. Jelikož jsou obě minima, platí $|\overline{\xi}| > |\overline{\zeta}|$, protože jinak ζ nebude minimum. Platí tedy $0 < \zeta - \xi < \zeta$. Protože je ζ minimum, musí také platit $|\overline{\zeta} - \overline{\xi}| > |\overline{\zeta}|$. Pokud $\overline{\zeta}$ a $\overline{\xi}$ mají stejné znaménko, není toto možné. Proto $\overline{\zeta\xi} < 0$.

Naopak předpokládejme, že $|\overline{\xi}| > |\overline{\zeta}|$ a $\overline{\zeta\xi} < 0$. Předpokládejme, že ξ není minimum $\mathcal{L}$. Pak existuje $\omega \in \mathbb{Q}(\sqrt{N})$ takové, že $|\omega| < \xi$ a $|\overline{\omega}| < |\overline{\xi}|$. Protože $\omega = a\xi + b\zeta$ pro nějaká $a,b \in \mathbb{Z}$, $|a\xi + b\zeta| < \xi$ a $|a\overline{\xi} + b\overline{\zeta}| < |\overline{\xi}|$. Pokud $ab = 0$, pak buď $a = 0$ nebo $b = 0$. Pokud $a = 0$, pak druhá rovnost je v rozporu s předpokladem. Pokud $b = 0$, pak z první rovnosti plyne $\xi < \xi$, což je patrně nepravda. Pokud $ab > 0$, pak $|a\xi + b\zeta| > \xi$ a pokud $ab < 0$, pak protože $\overline{\xi\zeta} < 0$, platí $|a\overline{\xi} + b\overline{\zeta}| > |\overline{\xi}|$. Proto ξ musí být minimum. Podobnou argumentací bychom dostali, že ζ musí být minimum.

Uvažujíce sousednost, předpokládejme že existuje jiné minimum ω mezi minimy ξ a ζ. Protože $\omega = a\xi + b\zeta$, pro nějaká $a,b \in \mathbb{Z}$, platí $\xi < |a\xi + b\zeta| < \zeta$ a $|\overline{\zeta}| < |a\overline{\xi} + b\overline{\zeta}| < |\overline{\xi}|$. Platí-li $\zeta > \xi > 0$, pak první rovnost vyžaduje $b = 0$ a pak se druhá rovnost zjednoduší na $|a| < 1$, což znamená $a = 0$, což je spor. Proto jsou ξ a ζ sousední minima.

□

Nyní je možné dokázat, že $\xi = 1$ a $\zeta = \sqrt{159 + 12}$ z minulého příkladu jsou opravdu sousední minima.

Vyhledávání posloupnosti sousedních minim nám nabídne propojení s řetězovými zlomky (a vzdálenostmi). Následující lemmata vychází z práci [Wil85] Williamse.

Lemma 25. *Nechť $\mathcal{L}$ a $\mathcal{L}'$ jsou redukované mříže. Pokud $\xi\mathcal{L}' = \mathcal{L}$, pak ξ je minimum v $\mathcal{L}$.*

Důkaz. Protože $1 \in \mathcal{L}'$, $\xi \in \mathcal{L}$. Pokud ξ není minimum v $\mathcal{L}$, pak existuje $\zeta \in \mathcal{L}$, takové, že $\zeta \neq 0$ a $|\zeta| < |\xi|$ a $|\overline{\zeta}| < |\overline{\xi}|$. Nechť $\beta = \zeta/\xi$ a tedy $\beta \in \mathcal{L}'$. $|\beta| = |\zeta/\xi| < 1$ a $|\overline{\beta}| = |\overline{\zeta}/\overline{\xi}| < 1$, což je spor s předpokladem, že $\mathcal{L}'$ je redukovaný. Proto ξ je minimum v $\mathcal{L}$.

□

Nyní uvažujme opak tohoto tvrzení. Zápisem $\lfloor x \rfloor$ značíme dolní celou část x.

Lemma 26. *Nechť $\mathcal{L} = [1,\xi]$, kde 1 a ξ jsou sousední minima v $\mathcal{L}$ a platí $1 > \xi > 0$. Nechť $\mathcal{L}' = (1/\xi)\mathcal{L}$. Pak $\mathcal{L}'$ je redukovaná mříž.*

Důkaz. $\mathcal{L}' = (1/\xi)[1,\xi] = [1/\xi,1] = [1/\xi - \lfloor 1/\xi \rfloor,1]$ a tedy $1 \in \mathcal{L}'$. To nám stačí k tomu, abychom mohli ukázat, že 1 a $\xi' = 1/\xi - \lfloor 1/\xi \rfloor$ jsou sousední minima. 1 a ξ' jsou báze $\mathcal{L}'$ a $1 > \xi' > 0$. Kvůli $0 < \xi < 1$ platí $\lfloor 1/\xi \rfloor > 1$. Protože $\overline{\xi} < 0$, platí

$\overline{\xi'} = 1/\overline{\xi} - \lfloor 1/\xi \rfloor < 0 - 1 = -1$. Tím máme splněny podmínky $\overline{\xi'} \cdot 1 < 0$ a $|\xi'| > 1$. Proto podle věty 24, 1 a ξ' jsou sousední minima $\mathcal{L}'$ a tedy $\mathcal{L}'$ je redukovaná mříž. □

Tyto důkazy nám ukazují, jak je možné nalézt minimum sousední k 1 v nové mříži. Další lemma nám ukazuje využití těchto minim [Wil85]:

Lemma 27. *Nechť $\mathcal{L}, \mathcal{L}', \xi$ a ξ' jsou stejná jako výše. Nechť ζ je minimum sousedící s ξ (různé od 1) v $\mathcal{L}$. Pak $\zeta = \xi\xi'$.*

