Bachelorscriptie

Het Gaussische grachtenprobleem

Universiteit Utrecht

Auteur: Tara Butter (3905551)
Begeleider: Dr. Steven Wepster

Januari 2018

Inhoudsopgave

1 Inleiding **3**

2 Een wandeling naar oneindig over priemgetallen **5**

3 Gaussische gehelen **6**
3.1 Achtergrond 6
3.2 Eigenschappen van Gaussische gehelen 11

4 Het Gaussische grachtenprobleem **17**

5 De bedenker **19**

6 Ontdekkingen tot nu toe **21**
6.1 Jordan en Rabung 21
6.2 Guy 24
6.3 Haugland 24
6.4 Gethner en Stark 29
6.5 Vardi 31
6.6 Gethner, Wagon en Wick 32

7 Waarom is dit een lastig probleem? **38**

8 Een oneindige zoektocht naar een oneindige wandeling **40**

Referenties **42**

Bijlage 1 **44**

1 Inleiding

Kun je wandelen naar oneindig? Als je over de reële getallenlijn loopt over de gehele getallen, dan kun je oneindig doorlopen met een begrensde staplengte. Kan dit ook als je alleen op priemgetallen mag staan? Het antwoord op deze vraag zullen we kort bespreken in hoofdstuk 2. Als we het antwoord hebben op deze vraag, kunnen we deze vraag proberen toe te passen op een andere verzameling gehelen dan de reële gehele getallen: de Gaussische gehelen. De achtergrond en eigenschappen van deze verzameling zal ik bespreken in hoofdstuk 3. Kun je over Gaussische priemgetallen naar oneindig lopen met begrensde staplengte? Rond 1960 is iemand met dit idee gekomen en sindsdien wordt dit "The Gaussian moet problem"genoemd. Ik heb dit vrij vertaald naar 'Het Gaussische grachtenprobleem'. In hoofdstuk 4 zal ik verder uitleggen wat dit probleem inhoudt.

Interessant is dat er over het Gaussische grachtenprobleem (nog) niet zo veel bekend is. Dit is de reden dat ik besloten heb mij hierin te verdiepen. Ik kwam er al snel achter dat er weinig literatuur over te vinden is en dat er zelfs onduidelijkheid lijkt te bestaan over wie nu eigenlijk als eerst gekomen is met dit probleem. Aan de hand van de geringe literatuur en zelfs persoonlijk mailcontact met de schrijver van één van de geraadpleegde boeken, heb ik uitgezocht wie waarschijnlijk de bedenker is geweest van het Gaussische grachtenprobleem. De opgedane informatie tijdens dit onderzoek is terug te vinden in hoofdstuk 5.

Het Gaussische grachtenprobleem is tot nog toe een onopgelost probleem. Een aantal wiskundigen heeft zich door de jaren heen gebogen over dit probleem en dit heeft geleid tot verschillende vermoedens over het al dan niet bestaan van een wandeling naar oneindig met begrensde staplengte over Gaussische priemgetallen. Vanuit verschillende invalshoeken zijn argumenten voor of tegen het bestaan van een dergelijke wandeling gegeven, onderbouwd met bewijzen. Deze verschillende invalshoeken en vermoedens heb ik onder elkaar gezet in hoofdstuk 6, waarin ik de essentie van de bewijzen en conclusies heb geprobeerd te reproduceren en toelichten.

Tijdens het schrijven van deze scriptie ben ik mij ook het volgende gaan afvragen: waarom is het nou eigenlijk zoveel moeilijker om het Gaussische grachtenprobleem op te lossen dan om antwoord te geven op de vraag of een wandeling naar oneindig met begrensde staplengte bestaat over de reële as? Ik heb hierover nagedacht en mijn gedachten opgeschreven in hoofdstuk 7.

De scriptie is geschreven op een manier waarop hij begrijpelijk is voor eerstejaarsstudenten Wiskunde. Scholieren die geïnteresseerd zijn in wiskunde zouden een eind kunnen komen, maar kennis van wiskundige (basis)notaties, modulorekenen en enig begrip van het complexe vlak zijn vereisten voor het begrip van de tekst. Ik heb moderne notaties gebruikt en deze ook geïntroduceerd indien ik dat relevant achtte.

De achtergrondinformatie die nodig is geweest voor het schrijven van deze scriptie heb ik gehaald uit inleidende boeken over getaltheorie en boeken over wiskundegeschiedenis, waar mogelijk aangevuld met de originele notaties en formuleringen uit de originele bronnen. Echter, de artikelen die specifiek over het Gaussische grachtenprobleem gaan, zijn de belangrijkste literatuur die ik heb gebruikt. Het doel in deze scriptie is immers 'meer te weten komen over het Gaussische grachtenprobleem' en daarvoor is het raadplegen van de weinige literatuur die over dit probleem te vinden is het grootste gedeelte van mijn onderzoek geweest. Ik heb in de hoofdstukken duidelijk aangegeven om welk artikel het in de tekst gaat en ik heb bewust gekozen voor het vaak refereren naar deze artikelen in de tekst.

2 Een wandeling naar oneindig over priemgetallen

Als je van de ene kant van een sloot naar de andere kant droog wilt overkomen, dan moet óf de sloot smal genoeg zijn om overheen te kunnen stappen met de staplengte die jij hebt, óf er moeten stapstenen in het water liggen die maximaal jouw staplengte uit elkaar liggen. Vanuit dit praktische probleem kunnen we ons de volgende vraag stellen: 'kun je met begrensde staplengte van de oorsprong naar oneindig lopen over de reële as met slechts priemgetallen als stapstenen?'. Zoals we weten bevat de getallenlijn van natuurlijke getallen $\mathbb{N}$, priemgetallen en deelbare (samengestelde) getallen. Willen we naar oneindig lopen met een maximale staplengte k, dan moet het aantal deelbare getallen tussen twee priemgetallen niet groter zijn dan $k-1$.
Hoewel de naam 'slotenprobleem' beter bij dit probleem zou passen, noemt men dit het algebraïsche grachtenprobleem (zie [WR]).

Stelling 2.1. *Het is niet mogelijk om over de natuurlijke priemgetallen naar oneindig te lopen met maximale staplengte $k \in \mathbb{N}$, k willekeurig.*

Bewijs. Stel $m, k \in \mathbb{N}$ en $1 < m \leq k+1$. Dan geldt

$$\begin{aligned} (k+1)! &= 1 \cdot 2 \cdot 3 \cdots m \cdots k \cdot (k+1) \ , \\ \text{dus} \qquad m + (k+1)! &= m + 1 \cdot 2 \cdot 3 \cdots m \cdots k \cdot (k+1) \\ &= m(1 + 1 \cdot 2 \cdot 3 \cdots (m-1) \cdot (m+1) \cdots k \cdot (k+1)) \ . \end{aligned}$$

Dit betekent dat $m + (k+1)!$ deelbaar is door m (en dus een samengesteld getal). Gezien wij m hebben gekozen als willekeurig getal tussen 1 en $k+1$, geldt dat zowel $2 + (k+1)!$ als $3 + (k+1)!$ als $4 + (k+1)!$ als ... als $(k+1) + (k+1)!$ deelbare getallen zijn. We hebben nu k opeenvolgende gehele getallen gevonden die niet priem zijn en dus een sloot gevonden die te groot is om overheen te stappen met staplengte k. □

3 Gaussische gehelen

Om het Gaussissche grachtenprobleem uit te kunnen leggen, is eerst kennis nodig van een nieuwe verzameling: de Gaussische gehelen $\mathbb{Z}[i]$. Dit zijn alle getallen van de vorm $a + bi$, met $a, b \in \mathbb{Z}$ en $i^2 = -1$. In dit hoofdstuk zal ik achtergrondinformatie geven over het ontstaan van deze getallen en zal ik vervolgens de eigenschappen van Gaussische gehelen uitwerken.

3.1 Achtergrond

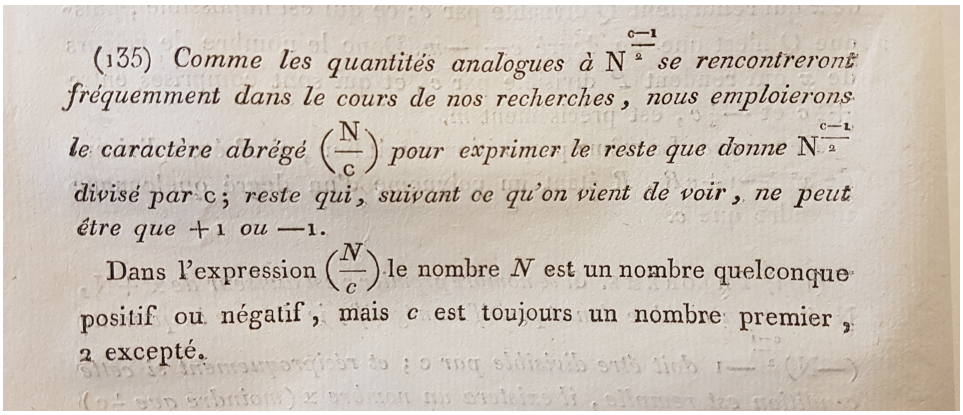
De boven genoemde verzameling heet de verzameling van Gaussische gehelen, omdat deze geïntroduceerd zijn door Carl Friedrich Gauss (1777-1855)[1]. Gauss was een negentiende-eeuwse wiskundige uit Duitsland die als eerste een bewijs formuleerde voor de kwadratische wederkerigheidswet in zijn boek *Disquisitiones Arithmeticae* [G1]. Om te begrijpen hoe hij op deze nieuwe verzameling gehele getallen is gekomen en hoe deze verzameling werkt, moeten we eerst teruggaan in de tijd en in de ontwikkeling van de getaltheorie. Onderstaande geschiedenis kan worden teruggevonden in [Bo, h.15, 17, 19], [SW, h.21] en [K, h.13].

