Radboud Universiteit Nijmegen

Faculteit der Natuurwetenschappen, Wiskunde en Informatica.

Kwadraatrepresentatie

Het representeren van natuurlijke getallen als som van kwadraten.

Bachelorscriptie

Auteur:
Stijn van de Lockand

Studentnummer:
s4495659

Begeleider:
Wieb Bosma

Tweede Lezer
Bernd Souvignier

10 juli 2017

Voorwoord

In deze scriptie zullen we gaan bekijken welke getallen we als som van n kwadraten kunnen representeren en hoe we deze representaties op efficiënte manier kunnen vinden. Aangezien de algoritmes die deze representaties geven gebruik maken van verschillende gebieden in de getaltheorie zal er een breed spectrum van informatie besproken worden. Ook komt complexiteit aan bod, omdat we willen weten hoe efficiënt de besproken algoritmes zijn.

Deze scriptie is geschreven voor mensen die als voorkennis het verplichte deel van de bachelor wiskunde aan de Radboud Universiteit Nijmegen met beginjaar 2014 hebben.

Inhoudsopgave

1 Inleiding

Er zijn veel bekende wiskundigen die zich bezig gehouden hebben met het representeren van getallen als som van kwadraten. Zo liet Fermat zien welke priemgetallen als som van twee kwadraten geschreven kunnen worden en gaven Legendre, Hermit, Serret, Gauss en Jacobsthal algoritmes om priemgetallen als som van twee kwadraten te schrijven.

Het overlappende thema geeft het probleem, de enige algoritmes die goed onderzocht zijn, zijn de algoritmes voor het representeren van priemgetallen als som van twee kwadraten, maar hoe zit het met natuurlijke getallen, of getallen die niet als som van twee kwadraten, maar wellicht met meer kwadraten geschreven kunnen worden. Er is hier nog niet veel naar gekeken, omdat er nog geen goede reden is om getallen te representeren als som van kwadraten.

In deze scriptie zullen we bekijken welke getallen representeerbaar zijn als som van 2, 3 en 4 kwadraten en waar het mogelijk is verschillende algoritmes bekijken om de representaties te vinden. We hoeven niet naar sommen van meer dan 4 kwadraten te kijken, omdat zal blijken dat we met sommen van 4 kwadraten alle natuurlijke getallen kunnen representeren. We zullen geen brute force algoritmes bespreken, aangezien deze niet efficiënt en niet interessant zijn.

Veel bevindingen op het gebied van representaties als 3 of 4 kwadraten zijn opgesomd in het werk van Rabin en Shallit [5] en hier zal dus vaak naar verwezen worden.

2 Som van twee kwadraten

2.1 Representeerbare getallen

Voordat we naar algoritmes gaan kijken die getallen als som van twee kwadraten kunnen representeren, is het belangrijk om te weten welke getallen te representeren zijn als som van twee kwadraten. Het is belangrijk dat we 0 als kwadraat tellen (namelijk 0^2) en dat een kwadraat h^2 dus te representeren is als som van twee kwadraten $h^2 = h^2 + 0^2$. We volgen voornamelijk het bewijs zoals Stillwell gegeven heeft in [13] Sectie 6, met wat toevoeginen uit het werk van Grosswald [6] Chapter 2.

Stelling 2.1.1 (Fermats twee kwadraten stelling) *Een priemgetal p is te schrijven als som van twee kwadraten dan en slechts dan als $p \not\equiv 3 \mod 4$*

Voor het bewijs van Fermats stelling gaan we de gehelen van Gauss ($\mathbb{Z}[i]$) gebruiken en hebben we de volgende definities nodig.

Voor een element $z = a + bi$ uit $\mathbb{Z}[i]$ met $a, b \in \mathbb{Z}$, noemen we $\overline{z} = a - bi$ de **complex geconjugeerde**.

Voor een element $z = a + bi$ uit $\mathbb{Z}[i]$ met $a, b \in \mathbb{Z}$, noemen we $N(z) = a^2 + b^2$ de **norm** van z. Merk op dat $z\overline{z} = N(z)$

Een **priemelement** uit de gehelen van Gauss is een $\gamma \in \mathbb{Z}[i]$ met norm groter dan 1 die niet het product is van elementen uit $\mathbb{Z}[i]$ van kleinere norm.

Al hoewel we het niet zullen bewijzen geldt binnen $\mathbb{Z}[i]$ de priemdeler eigenschap; als voor $a, b, p \in \mathbb{Z}[i]$ met p een priemelement geldt dat p een deler is van ab, dan is p een deler van a of van b.

De volgende stelling laat zien waarom priemelementen uit $\mathbb{Z}[i]$ een rol zullen spelen in het bewijs van Fermats twee kwadraten stelling.

Stelling 2.1.2 *Voor een priemgetal $p \in \mathbb{N}$ geldt:*
p is een som van twee kwadraten $\Leftrightarrow$ p is geen priemelement uit $\mathbb{Z}[i]$.

Bewijs. ($\Rightarrow$) Stel $p \in \mathbb{N}$ is een priemgetal met $p = a^2 + b^2$ met $a, b \in \mathbb{Z}$ dan

$$p = (a + bi)(a - bi)$$

en $N(a + bi) = N(a - bi) < N(p) = p^2$, dus p is geen priemelement uit $\mathbb{Z}[i]$.

($\Leftarrow$) Stel $p \in \mathbb{N}$ is een priemgetal maar geen priemelement uit $\mathbb{Z}[i]$, dan is p dus het product van delers met kleinere norm:

$$p = (a + bi)\gamma$$

voor $a, b \in \mathbb{Z}, (a + bi), \gamma \in \mathbb{Z}[i]$ met norm kleiner dan p^2. Maar dan

$$\begin{aligned} p^2 &= (a + bi)\gamma\overline{(a + bi)\gamma} \\ &= (a + bi)(a - bi)\gamma\overline{\gamma} \\ &= (a^2 + b^2)N(\gamma) \end{aligned}$$

met $a^2+b^2>1$ en $N(\gamma)>1$ en beide zijn gehele getallen. De enige factorisatie van p^2 die hieraan voldoet is pp, dus $p=a^2+b^2$. □

Dit betekent dat wanneer we bewijzen dat een priemgetal p een priemelement uit $\mathbb{Z}[i]$ is dan en slechts dan als $p \equiv 3 \mod 4$ we Fermats stelling bewezen hebben. Hiervoor hebben we nog één lemma nodig.

Lemma 2.1.3 *Een priemgetal $p = 4n+1$ voor een $n \in \mathbb{N}$ deelt m^2+1 voor een $m \in \mathbb{Z}$.*

Bewijs. De enige elementen binnen $(\mathbb{Z}/p\mathbb{Z})$ die hun eigen inverse zijn, zijn 1 en $-1 \equiv -1 \mod p$. Dit betekent dat in $(p-1)!$ elk element tegen zijn inverse weg valt op 1 en -1 na, dus

$$\begin{aligned}
-1 &\equiv 1\cdot(-1) \pmod p \\
&\equiv (p-1)! \pmod p \\
&\equiv 1\cdot 2\cdots 4n \pmod p \\
&\equiv (1\cdot 2\cdots 2n)((-2n)\cdots(-2)\cdot(-1)) \pmod p \\
&\quad (\text{omdat } p-k \equiv -k \mod p) \\
&\equiv (1\cdot 2\cdots 2n)^2(-1)^{2n} \pmod p \\
&\equiv (1\cdot 2\cdots 2n)^2 \pmod p.
\end{aligned}$$

Dus met $m=(2n)!$ krijgen we $m^2 \equiv -1 \mod p$ en dus $p \mid (m^2+1)$. □

Bewijs van Fermats twee kwadraten stelling. Elk priemgetal is gelijk aan 2 of gelijk aan 1 (mod 4) of 3 (mod 4).

$2 = 1^2+1^2$ en dus een som van twee kwadraten.

Stel $p = 1 \mod 4$, dan $p \mid (m^2+1)$ voor een $m \in \mathbb{Z}$, en

$$m^2+1 = (m-i)(m+i).$$

Echter deelt p wel (m^2+1) maar niet $(m-i)$ of $(m+i)$ want $\frac{m-i}{p}, \frac{m+i}{p} \notin \mathbb{Z}[i]$, dus p is geen priemelement uit $\mathbb{Z}[i]$ en dus een som van twee kwadraten.

Stel $p = 3 \mod 4$, stel $a, b \in \mathbb{Z}$. Aangezien $a^2 \equiv 0 \mod 4$ of $a^2 \equiv 1 \mod 4$ en hetzelfde geldt voor b, krijgen we $a^2+b^2 \equiv c \mod 4$ voor een $c \in \{0,1,2\}$ en aangezien $p = 3 \mod 4$ is dus $p \neq a^2+b^2$. Dus p is niet te schrijven als som van twee kwadraten. □

Nu vast staat welke priemgetallen te representeren zijn als som van twee kwadraten, kunnen we bekijken welke natuurlijke getallen zo te representeren zijn.

Stelling 2.1.4 *Een natuurlijk getal $n \in \mathbb{N}$ is te representeren als som van twee kwadraten dan en slechts dan als elk priemgetal $q \equiv 3 \pmod 4$ dat n deelt dit in een even macht doet. Met andere woorden, de grootste $m \in \mathbb{N}$ waarvoor q^m een deler is van n is even voor elke priemfactor $q \equiv 3 \pmod 4$ van n.*

Bewijs. ($\Rightarrow$) Stel $q \equiv 3 \mod 4$ is een priemfactor van n. Stel $x^2 + y^2 = n$ voor een $x, y \in \mathbb{Z}$ dan $x^2 \equiv -y^2 \pmod{q}$, maar omdat -1 een kwadratische niet-rest is modulo q (zie hiervoor Lemma 2.3.3 en zijn gevolg), geldt dit alleen als $x \equiv y \equiv 0 \pmod{q}$. Dus zowel x als y is deelbaar door q, dus n is deelbaar door q^2. Stel $n = q^2 n_1$ en n_1 is deelbaar door q dan kunnen we hetzelfde argument gebruiken om te zien dat n_1 deelbaar moet zijn door q^2 en met inductie zien we dat q in een even macht voor moet komen.

($\Leftarrow$) Stel elke priemfactor $q \equiv 3 \pmod 4$ van n komt in even macht voor, dan is n te ontbinden in factoren die allen te schrijven zijn als som van twee kwadraten (q komt in een even macht, zeg m voor dus $q^m = (q^{m/2})^2 + 0^2$ en we hebben al gezien dat alle andere priemfactoren te schrijven zijn als som van twee kwadraten). Stel $x = a^2 + b^2, y = c^2 + d^2$ met $x, y \in \mathbb{N}, a, b, c, d \in \mathbb{Z}$ dan

$$\begin{aligned} xy &= (a^2 + b^2)(c^2 + d^2) \\ &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= (ac + bd)^2 + (ad - bc)^2. \end{aligned}$$

Dus met inductie zien we dat n te schrijven is als som van twee kwadraten. □

2.2 Legendres algoritme

In 1808 presenteerde Legendre het eerst bekende algoritme voor het representeren van een priemgetal $p \equiv 1 \pmod 4$ als som van twee kwadraten, wat besproken wordt door Davenport in [4] Sectie 5 en Barnes [1]. Dit algoritme maakt gebruik van Kettingbreuken.

2.2.1 Kettingbreuken

Definitie 2.2.1 *Een **kettingbreuk** is een "breuk"van de vorm*

$$q_0 + \cfrac{z_1}{q_1 + \cfrac{z_2}{q_2 + \cfrac{\cdots}{q_n}}} \quad \textit{of} \quad a_0 + \cfrac{z_1}{q_1 + \cfrac{z_2}{q_2 + \cfrac{z_3}{\cdots}}}$$

met $q_i, z_i \in \mathbb{Z}$ voor alle $i \in \mathbb{N}$.

*We noemen zo'n kettingbreuk een **simpele kettingbreuk** als $z_i = 1$ voor alle $i \in \mathbb{N}$.*

In deze definitie staat breuk tussen aanhalingstekens, omdat een oneindige kettingbreuk geen rationaal getal is.

Om kettingbreuken leesbaar te houden voeren we de volgende notaties in:

$$q_0 + \frac{z_1}{q_1+}\frac{z_2}{q_2+}\cdots := q_0 + \cfrac{z_1}{q_1 + \cfrac{z_2}{q_2 + \cfrac{1}{\cdots}}},$$

$$[q_0, q_1, \dots] := q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\dots}}}.$$

Vanaf nu zullen we met kettingbreuken simpele kettingbreuken bedoelen tenzij anders aangegeven.

Eindige kettingbreuken kunnen we omschrijven naar een gewone breuk waar de teller en noemer copriem zijn; zo wordt

$$\begin{aligned} q_0 + \frac{1}{q_1} &= \frac{q_0 q_1 + 1}{q_1} \\ q_0 + \frac{1}{q_1} \frac{1}{q_2} &= \frac{q_0 q_1 q_2 + q_0 + q_2}{q_1 q_2 + 1} \\ q_0 + \frac{1}{q_1} \frac{1}{q_2} \frac{1}{q_3} &= \frac{q_0 q_1 q_2 q_3 + q_0 q_3 + q_2 q_3 + 1}{q_1 q_2 q_3 + q_1 + q_3} \end{aligned}$$

Voor de teller en noemer van $[q_0, q_1, \dots, q_m]$ op zo'n manier uitgeschreven, schrijven we A_m respectievelijk B_m; deze worden ook wel de teller en noemer van de convergenten van de kettingbreuk genoemd, we zullen voor het gemak A_m en B_m convergenten noemen, ook al is dit niet de traditionele definitie. Hiermee krijgen we

$$\begin{aligned} A_0 &= q_0 & B_0 &= 1 \\ A_1 &= q_0 q_1 + 1 & B_1 &= q_1 \\ A_m &= q_m A_{m-1} + A_{m-2} & B_m &= q_m B_{m-1} + B_{m-2} \end{aligned} \tag{1}$$

en voor $m > 0$

$$A_m B_{m-1} - A_{m-1} B_m = (-1)^{m-1}. \tag{2}$$

2.2.2 Kwadratisch irrationale getallen

Kwadratisch irrationale getallen zijn verbonden aan kettingbreuken en spelen een belangrijke rol in Legendres algoritme voor het vinden van een representatie van een priemgetal $p \equiv 1 \pmod 4$ als som van twee kwadraten.