Důkaz. $\xi\xi' = \xi(1/\xi - \lfloor 1/\xi \rfloor) = 1 - \xi\lfloor 1/\xi \rfloor$ a tedy $[\xi,\xi\xi']$ jsou báze $\mathcal{L}$. Protože $1 > \xi' > 0$, platí $\xi > \xi\xi' > 0$. Vzhledem k $|\overline{\xi'}| > 1$, platí $|\overline{\xi\xi'}| > |\overline{\xi}|$. Díky $\overline{\xi'} < 0$, platí $\overline{\xi \cdot \xi\xi'} = \overline{(\xi)^2\xi'} < 0$. Proto, podle věty 24, ξ a $\xi\xi'$ jsou sousední minima. A konečně protože $\xi\xi' \neq 1$, platí $\zeta = \xi\xi'$

□

Všimněme si, že podobným procesem lze nalézt redukovanou mříž $\mathcal{L}'' = 1/\xi'\mathcal{L}'$ a tak dále... Pak $\mathcal{L}'' = 1/(\xi\xi')\mathcal{L}'$. Abychom tento vztah zobecnili, definujme si $\xi = \xi_1$ a $\mathcal{L} = \mathcal{L}_1$. Další členy dopočítáme pomocí vztahů

$$\mathcal{L}_{i+1} = \frac{1}{\xi}\mathcal{L}_i \quad \xi_{i+1} = 1/\xi_i - \lfloor 1/\xi_i \rfloor,\ i \in \mathbb{N}$$

Tyto budou tvořit posloupnost redukovaných mříží a jejich minim. Řetězec sousedních minim $\mathcal{L}_1$ bude definován:

$$\theta_n = \prod_{i=1}^{n-1} \xi_i \tag{2.32}$$

a pak

$$\theta_n\mathcal{L}_n = \mathcal{L}_1 \tag{2.33}$$

Protože každé $\mathcal{L}_n$ je redukovaná mříž, podle lemma 25 je každé θ_n minimum $\mathcal{L}_1$.

Ačkoliv to neplatí ve více dimenzích, je patrné, že ve 2 dimenzionálním prostoru tento řetězec sousedních minim dává kompletní (nicméně nekonečný) seznam minim se souřadnicí x z intervalu (0,1).

Lemma 28. *Nechť $\langle \phi, \overline{\phi} \rangle$ je minimum mříže $\mathcal{L}$ a platí $0 < \phi < 1$. Pak pro nějaké n platí $\phi = \theta_n$, kde θ_n je definováno rovnicí 2.32.*

Definujme *vzdálenost* v kontextu řetězce minim jako

$$D_{\mathbb{L}}(\mathcal{L}_n,\mathcal{L}_m) = log(\theta_n/\theta_m) \tag{2.34}$$

Ukáže se, že index $\mathbb{L}$ je zbytečný, ale teď nám poskytuje jistotu, kde právě měříme.

Příklad 12. Uvažujme kroky řetězového rozvoje čísle $\sqrt{177}-13$ a vzdálenosti kvadratických forem $D_{\mathbb{F}}$ na konci každého kroku:

$$\begin{aligned}
x_1 &= \tfrac{1}{\sqrt{177}-13} = \tfrac{\sqrt{177}+13}{8} = 3+\tfrac{\sqrt{177}-11}{8}, \quad D_{\mathbb{F}}(F_0,F_1) = log(\tfrac{\sqrt{177}+13}{8}) \\
x_2 &= \tfrac{8}{\sqrt{177}-11} = \tfrac{\sqrt{177}+11}{7} = 3+\tfrac{\sqrt{177}-10}{7}, \quad D_{\mathbb{F}}(F_0,F_2) = log(\tfrac{3\sqrt{177}+40}{7}) \\
x_3 &= \tfrac{7}{\sqrt{177}-10} = \tfrac{\sqrt{177}+10}{11} = 2+\tfrac{\sqrt{177}-12}{11}, \quad D_{\mathbb{F}}(F_0,F_3) = log(\tfrac{10\sqrt{177}+133}{11}) \\
x_4 &= \tfrac{11}{\sqrt{177}-12} = \tfrac{\sqrt{177}+12}{3} = 2+\tfrac{\sqrt{177}-12}{3}, \quad D_{\mathbb{F}}(F_0,F_4) = log(\tfrac{23\sqrt{177}+306}{3}) \\
x_5 &= \tfrac{3}{\sqrt{177}-12} = \tfrac{\sqrt{177}+12}{11} = 3+\tfrac{\sqrt{177}-10}{11}, \quad D_{\mathbb{F}}(F_0,F_5) = log(\tfrac{194\sqrt{177}+2581}{11})
\end{aligned}$$

Rozvoj řetězovými zlomky odpovídá kvadratickým formám, které odpovídají ideálům, které jsou asociované s mřížemi, které obsahují 1. V tomto případě, mříž asociovaná s x_1 je $\mathcal{L}_1 = [1,1/x_1] = [1,\sqrt{177}-13]$ a $1/x_1$ je minimum sousední k 1 v $\mathcal{L}_1$. Odsuď:

$$\mathcal{L}_2 = \frac{1}{\sqrt{177}-13}\mathcal{L}_1 = \left[\frac{1}{\sqrt{177}-13},1\right] = \left[\frac{\sqrt{177}+13}{8},1\right] = \left[1,\frac{\sqrt{177}-11}{8}\right] = [1,1/x_2]$$

$$\mathcal{L}_3 = \frac{8}{\sqrt{177}-11}\mathcal{L}_2 = \left[\frac{8}{\sqrt{177}-11},1\right] = \left[\frac{\sqrt{177}+11}{7},1\right] = \left[1,\frac{\sqrt{177}-10}{7}\right] = [1,1/x_3]$$

...