Leonhard Euler (1707-1783), een 18$^{\text{e}}$-eeuwse Zwitserse wiskundige, hield zich tussen 1730 en 1740 bezig met het bewijzen van de stellingen in de getaltheorie die Pierre de Fermat (1601-1665) om en nabij 100 jaar eerder zonder bewijs had geformuleerd. Fermat is voornamelijk bekend om zijn laatste stelling, waarvoor pas in 1995 een bewijs is gegeven door Andrew Wiles (Fermat had dus vaker de neiging om stellingen te formuleren zonder bewijs). Naar aanleiding van de ontdekkingen van Fermat op het gebied van congruenties modulo een priemgetal, onderzocht Euler de oplosbaarheid van de vergelijking $x^2 \equiv a \pmod{p}$, waarbij p oneven priem en $a \in \mathbb{Z}$. Als deze vergelijking oplosbaar is, dan noemt men a een kwadraatrest modulo p, als deze niet oplosbaar is noemt men a een niet-rest modulo p. Zo is 3 een kwadraatrest modulo 13, omdat $4^2 \equiv 3 \pmod{13}$ en is 3 een niet-rest modulo 5, omdat de vergelijking $x^2 \equiv 3 \pmod{5}$ geen oplossingen heeft.
Euler heeft in die tijd criteria vastgesteld voor het bestaan van oplossingen voor de formule $x^2 \equiv a \pmod{p}$, die hij heeft beschreven in zijn artikel *Theoremata circa residua ex divisione potestatum relicta* [Eu1]. Adrien-Marie Legendre (1752-1833) heeft in zijn boek *Essai sur la Théorie des Nombres*

[1] [Bo, p.465].

[Le] een nieuwe notatie ingevoerd voor deze criteria in 1798, om het bespreken van kwadraatresten te vergemakkelijken en om stellingen beknopter te kunnen weergeven. Deze notatie wordt geïntroduceerd in de volgende definitie, zoals gegeven in [Le, 135] (naar eigen vertaling[2], zie figuur 1 voor de originele definitie).

Definitie 3.1 (Legendre symbool)**.** *Gezien we hoeveelheden analoog aan* $a^{\frac{p-1}{2}}$ *nog veel zullen tegenkomen, zullen we de afgekorte notatie* $\left(\frac{a}{p}\right)$ *gebruiken voor het uitdrukken van de rest die a geeft gedeeld door p. We hebben gezien dat dit slecht* ± 1 *kan zijn. In de notatie* $a^{\frac{p-1}{2}}$ *kan a een positief of negatief getal zijn, maar p is altijd een priemgetal ongelijk aan 2.*



(135) *Comme les quantités analogues à* $\mathrm{N}^{\frac{c-1}{2}}$ *se rencontreront fréquemment dans le cours de nos recherches, nous emploierons le caractère abrégé* $\left(\frac{\mathrm{N}}{\mathrm{c}}\right)$ *pour exprimer le reste que donne* $\mathrm{N}^{\frac{c-1}{2}}$ *divisé par* c; *reste qui, suivant ce qu'on vient de voir, ne peut être que* $+1$ *ou* -1.

Dans l'expression $\left(\frac{N}{c}\right)$ le nombre N est un nombre quelconque positif ou négatif, mais c est toujours un nombre premier, 2 excepté.

Figuur 1: Originele introductie van het Legendresymbool[3].

Bovenstaande definitie heeft nog een vertaalslag naar kwadraatresten nodig om te worden toegepast. Die kan worden gemaakt met het criterium van Euler in de notatie van Legendre en zoals in [Beu, 11.1.3].

Definitie 3.2 (Criterium van Euler)**.** *Zij p oneven priem en* $a \in \mathbb{Z}$*. Dan definiëren we*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{als } a \text{ kwadraatrest modulo } p \text{ is} \\ -1 & \text{als } a \text{ niet-rest modulo } p \text{ is} \\ 0 & \text{als } p \text{ een deler is van } a \end{cases}.$$

[2]Ik heb deze definitie zelf vrij vertaald en bovendien de notatie aangepast aan de notatie die in de rest van de scriptie wordt gehanteerd.

[3]foto van [Le, p.186].

Een aantal stellingen die Euler heeft bedacht, zal ik hieronder geven als aanloop voor het begrip van kwadratische wederkerigheid (en van Gaussische gehele getallen). Ik zal deze stellingen geven zonder bewijs (behalve stelling 3.3, later zal duidelijk worden waarom) en in de notatie van Legendre, die nog niet bestond in de tijd dat Euler deze stellingen bedacht. De stellingen zijn geformuleerd als in [Beu, h.11], waar ook de bewijzen van de stellingen terug te vinden zijn. Ik heb de originele bronnen van Euler geraadpleegd en onderstaande stellingen zijn terug te vinden in [Eu1]. Het ligt echter buiten het bestek van deze scriptie om onderstaande stellingen in originele vorm uit de literatuur te halen.

Stelling 3.3. *Zij p een oneven priemgetal. Dan zijn er precies $\frac{p-1}{2}$ kwadraatresten en $\frac{p-1}{2}$ niet-resten modulo p.*

Bewijs. Ten eerste geldt $x^2 \equiv (-x)^2 \equiv (p-x)^2 \pmod{p}$, waardoor het voldoende is om $x^2 \pmod{p}$ te bepalen voor $x = 1, 2, ..., (p-1)/2$ om alle kwadraatresten te vinden. Ten tweede zijn de zo gevonden kwadraatresten allen uniek. Stel namelijk van niet en $x^2 \equiv y^2 \pmod{p}$ voor $1 \leq x, y < p/2$. Dan is p een deler van $x^2 - y^2 = (x+y)(x-y)$ en wegens gevolg 3.12 geldt dat p een deler is van ofwel $(x+y)$, ofwel $(x-y)$. Er geldt echter $x + y < p/2 + p/2 = p$, dus p is geen deler van $x + y$ en moet dan een deler zijn van $x - y$, dus $x + y \equiv 0 \pmod{p}$ en dus $x \equiv y \pmod{p}$. Dit is alleen mogelijk als $x = y$ en dus hebben we alle (unieke) kwadraatresten modulo p gevonden en zijn de overige $(p-1)/2$ restklassen niet-resten modulo p. □

Stelling 3.4. *Zij p een oneven priemgetal.*

- *Het product van twee kwadraatresten modulo p is weer een kwadraatrest modulo p;*
- *Het product van een kwadraatrest en een niet-rest modulo p is weer een niet-rest modulo p;*
- *Het product van twee niet-resten modulo p is een kwadraatrest modulo p.*

Bovenstaande beweringen kunnen worden samengevat met

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad ,$$

$a, b \in \mathbb{Z}$ en a, b geen delers van p.

Ik zal het gebruik van het Legendresymbool en stelling 3.4 illustreren aan de hand van de volgende voorbeelden.

Voorbeeld 3.5. *We zeggen dat* 3 *een kwadraatrest modulo* 13 *is, omdat* $4^2 \equiv 3 \pmod{13}$. *We zien*

$$\begin{aligned}\left(\frac{3}{13}\right) &\equiv 3^6 \pmod{13} \ (= 729) \\ &\equiv 1 \pmod{13} \ .\end{aligned}$$

We zeggen dat 5 *een niet-rest modulo* 13 *is, omdat er geen oplossingen bestaan voor de vergelijking* $x^2 \equiv 5 \pmod{13}$. *Bovendien zien we*

$$\begin{aligned}\left(\frac{5}{13}\right) &\equiv 5^6 \pmod{13} \ (= 15625) \\ &\equiv -1 \pmod{13} \ .\end{aligned}$$

Stelling 3.4 is nu gemakkelijk na te gaan.