Definitie 2.2.2 *Een irrationaal getal dat de oplossing is van een kwadratische vergelijking met gehele coëfficiënten heet een* ***kwadratisch irrationaal getal****.*

Een voorbeeld van een kwadratisch irrationaal getal is $\sqrt{N}$ van een natuurlijk getal N dat geen kwadraat is. Als $\sqrt{N} \notin \mathbb{Z}$ geldt ook dat $\sqrt{N} \notin \mathbb{Q}$, want als $a, b \in \mathbb{Z}$ met $\text{ggd}(a, b) = 1$ dan $(\frac{a}{b})^2 \notin \mathbb{Z}$. Dus $\sqrt{N}$ is irrationaal en een oplossing voor $x^2 - N = 0$.

We kunnen direct een verband zien met kettingbreuken als we naar volledig periodieke kettingbreuken gaan kijken.

Definitie 2.2.3 *Een **volledig periodieke kettingbreuk** α is een kettingbreuk die periodiek is vanaf het begin. Dit wil zeggen*

$$\alpha = [\ \overline{q_0, q_1, \ldots, q_m}\ ],$$

waar de overlijning betekent dat het overlijnde stuk oneindig herhaald wordt, dus

$$\alpha = q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\cdots\frac{1}{q_m+}\frac{1}{\alpha}.$$

Stel we hebben zo'n $\alpha = q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\cdots\frac{1}{q_m+}\frac{1}{\alpha}$ die positief is, dan zien we net zoals bij (1), dat

$$\alpha = \frac{\alpha A_m + A_{m-1}}{\alpha B_m + B_{m-1}}.$$

Uitgeschreven levert dit op

$$\alpha^2 B_m + \alpha(B_{m-1} - A_m) - A_{m-1} = 0. \tag{3}$$

Aangezien α een oneindige kettingbreuk heeft, is α irrationaal en omdat $A_m, A_{m-1}, B_m, B_{m-1} \in \mathbb{Z}$ is α een kwadratisch irrationaal getal.

We voeren nu voor een kettingbreuk $[a_0, a_1, \ldots, a_n]$ de notatie $A_n = [[a_0, a_1, \ldots, a_n]]$ in (dit geeft ook automatisch $B_n = [[a_1, a_2, \ldots, a_n]]$). Euler liet met een formule (Eulers formule) zien dat we A_n kunnen berekenen door de som te nemenen van: het product van alle termen (dus $a_0 \cdot a_1 \cdots a_n$), alle producten van alle termen met één paar opvolgende termen weggelaten, alle producten van alle termen met twee paren van opvolgende termen weggelaten, enzovoorts. Hierbij wordt het product waar precies alle termen weggelaten zijn 1. Dit wordt duidelijker met een voorbeeld.

$$[[q_0, q_1, q_2, q_3]] = q_0q_1q_2q_3 + q_2q_3 + q_0q_3 + q_0q_1 + 1,$$

waar we bijvoorbeeld q_0q_3 krijgen door het opvolgende paar q_1, q_2 weg te laten. Een voorbeeld met oneven lengte eindigt nooit op een 1, omdat er altijd een even aantal termen wordt weggelaten.

$$[[q_0, q_1, q_2, q_3, q_4]] = q_0q_1q_2q_3q_4 + q_2q_3q_4 + q_0q_3q_4 + q_0q_1q_4 + q_0q_1q_2 + q_4 + q_2 + q_0,$$

Waar we bijvoorbeeld q_2 krijgen door de paren q_0, q_1 en q_3, q_4 weg te laten.

Als we de definitie/constructie van A_m en B_m bekijken net boven (1) zien we dat in het algemeen geldt

$$A_m = q_0B_m + [[q_2, \ldots, q_m]]$$

of uitgeschreven

$$[[q_0, q_1, \ldots, q_m]] = q_0[[q_1, \ldots, q_m]] + [[q_2, \ldots, q_m]]. \tag{4}$$

We weten dat voor de eerste twee gevallen geldt $[[a_0]] = a_0$ en $[[a_0, a_1]] = a_0a_1 + 1$. Dus als we uitgaande van de correctheid van Eulers formule voor

de twee convergenten van het rechter lid van (4) kunnen bewijzen dat Eulers formule geldt voor het linker lid hebben we met inductie bewezen dat Eulers formule altijd correct is.

Stel Eulers formule klopt voor convergenten met $m-1$ of minder coëfficiënten, dan is $[[q_1, \ldots, q_m]]$ de som van de producten van de termen op alle manieren met elke mogelijkheid van opvolgende paren weggelaten, dus $q_0[[q_1, \ldots, q_m]]$ is de som van alle producten van de termen met elke mogelijkheid van opvolgende paren behalve de paren die q_0 bevatten weggelaten. Dit houdt in dat precies alle producten waar het paar q_0, q_1 weggelaten moeten komen uit $[[q_2, \ldots, q_m]]$ en dat is precies wat Eulers formule oplevert voor $[[q_2, \ldots, q_m]]$, dus Eulers formule is correct.

Door met Eulers formule $[[a_0, a_1, \ldots, a_n]]$ uit te schrijven zien we direct dat

$$[[a_0, a_1, \ldots, a_n]] = [[a_n, a_{n-1}, \ldots, a_0]]$$

Dit betekent dat als we in ons geval $\beta = [\,\overline{q_m, q_{m-1}, \ldots, q_0}\,]$ nemen, en de convergenten van β met een accent aangeven, krijgen we

$$A_m^{'} = A_m, \quad A_{m-1}^{'} = B_m, \quad B_m^{'} = A_{m-1}, \quad B_{m-1}^{'} = B_{m-1}$$

Dus krijgen we voor de β

$$\beta = \frac{\beta A_m^{'} + A_{m-1}^{'}}{\beta B_m^{'} + B_{m-1}^{'}} = \frac{\beta A_m + B_m}{\beta A_{m-1} + B_{m-1}}$$

en dus

$$\beta^2 A_{m-1} + \beta(-A_m + B_{m-1}) - B_m = 0$$

Hiermee zien we dat $-\frac{1}{\beta}$ een oplossing is voor (3). Aangezien α en β door constructie hetzelfde teken hebben, betekent dit dat $-\frac{1}{\beta}$ het andere nulpunt is van de kwadratische vergelijking van α. We noemen $-\frac{1}{\beta}$ de **geconjugeerde** van α. We weten dat $\beta > 1$, omdat $q_m \geq 1$ en dus hebben we het volgende lemma.

Lemma 2.2.4 *Elke positieve volledig periodieke kettingbreuk is gelijk aan een kwadratisch irrationaal getal α dat groter is dan 1 en een geconjugeerde $-\frac{1}{\beta}$ heeft, waar β de kettingbreuk is met de termen omgedraaid. Deze geconjugeerde ligt tussen -1 en 0.*

Dit lemma vraagt om een nieuwe definitie.

Definitie 2.2.5 *Een kwadratisch irrationaal getal α heet **gereduceerd** als $\alpha > 1$ en voor zijn geconjugeerde α' geldt $-1 < \alpha' < 0$.*

Stelling 2.2.6 *Een kettingbreuk van een gereduceerd kwadratisch irrationaal getal is volledig periodiek.*

Bewijs. Stel α is een gereduceerd kwadratisch irrationaal getal, dan zijn er $a, b, c \in \mathbb{Z}$ met $a, c \neq 0$ zodanig dat

$$a\alpha^2 + b\alpha + c = 0.$$

Dit geeft voor bepaalde $P, Q \in \mathbb{Z}$ en $D \in \mathbb{N}$, waarbij D geen kwadraat is

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{P \pm \sqrt{D}}{Q}.$$

Aangezien we het teken van $\sqrt{D}$ kunnen aanpassen door dat van P en Q aan te passen kunnen we zelfs aannemen dat

$$\alpha = \frac{P + \sqrt{D}}{Q}$$

en dat geeft voor de geconjugeerde

$$\alpha' = \frac{P - \sqrt{D}}{Q}.$$

Er zijn een aantal belangrijke eigenschappen die we nu vast kunnen stellen.

1. $\alpha - \alpha' = 2\frac{\sqrt{D}}{Q} > 0$ en dus $Q > 0$.
2. $\alpha + \alpha' = 2\frac{P}{Q} > 0$ en dus $P > 0$.
3. $\alpha' < 0$, dus $P < \sqrt{D}$.
4. $\alpha > 1$, dus $Q < P + \sqrt{D} < 2\sqrt{D}$.
5. $\frac{P^2 - D}{Q} = \frac{b^2 - (b^2 - 4ac)}{2a} = 2c$, dus $(P^2 + D)$ is een veelvoud van Q.

We kunnen α nu gaan ontwikkelen als kettingbreuk. $\alpha > 1$, dus er zijn $q_0 \in \mathbb{N}$ en $\alpha_1 \in \mathbb{R}$ zodanig dat

$$\alpha = q_0 + \frac{1}{\alpha_1} \tag{5}$$

maar $q_0 + 1 > \alpha$. We zullen vanaf nu zo'n q_0 het **gehele deel** van α noemen. Dit betekent dat

$$\alpha' = q_0 + \frac{1}{\alpha_1'},$$

dit geeft

$$\alpha_1' = \frac{-1}{q_0 - \alpha'}.$$

Aangezien $q_0 \in \mathbb{N}$ en $\alpha' < 0$, hebben we $q_0 - \alpha' > 1$, dus $-1 < \alpha_1' < 0$, dus α_1 is een gereduceerd kwadratisch irrationaal getal. Dit betekent ook dat als we op een zelfde manier $\alpha_2, \alpha_3, \ldots$. definiëren, deze ook gereduceerde kwadratisch irrationale getallen zijn.

We kunnen de bijbehorende vergelijking voor α_1 vinden uit die van α

$$\frac{1}{\alpha_1} = \alpha - q_0 = \frac{P - Qq_0 + \sqrt{D}}{Q}.$$

Definieer $P_1 = -P + Qq_0$ en $Q_1 = \frac{D-P_1^2}{Q}$, dan

$$\alpha_1 = \frac{Q}{-P_1 + \sqrt{D}} = \frac{P_1 + \sqrt{D}}{Q_1}.$$

Het is duidelijk dat $P_1 \in \mathbb{Z}$, maar ook $Q_1 \in \mathbb{Z}$, want $(D - P^2)$ is een veelvoud van Q en $P_1 \equiv -P \pmod{Q}$. Omdat α_1 gereduceerd is, zijn P_1 en Q_1 zelfs natuurlijk en is $(P_1^2 - D)$ een veelvoud van Q_1. We kunnen dit proces blijven herhalen en krijgen zo

$$\alpha_n = \frac{P_n + \sqrt{D}}{Q_n},$$

met dezelfde eigenschappen als eerder gegeven voor α, P, Q en D. Nu moet voor elk paar P_n, Q_n gelden dat $0 < P_n < \sqrt{D}$ en $0 < Q_n < 2\sqrt{D}$, aangezien zowel P_n als Q_n natuurlijk zijn, zijn er maar een eindig aantal verschillende mogelijkheden. Dus uiteindelijk komen we op een paar P_n, Q_n uit dat al eerder is voorgekomen, dus $\alpha_n = \alpha_m$ voor een $m < n$, dus α is periodiek.

We hebben nu voor α_n als geconjugeerde $\alpha_n' = q_n + \frac{1}{\alpha_{n+1}}$. Definieer nu $\beta_n = -\frac{1}{\alpha_n'}$. Dan geldt $\beta_n > 1$ en

$$-\frac{1}{\beta_n} = q_n - \beta_{n+1}, \quad \text{of} \quad \beta_{n+1} = q_n + \frac{1}{\beta_n}.$$

Dus q_n is zowel het gehele deel van α_n als van β_{n+1}.

Stel $\alpha_n = \alpha_m$, met $n < m$. Dan zijn hun geconjugeerden ook gelijk en dus $\beta_n = \beta_m$. Met wat we hierboven gezien hebben betekent dit dat q_n het gehele deel is van β_n en q_m van β_m, dus $q_n = q_m$. Aangezien

$$\alpha_{n-1} = q_{n-1} + \frac{1}{\alpha_n} \qquad \alpha_{m-1} = q_{m-1} + \frac{1}{\alpha_m},$$

geldt ook $\alpha_{n-1} = \alpha_{m-1}$ en als we dit doorzetten krijgen we $\alpha_{m-n} = \alpha$. Dit betekent dat

$$\alpha = [q_0, q_1, \ldots, q_{m-n-1}, \alpha].$$

Dus α is volledig periodiek. □

We moeten nog een aantal eigenschappen voor de kettingbreuk van $\sqrt{N}$ bewijzen, voor een natuurlijk getal N, voordat we naar het algoritme van Legendre kunnen gaan kijken.