a je patrné, že podle stejného vzorce bude posloupnost pokračovat. Definujme tedy zobrazení

$$\Phi_{\mathbb{T},\mathbb{L}}(x_n) = \Phi_{\mathbb{T},\mathbb{I}}(\Phi_{\mathbb{I},\mathbb{L}}(x_n)) = [1,1/x_n] = \mathcal{L}_n \tag{2.35}$$

z kterého je patrné, že posloupnost mříží je periodická.
Dosazením do rovnice 2.32, na příklad do $\theta_3 = (\sqrt{177}-13)(\frac{\sqrt{177}-11}{8}) = 40-3\sqrt{177}$. Pro $\theta_1 = 1$,

$$D(\mathcal{L}_1,\mathcal{L}_3) = log(1/(40-3\sqrt{177})) = log((3\sqrt{177}+40)/7)$$

Je zřejmé, že definice vzdálenosti v mřížích odpovídá definici vzdáleností kvadratických forem. Všimněme si, že tyto vzdálenosti musí být stále uvažovány modulo R (regulátor), protože posloupnost mříží je také cyklická.

2.5 Zobecněná definice vzdálenosti

Vraťme se zpátky k ideálům. Pokud $I_1 = L(\mathcal{L}_1)\mathcal{L}_1$ a $I_n = L(\mathcal{L}_n)\mathcal{L}_n$ je jiný ideál odpovídající mříži která je v posloupnosti dále, pak

$$\theta_n \mathcal{L}_n = \mathcal{L}_1$$

$$L(\mathcal{L}_1)L(\mathcal{L}_n)\theta_n\mathcal{L}_n = L\mathcal{L}_1)L(\mathcal{L}_n)\mathcal{L}_1$$

$$(L(\mathcal{L}_1)\theta_n)I_n = (L(\mathcal{L}_n)I_1 \tag{2.36}$$

kde θ_n je minimum definované v [2.32] a $\mathcal{L}_n$ je n-tá mříž v řetězci redukovaných mříží začínajícím $\mathcal{L}_1$. Dále znovu platí, že vzdálenost (na tomto místě mezi ideály) je dána $D(I_1,I_n) = -log(\theta_n)$. Definice vzdálenosti v tomto tvaru funguje pro redukované ideály, ale zatím ještě nebyla použita na ideály neredukované. Abychom našli vztah mezi definicemi redukovaných mříží a řetězových zlomků, všimněme si, že definice redukovaného řetězového zlomku nám dává pro výraz $x_i = \frac{\sqrt{N}+P_{i-1}}{Q_i}$ nerovnosti

$$\frac{\sqrt{N}+P_{i-1}}{Q_i} > 1$$

$$0 < \frac{\sqrt{N}-P_{i-1}}{Q_i} < 1$$

a tedy je jasné, že pokud $\mathcal{L}_x = [1,1/x]$, pak 1 a x jsou sousední minima a mříž je redukovaná. Proces vypořádání se s neredukovanými mřížemi má mnoho společného s procesem redukce řetězových zlomků, jak bylo ukázáno v důkazu lemmatu 10. Obecnější pohled na věc lze získat v [Wil85].

Lemma 29. *Nechť I je primitivní ideál v $\mathbb{Z}[\sqrt{N}]$. Existuje redukovaný ideál I_n a $\theta_n \in I$ takové, že*

$$(L(I)\theta)I_n = (L(I_n))I \tag{2.37}$$

Důkaz. Nechť $I = [Q,\sqrt{N}+P]$. Pak asociovaná mříž $\mathcal{L}_I = [1,\frac{\sqrt{N}+P}{Q}] = [1,\xi_1]$. Pokud I je redukovaný, $I_n = I$, $u = L(I)$ a důkaz je hotov. Pokud I není redukovaný, pak $\mathcal{L}_I$ také není redukovaný. Bez újmy na obecnosti předpokládejme, že $0 < \xi_1 < 1$. Nechť $\mathcal{L}_2 = 1/\xi_1\mathcal{L}_1 = [1/\xi,1] = [1,1/\xi - \lfloor 1/\xi - 1/2 \rfloor]$. Pak $\xi_1\mathcal{L}_2 = \mathcal{L}_I$. Pokračujeme obdobným způsobem a užitím lemma 10 a korespondence mezi mřížemi a řetězovými zlomky pro nějaké n, dostáváme, že ξ_n je redukované, a proto $\mathcal{L}_n$ je redukované. Jako v 2.32, vezměme

$$\theta_n = \prod_{i=+}^{n-1} \xi_i$$

a tedy

$$\theta_n \mathcal{L}_n = \mathcal{L}_I$$

Pak $(L(I)\theta_n)I_n = L(I_n))I$

□

Nechť I_1, J_1 jsou redukované primitivní ideály. Nechť K_1 je primitivní ideál získaný násobením ideálů I_1 a J_1 takový, že $(s)K_1 = I_1J_1$, $s \in \mathbb{Z}$, kde s je společný

faktor I_1 a J_1. Z lemma 29 víme, že pak existuje redukovaný ideál K_j a $\lambda_j \in K_1$, takové, že

$$(L(K_1)\lambda_j)K_j = (L(K_j))K_1 \tag{2.38}$$

odpovídající $D(K_1,K_j) = -log(\lambda_j)$.

Nechť $I_n \sim I_1$ a $J_m \sim J_1$ a nechť H_1 je primitivní ideál získaný násobením I_n a J_m a odstraněním faktoru. Nechť t je odstraněný faktor, takže $(t)H_1 = I_nJ_m$, $t \in \mathbb{Z}$. Z lemma 29 víme, že pak existuje redukovaný ideál H_k a $\eta_k \in K_1$, takové, že

$$(L(H_1)\eta_k)H_k = (L(H_k))H_1 \tag{2.39}$$

odpovídající $D(H_1,H_k) = -log(\eta_k)$.