Euler kwam met deze stellingen en de ontdekkingen van Fermat uiteindelijk in 1741 tot de wet van kwadratische wederkerigheid, die pas gepubliceerd werd in 1783 door de academie van Sint Petersburg [Eu2], nadat Euler was overleden. Deze wet kan met de notatie van Legendre als volgt worden geformuleerd (zie [Beu, 11.1.6] voor stelling met bewijs):

Stelling 3.6 (Kwadratische wederkerigheidswet)**.** *Zij* p, q *een tweetal verschillende oneven priemgetallen. Dan geldt:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \ .$$

Gezien p *nooit een deler zal zijn van* q*, is het Legendresymbool altijd gelijk aan* ± 1 *en kunnen we bovenstaande vergelijking ook schrijven als*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \ .$$

Anders gezegd, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$*, tenzij* $p \equiv q \equiv -1 \pmod{4}$*, in welk geval geldt* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ *(want dan zijn* $\frac{p-1}{2}$ *en* $\frac{q-1}{2}$ *beide oneven en dan geldt* $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -1$*).*

Ik zal de Kwadratische wederkerigheidswet toelichten met een voorbeeld, waaruit de toepassing ervan duidelijk zal worden.

Voorbeeld 3.7. *We gaan eerst onderzoeken of* $x^2 \equiv 31 \pmod{43}$ *een oplossing heeft, met behulp van kwadratische wederkerigheid.*

$$\left(\frac{31}{43}\right) = \left(\frac{43}{31}\right)(-1)^{\frac{31-1}{2}\frac{43-1}{2}} \tag{1}$$

$$= -\left(\frac{43}{31}\right) = -\left(\frac{12}{31}\right)$$

$$= -\left(\frac{4}{31}\right)\left(\frac{3}{31}\right) \tag{2}$$

$$= -\left(\frac{3}{31}\right) = -\left(\frac{31}{3}\right)(-1)^{\frac{3-1}{2}\frac{31-1}{2}} \tag{3}$$

$$= -\left(-\left(\frac{1}{3}\right)\right) = \left(\frac{1}{3}\right) = 1 \ . \tag{4}$$

Regels (1) *en* (3) *zijn directe toepassingen van kwadratische wederkerigheid, regel* (2) *volgt uit stelling 3.4 (multiplicativiteit van het Legendresymbool en het feit dat* $\left(\frac{4}{31}\right) = 4^{\frac{31-1}{2}} \equiv 1 \pmod{31}$*). We hebben nu dus bewezen dat* 31 *een kwadraatrest modulo* 43 *is.*

Kwadratische wederkerigheid geeft een verband aan tussen de vergelijkingen $x^2 \equiv p \pmod{q}$ en $x^2 \equiv q \pmod{p}$. Zoals eerder vermeld is Gauss de eerste wiskundige die een bewijs heeft geleverd voor de kwadratische wederkerigheidswet in 1801. Na het geven van dit bewijs daagde Gauss zichzelf uit tot het vinden en bewijzen van ditzelfde verband tussen de vergelijkingen $x^4 \equiv p \pmod{q}$ en $x^4 \equiv q \pmod{p}$ (dit verband heet bikwadratische wederkerigheid en Gauss is helaas niet gekomen tot een bewijs hiervan). Hij is hiertoe de studie van Euler opnieuw begonnen voor deze nieuwe vergelijkingen en is op zoek gegaan naar criteria voor de oplosbaarheid van bikwadratische congruentievergelijkingen (we zitten nu rond 1820)[4]. Dit bleek lastiger en eigenlijk zo goed als niet oplosbaar met slechts reële gehele getallen en Gauss besloot dat hij verder zou moeten kijken dan slechts gehele getallen in het reële vlak. Zo is hij gekomen tot gehele getallen van de vorm $a + bi$: nu Gaussische gehelen genoemd. De eigenschappen van deze getallen zoals wij ze nu kennen (uitgewerkt in de volgende paragraaf, 3.2) heeft hij uitgewerkt in *Theoria Residorum Biquadraticorum: Commentatio*

[4] [K, p.356].

Secunda [G2][5]. Een argument voor het gebruik van juist deze getallen zou het volgende kunnen zijn: kijk nog eens naar het bewijs van stelling 3.3 op pagina 8. Als we kijken naar uniciteit van de kwadraatresten, dan kijken we naar het geval dat $x^2 \equiv y^2 \pmod{p}$ en dus naar p als priemdeler van $x^2 - y^2 = (x-y)(x+y)$. Doen we dit voor bikwadratische wederkerigheid, dan zien we dat $x^4 - y^4 = (x^2 - y^2)(x^2 + y^2)$. Het eerste deel is te ontbinden zoals in het bovengenoemde bewijs, maar het tweede deel is alleen te ontbinden in $x^2 + y^2 = (x + yi)(x - yi)$; in Gaussische gehelen. Dit is hoogstwaarschijnlijk geen toeval.

3.2 Eigenschappen van Gaussische gehelen

De verzameling van Gaussische gehelen lijkt in veel opzichten op de verzameling van reële gehele getallen. Hieronder zal ik een aantal belangrijke eigenschappen van $\mathbb{Z}[i]$ noemen. Bewijzen zijn eventueel te vinden in [HW, h.XII] en [G2v].

1. De eenheidselementen van de Gaussische gehelen zijn ± 1 en $\pm i$.

2. Een deler in $\mathbb{Z}[i]$ is op dezelfde manier gedefinieerd als een deler in $\mathbb{Z}$: $y \in \mathbb{Z}[i]$ is een deler van $x \in \mathbb{Z}[i]$ dan en slechts dan als er een $\alpha \in \mathbb{Z}[i]$ bestaat zodanig dat $x = \alpha y$.

   - De triviale delers van $x \in \mathbb{Z}[i]$ zijn $\pm 1, \pm x, \pm i, \pm xi$ (zoals $\pm 1, \pm z$ triviale delers zijn in $\mathbb{Z}$).
   - Als α een deler is van y en y is een deler van x, dan is α een deler van x.
   - Als α een deler is van zowel x_1 als van x_2 als van ... als van x_n, dan is α een deler van $\beta_1 x_1 + \beta_2 x_2 + ... + \beta_n x_n$, met $\beta_i \in \mathbb{Z}[i]$ willekeurig.

3. De norm van $x \in \mathbb{Z}[i]$ is gedefinieerd als $N(x) = N(a + bi) = a^2 + b^2$.

   - $\bar{x} \in \mathbb{Z}[i]$ heet de geconjugeerde van $x \in \mathbb{Z}[i]$ als $N(x) = x\bar{x}$.
   - $N(x)N(y) = N(xy)$ (en i.h.a. $N(x_1)N(x_2)...N(x_n) = N(x_1 x_2 ... x_n)$).

[5] Van het origineel is helaas slechts het eerste deel (Commentatio Prima) in het bezit van de Universiteit Utrecht, maar niet dit deel. De vertaling ervan door W. Ewald ([G2v]) is wel te raadplegen.

- Als ϵ een eenheid in $\mathbb{Z}[i]$, dan heet ϵx een geassocieerde van x. Alle met x geassocieerde elementen zijn $\pm x, \pm xi$.
- $\epsilon \in \mathbb{Z}[i]$ is een eenheid in $\mathbb{Z}[i]$ dan en slechts dan als $N(\epsilon) = 1$.

4. Een priemgetal γ in $\mathbb{Z}[i]$ is een geheel getal in $\mathbb{Z}[i]$ dat niet deelbaar is door andere Gaussische gehele getallen dan de triviale delers (eenheden en geassocieerden van γ).

5. De afstand tussen twee getallen met $x = a_1 + b_1 i$ en $y = a_2 + b_2 i$ wordt gedefinieerd door $|x - y| = \sqrt{(a_1 - a_2)^2 + (b_1 - b_2)^2}$.

6. Een getal $x \in \mathbb{Z}[i]$ heet even dan en slechts dan als $N(x)$ is even in $\mathbb{Z}$ en oneven dan en slechts dan als $N(x)$ oneven in $\mathbb{Z}$. De som van twee Gaussische gehelen met dezelfde pariteit is even en de som van twee Gaussische gehelen met verschillende pariteit is oneven.

Gezien wij voor ons vraagstuk geïnteresseerd zijn in de Gaussische priemgetallen, gaan we hier dieper op in. Voor Gaussische priemgetallen geldt de volgende algemene stelling[6]:

Stelling 3.8 (Gaussische priemgetallen)**.** *Een getal in $\mathbb{Z}[i]$ is een Gaussisch priemgetal als het voldoet aan één van de twee onderstaande eisen:*

1. *Als $a, b \neq 0$, dan is $a + bi$ een Gaussische priem dan en slechts dan als $N(a + bi) = a^2 + b^2 = p$ met p een reëel priemgetal.*

2. *Een Gaussisch geheel getal van de vorm c of ci met $c \in \mathbb{Z}$ is een Gaussische priem dan en slechts dan als c een reëel priemgetal met $|c| \equiv 3 \mod 4$.*

Voor het bewijs van deze stelling is een aantal beweringen nodig die voortborduren op de eerder besproken theorie over kwadraatresten. Ik geef deze beweringen op de volgende pagina.

[6] Eisen zoals in [GWW, p.328].

Onderstaand gevolg is een direct resultaat van de definitie van het Legendre-symbool (gegeven zoals in [Beu, 11.1.5], echter daar zonder bewijs).