Lemma 2.2.7 *Voor een natuurlijk getal N heeft de kettingbreuk van de wortel de vorm*

$$\sqrt{N} = [\ q_0, \overline{q_1, q_2, \ldots, q_2, q_1, 2q_0}\ ].$$

Bewijs. Laat q_0 het gehele deel van $\sqrt{N}$ zijn, dan is $\sqrt{N}+q_0$ een kwadratisch irrationaal getal. Aangezien de geconjugeerde $-\sqrt{N}+q_0$ is en aangezien $-1 < -\sqrt{N}+q_0 < 0$ geldt zelfs dat $\sqrt{N}+q_0$ gereduceerd is. Neem nu $\alpha = \sqrt{N}+q_0$ en stel dat de periode van α gelijk is aan n, dan krijgen we

$$\alpha = [\ \overline{2q_0, q_1, q_2, \ldots, q_n}\ ]. \tag{6}$$

We hebben al gezien dat voor de inverse periode moet gelden

$$-\frac{1}{\alpha'} = [\ \overline{q_n, q_{n-1}, \ldots, q_1, 2q_0}\ ].$$

Maar met (6) hebben we omdat $\alpha' = -\sqrt{N}+q_n$

$$-\frac{1}{\alpha'} = [\ \overline{q_1, q_2, \ldots, q_n, 2q_0}\ ].$$

Dit geeft dat voor alle $m \in \mathbb{N}$ met $0 < m < n$ geldt dat $q_m = q_{n-m+1}$ en dus

$$\sqrt{N} = [\ q_0, \overline{q_1, q_2, \ldots, q_2, q_1, 2q_0}\ ].$$

□

2.2.3 Het algoritme

In deze sectie gaan we een priemgetal $p \equiv 1 \pmod 4$ schrijven als som van twee kwadraten door middel van het algoritme van Legendre. De eerste stap is om $\sqrt{p}$ te schrijven als kettingbreuk.

Lemma 2.2.8 *$\sqrt{p}$ kan geschreven worden als*

$$\sqrt{p} = [q_0, \overline{q_1, \ldots, q_m, q_m, \ldots, q_1, 2q_0}\ ]. \tag{7}$$

Met andere woorden, de kettingbreuk van $\sqrt{p}$ heeft periode van oneven lengte.

Dit kan bewezen worden door twee lemma's die Perron heeft bewezen in [11], Satz 3.18 en Satz 3.22.

Lemma 2.2.9 *De vergelijking $x^2 - Dy^2 = -1$ heeft een oplossing dan en slechts dan als het aantal termen in de periode van de kettingbreuk voor $\sqrt{D}$ oneven is.*

Lemma 2.2.10 *Voor een priemgetal $p \equiv 1 \pmod 4$ is $x^2 - py^2 = -1$ oplosbaar.*

Het spreekt voor zichzelf dat deze twee lemma's samen met de resultaten van Sectie 2.2.2 een bewijs geven voor Lemma 2.2.8.

We definieren α als de kettingbreuk

$$\begin{aligned} \alpha &= q_m + \frac{1}{q_{m-1}+} \cdots \frac{1}{q_1+} \frac{1}{2q_0+} \frac{1}{q_1+} \cdots \\ &= [\ \overline{q_m, \ldots, q_1, 2q_0, q_1, \ldots, q_m}\ ] \end{aligned}$$

waar de q_i deze zijn van (7).

Omdat $\sqrt{p} = [q_0, q_1, \ldots, q_m, \overline{q_m, \ldots, q_1, 2q_0, q_1, \ldots, q_m}\,]$ krijgen we $\sqrt{p} = [q_0, q_1, \ldots, q_m, \alpha]$ of $\sqrt{p} = \frac{\alpha A_m + A_{m-1}}{\alpha B_m + B_{m-1}}$(zie (1)). Dit betekent dat we met (2) α kunnen schrijven als een kwadratisch irrationaal getal.

$$\begin{aligned}
\sqrt{p} &= \frac{\alpha A_m + A_{m-1}}{\alpha B_m + B_{m-1}} \\
\Rightarrow \qquad (\alpha B_m + B_{m-1})\sqrt{p} &= \alpha A_m + A_{m-1} \\
\Rightarrow \qquad \alpha(A_m - B_m\sqrt{p}) &= -A_{m-1} + B_{m-1}\sqrt{p} \\
\Rightarrow \qquad \alpha &= \frac{-A_{m-1} + B_{m-1}\sqrt{p}}{A_m - B_m\sqrt{p}} \\
\Rightarrow \qquad \alpha &= \frac{(-A_{m-1} + B_{m-1}\sqrt{p})(A_m + B_m\sqrt{p})}{(A_m - B_m\sqrt{p})(A_m + B_m\sqrt{p})} \\
\Rightarrow \qquad \alpha &= \frac{-A_m A_{m-1} + pB_m B_{m-1} + (-1)^{m-1}\sqrt{p}}{A_m^2 - pB_m^2}.
\end{aligned}$$

Als we α' schrijven voor de geconjugeerde van α krijgen we

$$\alpha' = \frac{-A_m A_{m-1} + pB_m B_{m-1} + (-1)^m\sqrt{p}}{A_m^2 - pB_m^2}$$

en

$$\alpha\alpha' = \frac{(-A_m A_{m-1} + pB_m B_{m-1})^2 - p}{(A_m^2 - pB_m^2)^2} = -1.$$

Dus als we het volgende definiëren

$$x = pB_m B_{m-1} - A_m A_{m-1}$$

$$y = A_m^2 - pB_m^2$$

krijgen we $p = x^2 + y^2$.

Nu moeten we nog een constructie vinden voor de kettingbreuk van $\sqrt{p}$. Noem nu $h(n)$ het gehele deel van n. Definieer

$$\begin{aligned}
\alpha_0 &= \sqrt{p} + h(\sqrt{p}) \\
\alpha_n &= \frac{1}{\alpha_{n-1} - h(\alpha_{n-1})}
\end{aligned}$$

Zodra je een n gevonden hebt zodat $\alpha_n = \alpha_0$, geldt

$$\sqrt{p} = [h(\sqrt{p}), \overline{h(\alpha_1), \ldots, h(\alpha_n)}\,]$$

Dit is dezelfde constructie die we bij (5) hebben gebruikt om aan te tonen dat gereduceerde kwadratische irrationale getallen zich als kettingbreuk uit laten bouwen met behulp van andere gereduceerde kwadratische irrationale getallen.

We kunnen met een voorbeeld zien dat het werkt. Neem $p = 29$, dan kunnen we berekenen dat $\sqrt{29} = [5, \overline{2, 1, 1, 2, 10}\,]$, dit houdt in dat

$$\begin{aligned} A_m &= [[5, 2, 1]] = 16, & A_{m-1} &= [[5, 2]] = 11, \\ B_m &= [[2, 1]] = 3, & B_{m-1} &= [[2]] = 2. \end{aligned}$$

Dit geeft

$$x = 29 \cdot 3 \cdot 2 - 16 \cdot 11 = -2, \qquad y = 16^2 - 29 \cdot 3^2 = -5.$$

En we zien dat $29 = (-2)^2 + (-5)^2$.

Wat we nu nog willen weten is hoe efficiënt dit algoritme is. Hiervoor bespreken we eerst kort een stukje theorie over complexiteitstheorie.

2.2.4 Complexiteit

In deze scriptie zal de complexiteit van de algoritmes niet uitvoerig behandeld worden en hebben we aan een aantal eenvoudige definities genoeg.

Definitie 2.2.11 ***Big O*** $(\mathcal{O})$ *is een notatie die gebruikt wordt om de complexiteit van een functie of algoritme aan te geven. Stel* f, g *zijn reële functies dan betekent* $f(x) = \mathcal{O}(g(x))$ *dat er een positief reëel getal* M *en een reëel getal* x_0 *bestaan zodanig dat voor elke* $x > x_0$ *geldt* $|f(x)| < M\,|g(x)|$.

Voor algoritmes wordt $\mathcal{O}$ gebruikt voor het aantal operaties die het kost om een algoritme uit te voeren.

We zullen een voorbeeld doornemen van $\mathcal{O}$. Laat $f(x) = 6x^5 - 12x^3 + 3x^2 + 1$, dan geldt

$$\begin{aligned} |f(x)| &= \left|6x^5 - 12x^3 + 3x^2 + 1\right| \\ &\leq \left|6x^5\right| + \left|12x^3\right| + \left|3x^2\right| + |1| \\ &< 7x^5 \qquad\qquad \text{(Voor groot genoege } x\text{)} \end{aligned}$$

Dus $f(x) = \mathcal{O}(x^5)$.

Algoritmes kunnen we onderscheiden in twee complexiteitsklassen, algoritmes die oplosbaar zijn in polynomiale tijd en algoritmes die dit niet zijn. Algoritmes die niet binnen polynomiale tijd oplosbaar zijn, worden in het algemeen gezien als inefficiënte algoritmes die snel in complexiteit zullen stijgen voor grotere input.

Definitie 2.2.12 *Een algoritme is oplosbaar binnen* ***polynomiale tijd*** *als hij met input van grootte* n *een complexiteit heeft van* $\mathcal{O}(n^k)$ *voor een positieve* k.

Merk op dat een algoritme waarbij de complexiteit niet als een macht van de grootte van de input genoteerd wordt, dit niet betekent dat hij niet binnen polynomiale tijd oplosbaar is, want er kan wel een bovenafschatting zijn die een

macht van de grootte van de input is.

De grootte van de input van een getal is in het algemeen niet de waarde van het getal zelf. Wij zullen voor onze algoritmes als input enkel natuurlijke getallen n hebben en hiervoor kunnen we de complexiteit aangeven met $\log_2(n)$ of simpel weg $\log(n)$, dit geeft de lengte van het natuurlijk getal als deze binair geschreven wordt. We zullen het ook ooit over verwachte polynomiale tijd hebben, hiermee wordt bedoeld dat er ergens willekeurig iets gekozen moet worden en met de verwachte kans dat we een juiste keuze maken, zal het algoritme in polynomiale tijd uit te voeren zijn.

2.2.5 Efficiëntie van het algoritme

Hiervoor hebben we een bovengrens nodig voor het aantal termen waaruit de kettingbreuk van $\sqrt{p}$ kan bestaan. In theorem 4.2 van [2] bewijst Becceanu het volgende lemma.

Lemma 2.2.13 *Voor een natuurlijk getal $D > 1$ dat geen kwadraat is, geldt voor een $k \in \mathbb{N}$ dat $k^2 < D < (k+1)^2$ en dat de lengte van de periode van de kettingbreuk van $\sqrt{D}$ kleiner is dan $\frac{7}{4}k + \frac{3}{4}$.*

Voor een groot genoege D betekent dit dat het aantal stappen kleiner is dan $2k$ of $2\sqrt{D}$ en dat het algoritme voor het uitrekenen van de kettingbreuk voor $\sqrt{D}$ een complexiteit heeft van $\mathcal{O}(f(D) \cdot D^{\frac{1}{2}})$ waar $f(D)$ de complexiteit is voor het uitrekenen van één volgende getal in de kettingbreuk. We hebben in Sectie 2.2.3 gezien dat dit neer komt op een breuk, aftrekking en het berekenen van het gehele deel van een getal. Al hoewel deze allemaal in polynomiale tijd kunnen, is $\mathcal{O}(D^{\frac{1}{2}})$ al geen polynomiale tijd en zal Legendres algoritme op deze manier niet binnen polynomiale tijd te berekenen zijn.

Lenstra [9] geeft aan dat door het algoritme anders aan te pakken de complexiteit van het algoritme van Legendre voor het bepalen van een representatie als som van twee kwadraten voor een priemgetal $p \equiv 1 \pmod 4$ gelijk wordt aan $\mathcal{O}(p^{\frac{1}{4}})$ of door het aannemen van de Riemann-hypothese zelfs $\mathcal{O}(p^{\frac{1}{5}})$, maar beide is geen polynomiale tijd, aangezien de input van grootte $\log_2 p$ is.

2.3 Algoritmes vanuit kwadratische resten

2.3.1 Serret en Hermite

In 1948 publiceerden zowel Serret [12] als Hermite [7] een artikel met vrijwel hetzelfde algoritme voor het representeren van een priemgetal $p \equiv 1 \pmod 4$ als som van twee kwadraten. Met notaties zoals besproken in Sectie 2.2 is het algoritme te beschrijven met de volgende twee stappen.

1. Vind een $h \in \mathbb{N}$ met $0 < h < \frac{p}{2}$ zodanig dat $h^2 \equiv -1 \pmod p$
2. Bepaal de kettingbreuk voor $\frac{h}{p}$ totdat $B'_{k+1} < \sqrt{p} < B'_{k+2}$. Dan geldt

$$p = (hB'_{k+1} - pA'_{k+1})^2 + (B'_{k+1})^2.$$

In dit geval gebruiken we de notatie A'_n en B'_n in plaats van A_n en B_n voor de convergenten van de kettingbreuk van $\frac{h}{p}$, omdat we deze later willen kunnen onderscheiden van de convergenten van een andere kettingbreuk. Dit zijn dus geen geconjugeerden of dergelijke.

We kunnen weer het voorbeeld $p = 29$ nemen om dit algoritme uit te testen. We zien dat $12^2 \equiv 144 \equiv -1 \pmod{29}$ en $12 < \frac{29}{2}$. We berekenen dat voor $\frac{12}{29}$ geldt dat $B'_2 = 5$ en $B'_3 = 12$. We berekenen nu

$$\begin{aligned}(12B'_2 - 29A'_2)^2 + (B'_2)^2 &= (12 \cdot 5 - 29 \cdot 2)^2 + 5^2 \\ &= 2^2 + 5^2 \\ &= 29\end{aligned}$$

2.3.2 Brillhart

In 1972 liet Brillhart [3] zien dat het niet nodig is om de convergenten uit te rekenen en dat we in plaats van het bepalen van de kettingbreuk eenvoudigweg het algoritme van Euclides kunnen toepassen. Dit algoritme gaat als volgt

1. Vind een $h \in \mathbb{N}$ met $0 < h < \frac{p}{2}$ zodanig dat $h^2 \equiv -1 \pmod{p}$
2. Pas het algoritme van Euclides toe op p en h met resten $R_1, R_2, \ldots$ totdat je een k vindt zodanig dat $R_k < \sqrt{p} < R_{k-1}$. Dan

$$\begin{aligned} p &= R_k^2 + R_{k+1}^2 && \text{als } R_1 > 1, \\ p &= h^2 + 1 && \text{als } R_1 = 1. \end{aligned}$$

Laten we weer het voorbeeld $p = 29$ testen. We hebben in Sectie 2.3.1 gezien dat $12^2 \equiv -1 \pmod{29}$ en $12 < \frac{29}{2}$. Het algoritme van Euclides geeft

$$\begin{aligned} 29 &= 2 \cdot 12 + 5, \\ 12 &= 2 \cdot 5 + 2, \\ 5 &= 2 \cdot 2 + 1, \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Aangezien $5 < \sqrt{29}$, krijgen we $p = 5^2 + 2^2$.