Existují tedy minima μ_n a ϕ_m v mřížích odpovídajících ideálům I_1 a J_1, takové že

$$(L(I_1)\mu_n)I_n = (L(I_n))I_1 \tag{2.40}$$

a

$$(L(J_1)\phi_m)J_m = (L(J_m))J_1 \tag{2.41}$$

odpovídající $D(I_1,I_n) = -log(\eta_n)$ a $D(J_1,J_m) = -log(\phi_m)$.

Kombinací 2.30 a (2.38-2.41) dostáváme:

$$(L(H_k))K_j = \left(\frac{L(H_k)L(K_j)}{L(K_1)\lambda_j}\right)K_1 = \left(\frac{L(H_k)L(K_j)}{L(K_1)\lambda_j s}\right)I_1J_1 =$$

$$\left(\frac{L(H_k)L(K_j)L(I_1)L(J_1)\mu_n\phi_m}{L(K_1)\lambda_j sL(I_n)L(J_m)}\right)I_nJ_m =$$

$$\left(\frac{L(H_k)L(K_j)s\mu_n\phi_m}{\lambda_j L(I_n)L(J_m)}\right)I_nJ_m =$$

$$\left(\frac{L(H_k)L(K_j)s\mu_n\phi_m t}{\lambda_j L(I_n)L(J_m)}\right)H_1 =$$

$$\left(\frac{L(H_k)L(K_j)s\mu_n\phi_m t}{\lambda_j L(H_1)}\right)H_1 =$$

$$\left(\frac{L(K_j)s\mu_n\phi_m\eta_k}{\lambda_j t}\right)H_k$$

Definujme

$$\psi = \frac{s\mu_n\phi_m\eta_k}{t\lambda_j}.$$

Pak

$$(L(K_j)\psi)H_k = (L(H_k))K_j \tag{2.42}$$

Protože K_j a H_k jsou redukované, podle lemma 25 je ψ minimum mříže $\mathcal{L}_{K_j}$ a tedy pro nějaké n platí $\psi = \theta_n$. Proto

$$D(K_j,H_k) = -log(\psi) = -log(\eta_n) - log(\phi_m) - log(\eta_k) + log(\lambda_j) - log(s/t) =$$

$$= D(I_1,I_n) + D(J_1,J_m) + \zeta$$

kde $\zeta = D(H_1,H_j) - D(K_1,K_j) + log(t/s)$ bude malé v porovnání s $D(K_j,H_k)$ pro velká m, n.

Když k této skutečnosti uvážíme korespondenci mezi násobením ideálů a skládáním forem, můžeme toto tvrzení přeformulovat v jazyce forem.

Věta 30. *Pokud $F_1 \sim F_n$ jsou ekvivalentní formy, $G_1 \sim G_m$ jsou ekvivalentní formy a $D_{\rho,1}$ je redukční vzdálenost pro $F_1 * G_1$ a $D_{\rho,2}$ je redukční vzdálenost pro $F_n * G_m$ a s a t jsou faktory, které se při skládání vyrušily. Pak*

$$D(F_1 * G_1,F_n * G_m) = D(F_1,F_n) + D(G_1,G_n) + \zeta$$

kde $\zeta = D_{\rho,2} - D_{\rho,1} + log(t/s)$.

Důkaz. Užitím korespondence mezi násobením ideálů a skládáním forem plyne přímo z výše odvozeného faktu pro ideály.

□

Protože druhá mocnina libovolného středu symetrie má první koeficient 1, všimněme si, že pokud by vzdálenost okolo nějakého cyklu neměla žádný vztah se vzdáleností kolem hlavního cyklu, pak by tento výsledek byl ovlivněn tím, ke kterému ze středů symetrie se tato vzdálenost váže. Z definice 19 víme, že $R = D(F_0,F_\pi)$ v hlavním cyklu. V tuto chvíli je jasné, že vzdálenost v ostatních cyklech musí být stejná.

Lemma 31. *Nechť A je primitivní nejednoznačný cyklus s periodou π. Pak*

$$R = D(F_0,F_\pi)$$

Důkaz. Nechť $\{F_i\}$ má periodu π a nechť F_0 a $F_{\pi/2}$ jsou dva středy symetrie cyklu A. Pak $F_0 * F_0 = 1 = F_{\pi/2} * F_{\pi/2}$, $D_{\rho,1} = D_{\rho,2} = 0$ a s a t jsou první koeficienty. Proto

$$0 = D(F_0 * F_0,F_{\pi/2} * F_{\pi/2}) = 2D(F_0,F_{\pi/2}) + log(t/s) = D(F_0,F_\pi)$$

kde 3. krok je získán z druhého pomocí faktu, že součin v $D(F_0,F_{\pi/2})$ obsahuje poslední jmenovatel t a neobsahuje první jmenovatel s.

Proto $D(F_0,F_\pi) = nR$. Uvažujme skládání F_0 s formami v hlavním cyklu. Máme $D(F_0,F_\pi) \leq R$ a tedy $D(F_0,F_\pi) = R$

□

3. Algoritmus SQUFOF

Nyní konečně nastala chvíle, kdy můžeme přistoupit k popisu samotného algoritmu. V této kapitole nabídneme nejenom prostý popis jedné implementace, ale také náhled na trošku odlišný přístup, který je použit v jiné mutaci algoritmu SQUFOF.

Není jisté, zda Shanks měl rigorózně dokázána všechna důležitá fakta ohledně vzdáleností, ale je jisté, že porozuměl vnitřní struktuře a vzdálenostem natolik, že dokázal vyvinout algoritmus SQUFOF.