Gevolg 3.9. *Zij p een oneven priemgetal. Dan is $\left(\frac{-1}{p}\right)$ gelijk aan 1 als $p \equiv 1 \pmod 4$ en aan -1 als $p \equiv -1 \pmod 4$.*

Bewijs. We weten dat

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{(p-1)}{2} \pmod p} \quad . \tag{5}$$

Gezien p een oneven priemgetal is, weten we dat (5) gelijk is aan 1 als $\frac{(p-1)}{2}$ even is, dus als $(p-1)$ deelbaar is door 4. Dan $(p-1) \equiv 0 \pmod 4$ en dus $p \equiv 1 \pmod 4$.
Als $\frac{(p-1)}{2}$ oneven is, dus als $(p-1)$ deelbaar is door 2, maar niet door 4, dan is (5) is gelijk aan -1. Dan geldt $(p-1) \equiv 2 \pmod 4$ en dus $p \equiv -1 \pmod 4$
□

Dit gevolg hebben we nodig om de volgende stelling intuïtief te maken. Ik zal deze stelling geven zonder bewijs. Het bewijs kan worden gevonden in [Beu, pp.127-128].

Stelling 3.10. *Zij p een priemgetal zodanig dat $p \equiv 1 \pmod 4$. Dan zijn er $a, b \in \mathbb{Z}$ zodanig dat $p = a^2 + b^2$.*

Ook een belangrijke stelling die we nodig hebben om stelling 3.8 te bewijzen is de volgende, die ik ook zonder bewijs zal geven (voor bewijs en toelichting zie [Beu, pp.23-26]).

Stelling 3.11 (Hoofdstelling van de rekenkunde)**.** *Elk natuurlijk getal > 1 is ofwel priem, ofwel op precies één manier te schrijven als product van priemgetallen, op volgorde van factoren na.*
Formeel gezegd: ieder natuurlijk getal $n > 1$ kan geschreven worden in de vorm $p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$, met $k_1, k_2, ..., k_r \in \mathbb{N}$ en $p_1 < p_2 < ... < p_r$ priemgetallen.

Uit de hoofdstelling van de rekenkunde volgt onderstaande bewering, waarvan het belang later duidelijk zal worden.

Gevolg 3.12 (Unieke priemfactorisatie)**.** *Zij p priem en een deler van $z = z_1 z_2$, met $z, z_1, z_2 \in \mathbb{Z}$. Dan is p ofwel een deler van z_1, ofwel een deler van z_2 (of van zowel z_1 als van z_2).*

Bewijs. Zij p een priemdeler van z en $z = z_1 z_2$. Zeg $z_1 = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ en $z_2 = q_1^{l_1} q_2^{l_2} ... q_r^{l_r}$, dan wegens unieke priemfactorisatie zijn de priemdelers van z_1 en z_2 ook de enige priemdelers van z. Dus p is ofwel een priemdeler van z_1, ofwel van z_2, ofwel van z_1 én z_2 (want p_i en q_i hoeven niet verschillend te zijn).

□

Let op: bovenstaande stellingen (3.10 en 3.11) gaan over de reële gehele getallen. De stellingen die volgen zullen gaan over de Gaussische gehele getallen (voornamelijk over Gaussische priemgetallen). Deze stellingen zal ik wederom geven zonder bewijs of hulpstellingen, deze zijn terug te vinden in [HW, h.XII]. Bovenstaande en komende stellingen gaan we uiteindelijk gebruiken voor het formuleren van een bewijs voor stelling 3.8.

Stelling 3.13. *Als y een deler is van x, dan zijn alle geassocieerden van y delers van alle geassocieerden van x.*

Stelling 3.14. *Zij $\gamma \in \mathbb{Z}[i]$ zodanig dat $N(\gamma) = p$ met p een reëel priemgetal, dan is γ een Gaussisch priemgetal.*

Stelling 3.15 (Hoofdstelling van de rekenkunde voor Gaussische gehelen)**.** *Ieder Gaussisch geheel met een norm > 1 is op een unieke manier te schrijven als product van Gaussische priemgetallen, op de volgorde van de factoren en de vermenigvuldiging met eenheden na.*
(Net als stelling 3.11 heeft deze stelling als gevolg dat als γ een deler is van $x = x_1 x_2$ met $x, x_1, x_2 \in \mathbb{Z}[i]$, dat γ dan een deler is van x_1 of x_2 of beide).

We hebben nu alle benodigdheden om een bewijs te formuleren voor stelling 3.8 (gebruikmakende van de ideën uit [HW, h.XV], toegepast op de manier waarop ik stelling 3.8 heb geformuleerd). Dit bewijs staat op de volgende pagina.

Bewijs.
1. Getallen van de vorm $a+bi$, met $a, b \neq 0$.
"$\Rightarrow$" Stel $\gamma = a + bi$ is een Gaussisch priemgetal en stel $a^2 + b^2$ is niet reëel priem. Dan wegens unieke priemfactorisatie in $\mathbb{Z}$ bestaat er een p, reëel priem, die een deler is van $N(\gamma)$. We weten dat γ een deler is van $N(\gamma)$ (immers $N(\gamma) = \gamma\bar{\gamma}$) en wegens stelling 3.15 geldt dan dat γ een deler is van ofwel p, ofwel van een andere priemfactor van $N(\gamma)$, waardoor we zonder verlies aan algemeenheid kunnen aannemen dat γ een deler is van p. Dan $p = \gamma\alpha$ voor een $\alpha \in \mathbb{Z}[i]$ en dus $N(\gamma)N(\alpha) = N(p) = p^2$. Wegens unieke priemfactorisatie in $\mathbb{Z}$ geldt nu ofwel $N(\gamma) = p^2$, dus dan $\gamma = p$, wat onmogelijk is omdat $\gamma = a + bi \notin \mathbb{Z}$, ofwel $N(\gamma) = p$. Dus $a^2 + b^2 = p$ met p een reëel priemgetal.
"$\Leftarrow$" Stel $a^2 + b^2 = p$ met p een reëel priemgetal. Dan wegens stelling 3.14 geldt dat $\gamma = a + bi$ een Gaussisch priemgetal is.

2. Getallen van de vorm c of ci.
"$\Rightarrow$" Deelbare getallen in $\mathbb{Z}$ zijn deelbaar in $\mathbb{Z}[i]$, dus c moet reëel priem zijn. Er zijn drie mogelijkheden voor c:

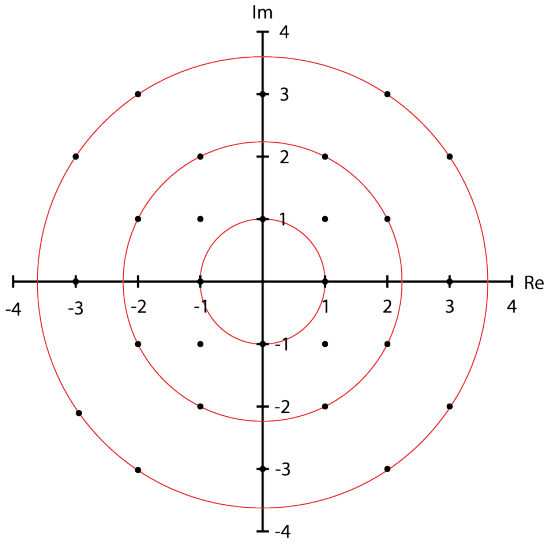
i) $c = 2$. Dit is echter geen Gaussisch priemgetal, want $2 = (1+i)(1-i)$.

ii) c een reëel priemgetal met $|c| \equiv 1 \pmod 4$ (we nemen de absolute waarde van c, zodat we niet in de problemen komen als we geassocieerden van c of ci bekijken). Dan wegens gevolg 3.9 en definitie 3.1 bestaat er een x zodat $x^2 \equiv -1 \pmod c$, dus c is een deler van $x^2 + 1 = (x + i)(x - i)$. Wegens stelling 3.15 geldt dat als c een Gaussisch priemgetal is, dan deelt c owel $x + i$, ofwel $x - i$. Echter, $\frac{x}{c} \pm \frac{i}{c}$ zijn geen gehele getallen en c is geen Gaussisch priemgetal.

iii) c is een reëel priemgetal met $|c| \equiv 3 \pmod 4$. Stel c niet Gaussisch priem. Dan wegens unieke priemfactorisatie in $\mathbb{Z}[i]$ bestaat er een γ Gaussisch priem die c deelt. Er is dus een $\alpha \in \mathbb{Z}[i]$ zodanig dat $\gamma\alpha = c$ en dan geldt $N(\gamma)N(\alpha) = N(c) = c^2$. Er geldt ofwel $N(\alpha) = 1$ (dus α is een eenheid) en dan is γ gelijk aan c (of αc) en dus is c een Gaussisch priemgetal, ofwel $N(\gamma) = a^2 + b^2 = c$. Dit laatste geval is niet mogelijk als $|c| \equiv 3 \pmod 4$, gezien kwadraten gelijk zijn aan 0 of 1 (mod 4) ($a \in \mathbb{Z}$ is 0, 1, 2 of 3 (mod 4), dus a^2 is 0 of 1 (mod 4)), dus een som van twee kwadraten is gelijk aan 0, 1 of 2 (mod 4) (i.h.b. gelijk aan 1 (mod 4), omdat c oneven priem). Dus c is een Gaussisch priemgetal.