Brillhart bewees de correctheid van dit algoritme aan de hand van de correctheid van het algoritme van Serret en Hermite en een stelling uit [11].

Stelling 2.3.1 *Voor $P, Q \in \mathbb{N}$ met $P > Q > 1$ en $\gcd(P, Q) = 1$ heeft $\frac{P}{Q}$ een symmetrische kettingbreuk met een even aantal termen als $Q^2 + 1$ deelbaar is door P.*

Bewijs. Perron [11] bewijst in Satz 2.3 dat elk rationaal getal op precies 1 manier als symmetrische kettingbreuk met even aantal termen te schrijven is. Dus als $\frac{P}{Q}$ een kettingbreuk heeft van $n+1$ termen met n oneven, dan

$$\frac{P}{Q} = [q_0, q_1, \ldots, q_1, q_0] = \frac{A_n}{B_n} \tag{8}$$

omdat A_n en B_n copriem zijn (zo zijn ze namelijk gedefinieerd), geldt $P = A_n, Q = B_n$. Perron [11] heeft in paragraaf 11 bewezen dat als $\frac{A_n}{B_n} = [a_0, a_1, \ldots, a_n]$ dan $\frac{A_n}{A_{n-1}} = [a_n, a_{n-1}, \ldots, a_0]$ en dus is voor ons $\frac{A_n}{A_{n-1}} = \frac{A_n}{B_n}$ en dus $A_{n-1} = B_n$, dus uit (2) volgt

$$A_n B_{n-1} - B_n^2 = (-1)^{n-1}$$

en omdat we vastgesteld hebben dat $P = A_n, Q = B_n$

$$PB_{n-1} = Q^2 + (-1)^{n-1}$$

dus $Q^2 + (-1)^{n-1}$ is deelbaar door P. Dit samen met Perron Satz 2.3 bewijst de stelling. □

Perron[11] bewijst in paragraaf 11 ook dat voor coprieme P en Q waar $\frac{P}{Q}$ een periode heeft van lengte $2k$ dat $2A_{2k+1} = A_k^2 + A_{k-1}^2$.

Uit (1) zien we nu, omdat we weten dat $p = A_{2k+1}, h = A_{2k}$,

$$p = q_{2k+1}h + A_{2k-1}, \quad h = q_{2k}A_{2k-1} + A_{2k-2}, \quad A_{2k-1} = q_{2k-1}A_{2k-2} + A_{2k-3}, \quad \ldots$$

Omdat $A_{n+1} > A_n$ voor elke $n \in \mathbb{N}$, geeft dit het algoritme van Euclides. Dit betekent dat $A_{2k-1} = R_1, A_{2k-2} = R_2, \ldots$ Dus $p = R_k^2 + R_{k+1}^2$.
We moeten nog aantonen dat R_k de eerste rest is kleiner dan $\sqrt{p}$. Het is duidelijk dat $R_k < \sqrt{p}$.

Als $k = 1$, dan is R_k dus de eerste rest kleiner dan $\sqrt{p}$.

Als $k > 1$, dan zien we uit (8) dat $R_{k-1} = A_{k+1} = B'_{k+2}$ en bij het algoritme van Serret en Hermite is $B'_{k+2} > \sqrt{p}$.

Als $R_1 = 1$, dan $p = q_0 h + 1$ en $p/h = [q_0, q_0] = q_0 + \frac{1}{q_0}$, dus $q_0 = h$ en $p = h^2 + 1$.

Nu we weten dat het algoritme werkt, zijn er nog twee dingen die we moeten achterhalen; we moeten namelijk h nog bepalen en willen weten hoe efficiënt het algoritme is. Het bepalen van $h \equiv -1 \pmod{p}$ kan op veel verschillende manieren, een efficiënte manier is besproken in [5].

We weten door middel van de hoofdstelling van de algebra dat de veelterm $x^2 + 1 = 0$ hoogstens twee nulpunten heeft in $(\mathbb{Z}/p\mathbb{Z})$. We kunnen met behulp van het Legendre-symbool en Eulers criterium aantonen dat er precies twee oplossingen bestaan.

Definitie 2.3.2 *Als A de verzameling van alle priemgetallen is, is het Legendre-symbool een functie $(\mathbb{N} \times A) \longrightarrow \{-1, 0, 1\}$ gedefinieerd door*

$$\left(\frac{a}{p}\right) := \begin{cases} -1 & \text{als } a \text{ een kwadratische niet-rest is modulo } p, \\ 0 & \text{als } a \equiv 0 \pmod{p}, \\ 1 & \text{als } a \text{ een kwadratische rest is modulo } p \\ & \text{en } a \not\equiv 0 \pmod{p} \end{cases}$$

Lemma 2.3.3 (Eulers criterium) *Laat p een priemgetal zijn en a een natuurlijk getal dat copriem is met p, dan*

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

Bewijs. Aangezien $a \neq 0$, geldt met de kleine stelling van Fermat $a^{p-1} \equiv 1 \pmod{p}$ oftewel

$$a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}.$$

Als a een kwadratische rest is, dan bestaat er een $x \in (\mathbb{Z}/p\mathbb{Z})$ zodanig dat $x^2 = a$. Hiermee geldt voor het linker lid $a^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, vanwege de kleine stelling van Fermat. Omdat $x^2 \equiv y^2 \pmod{p} \Leftrightarrow x \equiv y \pmod{p}$ of $x \equiv -y \pmod{p}$, en omdat $-y \not\equiv y \pmod{p}$ voor $p = 4k+1$ met $k \in \mathbb{N}$, zijn er precies $2k$ kwadratische resten in $(\mathbb{Z}/p\mathbb{Z})$. Met de hoofdstelling van de algebra zien we dat precies alle kwadratische resten de nulpunten geven van $a^{\frac{p-1}{2}} - 1$, dus in alle andere gevallen wordt $(a^{\frac{p-1}{2}} + 1)$ gelijk aan 0. Dit betekent dat als a geen kwadratische rest is, dan geldt $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Omdat $(-1)^{\frac{2k}{2}} = 1$, is -1 een kwadratische rest voor alle priemgetallen van de vorm $p = 4k + 1$, dus is er minstens 1 nulpunt voor $x^2 + 1 = 0$. Noem dit nulpunt u_1, dan is $u_2 = -u_1 = p - u_1$ ook een nulpunt en aangezien p oneven is geldt $u_2 = p - u_1 \neq u_1$.

Zoals gezien in het bewijs van Lemma 2.3.3 zijn voor $p = 4k + 1$ de oplossingen van $x^{2k} - 1 = 0$ precies alle $2k$ kwadratische resten.
Bekijk nu voor $0 \leq b < p$ de veelterm

$$f_b(x) = (x - b)^2 + 1 = x^2 - 2bx + b^2 + 1$$

Dan zijn de nulpunten van f_b dus $u_1 + b$ en $u_2 + b$. Als nu precies één van deze nulpunten, zeg dat $u_1 + b$ een kwadratische rest is, dan geldt

$$\text{ggd}(f_b(x), x^{2k} - 1) = x - u_1 - b \tag{9}$$

wat zou betekenen dat we u_1 en u_2 (en dus h) gevonden hebben. Voor het vinden van zo'n b gebruiken we het volgende lemma.

Lemma 2.3.4 *Voor $a_1, a_2 \in (\mathbb{Z}/p\mathbb{Z})$ met $a_1 \neq a_2$ geldt*

$$\#\{b : b \in (\mathbb{Z}/p\mathbb{Z}),\ a_1 + b \text{ en } a_2 + b \text{ zijn van verschillend type}\} = \frac{p-1}{2}$$

Met verschillend type bedoelen we dat beide niet 0 zijn en dat precies één van de twee een kwadratische rest is modulo p.

Bewijs. $a_1 + b$ en $a_2 + b$ zijn van verschillend type dan en slechts dan als beide ongelijk zijn aan 0 en met Eulers criterium

$$\left(\frac{a_1 + b}{a_2 + b}\right)^{(p-1)/2} \not\equiv 1 \pmod{p},$$

want dit quotiënt is equivalent aan 1 dan en slechts dan als de teller en noemer beide equivalent zijn aan 1 of beide equivalent zijn aan -1.

Aangezien voor elke $x \in (\mathbb{Z}/p\mathbb{Z})^*$ geldt dat $x^{p-1} \equiv 1 \pmod{p}$, geldt dus

$$\left(\frac{a_1 + b}{a_2 + b}\right)^{(p-1)/2} \equiv -1 \pmod{p}.$$

We hebben al gezien dat $x^{2k} - 1$ precies de $\frac{p-1}{2}$ kwadratische resten als nulpunt heeft in $(\mathbb{Z}/p\mathbb{Z})$. Bekijk de afbeelding

$$\phi : ((\mathbb{Z}/p\mathbb{Z}) - \{-a_2\}) \longrightarrow ((\mathbb{Z}/p\mathbb{Z}) - \{1\}), \qquad \phi(b) = \frac{a_1 + b}{a_2 + b}$$

Dit is welgedefinieerd, omdat voor elke $b \in ((\mathbb{Z}/p\mathbb{Z}) - \{-a_2\})$ geldt dat $a_2 + b \neq 0$
Stel $\frac{a_1+b}{a_2+b} \equiv \frac{a_1+b'}{a_2+b'} \pmod{p}$, dan

$$\begin{aligned}
(a_1 + b)(a_2 + b') &\equiv (a_1 + b')(a_2 + b) \\
a_1 b' + a_2 b &\equiv a_1 b + a_2 b' \\
(a_1 - a_2)b' &\equiv (a_1 - a_2)b \\
b &\equiv b' \qquad\qquad (\text{want } a_1 \not\equiv a_2)
\end{aligned}$$

Dus ϕ is een bijectie. Dit betekent dat er voor precies $\frac{p-1}{2}$ waardes b geldt dat $\phi(b)^{(p-1)/2} = -1$ □

Dit betekent dat we de gezochte b gemiddeld in $\frac{2p}{p-1} \approx 2$ pogingen zullen vinden als we hem willekeurig pakken uit $(\mathbb{Z}/p\mathbb{Z})$.

De volgende stap is om de ggd te berekenen zoals in (9). Schrijf $2k$ in binaire representatie, dus $2k = 2^{d_1} + 2^{d_2} + \cdots + 2^{d_m}$. Als dan $d = 2^r$ voor een natuurlijk getal r, kan $t^r \pmod{f_b(x)}$ berekend worden door herhaald x te kwadrateren mod $f_b(x)$, dus met

$$g_1 \equiv x^2 \pmod{f_b(x)}, \quad g_2 \equiv g_1^2 \pmod{f_b(x)}, \ldots, \quad g_r \equiv g_{r-1}^2 \pmod{f_b(x)}.$$

Omdat $f_b(x) = x^2 - 2bx + b^2 + 1$, zal elke g_i van de vorm $c_0x + c_1$ zijn met $c_0, c_1 \in (\mathbb{Z}/p\mathbb{Z})$. Dit betekent dat er een vaste bovengrens bestaat voor het berekenen van g_{i+1} uit g_i die afhangt van f_b en niet van g_i, dus kan $x^{2^i} \pmod{f_b(x)}$, met $0 \leq i \leq \log_2 p$ berekend worden in $\mathcal{O}(\log p)$ operaties. Noem nu $g(x) = x^{2k} \pmod{f_b x}$, aangezien $2k = 2^{d_1} + 2^{d_2} + \cdots + 2^{d_m}$ kan $g(x)$ met m vermenigvuldigingen uitgerekend worden. Omdat geldt $\text{ggd}(f_b(x), x^{2k}-1) = \text{ggd}(f_b x, g(x)-1)$ kan (9) in $\mathcal{O}(\log p)$ operaties berekend worden.

Van het algoritme van Euclides voor n en m is bekend dat dit gemiddeld in polynomiale tijd berekend kan worden.

Dit alles bij elkaar betekent dat het algoritme van Brillhart in verwachte polynomiale tijd uitgevoerd kan worden.

2.3.3 Rabin

In 1977 publiceerde Rabin een algoritme dat ook gebruik maakt van het algoritme van Euclides en vergelijkbare complexiteit heeft. Dit algoritme is later uitgebreider besproken in een artikel van Rabin en Shallit [5] en gaat als volgt.

1. Vind een $h \in (\mathbb{Z}/p\mathbb{Z})$ zodanig dat $h^2 \equiv -1 \pmod{p}$
2. Bereken $\text{ggd}(h + i, p) = x + iy$ binnen $\mathbb{Z}[i]$, dan $p = x^2 + y^2$

Laten we weer naar ons voorbeeld $p = 29$ gaan kijken. We krijgen net als in Sectie 2.3.2 dat $h = 12$. Het algoritme van Euclides met 29 en $12 + 9$ geeft nu

$$\begin{aligned} 29 &= 2(12 + i) + (5 - 2i), \\ 12 + i &= (2 + i)(5 - 2i) + 0. \end{aligned}$$

Dus $\text{ggd}(29, 12 + i) = 5 - 2i$ en $p = 5^2 + (-2)^2$.