3.1 SquFoF

Hledání vhodné čtvercové formy

Pomocí rekurentních vztahů 2.8, 2.9 a 2.7 počítáme koeficienty rozvoje řetězovými zlomky čísla $\sqrt{N}$. Tím procházíme hlavním cyklem. Uvažujeme při tom formy s diskriminantem $\Delta = 4N$ ve tvaru

$$F_i = \left(Q_i, 2P_i, -Q_{i+1}\right)$$

Pro rychlost algoritmu je důležité, že si stačí pamatovat koeficienty aktuální a poslední navštívené formy. Hlavní cyklus prohledáváme do té doby, dokud nenalezneme takovou formu Fi_i, jejíž Q_i je druhá mocnina celého čísla.

Příklad. Nechť $N = 3193$. Počítáme rozvoj $\sqrt{N}$ řetězovými zlomky. To děláme do té doby, dokud nenalezneme $Q_{10} = 49$. Kvadratická forma pro tento člen je rovna $F = 49x^2 + 58xy - 48y^2$.

Výpočet inverzu odmocniny čtvercové formy

Využijeme vztahu pro výpočet odmocniny čtvercové formy (lze snadno ověřit z definice skládání 16).

$$(a^2, b, -c) \sim (a, b, -ac)^2$$

$$(49, 58, -48) \sim (7, 2\dot{2}4, -336)^2$$

Tato forma ale není redukovaná. Proto ji dále redukujeme s $D_\rho = 0$ na $G = 7x^2 + 100xy - 99y^2$, což je kvadratická forma, která je druhou odmocninou F.

Hledání středu symetrie a vrácení výsledku

Podle věty 20, je G ve třídě řádu 2 nebo 1, což znamená, že G je nejednoznačná forma a tedy má 2 středy symetrie ve svém cyklu.

Díky větě 30, platí $2D(G_s, G) = D(1, F) (mod\ R)$.
Tedy $D(G_s, G) = D(1, F)/2\ (mod\ R/2)$.
Protože jsou středy symetrie od sebe vzdáleny $R/2$, víme že najdeme střed symetrie ve vzdálenosti $D(1, F)/2$ od G.

Nyní, pokud by byl koeficient u středu symetrie ± 1, byla by naše 7 byla v rozvoji řetězovými zlomky někde před F. Pokud by koeficient byl 2, pak může být střed symetrie složen s G, abychom rychleji nalezli 14 v nějaké dřívější části hlavního cyklu. Jakmile ho najdeme, dává nám střed symetrie netriviální faktor N.

V našem případě po 6 krocích získáváme 31, jakožto faktor 3193.

Optimalizace výběru formy

Druhá fáze tohoto algoritmu může být výrazně urychlena (aspoň pro větší čísla), pokud si ukládáme kvadratické formy s indexy ve tvaru mocniny 2. V tomto příkladu, $F = F_{10}$, a tedy G je zhruba na 5. pozici ve svém cyklu. Složením G^{-1} s F_4 a F_1 se dostaneme blízko a paralelní prohledávání v obou směrech rychle nalezne střed symetrie. V tomto případě je nezbytné uložit $log_2 k$ forem pro k kroků a tedy je efektivnější kontrolovat každý čtverec, abychom viděli, jestli funguje, než kontrolovat každou odmocninu proti minulému pseudo-čtverci, abychom předpověděli, zda bude fungovat.

3.2 Popis algoritmu 1

Algorithm 1 SQUFOF 1

$Q_0 \leftarrow 1$, $P_0 \leftarrow \lfloor \sqrt{N} \rfloor$, $Q_1 \leftarrow N - P_0^2$, $r \leftarrow \lfloor \sqrt{N} \rfloor$
while $Q_i \neq$ čtverec pro nějaké i **do**
  $b_i \leftarrow \lfloor \frac{r+P_{i-1}}{Q_i} \rfloor$
  $P_i \leftarrow b_i Q_i - P_{i-1}$
  $Q_{i+1} \leftarrow Q_{i-1} + b_i(P_{i-1} - P_i)$
  if $i = 2^n$ pro nějaké n **then**
    Ulož $(Q_i, 2 \cdot P_i) F_0 = (\sqrt{Q_i}, 2 \cdot P_{i-1}, \frac{P_{i-1}^2 - N}{Q_i})$
Slož F_0 s uloženými formami podle binární reprezentace $i/2$ a výsledek ulož do F_0
$F_0 = (A,B,C)$
$Q_0 \leftarrow |A|$, $P_0 \leftarrow B/2$, $Q_1 \leftarrow |C|$
$q_0 \leftarrow Q_1$, $p_0 \leftarrow P_0$, $q_1 \leftarrow Q_0$
while $P_i \neq P_{i-1}$ a $p_i \neq p_{i-1}$ **do**
  Použij stejnou rekurzivní formuli pro (Q_0,P_0,Q_1) a (q_0,p_0,q_1)
if $P_i = P_{i-1}$ **then**
  buď Q_i nebo $Q_i/2$ je netriviální faktor N
if $p_i = p_{i-1}$ **then**
  buď q_i nebo $q_i/2$ je netriviální faktor N

3.3 Alternativní verze algoritmu

Existují i jiné varianty algoritmu SQUFOF. Některé se liší pouze drobnými rozdíly v implementaci, jiné používají mírně odlišnou argumentaci proč fungují a využívají nějaký jiný ze vztahů pro kvadratické formy. Některé z těchto vztahů zde dokázány nebudou.

Nyní popíši variantu popsanou v práci Jasona E. Gowera a Samuela S. Wagstaffa Jr. [GSSW07]

Inicializace je prakticky stejná jako ve variantě, kterou jsme popsali výše.

Inicializace

Tato varianta algoritmu vyžaduje, aby zvolená kvadratická forma měla fundamentální diskriminant. V případě, že ho nemá, lze stejně jako v minulém případě použít malý trik a sice, pokud bude platit, že $N \equiv 1 \bmod 4$, pak nahradíme N za $2N$. Nyní můžeme předpokládat, že $N \equiv 2$ nebo $3 \bmod 4$. Takto získáme diskriminant $\Delta = 4N$, který bude fundamentálním vždy.