"$\Leftarrow$" c is reëel priemgetal met $|c| \equiv 3 \pmod 4$. Het bewijs gaat analoog aan geval iii) van bovenstaand bewijs van de implicatie de andere kant op. $\square$

Het Gaussische vlak

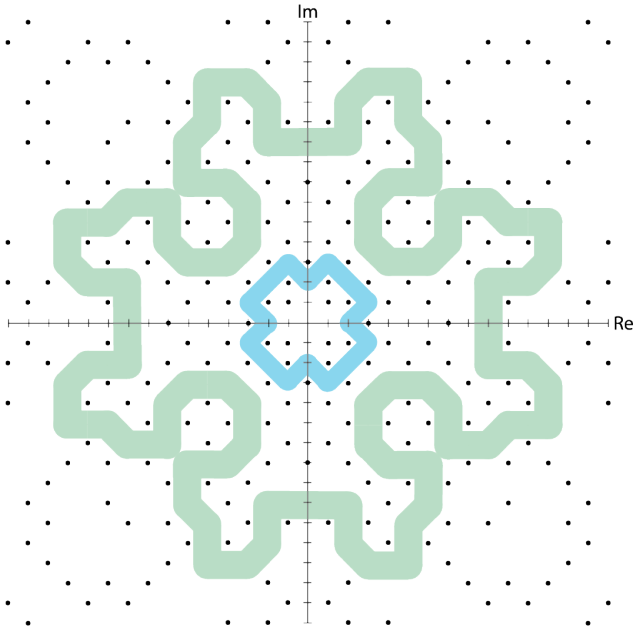


Figuur 2: Weergave van de Gaussische getallen $\{1\ ;\ 1+i\ ;\ 2+i\ ;\ 3+2i\}$ met hun geassocieerden. De cirkels waarop respectievelijk 1; $2+i$ en $3+2i$ met hun geassocieerden liggen zijn van binnen naar buiten met rood weergegeven (de tweede cirkel heeft straal $\sqrt{5}$ en de buitenste cirkel heeft straal $\sqrt{13}$).

De Gaussische gehelen zijn als roosterpunten in het complexe vlak weer te geven. In figuur 2 heb ik een aantal Gaussische punten in dit vlak getekend. Gezien alle geassocieerden dezelfde norm hebben, liggen alle getallen $\pm a \pm bi, \pm b \pm ai$ op dezelfde cirkel in het vlak, met in het bijzonder een straal van $\sqrt{p}$ als $N(\gamma) = p$ met γ Gaussisch priem en p een reëel priemgetal. Dat geassocieerden op dezelfde cirkel liggen is tevens de reden voor de achtvoudige symmetrie die het vlak van Gaussische gehelen bevat. Deze symmetrie is goed te zien in figuur 3 in het volgende hoofdstuk (4).

4 Het Gaussische grachtenprobleem

Nu we de verzameling van Gaussische gehelen hebben geïntroduceerd, kunnen we het Gaussische grachtenprobleem gaan uitdiepen. Dit probleem berust op de vraag: kun je vanuit de oorsprong naar oneindig lopen met eindige staplengte als je slechts de Gaussische priemgetallen als stapstenen kunt gebruiken? Het antwoord op deze vraag is een stuk minder eenvoudig te vinden dan het antwoord op de eerste vraag. Sterker nog, wiskundigen hebben zich beziggehouden met deze vraag, maar er is tot nog toe geen antwoord gevonden. In dit hoofdstuk zal ik bespreken hoe het Gaussische grachtenprobleem gezien kan worden.



Figuur 3: Het vlak gaat van 0 tot ± 15 en $\pm 15i$. De zwarte punten zijn de Gaussische priemgetallen in dit vlak.

Als we via de Gaussische priemgetallen naar oneindig willen lopen, moeten we een stapgrootte hebben waarmee we over een 'gracht' rond de oorsprong kunnen stappen. Ik heb in figuur 3 een visualisatie gemaakt van twee dergelijke grachten en ik zal dit toelichten aan de hand van de figuur. Laten we enkel het eerste octant bekijken, gezien dit wegens de achtvoudige symme-

trie van Gaussische priemgetallen representatief is voor het gehele vlak. Als we maximaal stapgrootte 1 toelaten, dan kan vanaf $1 + i$ slechts naar $2 + i$ worden gestapt, maar niet meer verder. Om naar het volgende priemgetal te stappen (3 of $3 + i$), dient een stap van $\sqrt{2}$ te worden genomen. Om $2 + i$ en de geconjugeerden daarvan ligt dus een gracht rond de oorsprong van breedte $\sqrt{2}$ (de blauwe gracht in de figuur). Laten we stapgrootte $\sqrt{2}$ toe, dan zien we dat we al een stuk verder komen: tot en met $11 + 4i$. Om naar het volgende priemgetal te stappen, is stapgrootte 2 nodig: we hebben een gracht gevonden rond de oorsprong van breedte 2 (groene gracht in de figuur). Het Gaussische grachtenprobleem is opgelost als bewezen kan worden dat voor iedere willekeurige stapgrootte k een gracht kan worden gevonden die groter is dan deze k.

5 De bedenker

Er is niet veel bekend over het Gaussische grachtenprobleem. Het is genoemd in slechts drie boeken ([Guy], [M], [Wag]) en vijf artikelen ([JR], [Ha], [GS], [V], [GWW]), waarbij het probleem in het boek [M] zelfs alleen genoemd wordt als onopgelost probleem en verder niet wordt uitgewerkt. Ik heb deze boeken en artikelen allen bestudeerd en het viel mij op dat opvattingen over wie nu eigenlijk als eerste kwam met het Gaussische grachtenprobleem verdeeld zijn. Sommige schrijvers zijn in de overtuiging dat Basil Gordon (1921-2012)[7] de eerste was die met dit probleem kwam, anderen schrijven het probleem toe aan Paul Erdös (1913-1996)[8]. Beiden lijken plausibel, gezien Gordon in 1959 ging werken voor het wiskundedepartement aan de *University of California-Los Angeles* waar hij gespecialiseerd was in onder andere getaltheorie en Erdös heeft bijna de helft van zijn 1500 artikelen gewijd aan problemen in de getaltheorie en heeft daarnaast in zijn artikel [Er] een bewijs gegeven voor de priemgetalstelling[9] die aan het einde van de achttiende eeuw al was bedacht door Gauss en Legendre (onafhankelijk van elkaar). Mijn doel is om in dit hoofdstuk duidelijk te krijgen aan wie het probleem toe te schrijven is en waar het misverstand van de andere schrijvers (vermoedelijk) vandaan komt.
Het eerste artikel dat over dit probleem is geschreven is *A conjecture of Paul Erdös concerning Gaussian primes* [JR] uit 1970 door J.H. Jordan en J.R. Rabung. Hierin is ook de eerste stap in de richting van de oplossing van het probleem gemaakt (meer hierover in hoofdstuk 6). Jordan en Rabung schrijven het Gaussische grachtenprobleem toe aan Paul Erdös. Volgens hen heeft Gordon het vermoeden van Erdös dat een wandeling naar oneindig over Gaussische priemen met begrensde staplengte bestaat aan het licht gebracht: "Recently Basil Gordon communicated to the authors a conjecture of Paul Erdös concerning the two-dimensional generalization of this problem" [JR, p.221]. Opvallend is dat deze rolverdeling in het artikel *A stroll through the Gaussian primes* [GWW] uit 1998 juist omgedraaid lijkt te zijn. Hierin beweren Ellen Gethner, Stan Wagon en Brian Wick dat men het probleem in eerste instantie toeschrijft aan Erdös, maar dat het eigenlijk als eerste is genoemd door Gordon in 1962 op het *Inernational Congress of Mathematicians* in Stockholm. Gethner, Wagon en Wick voegen hieraan toe dat

[7] [A, p.856].
[8] [Ba, p.19].
[9] Het aantal priemgetallen kleiner dan x noemen we $\pi(x)$. Er geldt $\pi(x) \sim x/\log x$ als $x \to \infty$ [Beu, 19.2.3] ($f(x) \sim g(x)$ betekent $f(x)/g(x) \to 1$ als $x \to \infty$).