Aangezien $h^2 \equiv -1 \pmod{p}$, geldt $(h+i)(h-i) = h^2+1 = mp$ voor een $m \in \mathbb{Z}$. $h \in (\mathbb{Z}/p\mathbb{Z})$ betekent dat $h < p$ en dus $N(h+i) = N(h-i) = h^2 + 1 < p^2$. Dus $1 < N(\text{ggd}(u + i, p)) < N(p)$ wat betekent dat $\text{ggd}(u + i, p) = x + iy$ een deler is van p, dus $N(x + iy) = x^2 + y^2$ is een deler van $N(p) = p^2$.

We hebben in de Sectie 2.3.2 gezien dat we h met $\mathcal{O}(\log p)$ operaties kunnen berekenen. De complexiteit van het algoritme van Euclides voor $z, w \in \mathbb{Z}[i]$ hangt van de norm van z en w af. Dit is omdat delen met rest vereist dat de norm van de rest kleiner is dan beide startwaardes en bij het algoritme van Euclides binnen de natuurlijke getallen moet de rest kleiner zijn dat beide startwaarde. Dit betekent dat de complexiteit van het algoritme van Euclides voor $z, w \in \mathbb{Z}[i]$ gelijk is aan $\mathcal{O}(\log(\max(N(z), N(w)))$. Aangezien bij het algoritme van Rabin de norm van p de grootste norm is bij het algoritme van Euclides, is ook het algoritme van Rabin uit te voeren in $\mathcal{O}(\log p)$ operaties.

2.4 Jacobsthal en Gauss

In 1906 publiceerde Jacobsthal een artikel waarin hij een constructie gaf voor het bepalen van de representatie van een priemgetal $p \equiv 1 \pmod 4$ als som van twee kwadraten. Gauss gaf in 1825 een formule voor het vinden van de representatie die een speciaal geval is van Jacobsthals constructie. Beide worden besproken in [4] en [9]. Ook al zijn dit geen efficiënte manieren om de representatie te bepalen (beide $\mathcal{O}(p)$ zoals beschreven in [9]) is het toch interessant om te bekijken. Jacobsthals formule maakt gebruik van het Legendre-symbool zoals gedefinieerd bij 2.3.2.

Jacobsthals constructie is als volgt:

1. kies $a, b \in \mathbb{Z}$ met $\left(\frac{a}{p}\right) = 1, \left(\frac{b}{p}\right) = -1$
2. bereken $\quad x = \frac{1}{2}\sum_{n=1}^{p-1}\left(\frac{n(n^2-a)}{p}\right), \quad y = \frac{1}{2}\sum_{n=1}^{p-1}\left(\frac{n(n^2-b)}{p}\right)$

   Dan is $p = x^2 + y^2$.

Het mooie van deze constructie is dat het heel overzichtelijk is wat er berekend moet worden, echter is is het berekenen van $2p-2$ Legendre-symbolen niet zeer efficiënt.

Gauss's formule is als volgt

Stelling 2.4.1 *Als p een priemgetal is met $p = 4k+1$ voor een $k \in \mathbb{N}$ en*

$$x \equiv \frac{(2k)!}{2(k!)^2} \pmod p, \qquad y \equiv (2k)!x \pmod p$$

dan $p = x^2 + y^2$.

Deze x is gelijk aan Jacobsthals constructie met $a = -1$.
Dit geeft $x = \frac{1}{2}\sum_{n=1}^{p-1}\left(\frac{n(n^2+1)}{p}\right)$.

Met Eulers criterium zien we dat $\left(\frac{n(n^2+1)}{p}\right) \equiv (n^3+n)^{2k} \pmod p$.
Omdat voor alle $n \in \mathbb{N}$ geldt dat $n^{p-1} \equiv 1 \pmod p$ krijgen we

$$\sum_{n=1}^{p-1} n^i \equiv \begin{cases} 0 \pmod p & \text{als } i \not\equiv 0 \pmod{p-1} \\ 1 \pmod p & \text{als } i \equiv 0 \pmod{p-1} \end{cases}$$

en dus $x \equiv \frac{(2k)!}{2(k!)^2} \pmod p$.

Al hoewel we hieruit y niet specifiek op de manier van Gauss kunnen vinden, weten we dat $p = x^2 + y^2$ dus $y = \sqrt{p - x^2}$.

2.5 Representatie van natuurlijke getallen

We hebben nu een aantal algoritmes besproken die priemgetallen $p \equiv 1 \pmod 4$ als som van twee kwadraten kunnen representeren, maar hebben nog geen algoritme gegeven dat dit doet voor alle representeerbare natuurlijke getallen.

Het algoritme van Legendre werkt voor alle getallen n waarvoor $\sqrt{n}$ een oneven periode heeft. Perron laat in [11] Satz 3.19 zien dat dit alle getallen zijn die te schrijven zijn als som van twee coprieme kwadraten. In het bijzonder geldt dit dus voor kwadraatvrije natuurlijke getallen.

De algoritmes zoals besproken in Sectie 2.3 werken voor alle getallen n waarvoor -1 een kwadratische rest is modulo n. Aangezien dit voor lang niet alle natuurlijke getallen geldt, werkt dit algoritme in het algemeen niet voor de natuurlijke getallen.

We zien dus dat de eerder beproken algoritmes niet in het algemeen zullen werken er zijn ook nog geen efficiënte algoritmes bekend die dit wel kunnen. We kunnen voor een natuurlijk getal n voor alle paren van natuurlijke getallen $x, y \leq \sqrt{n}$ proberen of $x^2 + y^2 = n$, maar dit is voor grotere n een heel traag algoritme.

Wat we ook zouden kunnen doen om n te representeren als som van twee kwadraten, is de priemfactorisatie zoeken. We weten uit eerdere resultaten dat elke priemgetal $p \equiv 3 \pmod 4$ in even macht voorkomt in de priemfactorisatie van n en we kunnen met de eerdere algoritmes de priemgetallen $q \equiv 1 \pmod 4$ schrijven als som van twee kwadraten. We weten ook dat het product van sommen van twee kwadraten weer een som van twee kwadraten oplevert. Het probleem met deze methode is dat het vinden van de priemfactorisatie heel erg inefficiënt is, zelfs zo inefficiënt dat dit het principe is waar verschillende encryptiemethodes gebruik van maken.

3 Som van drie kwadraten

3.1 Representeerbare getallen

3.1.1 Kwadratische vormen

In deze sectie gaan we bewijzen welke getallen representeerbaar zijn als som van drie kwadraten. Dit zullen we doen met een bekend bewijs van Dirichlet dat beschreven staat in Chapter 4 van [6]. Dit bewijs maakt gebruik van kwadratische vormen.

Definitie 3.1.1 *Een **kwadratische vorm** is een veelterm van de vorm*

$$Q(x_1, x_2, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j.$$

Dus een homogene veelterm van graad 2.

Als we het over een **gehele kwadratische vorm** hebben zullen we bedoelen dat $a_{ii} \in \mathbb{Z}$ en voor $i \neq j, a_{ij} + a_{ji} \in \mathbb{Z}$. Vanaf nu zullen we met kwadratische vormen altijd gehele kwadratische vormen bedoelen. We mogen aannemen dat $a_{ij} = a_{ji}$ aangezien dit dezelfde veeltermen oplevert en zullen dit vanaf nu ook doen.

Definitie 3.1.2 *De determinant van de matrix $A = (a_{ij})$ die bestaat uit de coëfficiënten van $Q(x_1, \ldots, x_n)$ heet de **determinant van Q** en wordt genoteerd door d(Q).*

We kunnen het verband tussen A en Q eenvoudig laten zien. Als we x de kolomvector van $x_1, x_2, \ldots, x_n$ nemen, dan geldt voor $\cdot$ het inproduct en x^t de getransponeerde van x

$$x^t \cdot (Ax) = Q(x_1, x_2, \ldots, x_n).$$

Zij $C = (c_{ij})$ een matrix met gehele coëfficiënten. Als we $y_1, \ldots, y_n$ definiëren door

$$x_i = \sum_{j=1}^{n} c_{ij} y_j \tag{10}$$

en als de determinant $|C|$ van C gelijk is aan 1

$$y_j = \sum_{i=1}^{n} d_{ji} x_i \tag{11}$$

met d_{ji} gehele getallen en de x_i's van een kwadratische vorm $Q(x_1, \ldots, x_n)$ vervangen door de (10) gedefinieerde waardes, krijgen we een nieuwe kwadratische vorm $Q_1(y_1, \ldots, y_n)$. We zeggen dat als Q en Q_1 door (10) en (11) in elkaar te transformeren zijn dat $Q \sim Q_1$. Het is direct te zien dat $\sim$ een equivalentierelatie is.

Definitie 3.1.3 *We noemen een kwadratische vorm Q met bijbehorende matrix $A = (a_{ij})_{i,j\in\{1,2,\ldots,k\}}$ een **kwadratische diagonaalvorm** als voor alle $i, j \in \{1, 2, \ldots, k\}$ geldt $a_{ii} \neq 0$ en voor $i \neq j$ geldt $a_{ij} = 0$.*

Als Q een kwadtratische diagonaalvorm is zonder negatieve coëfficiënten is $Q = \sum_{i=0}^{k} a_{ii}x_i^2$ een som van kwadraten. Als Q_1 met de eerder gedefinieerde equivalentierelatie $\sim$ equivalent is aan een zo'n Q, dan noemen we Q_1 **positief definiet**.

3.1.2 De representeerbare getallen

Grosswald bewijst in Chapter 4.5 van [6] de volgende twee lemmas.

Lemma 3.1.4 *Een kwadratische vorm $Q = \sum_{i,j=1}^{3} a_{ij}x_ix_j$ is positief definiet dan en slechts dan als alle leidende hoofdminoren van de bijbehorende matrix $A = (a_{ij})$ positief zijn. Dit wil zeggen dat*

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} > 0, \qquad \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} > 0, \qquad |a_{11}| > 0.$$

Lemma 3.1.5 *Elke positief definiete kwadratische vorm $Q = \sum_{i,j=1}^{3} a_{ij}x_ix_j$ met determinant 1 is equivalent aan een som van drie kwadraten.*

Dit betekent dat wanneer we voor een natuurlijk getal n een positief definite kwadratische vorm $Q = \sum_{i,j=1}^{3} a_{ij}x_ix_j$ vinden die voor zekere x_1, x_2 en x_3 gelijk is aan n, hij te representeren is als som van drie kwadraten.

Stelling 3.1.6 (Legendres drie kwadraten stelling) *Een natuurlijk getal n is te schrijven als som van drie kwadraten tenzij $n = 4^a(8k + 7)$ met $a, k \in \mathbb{N}$.*

Bewijs. Stel $n \equiv 4^a(8k + 7)$ met $a, k \in \mathbb{N}$, als $a > 0$ dan is n deelbaar door 4^a en omdat geldt

$$x^2 + y^2 + z^2 = \frac{n}{4} \Leftrightarrow (2x)^2 + (2y)^2 + (2z)^2 = n,$$

geldt ook: $4^a(8k + 7)$ is te schrijven als som van drie kwadraten dan en slechts dan als $8k + 7$ te schrijven is als som van drie kwadraten.

Aangezien 0, 1 en 4 alle kwadratische resten mod 8 zijn, kan een som van drie kwadraten nooit 7 mod 8 zijn, dus n is niet te schrijven als som van drie kwadraten.

Stel n natuurlijk getal met $n \neq 4^a(8k+7)$ voor $a, k \in \mathbb{N}$. Bekijk de kwadratische vorm

$$Q(x_1, x_2, x_3) = a_{11}x_1^2 + 2a_{12}x_1x_2 + 2x_1x_3 + a_{22}x_2^2 + nx_3^2,$$

dan $Q(0, 0, 1) = n$, dus als Q positief definiet is en determinant 1 heeft, is n te schrijven als som van drie kwadraten. Met Lemma 3.1.4 en lemma zien we dat

hiervoor moet gelden dat

$$a_{11} > 0, \qquad b = a_{11}a_{22} - a_{12}^2 > 0, \qquad d = \begin{vmatrix} a_{11} & a_{12} & 1 \\ a_{21} & a_{22} & 0 \\ 1 & 0 & n \end{vmatrix} = 1.$$

Aangezien $d = nb - a_{22}$ en kan de laatste conditie vervangen worden door $a_{22} = bn - 1$. Hiermee zien we voor $n \geq 2$ als aan de tweede conditie voldaan is dat $a_{22} = nb - 1 \geq 2b - 1 > 0$ en $a_{11}a_{22} = a_{12}^2 + b > 0$, dus $a_1 1 > 0$. Dit betekent dat we de eerste conditie kunnen schrappen.

Om te laten zien dat we de geschikte a_{ij} kunen krijgen gebruiken we een bekende stelling van Dirichlet die zegt dat voor $\text{ggd}(k, m) = 1$ geldt dat $\{kr + m \mid r \in \mathbb{N}\}$ oneindig veel priemgetallen bevat.

Stel $n \equiv 2 \pmod 8$ of $n \equiv 6 \pmod 8$. Omdat $\text{ggd}(4n, n-1) = 1$ zien we met Dirichlets stelling dat er een $m \in \mathbb{Z}$ en een priemgetal p bestaan zodanig dat $4nm + (n-1) = p$. Neem $b = 4m + 1$ zodat $p = bn - 1$, dan zien we met het Legendresymbool en Jacobisymbool dat

$$\left(\frac{-b}{p}\right) = \left(\frac{b}{p}\right) = \left(\frac{p}{b}\right) = \left(\frac{bn-1}{p}\right) = \left(\frac{-1}{b}\right) = 1.$$

Dit gebruikt wat theorie over Jacobisymbolen wat niet besproken is in deze scriptie, dit is wel te vinden in Chapter 5.2 van [8]. Dit betekent dat $a_{22} = bn - 1 = p > 0$ en dat $-b \equiv a_{12}^2 \pmod p$ een oplossing heeft. Hiermee zien we ook dat a_{22} een deler is van b en dat $a_{11} = (b + a_{12}^2)/a_{22}$ een geheel getal is en dus dat er een positief definiete Q bestaat met determinant 1 die n aanneemt, dus n is te schrijven als som van drie kwadraten.