Zvolíme si tedy hlavní formu $F_0 = (1,2q_0,q_0^2 - N)$, kde q_0 je $\lfloor\sqrt{N}\rfloor$.

Poznámka. Není na škodu zmínit, že $\Delta = b^2 - 4ac = (2q_0)^2 - 4.1.(q_0^2 - N) = 4q_0^2 - 4q_0^2 + 4N = 4N$

Hledání vhodné čtvercové formy

Formy hlavního cyklu spočítáme následovně

$$F_n = \rho^n(F_0) = \big((-1)^{n-1},2P_n,(-1)^n Q_n\big),$$

kde P_n a Q_n jsou dopočítány za pomocí rovnic 2.4 a 2.4. Nyní algoritmus prochází tento hlavní cyklus a hledá čtvercovou formu ve tvaru $(*,*,c^2)$. Poznamenejme, že to se nám povede pouze pro nějaké n sudé. Je důležité míti na vědomí, že všechny formy z daného cyklu mají stejný diskriminant, tedy $4N$. Předpokládejme, že jsme našli formu $F_n = (-Q,2P,S^2)$, kde $Q > 0$.

Výpočet inverzu odmocniny čtvercové formy

V první řadě vezmeme formu opačnou, resp. formu s F_n asociovanou, která je s formou opačnou ekvivalentní. Tím získáme formu $F_n^{-1} = (S^2,2P,-Q)$, kterou dosadíme do vztahu pro výpočet odmocniny binární kvadratické formy

$$(a^2,b,-c) \sim (a,b,-ac)^2$$

$$(S^2,2P,Q) \sim (-S,2P,SQ)^2$$

Nyní si zadefinujeme získanou formu $F_n^{-1/2} = (-S,2P,SQ)$, jako inverz odmocniny F_n, vzhledem ke skládání forem. Tato forma nebude redukovaná. Vezměme si tedy formu $G_0 = (-S_{-1},2R_0,S_0)$, která je redukcí formy $F_n^{-1/2}$, kde

$$R_0 = P + S\left\lfloor\frac{q_0 - P}{S}\right\rfloor, \qquad S_{-1} = S, \qquad S_0 = \frac{N - R_0^2}{S}.$$

Hledání faktoru N

Užitím $R_m = t_{m-1}S_{m-1} - R_{m-1}$, $S_m = S_{m+2} + t_{m-1}(R_{m-1} - R_m)$ a $t_m = \left\lfloor \frac{q_0+R_m}{S_m} \right\rfloor$, pro všechna $m \geq 1$, což je mimochodem analogické k počítání koeficientů P_n, Q_n a q_n pro řetězové zlomky, dostáváme novou řadu forem:

$$G_m = \left((-1)^{m-1}S_{m-1}, 2R_m, (-1)^m S_m\right)$$

Nyní předpokládejme, že nalezneme m takové, že $R_m = R_{m+1}$. Očekáváme, že to nastane přibližně $m \approx n/2$.

Máme tedy:

$$R_m = t_{m-1}S_{m-1} - R_{m-1} \overset{R_m=R_{m-1}}{\Rightarrow} R_m = t_m S_m - R_m \Rightarrow R_m = \frac{t_m S_m}{2}$$

Do rovnice determinantu $\Delta = b^2 - 4ac$ dosadíme $a = (-1)^m S_{m-1}$,$b = 2R_m$,$c = (-1)^{m-1}S_m$, čímž získáme

$$\Delta = 4R_m^2 + 4S_{m-1}S_m \overset{\Delta=4N}{\Rightarrow} N = R_m^2 + S_{m-1}S_m$$

A kombinací výše zmíněných dostáváme klíčový vztah:

$$N = R_m^2 + S_{m-1}S_m \overset{R_m=\frac{t_m S_{m-1}}{2}}{\Rightarrow} N = \left(\frac{t_m S_m}{2}\right)^2 + S_{m-1}S_m \Rightarrow$$

$$N = S_m(S_{m-1} + S_m\frac{t_m^2}{4})$$

Tento vztah nám dává možnou faktorizaci N.

Poznámka. Čtvercovou formu F_n nazveme nevlastní, pokud je tato faktorizace triviální. Pokud je nalezen netriviální faktor N, pak F_n je vlastní čtvercová forma.

Poznámka. Poznamenejme, že všechny výpočty, krom těch, kde se vyskytují F_0 a G_0 probíhají s čísly, která jsou menší než $2\sqrt{N}$.

3.4 Popis algoritmu 2

Algorithm 2 SQUFOF 2

$Q_0 \leftarrow 1$, $P_0 \leftarrow \lfloor\sqrt{kN}\rfloor$, $Q_1 \leftarrow kN - P_0^2$, $r \leftarrow \lfloor\sqrt{kN}\rfloor$
while $Q_i \neq$ čtverec pro nějaké i **do**
  $b_i \leftarrow \lfloor\frac{r+P_{i-1}}{Q_i}\rfloor$
  $P_i \leftarrow b_iQ_i - P_{i-1}$
  $Q_{i+1} \leftarrow Q_{i-1} + b_i(P_{i-1} - P_i)$
$b_0 \leftarrow \lfloor\frac{r-P_{i-1}}{\sqrt{Q_i}}\rfloor$, $P_0 \leftarrow b_0\sqrt{Q_i} + P_{i-1}$, $Q_0 \leftarrow \sqrt{Q_i}$, $Q_1 \leftarrow \frac{kN-P_0^2}{Q_0}$, $r \leftarrow \lfloor\sqrt{kN}\rfloor$
while $P_i \neq P_{i-1}$ **do**
  $b_i \leftarrow \lfloor\frac{r+P_{i-1}}{Q_i}\rfloor$
  $P_i \leftarrow b_iQ_i - P_{i-1}$
  $Q_{i+1} \leftarrow Q_{i-1} + b_i(P_{i-1} - P_i)$
if $NSD(N,P_i) \neq 1 \& NSD(N,P_i) \neq N$ **then**
  P_i je netriviální faktor N
else
  Vem jinou hodnotu k a pusť algoritmus znovu