Erdös via persoonlijke communicatie heeft bevestigd dat het idee niet van hem kwam en dat hij zelf van mening is dat de wandeling naar oneindig over Gaussische priemen niet bestaat. Gethner heeft ook het artikel *Periodic Gaussian moats* [GS] geschreven samen met H.M. Stark en Wagon heeft het boek *Mathematica in action* [Wag] geschreven. Het probleem wordt in dit artikel en dit boek ook toegeschreven aan Gordon.
Bij het lezen van het stuk over het Gaussische grachtenprobleem in het boek *Unsolved problems in Number theory* [Guy] van Richard Guy, viel mij op dat daarin de naam Erdös helemaal niet genoemd wordt. Het probleem wordt toegeschreven aan Theodore Motzkin en Basil Gordon. Gezien Richard Guy nog in leven is, besloot ik hem een mail te sturen en te vragen aan wie hij het Gaussische grachtenprobleem toeschrijft en hoe hij wist dat ook Motzkin zich bezighield met het probleem. Guy's verklaring is dat hij voor het eerst van dit probleem hoorde in een persoonlijk gesprek met Motzkin, die dus vermoedelijk in dat gesprek het probleem heeft toegeschreven aan Basil Gordon. De mail die ik naar meneer Guy heb gestuurd en het antwoord daarop is bijgevoegd in Bijlage 1.
Bij het lezen van de overige bronnen waarin het probleem terugkomt, lijkt er een plausibele verklaring te zijn voor het verschil in opvattingen van Jordan en Rabung die het probleem toeschrijven aan Erdös; en Gethner, Wagon en Wick die het juist toeschrijven aan Gordon. Hugh L. Montgomery beschrijft in zijn boek *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*[M] tien lezingen die hij heeft gegeven op de *NSF-CBMS Regional Conference* die in mei 1990 werd gehouden op de *Kansas State University* en noemt het Gaussische grachtenprobleem als één van de onopgeloste problemen die aan bod zijn gekomen op dit congres. Hij schrijft het probleem toe aan Paul Erdös en dat lijkt nu ook logisch, gezien dit congres plaatsvond vóórdat het artikel [GWW] verscheen en dus voordat Erdös zelf verklaarde dat hij niet degene was die dit probleem heeft bedacht. Noorse wiskundige Jan Kristian Haugland verwijst in zijn artikel *En spasertur på komplekse primtall* (Een wandeling over complexe priemgetallen) [Ha] naar het artikel van Gethner, Wagon en Wick: Haugland had het artikel [GWW] dus al gelezen en wist wél dat Erdös dit probleem niet aan zichzelf toeschreef. Basil Gordon is dus de eerste die kwam met dit probleem, Paul Erdös heeft er waarschijnlijk als eerste een vermoeden over uitgesproken.

6 Ontdekkingen tot nu toe

Er is, zoals we in afgelopen hoofdstukken hebben opgemerkt, dus al onderzoek gedaan naar het Gaussische grachtenprobleem. Echter, het is nog niet opgelost. Er zijn verscheidene stappen gezet, er zijn dingen ontdekt en er zijn standpunten aangenomen over het al dan niet geloven van de hypothese dat men met begrensde stapgrootte naar oneindig zou kunnen lopen over Gaussische priemgetallen. Hieronder zal ik de verschillende invalshoeken noemen, de één wat verder uitgewerkt dan de ander.

6.1 Jordan en Rabung

Het eerste artikel dat verscheen over het Gaussische grachtenprobleem is het artikel van J.H. Jordan en J.R. Rabung [JR] uit 1970. Hierin hebben zij met IBM360 Gaussische priemgetallen laten genereren en met de hand bepaald wat de afstanden tussen deze priemgetallen zijn. Zij hebben op deze manier bewezen dat een gracht van 4 bestaat als je vanuit de oorsprong over de Gausissche priemen naar buiten loopt.

Allereerst hebben Jordan en Rabung in hun artikel het vermoeden van Erdös dat een dergelijke wandeling mogelijk is[10] abstract geformuleerd:

Vermoeden 6.1. *Er bestaat een M en een rij Gaussische priemen $\{\gamma_j\}_1^\infty$, zodanig dat $|\gamma_1| < M$, $|\gamma_j - \gamma_{j-1}| < M$ en $\lim |\gamma_j| = \infty$.*

Het eerste priemgetal in de rij wordt dus van boven begrensd door een getal M, dit zorgt ervoor dat de wandeling überhaupt in de buurt van de oorsprong kan starten. De afstand tussen twee opeenvolgende priemgetallen wordt ook van boven begrensd door hetzelfde getal M (want we zijn op zoek naar een wandeling naar oneindig met een begrensde stapgrootte) en de rij met Gaussische priemen loopt oneindig door (we willen immers met begrensde stapgrootte over deze rij 'stapstenen' naar oneindig lopen).
Het volgende dat Jordan en Rabung stellen is dat, gezien alle Gaussische priemgetallen behalve $1 + i$ oneven zijn, $|\gamma_j - \gamma_{j-1}| \geq \sqrt{2}$. Hiervan zal ik een bewijs formuleren.

[10] Let wel: dat Erdös vermoedt dat deze wandeling mogelijk is, is de interpretatie van Jordan en Rabung, in hoofdstuk 5 is aangegeven dat Erdös zelf waarschijnlijk niet geloofde in dit vermoeden.

Stelling 6.2. $|\gamma_j - \gamma_{j-1}| \geq \sqrt{2}$.

Bewijs. Neem twee verschillende oneven Gaussische priemgetallen $\gamma_1 = a_1 + b_1 i$ en $\gamma_2 = a_2 + b_2 i$ $(a_i, b_i \in \mathbb{Z})$, dan is de afstand tussen deze twee getallen gelijk aan

$$|\gamma_2 - \gamma_1| = \sqrt{(a_2 - a_1)^2 + (b_2 - b_1)^2} \ .$$

Stel dat deze afstand kleiner zou zijn dan $\sqrt{2}$, ofwel stel

$$\begin{aligned} \sqrt{(a_2 - a_1)^2 + (b_2 - b_1)^2} < \sqrt{2} \ , \qquad \text{dus} \\ (a_2 - a_1)^2 + (b_2 - b_1)^2 < 2 \ , \end{aligned}$$

dan zijn er twee opties: óf zowel $(a_2 - a_1)^2$ als $(b_2 - b_1)^2$ zijn beiden gelijk aan 0, óf één van beiden is gelijk aan 1 en de ander is gelijk aan 0. Het eerste geval is niet mogelijk, gezien dit zou betekenen dat de afstand tussen de twee priemgetallen nul is en dus dat $\gamma_1 = \gamma_2$. Echter, we hebben gesteld dat γ_1 en γ_2 verschillend zijn, dus $|\gamma_2 - \gamma_1| > 0$. In het tweede geval is het reële deel (a_i) hetzelfde gebleven en het imaginaire deel (b_i) met 1 toegenomen, of andersom. Dit betekent zonder verlies van algemeenheid, dat $a_2 + b_2 i$ even is als $a_1 + b_1 i$ oneven is. Echter, we hebben twee oneven Gaussische priemgetallen gekozen (dan hebben we keuze uit alle Gaussische priemen behalve $1 + i$), dus ook dit geval leidt tot een tegenspraak.
De afstand tussen γ_1 en γ_2 is dus niet kleiner dan 2 en dus geldt

$$|\gamma_2 - \gamma_1| \geq \sqrt{2} \ .$$

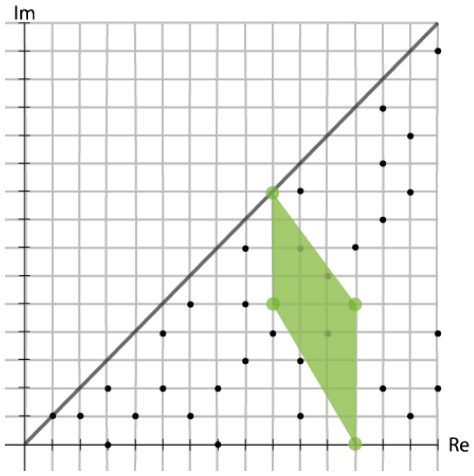
De oneven verschillende Gaussische priemgetallen zijn willekeurig gekozen, dus geldt voor alle verschillende oneven Gaussische priemgetallen dat

$$|\gamma_j - \gamma_{j-1}| \geq \sqrt{2} \ .$$

□

Hiermee is aangetoond dat de stapgrootte minstens $\sqrt{2}$ moet zijn om van $1 + i$ over de Gaussische priemgetallen naar oneindig te lopen.

Grachten zoeken



Figuur 4: De zwarte punten zijn de Gaussische priemgetallen in het eerste octant van het Gaussische vlak (dit octant ligt tussen de reële as en de schuine zwarte lijn). De groene punten zijn de gegeven hoekpunten voor de gracht van breedte 2 en het groene vlak is wat je krijgt als je deze punten verbindt, ofwel de 'gracht' van breedte 2 volgens Jordan en Rabung.