Stel $n \equiv 1 \pmod 8$ of $n \equiv 3 \pmod 8$ of $n \equiv 5 \pmod 8$. Kies een $c \in \mathbb{N}$ zodanig dat $cn - 1 \equiv 2 \pmod 4$, dan $\text{ggd}(4n, (cn-1)/2) = 1$ en bestaan er volgens Dirichlets stelling een $m \in \mathbb{N}$ en een priemgetal p zodanig dat $4nm + (cn-1)/2 = p$. Neem $b = 8m + c$, dan geldt $2p = (8m + c)n - 1 = bn - 1$. We kunnen nu door slim te rekenen met Jacobisymolen zien dat voor alle drie gevallen $-b$ een kwadratische rest is modulo 8.

Bijvoorbeeld voor $n \equiv 1 \pmod 8$, kunnen we $c = 3$ nemen, zodat $b \equiv 3 \pmod 8$ en $p \equiv (2n-1)/2 \equiv 1 \pmod 4$. Omdat $\left(\frac{-2}{b}\right) = \left(\frac{-1}{b}\right)\left(\frac{2}{b}\right) = 1$, krijgen we

$$\left(\frac{-b}{p}\right) = \left(\frac{b}{p}\right)\left(\frac{-2}{b}\right) = \left(\frac{-2p}{b}\right) = \left(\frac{1-bn}{b}\right) = \left(\frac{1}{b}\right) = 1.$$

Nu zien we op dezelfde manier als bij $n \equiv 2 \pmod 8$ en $n \equiv 6 \pmod 8$ dat $a_{22} = bn - 1 = 2p$ en dat zowel $-b \equiv x^2 \pmod p$ als $-b \equiv x^2 \pmod 2$ een oplossing hebben. Dus $-b \equiv a_{12}^2 \pmod{2p}$ heeft een oplossing zodat $a_{11} = (b + a_{12}^2)/a_{22}$ een geheel getal is. Dit betekent dat er een positief definiete Q bestaat met determinant 1 die n aanneemt.

Stel $n \equiv 0 \pmod 8$ of $n \equiv 4 \pmod 8$, dan geldt $n \equiv 0 \pmod 4$ en is n deelbaar

door 4, wat betekent zoals we eerder gezien hebben dat n te schrijven is als som van drie kwadraten dan en slechts dan als $\frac{n}{4}$ dat is. Dit betekent dat tenzij $n = 4^a(8k+7)$ voor bepaalde $a, k \in \mathbb{N}$, we altijd door herhaaldelijk door 4 te delen op een van de andere situaties uitkomen. □

3.2 Rabin en Shallit voor priemgetallen als som van drie kwadraten

In deze sectie gaan we een algoritme uit [5] bespreken dat een priemgetallen $p \not\equiv 7 \pmod 8$ als som van 3 kwadraten representeert. Als $p = 2$ of $p \equiv 1 \pmod 4$ kunnen we met verschillende algoritmes uit Sectie 2 een representatie voor p als som van twee kwadraten vinden. We hoeven dus alleen het geval $p \equiv 3 \pmod 8$ te bekijken. We zullen dit gaan doen met behulp van het algoritme voor het vinden van $h \equiv -1 \pmod p$ uit Sectie 2.3.2 en het algoritme voor de representatie als som van twee kwadraten uit Sectie 2.3.3. Hiernaast zullen we een paar lemmas nodig hebben.

Lemma 3.2.1 *$\mathbb{Z}[\sqrt{-2}]$ is een Euclidisch domein. Dit wil zeggen dat we het algoritme van Euclides kunnen toepassen binnen $\mathbb{Z}[\sqrt{-2}]$.*

Bewijs. Het is duidelijk dat $\mathbb{Z}[\sqrt{-2}]$ een commutative ring is. Definieer binnen $\mathbb{Z}[\sqrt{-2}]$ voor $z = a + b\sqrt{-2}$ dat $|z| = \sqrt{a^2 + 2b^2}$. Stel we hebben $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$ en bekijk een rooster van rechthoeken met breedte $|\beta|$ en lengte $\left|\beta\sqrt{-2}\right| = \sqrt{2}\,|\beta|$ waarvan de eerste hoekpunten 0, β, $\beta\sqrt{-2}$ en $\beta(1+\sqrt{-2})$ heeft. Noem de afstand van α tot het dichtstbijzijnde hoekpunt van het rooster ρ. Aangezien de afstand van een hoekpunt tot het middelpunt van een rechthoek in het rooster gelijk is aan $\sqrt{\left(\frac{|\beta|}{2}\right)^2 + \left(\frac{|\beta|}{\sqrt{2}}\right)^2}$ en α maximaal die afstand van een hoekpunt op het rooster ligt, geldt

$$\begin{aligned} |\rho|^2 &\leq \left(\frac{|\beta|}{2}\right)^2 + \left(\frac{|\beta|}{\sqrt{2}}\right)^2 \\ &= \frac{3\,|\beta|^2}{4}. \end{aligned}$$

Dus er bestaan voor iedere α en β een μ en een ρ zodanig dat $\alpha = \mu\beta + \rho$ en $|\rho| < |\beta|$. Dit betekent dat we het algoritme van Euclides toe kunnen passen binnen $\mathbb{Z}[\sqrt{-2}]$. □

Lemma 3.2.2 (Het lemma van Gauss) *Laat p een oneven priemgetal zijn en a een geheel getal dat copriem is met p. Definieer*

$$n = \left|\left\{ma \mid m \in \mathbb{N},\ \ 1 \leq m \leq \frac{p-1}{2},\ \ ma \pmod p \text{ is groter dan } \frac{p-1}{2}\right\}\right|.$$

Dan geldt $\left(\frac{a}{p}\right) = (-1)^n$.

Bewijs. Neem $Z = a \cdot 2a \cdot 3a \cdot \cdots \cdot \frac{p-1}{2}a$, dan hebben we $\frac{p-1}{2}$ termen en geldt dus $Z \equiv a^{(p-1)/2} \left(1 \cdot 2 \cdot 3 \cdot \cdots \cdot \frac{p-1}{2}\right) \pmod{p}$.

Definieer nu de functie f als volgt

$$f(x) = \begin{cases} x & \text{als } 1 \leq x \leq \frac{p-1}{2}, \\ p - x & \text{als } \frac{p-1}{2} \leq p-1. \end{cases}$$

Aangezien $p - x \equiv x \pmod{p}$ en n het aantal keer is dat een term uit Z in het tweede geval van f valt, krijgen we

$$Z \equiv (-1)^n \left(f(a) \cdot f(2a) \cdot \cdots \cdot f(\frac{p-1}{2}a) \right).$$

Stel $f(ra) \equiv f(sa) \pmod{p}$ voor $r, s \in \mathbb{N}$, dan geldt $r \equiv \pm s \pmod{p}$. Dit betekent dat alle $f(a), f(2a), \ldots, f(\frac{p-1}{2}a)$ allemaal verschillend zijn en dus geldt

$$Z \equiv (-1)^n \left(1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2}\right) \pmod{p}.$$

Dit betekent dat

$$a^{(p-1)/2} \left(1 \cdot 2 \cdot 3 \cdot \cdots \cdot \frac{p-1}{2}\right) \equiv (-1)^n \left(1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2}\right) \pmod{p},$$

en omdat $\left(1 \cdot 2 \cdot 3 \cdot \cdots \cdot \frac{p-1}{2}\right) \not\equiv 0 \pmod{p}$, krijgen we

$$a^{(p-1)/2} \equiv (-1)^n \pmod{p}.$$

□

Lemma 3.2.3 *-2 is een kwadratische rest voor $p \equiv 3 \pmod{8}$.*

Bewijs. We gaan het lemma van Gauss gebruiken, dus we bekijken

$$-2 \cdot 1, -2 \cdot 2, \ldots, -2 \cdot \frac{p-1}{2}.$$

We zien dat er hiervan $\lfloor \frac{p-1}{2} \rfloor$ groter zijn dan $p-1$ modulo p. Dus als $p = 8k+3$ voor een $k \in \mathbb{N}$, dan is n, zoals in het lemma van Gauss, gelijk aan $2k$. Dus $\left(\frac{-2}{p}\right) = (-1)^{2k} = 1$. □

Als we nu het algoritme voor het vinden van $h \equiv -1 \pmod{p}$ uit Sectie 2.3.2 iets aanpassen, door f_b aan te passen naar

$$f_b(x) = (x-b)^2 + 2,$$

vinden we een $h \equiv -2 \pmod{p}$. We kunnen nu zoals in Sectie 2.3.3 met het algoritme van Euclides een representatie voor p vinden. Echter moeten we dit nu in $\mathbb{Z}[\sqrt{-2}]$ doen. Want $\text{ggd}(h + \sqrt{-2}, p) = x^2 + 2y^2$ voor bepaalde $x, y \in \mathbb{Z}$ en $N(h + \sqrt{-2}) = N(h - \sqrt{-2}) < N(p)$, dus $p = x^2 + y^2 + y^2$.

Aangezien we nu voor elke situatie het algoritme van Rabin voor twee kwadraten kunnen toepassen, is dit algoritme ook uit te voeren in $\mathcal{O}(\log p)$ operaties.

3.3 Algoritme gebaseerd op vermoedens

Rabin en Shallit [5] gaven ook een algoritme voor het representeren van (bijna) alle natuurlijke getallen die representeerbaar zijn als som van 3 kwadraten. De efficiëntie van dit algoritme hangt echter af van een aantal vermoedens.

Vermoeden 3.3.1 *Conjecture H van Hardy en Littlewood. Elk groot genoeg natuurlijk getal n is een kwadraat of de som van een priemgetal en een kwadraat. Het aantal oplossingen $N(n)$ hiervoor is*

$$N(n) \sim \frac{\sqrt{n}}{\log n} C(n),$$

met $C(n)$ gedefinieerd als

$$C(n) = \prod_{p \text{ een oneven priemgetal}} 1 - \frac{(\frac{n}{p})}{p-1}$$

Met groot genoeg wordt bedoeld dat er een natuurlijk getal N bestaat zodanig dat het geldt voor elke $n > N$.

$\frac{\sqrt{n}}{\log n}$ is al een redelijke schatting, aangezien er ongeveer $\sqrt{n}$ kwadraten kleiner zijn dan n en van deze kwadraten zijn er ongeveer $\log n$ priem.

Voor het volgende vermoeden bestaat al een bewijs, maar dit hangt af van het waar zijn van de Riemann Hypothese.

Vermoeden 3.3.2 *Er bestaat een constante $M \in \mathbb{N}$ zodanig dat*

$$C(n) > \frac{M}{\log \log n}.$$

Het laatste vermoeden die we nodig hebben gaat over een meer specifiek geval.

Vermoeden 3.3.3 *Elk natuurlijk getal $n = 8k + 3$ met $k \geq 1$ kan geschreven worden als som van een kwadraat en twee keer een priemgetal, dus*

$$n = x^2 + 2p$$

voor een $x \in \mathbb{N}$ en een priemgetal p.
Het aantal verschillende presentaties is

$$M(k) \sim \frac{\sqrt{k}}{2 \log k} C(k)$$

Met C(k) hetzelfde als vermoeden 3.3.1.

Met het aannemen van deze vermoedens beschrijven we het algoritme als volgt: Stel N is representeerbaar als som van 3 kwadraten, dan $N \neq 4^a(8k + 7)$ voor elke $a, k \in \mathbb{N}$.

Als N een kwadraat is zijn we klaar.

Als $N \equiv 0 \pmod 4$ voer dan het algoritme uit op $\frac{N}{4}$; als $x^2 + y^2 + z^2 = \frac{N}{4}$ dan $(2x)^2 + (2y)^2 + (2z)^2 = N$.

Als $N \equiv 3 \pmod 8$

1. Neem x een willekeurig natuurlijk getal met $x \leq \sqrt{N}$.
2. Bereken $p = \frac{1}{2}(n - x^2)$.
3. Herhaal dit totdat p priem is.
4. Bereken y, z zodanig dat $p = y^2 + z^2$, dan is $N = x^2 + (y + z)^2 + (y - z)^2$

Als $N \equiv 1 \pmod 4$ of $N \equiv 2 \pmod 4$

1. Neem x een willekeurig natuurlijk getal met $x \leq \sqrt{N}$.
2. Bereken $p = n - x^2$.
3. Herhaal totdat p priem is.
4. Bereken y, z zodanig dat $p = y^2 + z^2$, dan is $N = x^2 + y^2 + z^2$

We moeten nog bewijzen dat in deze laatste twee gevallen $p = 2$ of $p \equiv 1 \pmod 4$ want anders kunnen we geen kwadraatrepresentatie bepalen voor p.

Stel $n \equiv 3 \pmod 8$, als $n = x^2 + 2p$, dan $x^2 + 2p \equiv 3 \pmod 8$. Aangezien $0, 1$ en 4 de kwadratische resten zijn in $(\mathbb{Z}/8\mathbb{Z})$, moet gelden dat $2p \equiv 2$, 3 of $7 \pmod 8$ en dus $p \equiv 1$ of $5 \pmod 8$ wat betekent dat $p \equiv 1 \pmod 4$.

Stel $n \equiv 1 \pmod 4$ en $n = x^2 + p$, dan $x^2 + p \equiv 1 \pmod 4$. Omdat 0 en 1 de kwadratische resten zijn in $(\mathbb{Z}/4\mathbb{Z})$, geldt dus dat $p \equiv 0 \pmod 4$ of $p \equiv 1 \pmod 4$. Als $p \equiv 0 \pmod 4$, dan kan p geen priem zijn, dus $p \equiv 1 \pmod 4$.