Problémy

- Všechny formy je nutné testovat na čtvercovost. To ovšem díky existenci rychlých algoritmů není zásadní problém.
- Může se nám stát, že nalezneme pouze triviální faktorizaci. V tomto případě se můžeme vrátit k F_n a od ní pokračovat v hledání jiné čtvercové formy. Tento postup je však velice časově náročný. Namísto toho se ukazuje jako lepší sledovat určité formy a poté je testovat, zda jsou vlastní.
- Může nastat stav, kdy v celém hlavním cyklu není žádná vlastní čtvercová forma. V tom případě pustíme SQUFOF na vstup mN pro nějaké malé m.

4. Složitost

4.1 Složitost algoritmu

Byť se na to tato práce nezaměřuje, sluší se závěrem zmínit, jak je na tom algoritmus SQUFOF s asymptotickou časovou složitostí.

V [Sha75b] Shanks uvádí, že pro N složené z $k+1$ prvočinitelů je průměrná vzdálenost mezi dvěma čtvercovými kvadratickými formami, po jejichž nalezení již snadno získáme faktory N, rovna

$$\Delta n = ln(8)\frac{2+\sqrt{2}}{4}\frac{\sqrt[4]{N}}{2^k-1}.$$

Protože hledání čtvercové formy je nejpomalejší část algoritmu, znamenalo by toto tvrzení, že SQUFOF je algoritmus s asymptotickou složitostí $\mathcal{O}(\sqrt[4]{N})$.

Bohužel, Shanks nikdy důkaz tohoto tvrzení nezveřejnil. I vzhledem k tomuto faktu nebyl precizní důkaz asymptotické složitosti algoritmu SQUFOF zatím nalezen. Nicméně, složitost SQUFOF může být poměrně dobře odhadnuta [Bue89]. Pro redukované formy s prvním koeficientem a, $0 < a < 2\sqrt{N}$, je $\mathcal{O}(\sqrt{N})$ celých čísel, která mohou být prvním koeficientem kvadratické formy. K tomu, aby čtvercová forma byla redukovaná, musí být její první koeficient menší, než $\sqrt{2}N^{1/4}$. Takových celých čísel je tedy $\mathcal{O}(N^{1/4})$. V nejhorším případě má N pouze jeden nejednoznačný cyklus různý od cyklu hlavního. To znamená, že pouze zhruba jedna polovina těchto čtvercových forem je v nejednoznačném cyklu, který není hlavní, což nám ale do výpočtu složitosti přidá pouze konstantu. Vydělením již získaných dvou odhadů získáme aproximaci pro počet forem mezi každými dvěma čtvercovými formami, tedy $\mathcal{O}(\sqrt{N}/N^{1/4})$. V porovnání s hledáním čtvercové formy jsou další části algoritmu zanedbatelně časově náročné, proto získáváme očekávanou asymptotickou složitost $\mathcal{O}(\sqrt[4]{N})$.

4.2 Měření a porovnání rychlosti

Poslední část této práce bude patřit praktickému porovnání rychlosti algoritmu SQUFOF s jinými algoritmy.

Porovnávat budeme algoritmy:

- Jednoduchá implementace v Javě (bez optimalizací) napsaná autorem
- Implementace SQUFOF z PSIQS Java package [Neu08]
- Implementace QS od Stefan Buttcher zveřejněná společně s [Bü01]

Měření probíhalo tak, že pro každou velikost čísla N byl vygenerován jeden balík 1000 náhodných složených čísel a ten byl poslán každému algoritmu. Měření proběhlo vždy 5x a za výsledek byl považován nejnižší dosažený čas (touto metodou se snažím zajistit co nejspravedlivější porovnání, které bude co nejméně narušeno jinými procesy).

V přiloženém grafu je na ose x zanesen dvojkový logaritmus velikost faktorizovaného čísla a na ose y je čas pro faktorizaci balíku 1000 hodnot v milisekundách.

4.3 Výsledky měření

Naměřené hodnoty

$log_2(N)$	SQUFOF (ms)	SQUFOF_psiqs (ms)	QS (ms)
30	236	5	538441
32	497	6	514662
34	1227	7	498036
36	2835	9	478811
38	6177	11	420607
40	14126	16	403069
42	29757	21	381090
44	68787	26	357885
46	156032	8145	343617
48	378362	111519	315057
50	740819	313274	307598