Jordan en Rabung laten in dit artikel zien dat de begrenzing M uit vermoeden 6.1 respectievelijk groter is dan 2, $\sqrt{10}$ en uiteindelijk 4. Dit doen zij door hoekpunten te geven van 'grachten' om de oorsprong heen die breedtes 2, $\sqrt{10}$ en 4 hebben. De eerste gracht van breedte 2 is eenvoudig zelf te tekenen, dit hebben we gedaan in hoofdstuk 4 (zie figuur 3 op pagina 17). De hoekpunten voor de gracht van breedte 2 die Jordan en Rabung geven zijn $\{12; 12+5i; 9+5i; 9+9i\}$. In figuur 4 heb ik deze hoekpunten getekend en de gracht ingekleurd. De keuze van deze hoekpunten voor de gracht van breedte 2 lijkt nu niet logisch. Mijn idee zou zijn dat deze gracht dan ook daadwerkelijk breedte twee zou hebben en dat er geen Gaussische priemgetallen in deze gracht zouden liggen. Echter, de afstand tussen $9+5i$ en $12+5i$ is al 5 en aan de zwarte stippen in de figuur is te zien dat in dit vlak wel degelijk Gaussische priemgetallen liggen. Het is waar dat je niet over deze gracht heen kunt stappen met stapgrootte < 2 en het 'kritieke punt' $11+4i$ waarna men vastloopt ligt inderdaad in deze gracht, maar ik kan niet ontdekken waarom deze vier punten precies gekozen zijn als hoekpunten van deze gracht. In het artikel wordt verder niet ingegaan op deze keuze. Ook van de eerste gracht van breedte $\sqrt{10}$ en verder gelegen grachten worden de

hoekpunten gegeven zonder illustratie of toelichting. Hiervan weet ik echter niet of de hoekpunten logisch zijn, gezien ik dit niet zelf met de hand heb bepaald zoals ik in hoofdstuk 4 wel heb gedaan voor de grachten van breedtes $\sqrt{2}$ en 2.

Een opvallende conclusie

In eerste instantie lijken Jordan en Rabung een neutraal standpunt in te nemen aangaande het al dan niet bestaan van een wandeling naar oneindig over Gaussische priemen met begrensde staplengte. Echter, na het geven van de hoekpunten van de gracht van breedte 4 wordt verteld dat meer dan 100 keer zoveel data nodig is geweest voor het zoeken naar deze gracht, als voor het zoeken naar de gracht van breedte $\sqrt{10}$. Hieruit wordt vervolgens de conclusie getrokken: "This leads us to believe that the conjecture is true"[JR, p.222]. Dit lijkt een vreemde conclusie, gezien mij het bestaan van een grotere gracht niet per definitie minder waarschijnlijk lijkt als er meer data nodig is voor het vinden ervan.

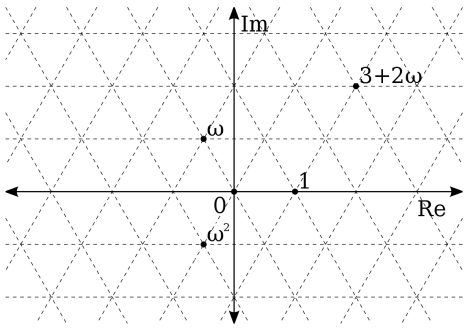
6.2 Guy

Richard Guy stelt in zijn boek [Guy] de vraag of het mogelijk is om over Gaussische priemgetallen naar oneindig te lopen en voegt daaraan toe: "presumably not"[Guy, p.34]. Hij grijpt terug naar het bewijs van Jordan en Rabung dat de stapgrootte minstens 4 moet zijn, maar geeft verder geen onderbouwing voor de uitspraak "presumably not".

6.3 Haugland

Noorse wiskundige Jan Kristian Haugland geeft in zijn artikel [Ha] aan dat discussie bestaat over de standpunten die men aanneemt ten opzichte van het vermoeden van Erdös. Dit vermoeden stelt Haugland op precies dezelfde manier als Jordan en Rabung doen in hun artikel [JR] (zie vermoeden 6.1). Hij vertelt hierbij dat Jordan en Rabung geloven dat het vermoeden juist is en dat Guy meer sceptisch is ten aanzien van de juistheid van het vermoeden. Hauglands eigen insteek is: het vermoeden van Erdös is onjuist. Het artikel is in het Noors en ik heb een poging gedaan tot het vertalen ervan. De uitleg hieronder is de informatie die ik heb opgemaakt uit deze eigen vertaling.

Figuur 5: Weergave van het driehoekige patroon dat Eisenstein-Jacobigehelen vormen in het vlak[12].



Andere gehelen in het complexe vlak

Haugland geeft aan dat er een gelijkenis bestaat tussen de Gaussische gehelen en de Eisenstein-Jacobigehelen ($\mathbb{Z}[\omega]$, dit zijn andere gehele getallen in het complexe vlak, van de vorm $a+b\omega$ met $\omega = (-1+\sqrt{-3})/2$ en $a, b \in \mathbb{Z}$) en laat zien dat een dergelijke wandeling over Eisenstein-Jacobipriemgetallen niet mogelijk is. 'Gezien de Eisenstein-Jacobigehelen veel overeenkomsten vertonen met de Gaussische gehelen, is het vermoeden van Erdös waarschijnlijk onjuist' [Ha, p.168]. Om de rest van het artikel te kunnen begrijpen, moeten we een paar dingen weten van Eisenstein-Jacobi(priem)getallen. Ik zal slechts de belangrijke eigenschappen onder elkaar zetten (zoals gevonden in [Guy, p.35]).

1. ω is een complexe oplossing van de vergelijking $\omega^2 + \omega + 1 = 0$.
2. Eistenstein-Jacobigehelen hebben een unieke priemfactorisatie (net als gehele getallen en Gaussische gehelen).
3. Er zijn 6 eenheidselementen in $\mathbb{Z}[\omega]$, namelijk ± 1, $\pm\omega$ en $\pm\omega^2$.
4. Eisenstein-Jacobigehelen vormen in het vlak een driehoekig patroon, zie figuur 5.
5. De norm van $x \in \mathbb{Z}[\omega]$ is op dezelfde manier gedefinieerd als de norm

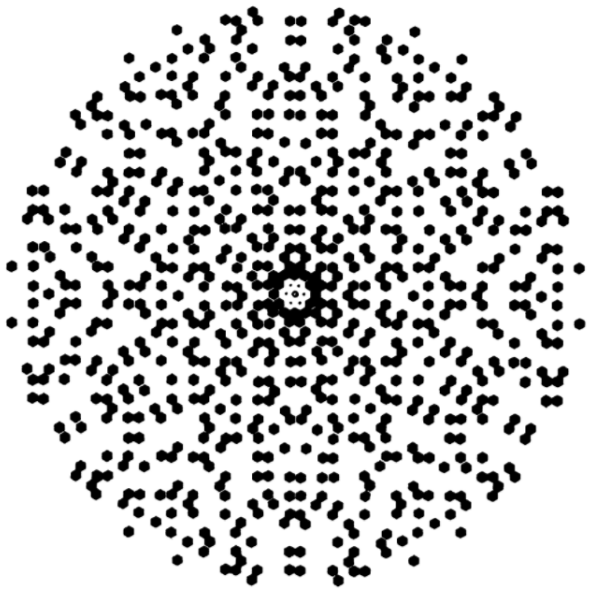
[12] Afbeelding van Wikimedia Commons,
https://commons.wikimedia.org/wiki/File:Eisenstein_integer_grid.svg;
Zelf afbeelding bijgewerkt (ω^2 toegevoegd).

in $\mathbb{Z}[i]$. Als we dus de norm nemen van $a + b\omega$, dan krijgen we

$$\begin{aligned} N(x) &= N(a + b\omega) \\ &= N\left(a - \tfrac{b}{2} + \tfrac{b\sqrt{3}}{2}i\right) \\ &= \left(a - \tfrac{b}{2}\right)^2 + \left(\tfrac{b\sqrt{3}}{2}\right)^2 \\ &= a^2 - ab + b^2 \ . \end{aligned}$$

6. Het getal 2 en de reële priemgetallen van de vorm $6k - 1$ zijn ook Eisenstein-Jacobipriem; 3 en de reële priemgetallen van de vorm $6k+1$ zijn samengesteld in $\mathbb{Z}[\omega]$. Dit reële priemgetal is dan gelijk aan de norm van een getal $x \in \mathbb{Z}[\omega]$ (bijvoorbeeld $7 = (2 - \omega)(2 - \omega^2) = 4 + 2 + 1 = N(2 + \omega)$; voor meer voorbeelden zie [Guy, p.35]).

7. Eisenstein-Jacobipriemgetallen bevat een hexagonale (zesvoudige) symmetrie, vanwege de zes eenheden. Zie hiervoor figuur 6.



Figuur 6: Hexagonale symmetrie van de Eisenstein-Jacobipriemgetallen[13].

[13] Afbeelding van [Guy, p.35].