Stel $n \equiv 2 \pmod 4$ en $n = x^2 + p$, dan kunnen we het vorige argument gebruiken om te zien dat $p \equiv 1 \pmod 4$ of $p \equiv 2 \pmod 4$ en het enige priemgetal dat gelijk is aan $2 \pmod 4$ is 2.

Dus als vermoedens 3.3.1, 3.3.2 en 3.3.3 waar zijn, dan kunnen we elk groot genoeg natuurlijk getal binnen verwachte polynomiale tijd als som van drie kwadraten schrijven.

4 Som van vier kwadraten

In de volgende twee secties gaan we bewijzen welke getallen representeerbaar zijn als som van vier kwadraten. Er zijn verschillende manieren om dit te bewijzen, wij zullen hier de Hurwitz quaternionen voor gebruiken, omdat deze later terug zullen komen bij een algoritme voor de representatie. Dit bewijs zal in het algemeen het bewijs van Stillwell uit [13] volgen.

4.1 Hurwitz quaternionen

Definitie 4.1.1 *De **Hurwitz quaternionen** is de verzameling*

$$\mathbb{H} := \left\{ a + bi + cj + dk : \text{ alle } a,b,c,d \in \mathbb{Z} \text{ of alle } a,b,c,d \in (\mathbb{Z} + \frac{1}{2}) \right\}$$

waar i, j en k zo gedefinieerd zijn als bij de gewone quaternionen.

De Hurwitz quaternionen zijn dus gelijk aan de verzameling $\mathbb{Z}[\frac{1+i+j+k}{2}, i, j, k]$. De norm op de Hurwitz quaternionen is gedefinieerd als $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2 = |a + bi + cj + dk|^2$.

Het is aan te tonen dat voor elke $\alpha, \beta \in \mathbb{H}$ er een $\mu \in \mathbb{H}$ bestaat zodanig dat $|\alpha - \mu\beta| < |\beta|$, wat niet zo is bij de gewone quaternionen. Hierdoor kunnen we het algoritme van Euclides niet toe passen op de gewone quaternionen.

Stel $a, b, c, d \in \mathbb{Z}$ dan $N(a + bi + cj + dk) \in \mathbb{Z}$. Stel $a, b, c, d \in (\mathbb{Z} + \frac{1}{2})$ dan zijn er $a', b', c', d' \equiv 1 \pmod 2$ zodanig dat $\frac{a'}{2} = a$, $\frac{b'}{2} = b$, $\frac{c'}{2} = c$, $\frac{d'}{2} = d$

$$\begin{aligned} N(a + bi + cj + dk) &= a^2 + b^2 + c^2 + d^2 \\ &= \frac{a'}{2}^2 + \frac{b'}{2}^2 + \frac{c'}{2}^2 + \frac{d'}{2}^2 \\ &= \frac{a'^2 + b'^2 + c'^2 + d'^2}{4} \end{aligned}$$

Aangezien $a', b', c', d' \equiv 1 \pmod 2$ geldt $a'^2, b'^2, c'^2, d'^2 \equiv 1 \pmod 4$ dus $N(a + bi + cj + dk) \in \mathbb{Z}$. Ook zijn de Hurwitz quaternionen gesloten onder optellen, aftrekken en vermenigvuldigen. Dit wil zeggen dat de Hurwitz quaternionen gehele getallen zijn en we priemelementen in de Hurwitz quaternionen kunnen definiëren.

Definitie 4.1.2 *Een **priemelement in de Hurwitz quaterionen** is een element uit de Hurwitz quaternionen van norm groter dan 1 die geen product is van twee elementen van norm groter dan 1.*

Net zoals bij de gehelen van Gauss en de quaternionen hebben we bij de Hurwitz quaternionen geconjugeerdes.

Definitie 4.1.3 *Voor een quaternion $q = a+bi+cj+dk$ heet $\overline{q} = a-bi-cj-dk$ zijn **geconjugeerde**.*

We willen natuurlijk dat $q\overline{q} = N(q)$ en dat is ook zo

$$\begin{aligned} q\overline{q} &= (a + bi + cj + dk)(a - bi - cj - dk) \\ &= a^2 - abi - acj - adk + abi - (bi)^2 - bcij - bdik \\ &\quad + acj - bcji - (cj)^2 - cdjk + adk - bdki - cdkj - (dk)^2 \\ &= a^2 + b^2 - bck + bdj + bck + c^2 - cdi - bdj + cdi + d^2 \\ &= a^2 + b^2 + c^2 + d^2 \end{aligned}$$

Aangezien de Hurwitz quaternionen net zoals de gewone quaterionen niet commutatief zijn, kunnen we niet zomaar spreken van een grootste gemene deler, maar moeten we een linkerdeler of rechterdeler kiezen.

Definitie 4.1.4 *Voor twee quaternionen α en β is γ een **gemene rechter deler** als*

$$\alpha = \delta\gamma, \qquad \beta = \varepsilon\gamma \qquad \text{voor een } \delta, \varepsilon$$

*We noemen γ de **grootste gemene rechter deler*** (ggrd) *als γ de gemene rechter deler is met de grootste norm.*

Aangezien we het algoritme van Euclides toe kunnen passen op de Hurwitz quaternionen om de ggrd te berekenen, weten we dat

$$\text{ggrd}(\alpha, \beta) = \mu\alpha + \nu\beta$$

voor zekere $\mu, \nu \in \mathbb{H}$.

We kunnen deze eigenschap gebruiken om het volgende lemma te bewijzen

Lemma 4.1.5 *Als p een priemgetal is dat ook een priemelement is in $\mathbb{H}$ en p deelt $\alpha\beta$ dan is p een deler van α of β.*

Bewijs. Stel p deelt $\alpha\beta$ maar p is geen deler van α, dan geldt

$$\text{ggrd}(p, \alpha) = \mu p + \nu\alpha = 1$$

en dus

$$\beta\mu p + \beta\nu\alpha = \beta$$

Omdat per aanname p een deler is van $\alpha\beta$, is p een deler van het linker lid en dus ook het rechter lid. □

4.2 Representeerbare getallen

We gaan nu de Hurwitz quaternionen gebruiken om te bewijzen dat alle natuurlijke getallen te representeren zijn als som van vier kwadraten.

Lemma 4.2.1 *Elk priemgetal p dat geen priemelement is in $\mathbb{H}$, kan geschreven worden als som van vier kwadraten.*

Bewijs. Neem een priemgetal p dat geen priemelement uit $\mathbb{H}$ is. Dan geldt voor bepaalde $a, b, c, d \in \mathbb{Z}$ of $a, b, c, d \in (\mathbb{Z} + \frac{1}{2})$ en $\gamma \in \mathbb{H}$

$$p = (a + bi + cj + dk)\gamma$$

Aangezien p zijn eigen geconjugeerde is, geldt ook

$$p = \overline{\gamma}(a - bi - cj - dk)$$

Als we beide vergelijkingen vermenigvuldigen

$$\begin{aligned} p^2 &= (a + bi + cj + dk)\gamma\overline{\gamma}(a - bi - cj - dk) \\ &= (a + bi + cj + dk)(a - bi = cj = dk)\gamma\overline{\gamma} \\ &= (a^2 + b^2 + c^2 + d^2)|\gamma|^2 \end{aligned}$$

Met $(a^2+b^2+c^2+d^2), |\gamma|^2 \in \mathbb{Z}_{>1}$, maar p is priem, dus $a^2+b^2+c^2+d^2 = |\gamma|^2 = p$.

Elke Hurwitz quaternion $q = a+bi+cj+dk$ met $a, b, c, d \in (\mathbb{Z}+\frac{1}{2})$ kan geschreven worden als $q = \omega + a' + b'i + c'j + d'k$, met $a', b', c', d' \in 2\mathbb{Z}$ en $\omega = \frac{\pm 1 \pm i \pm j \pm k}{2}$. Dit geeft $\omega\overline{\omega} = 1$. Als we nu p uitschrijven krijgen we

$$\begin{aligned} p &= (a + bi + cj + dk)(a - bi - cj - dk) \\ &= (\omega + a' + b'i + c'j + d'k)(\overline{\omega} + a' - b'i - c'j - d'k) \\ &= (\omega + a' + b'i + c'j + d'k)\overline{\omega}\omega(\overline{\omega} + a' - b'i - c'j - d'k) \end{aligned}$$

We kunnen nu het eerste gedeelte uitrekenen

$$(\omega + a' + b'i + c'j + d'k)\overline{\omega} = \omega\overline{\omega} + (a' + b'i + c'j + d'k)\overline{\omega} = A + Bi + Cj + Dk$$

Aangezien $\omega\overline{\omega} = 1$ en $a', b', c', d' \in 2\mathbb{Z}$ geldt $A, B, C, D \in \mathbb{Z}$.

$$\overline{(\omega + a' + b'i + c'j + d'k)\overline{\omega}} = \omega(\overline{\omega} + a' - b'i - c'j - d'k)$$

Dus $p = A^2 + B^2 + C^2 + D^2$. □

We willen bewijzen dat elk oneven priemgetal geen priemelement is in $\mathbb{H}$, waardoor we met het vorige lemma elk oneven priemgetal als som van vier kwadraten kunnen schrijven. Hiervoor hebben we eerst nog het volgende lemma nodig.

Lemma 4.2.2 *Voor elk oneven priemgetal $p = 2n + 1$ bestaan er $l, m \in \mathbb{Z}$ zodanig dat p een deler is van $1 + l^2 + m^2$*

Bewijs. Stel $x, y \in \{0, 1, 2, \ldots, n\}$ met $x^2 \equiv y^2 \pmod{p}$ dan

$$\begin{aligned} x^2 - y^2 \equiv 0 \pmod{p} &\Rightarrow (x - y)(x + y) \equiv 0 \pmod{p} \\ &\Rightarrow x \equiv y \text{ of } x + y \equiv 0 \pmod{p} \end{aligned}$$

Maar $x, y \leq n$ dus als $x^2 \equiv y^2$ dan $x \equiv y \pmod{p}$. Dit geeft ons $n + 1$ incongruente kwadraten. Maar omdat nu alle x^2 voor $x \in \{0, 1, 2, \ldots, n\}$ incongruent

zijn, zijn alle $-1-x^2$ dit ook, dit geeft $n+1$ incongruente $-1-m^2$.

Aangezien er maar $2n+1$ incongruente waardes zijn, moeten er dus $l, m \in \{0, 1, 2, \ldots, n\}$ zijn zodanig dat

$$l^2 \equiv -1 - m^2 \pmod{p}$$

Dus is p een deler van $1 + l^2 + m^2$. □

We hebben nu alles wat nodig is om het volgende lemma te bewijzen.

Lemma 4.2.3 *Elk oneven priemgetal p kan geschreven worden als som van vier kwadraten*

Bewijs. We weten uit Lemma 4.2.2 dat een oneven priemgetal p deler is van $1 + l^2 + m^2$ voor bepaalde $l, m \in \mathbb{N}$.
Stel p is een priemelement in $\mathbb{H}$.

$$1 + l^2 + m^2 = (1 + li + mj)(1 - li - mj)$$

Dit betekent dat we met Lemma 4.1.5 weten dat p een deler is van $(1+li+mj)$ of van $(1-li-mj)$. Echter is $p > 2$ en dus is $\frac{1}{p}$ geen coëfficiënt dat als reëel deel voor kan komen bij de Hurwitz quaternionen, dus p is geen deler van $(1+li+mj)$ of $(1-li-mj)$, dus p is geen priemelement uit $\mathbb{H}$, dus p is met Lemma 4.2.1 p te schrijven als som van vier kwadraten. □

We kunnen nu met het vorige lemma bewijzen dat alle natuurlijke getallen te representeren zijn als som van vier kwadraten.

Stelling 4.2.4 (Lagranges vier kwadraten stelling) *Elk natuurlijk getal is te schrijven als som van vier kwadraten.*

Bewijs. Het is eenvoudig in te zien dat ook $0, 1$ en 2 te schrijven zijn als som van vier kwadraten, dus als we bewijzen dat een product van sommen van vier kwadraten weer een som van vier kwadraten oplevert zijn we klaar.

$$\begin{aligned}(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = \quad & (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 \\ & + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 \\ & + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 \\ & + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2\end{aligned}$$

Met inductie zien we dat dit geldt voor elk eindig product van sommen van vier kwadraten. □

4.3 Algoritme met behulp van priemgetallen

Het eerste algoritme dat we gaan bekijken voor het representeren van een natuurlijk getal n als som van vier kwadraten maakt gebruik van de constructie voor het vinden van $h \equiv -1 \pmod{p}$ uit Sectie 2.3.2 en is bedacht door Rabin

en besproken in [5].

Laat n een natuurlijk getal zijn en bekijk

$$n = x^2 + y^2 + p \tag{12}$$

met $x, y, p \in \mathbb{N}$ en p priem. Als we zo'n vergelijking vinden voor n met $p \equiv 1 \pmod 4$ kunnen we één van de algoritmes voor representatie als som van twee kwadraten toepassen op p zodat $p = z^2 + w^2$ en $n = x^2 + y^2 + z^2 + w^2$. Het hoeft natuurlijk niet zo te zijn dat we altijd zo'n p vinden, maar we kunnen wel het aantal mogelijkheden beperken.

Lemma 4.3.1 *Als $n = 2(2k + 1)$ voor een natuurlijk getal k en als x, y, p een oplossing is voor (12), dan $p = 2$ of $p \equiv 1 \pmod 4$.*

Bewijs. $n \equiv 2 \pmod 4$. De enige kwadratische resten in $(\mathbb{Z}/4\mathbb{Z})$ zijn 0 en 1. Als $x^2 \equiv y^2 \equiv 1 \pmod 4$ dan kan p geen priem zijn, maar was een eis. Als $x^2 \equiv y^2 \equiv 0 \pmod 4$, moet n gelijk zijn aan 2, anders is n geen priem. Als een van de twee rest 1 heeft $\mod 4$ dan $p \equiv 1 \pmod 4$. □

We gaan dit gebruiken om de representatie voor n te vinden.