Vyhodnocení měření

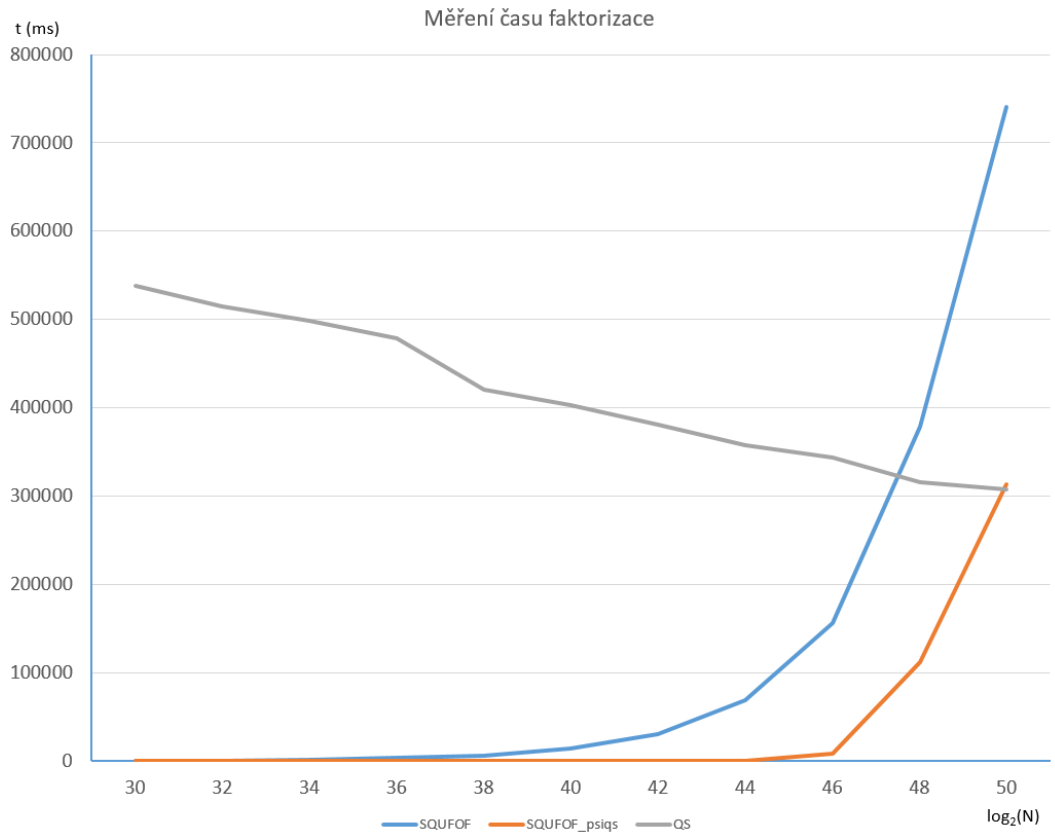
Naměřené hodnoty jsou vázány na konkrétní implementaci, verzi kompilátoru i hardware. Přes tuto zjevnou neobecnost však můžeme z měření vyčíst několik zajímavých faktů:

- optimalizacemi algoritmu se dá docílit velice výrazného zrychlení. Rozdíl mezi SQUFOF a SQUFOF_psiqs se ukazuje jako výrazný.
- pro čísla z rozsahu cca 30-45 bitů je algoritmus SQUFOF velice rychlý a z námi naměřených hodnot je patrné, proč je u takto velkých čísel mezi faktorizačními algoritmy jedničkou.

- kvadratické síto (QS) se díky své režii neukázalo pro čísla z tohoto rozsahu příliš vhodné a podle naznačeného trendu lze očekávat, že se k hodnotám na kterých pracuje optimálně teprve dostávalo. Nicméně je z grafu patrné, že pro hodnoty N delší než 50 bitů se situace změní a QS získá nad soupeři převahu.

Poznámka. Do testu měl být původně zahrnut i algoritmus CFRAC. Bohužel se však ukázalo, že pro vstupy, které byly v rámci testu použity, by byl čas běhu algoritmu neúnosně dlouhý a získání všech dat by při dodržení nastavené metodiky měření bylo problematické.

Poznámka. Testovací interval byl ukončen hodnotou 50, protože za ní velice prudce začal stoupat počet selhání obou implementací SQUFOF. Tato selhání významně ovlivnila čas běhu algoritmu a proto naměřené hodnoty pro $log_2(N) > 50$ již nepokládám za relevantní.



Závěr

V této práci jsme popsali matematické pozadí hojně využívaného faktorizačního algoritmu SQUFOF. Je zde shrnuta teorie z oblasti řetězových zlomků, binárních kvadratických forem , ideálů a mříží v rozsahu potřebném k popisu a pochopení tohoto algoritmu.

Nad rámec zadání tato práce přidává praktický pohled na efektivitu jednoduché implementace SQUFOF v porovnání s jinými dostupnými faktorizačními algoritmy.

Literatura

[Bü01] Stefan Bütcher. Factorization of large integers. 2001.

[Bue89] D. A. Buell. *Binary Quadratic Forms: Classical Theory and Modern Computations*. Springer-Verlag, 1989.

[DF64] B. N. Delone and D. K. Faddeev. *The Theory of Irrationalites of the Third Degree*. American Mathematical Societ, 1964.

[Gau66] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Yale University Press, 1966.

[GSSW07] Jason E. Gower and Jr. Samuel S. Wagstaff. *MATHEMATICS OF COMPUTATION*. 2007.

[Len01] H. W. Jr. Lenstra. A new method for factoring integers. 2001.

[MB75] Michael A. Morrison and John Brillhart. *A Method of Factoring and the Factorization of F_7*. Springer-Verlag, 1975.

[McM04] Stephen McMath. Daniel shanks' square forms factorization. 2004.

[McM05] Stephen McMath. Parallel integer factorization using quadratic forms. 2005.

[MvdP95] R. A. Mollin and A. J. van der Poorten. A note on symmetry and ambiguity. 1995.

[Neu08] Tilman Neumann. Psiqs: Parallel siqs implementation. http://www.tilman-neumann.de/index.html, 2007-2008.

[Rie85] Hans Riesel. *Prime Numbers and Computer Methods for Factorization*. Boston: Birkhuser, 1985.

[Sha75a] Daniel Shanks. Analysis and improvement of the continued fraction method of factorization. cca 1975.

[Sha75b] Daniel Shanks. Squfof notes. cca 1975.

[Sha89] Daniel Shanks. *On Gauss and Composition II*. Kluwer Academic Publishers, 1989.

[Wil85] Hugh C. Williams. Continued fractions and number-theoretic computations. 1985.