Stel $n = 2(2k + 1)$ en kies willekeurig $x, y \leq \sqrt{n}$, als we zo'n x en y vinden, zodanig dat $p = n - x^2 - y^2$ een priemgetal is, kunnen we een algoritme voor het vinden van een twee kwadraten representatie voor p toepassen en zijn we klaar. Wat echter gemiddeld sneller is, is om niet te testen of p priem is, maar gewoon het algoritme voor het vinden van een twee kwadraat representatie van Rabin toe te passen. Je doet één poging om een b te vinden zoals in Sectie 2.3.2, als dit niet werkt om $u^2 + 1 \equiv 0 \pmod p$ te vinden, kiezen we andere x en y.

Als $n \neq 2(2k+1)$ en n is oneven, bekijken we $m = 2n$. Aangezien n oneven is, is $n = 2k+1$ voor een natuurlijk getal k en $m = 2(2k+1)$. Als we een representatie kunnen vinden voor m kunnen we hieruit een representatie voor n bepalen. m is even, dus als $m = x^2+y^2+z^2+w^2$ dan moet gelden $x^2+y^2+z^2+w^2 \equiv 0 \pmod 2$ en kunnen we x, y, z, w opdelen in twee paar wiens kwadraten equivalent zijn mod 2, bijvoorbeeld $x^2 \equiv y^2 \pmod 2, z^2 \equiv w^2 \pmod 2$. Dit geeft ook meteen $x \equiv y \pmod 2, z \equiv w \pmod 2$ en

$$\begin{aligned} n = \frac{1}{2}m &= \frac{1}{2}(x^2 + y^2 + z^2 + w^2) \\ &= (\frac{1}{2}(x + y))^2 + (\frac{1}{2}(x - y))^2 + (\frac{1}{2}(z + w))^2 + (\frac{1}{2}(z - w))^2. \end{aligned}$$

Aangezien $x \equiv y \pmod 2, z \equiv w \pmod 2$, zijn $(\frac{1}{2}(x \pm y))$ en $(\frac{1}{2}(z \pm w))$ gehele getallen en hebben we dus een representatie voor n als som van vier kwadraten.

Als n even is en niet van de vorm $n = 2(2k + 1)$ dan $n = 2^d(2k + 1)$ met $d > 2$. In de vorige sectie hebben we bewezen dat een product van sommen van vier kwadraten weer een som van vier kwadraten is. Als d oneven is, dan $n = (2^{(d-1)/2})^2 \cdot 2(2k + 1)$ en als d even is, kunnen we vanuit de representatie

van 2 de representatie van 2^{d-1} berekenen.

We weten nu dat het algoritme werkt zolang n een representatie heeft zoals in (12). Linnik bewijst in [10] het volgende lemma.

Lemma 4.3.2 *Er bestaat een reële $A > 0$ en een natuurlijk getal n_0 zodanig dat*

$$n_0 < n \Rightarrow \textit{het aantal oplossingen van } (12) \textit{ is groter dan } \frac{An}{\log n \log\log n}.$$

We weten de waarde van deze n_0 echter niet en weten dus niet of er voor kleinere n altijd een oplossing is voor (12). Dit probleem is op te lossen door in plaats van een paar x, y te kiezen alle drietallen $x, y, z \leq \sqrt{n}$ op lexicongrafische volgorde af te gaan en na de controle of $u + 1 \equiv 0 \pmod{p}$ te controleren of $n - x^2 - y^2 - z^2$ een kwadraat is.

Dit betekent dat voor $n > n_0$ het algoritme voor een constante c binnen $\mathcal{O}(c \cdot \log^2 n \log\log n)$ waar we $\log^2 n$ hebben in plaats van $\log n$, omdat we nog een representatie voor p moeten zoeken nadat we (12) opgelost hebben. Voor $n < n_0$ hoeft dit algoritme niet binnen verwachte polynomiale tijd te werken.

4.4 Hurwitz quaternion algoritme

Rabin en Shallit [5] hebben een algoritme bedacht voor het vinden van een vier kwadraat representatie dat gebruikt maakt van de Hurwitz quaternionen. Naast wat we al besproken hebben in Sectie 4.1 zullen we nog twee definities nodig hebben om het algoritme te kunnen omshrijven.

Definitie 4.4.1 *Een $g \in \mathbb{H}$ heet een **eenheid** als $N(g) = 1$.*

Dit zijn de elementen $\pm 1, \pm i, \pm j, \pm h$ en $\frac{\pm 1 \pm i \pm j \pm h}{2}$.

Definitie 4.4.2 *Een $h \in \mathbb{H}$ heet een **geassocieerde** van g als er een eenheid ε bestaat zodanig dat $g = \varepsilon h$.*

Het is belangrijk om op te merken dat elk element uit $\mathbb{H}$ een geassocieerde heeft die bestaat uit enkel gehele coördinaten.

Het algoritme van Rabin en Shallit voor het representeren van $N \in \mathbb{N}$ als som van vier kwadraten, gaat als volgt

1. Schrijf N als product van een macht van 2 en een oneven getal, dus $N = 2^c n$ voor bepaalde $c, n \in \mathbb{N}$ met n oneven.
2. Vind $a, b \in (\mathbb{Z}/n\mathbb{Z})$ met $a, b < \frac{1}{2}|n|$, zodanig dat $a^2 + b^2 \equiv -1 \pmod{n}$.
3. Bereken $g = \text{ggrd}(a + bi + j, n) \in \mathbb{H}$.
4. Als $N(g) = n$, dan geven de vier coördinaten van elke geassocieerde van g die uit slechts gehele coördinaten bestaat de vier getallens wiens kwadraten gesommeerd n opleveren. Als $N(g) \neq n$ dan $N(g) = kn$ met $k \mid n$ en kunnen we stap 1 tot en met 4 van het algoritme uitvoeren op k en n/k.

5. Bereken vanuit de kwadraatrepresentatie van 2^c en de delers van n de kwadraatrepresentatie van N.

Dit algoritme spreekt niet voor zich en we zullen de meeste delen nog moeten bewijzen.

Rabin en Shallit bewijzen in [5] Theorem 3.1 de volgende stelling.

Stelling 4.4.3 *Als n oneven is en $\gcd(k, n) = 1$. Dan kunnen we een oplossing vinden voor $x^2 + y^2 \equiv k \pmod{n}$ in verwachte polynomiale tijd.*

Het idee van het bewijs is om w en z willekeurig te kiezen uit $(\mathbb{Z}/n\mathbb{Z})$ en nemen $r = w^2 + z^2$, dan zoeken we x en y zodanig dat

$$(x^2 + y^2)(w^2 + z^2) \equiv kr \pmod{n}$$

Door aan te tonen dat kr min of meer willekeurig is uit $(\mathbb{Z}/n\mathbb{Z})$ zouden we vaak een kr moeten krijgen die een een priemmacht is (p^m) waarvoor we eenvoudig een representatie van twee kwadraten kunnen vinden, dus $p = u^2 + v^2$, dan

$$(x^2 + y^2)(w^2 + z^2) \equiv u^2 + v^2 \pmod{n}$$

en krijgen we

$$\begin{aligned} x &\equiv (uw + vz)(w^2 + z^2)^{-1} \pmod{n} \\ y &\equiv (vw - uz)(w^2 + z^2)^{-1} \pmod{n} \end{aligned}$$

Hiermee is stap 2 dus binnen verwachte polynomiale tijd te berekenen.

Met de volgende stelling zullen we bewijzen dat ook stap 3 binnen verwachte polynomiale tijd berekend kan worden.

Stelling 4.4.4 *Stel $g, h \in \mathbb{H}$, dan kunnen we $\operatorname{ggrd}(g, h)$ met allemaal gehele coördinaten in verwachte polynomiale tijd berekenen.*

Voor het bewijs van deze stelling hebben we een aantal lemma's nodig.

Lemma 4.4.5 *Voor elk quaternion x bestaat er een Hurwitz quaternion h zodanig dat en $N(x - h) \leq \frac{1}{2}$. Hierbij bedoelen we dat x geen gehele coëfficiënten voor 1, i, j en k hoeft te hebben en dat deze reëel mogen zijn.*

Bewijs. Het is eenvoudig in te zien dat een quaternion x het verst van de Hurwitz quaterionen verwijdert ligt als hij in 2 coördinaten $\frac{1}{2}$ van een Hurwitz quaternion af ligt en in de andere twee coördinaten hetzelfde is. Dit betekent dat als h het dichtstbijzijnde Hurwitz quaternion van x is, dan $N(x - h) \leq 2 \cdot (\frac{1}{2})^2 = \frac{1}{2}$. □

Dit kunnen we gebruiken voor het volgende lemma.

Lemma 4.4.6 *Stel $h, g \in \mathbb{H}$, dan bestaan er $q, r \in \mathbb{H}$ zodanig dat $h = qd + r$ en $N(r) \leq \frac{1}{2}N(d)$.*

Bewijs. Neem q het Hurwitz quaternion het dichtst bij hd^{-1} en neem $r = h - qd$, dan krijgen we met Lemma 4.4.5

$$N(hd^{-1} - q) \leq \frac{1}{2}$$

en omdat voor de norm geldt dat $N(a \cdot b) = N(a) \cdot N(b)$,

$$N(r) = N(h - qd) = N(hd^{-1} - q)N(d) \leq \frac{1}{2}N(d).$$

□

Lemma 4.4.7 *Stel $g, h \in \mathbb{H}$, dan kunnen we* $\text{ggrd}(g, h)$ *binnen polynomiale tijd berekenen.*

Bewijs. Neem $g = qh + r$ zoals in Lemma 4.4.6 en herhaal dit met h en r totdat je op 0 uit komt. Dit is in feite het algoritme van Euclides.

Dit werkt omdat wanneer $g = qh + r$, dan $r = qh - g$ dus als x een gemene rechter deler is van h en r is hij dit ook van g, als x een gemene rechter deler is van h en g is hij dit ook van r, dus $\text{ggrd}(g, h) = \text{ggrd}(h, r)$.

Met Lemma 4.4.6 zien we dat elke stap de norm op zijn minst halveert en dus zijn we in maximaal $\log_2 \max(N(g), N(h))$ stappen klaar is. □

Aangezien elke Hurwitz quaternion een geassocieerde heeft met gehele coördinaten geeft Lemma 4.4.7 een bewijs voor stelling 4.4.4.

Nu weten we dat stap 2 en 3 kloppen en in polynomiale tijd uitgevoerd kunnen worden, moeten we stap 4 nog bewijzen. Omdat $a^2 + b^2 \equiv -1 \pmod{n}$, geldt $n \mid N(a + bi + j)$. Omdat $a, b < \frac{1}{2}|n|$, geldt $N(a + bi + j) < n^2$. Dit betekent dat $g \mid (a^2 + b^2 + 1)$ en $N(g) | n^2$, dus $N(g) = n$ of $N(g) = kn$ voor een $k \mid n$ en klopt het algoritme. Aangezien n maximaal $\log n$ keer zo opgesplitst kan worden kan het algoritme berekend worden in polynomiale tijd.

5 Slot

We hebben in deze scriptie verschillende algoritmes besproken voor het representeren van getallen als som van kwadraten en voor de volgende gevallen zijn er algoritmes die dit binnen (verwachte) polynomiale tijd kunnen bepalen.

1. De representatie van een priemgetal $p \equiv 1 \pmod 4$ als som van twee kwadraten door middel van het algoritme van Brillhart of Rabin uit Sectie 2.3.

2. De representatie van priemgetallen $p \not\equiv 7 \pmod 8$ als som van drie kwadraten door middel van een algoritme van Rabin en Shallit uit Sectie 3.2.

3. De representatie van natuurlijke getallen $n \neq 4^a(8k+7)$ met $a, k \in \mathbb{N}$ als som van drie kwadraten uit Sectie 3.3, mits we een aantal vermoedens aannemen.

4. De representatie van alle natuurlijke getallen als som van vier kwadraten uit Sectie 4.4.

In principe hebben we alleen geen algoritme dat in polynomiale tijd natuurlijke getallen n die representeerbaar zijn als som van twee kwadraten zo te representeren.

Referenties

[1] C.W. Barnes, The representation of primes of the form $4n+1$ as the sum of two squares, *L'Enseignement mathem*, volume XVIII, pp 289-299 (1972)

[2] M. Becceanu, *Period of the Continued Fraction of* $\sqrt{n}$, Princeton, 2003

[3] J. Brillhart, Note on Representing a Prime as a Sum of Two Squares, *Mathematics of computation*, volume 26, pp 1011-1013 (1972)

[4] H. Davenport, *The Higher Arithmetic*, Cambridge University Press, New York, 2008

[5] M.O. Rabin, J.O. Shallit, Randomized Algorithms in Number Theory, *Communications on Pure and Applied Mathematics*, volume XXXIX, pp s239-s256 (1986)

[6] E. Grosswald, *Representations of Integers as Sums of Squares*, Springer-Verlag, New York, 1985

[7] Hermite, Note au sujet de l'article précédent, *Journal de mathématiques pures et appliquées* 1^{re} *série*, volume 13, pp 15 (1848)

[8] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1982

[9] H.W. Lenstra, *Computational methods in number theory*, Mathematisch cetrum, Amsterdam, 1982

[10] Yu.V. Linnik, *An asymptotic formula in the Hardy-Littlewood additive problem*, Amer. Math. Soc. Translation, volume 46, pp 65-148 (1965)

[11] O. Perron, *Die lehre von den kettenbrüchen*, Springer, Wiesbaden, 1977

[12] J.A. Serret, Sur un théorème relatif aux nombres entiers, *Journal de mathématiques pures et appliquées* 1^{re} *série*, volume 13, pp 12-14 (1848)

[13] J. Stillwell, *Elements of number theory*, Springer, New York, 2003