Gekleurde equivalentieklassen

Haugland bewijst in zijn artikel de volgende stelling:

Stelling 6.3. *Voor iedere $M \in \mathbb{N}$ bestaat er een natuurlijk getal T zodat als $\{\beta_j\}_{j\geq 1}$ een oneindige rij van getallen in $\mathbb{Z}[\omega]$ (met $\omega = (-1+\sqrt{-3})/2$) die voldoen aan ggd$(T, N(\beta_j)) = 1$ voor alle j en $\lim|\beta_j| = \infty$, dan $|\beta_{j+1} - \beta_j| \geq M$ voor oneindig veel j.*

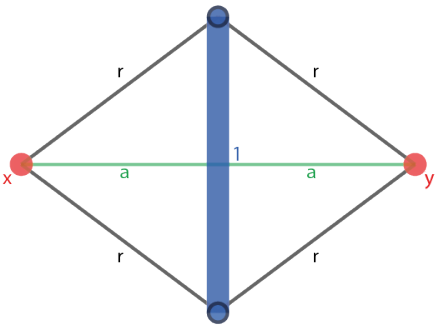
In de stelling staat dus dat er voor iedere stapgrootte (M) een gat tussen twee priemgetallen (β_j) bestaat die groter of gelijk is aan de gekozen stapgrootte (en gezien dit voor iedere M mogelijk is, is er dus ook altijd een gat te vinden tussen twee priemgetallen dat groter is dan de stapgrootte).
Het eerste dat Haugland noemt in zijn bewijs is dat de verdeling van de getallen x waarvoor $\text{ggd}(T, N(x)) = 1$ symmetrieën bevat, gezien we weten dat voor de norm $N(a + b\omega) = a^2 + ab + b^2$ het volgende geldt.

1. $N(x\omega) = N(x)$;
2. $N(a + b\omega + T) = N(a + b\omega) + T(T + 2a + b) \equiv N(a + b\omega) \pmod{T}$;
3. $N(a + b\bar{\omega}) = N(a + b\omega)$ (met $\bar{\omega}$ de geconjugeerde van ω).

Vervolgens merkt hij op dat de transformaties $x \mapsto x\omega$, $x \mapsto x + T$ en $x \mapsto \bar{x}$ afstandbewarende transformaties in $\mathbb{C}$ zijn, die tevens ook de verzameling $T\mathbb{Z}[\omega]$ genereren. Wegens bovenstaande symmetrieën is het dan afdoende om te kijken naar de dichtheid van de priemgetallen in $\mathbb{Z}[\omega]$ binnen de driehoek met hoekpunten $0, T$ en $T\omega$ (en dat is dan representatief voor heel $\mathbb{Z}[\omega]$). Voor het gemak noem ik deze driehoek B (Haugland doet dit niet, maar dit maakt het bespreken van de driehoek makkelijker). Haugland gebruikt in zijn bewijs dat de dichtheid (een reëel getal tussen 0 en 1) van de getallen x binnen bovengenoemde driehoek B die voldoen aan $\text{ggd}(T, N(x)) = 1^*$ willekeurig dicht bij 0 te brengen is. Hij bewijst dit aan de hand van de natuurlijke dichtheid van reële priemgetallen $p \equiv 1 \pmod 6$. Ik ga dit bewijs niet reproduceren, dit is terug te vinden in het artikel [Ha, p.169].

Haugland beschrijft het volgende principe: kleur de getallen die voldoen aan (*) rood en laat de rest van de getallen wit. De rode getallen zijn de getallen waar nu eventueel overheen kan worden gelopen, want de getallen met grootste gemene deler groter dan 1 met T zijn getallen met dezelfde (priem)delers als T (met uitzondering van de priemdelers van T, maar dit zijn er slechts eindig veel): deelbare getallen dus. Kleur de witte

getallen die géén rood getal om zich heen hebben binnen een afstand van $< r = \frac{1}{2}\sqrt{M^2+1}$ blauw. Nu heeft ieder roodgekleurd getal een aantal, zeg A, getallen in de buurt liggen die **niet** blauw zijn en als we de dichtheid van de rode getallen binnen driehoek B nu d noemen, dan is de dichtheid van de blauwe getallen in de driehoek minstens $1 - Ad$. Omdat we eerder gesteld hebben dat d zo dicht bij 0 kan worden gebracht als we willen, kunnen we zeggen dat de dichtheid van de blauwe getallen in driehoek B willekeurig dicht bij 1 komt. Nadat we alle blauwe getallen hebben gedefinieerd: maak alle witte en rode getallen (in het gehele vlak) dezelfde kleur, zeg geel. We hebben nu twee kleuren en kunnen een equivalentierelatie definiëren op deze kleuren. We zeggen dat x equivalent is met x' dan en slechts dan als er een rij $\{y_i\}$ van dezelfde kleur bestaat, die voldoet aan $|y_{i+1} - y_i| = 1$ en die zowel x als x' bevat. Na het definiëren van deze gekleurde equivalentieklassen, stelt Haugland dat er precies één equivalentieklasse bestaat die alle drie de randen van driehoek B raakt. Ook hiervoor geeft hij in het artikel [Ha, p.169] een bewijs dat ik niet zal reproduceren. De dichtheid van de blauwe getallen binnen driehoek B is willekeurig dicht bij 1 gebracht, dus het ligt het meest voor de hand dat de blauwe equivalentieklasse degene is die alledrie de randen raakt (voor onderbouwing van deze uitspraak, zie [Ha, p.169]). De conclusie berust nu op de periodiciteit van driehoek B en het feit dat de gele equivalentieklasse binnen één driehoek in de hoeken wordt ingesloten door de blauwe equivalentieklasse. Alle driehoeken in het vlak zijn rotaties, translaties en reflecties (afstandsbewarende transformaties) van de driehoek met hoekpunten $(Tx, T(x+1), T(x+\omega))$, waardoor de blauwe equivalentieklassen alle kanten op vertakken en de gele equivalentieklassen volledig omvatten: om naar oneindig te lopen moet dus meer dan eens een blauwe gracht worden overgestoken. De kleinste afstand die twee voorheen rode (dus begaanbare) getallen x, y die gescheiden worden door een



Figuur 7: De blauwe punten boven en onder zijn twee punten uit de blauwe gracht, die maximaal 1 uit elkaar liggen. De kleinste afstand die x en y van elkaar kunnen liggen als er een blauwe gracht tussen ligt is $2a$ (als de blauwe getallen dichter bij elkaar liggen, wordt de afstand tussen de rode getallen alleen maar groter).

blauwe gracht van elkaar liggen, is nu gelijk aan

$$\begin{aligned} |x-y| &= 2\sqrt{r^2 - \left(\tfrac{1}{2}\right)^2} \\ &= \sqrt{4\left(\left(\tfrac{1}{2}\sqrt{M^2+1}\right)^2 - \tfrac{1}{4}\right)} \\ &= \sqrt{M^2} \ = M \ . \end{aligned} \tag{6}$$

Om te verduidelijken waarom (6) de afstand aangeeft tussen de twee rode getallen, heb ik figuur 7 gemaakt, waarin te zien is hoe x en y ten opzichte van elkaar en ten opzichte van de blauwe gracht (en punten) liggen in de meest optimale situatie.

6.4 Gethner en Stark

Ellen Gethner is ook één van de auteurs van [GWW] en heeft dus meerdere onderzoeken naar het probleem gedaan. In het artikel [GS] dat zij geschreven heeft samen met H.M. Stark wordt het volgende vermoeden onderbouwd.

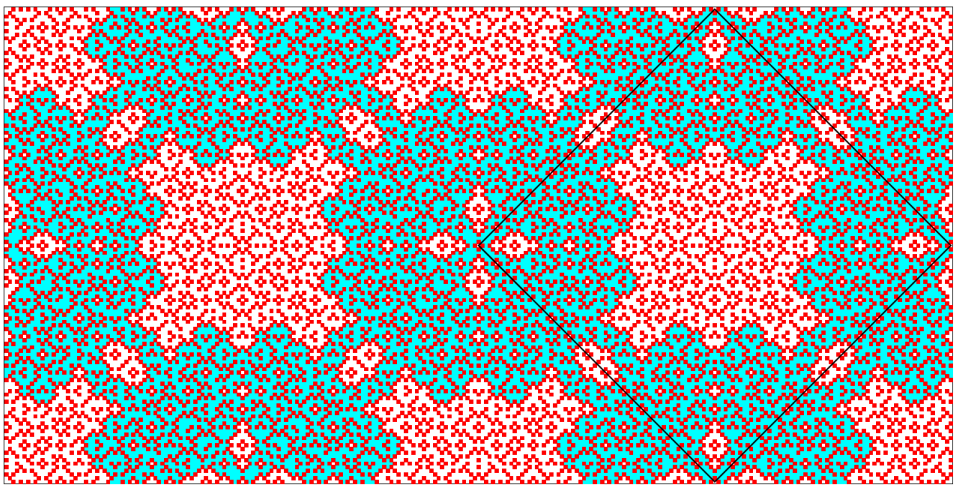
Vermoeden 6.4. *Zij $k > 0$ gegeven. Er bestaat een $M_k \in \mathbb{N}$ zodanig dat als men stappen zet van hooguit grootte k en begint op een willekeurig Gaussisch priemgetal in het vlak, dat men hooguit M_k stappen kan zetten op verschillende Gaussische priemgetallen voordat er op een samengesteld Gaussisch geheel moet worden gestapt.*

Er is dus volgens hen géén wandeling met begrensde staplengte naar oneindig over Gaussische priemgetallen mogelijk, ongeacht waar in het vlak het startpunt ligt. Gethner en Stark bewijzen dit voor stapgroottes $k = 2$ en $k = \sqrt{2}$. De insteek die zij hiervoor gebruiken is de periodiciteit van getallen modulo een ander getal.

Manier van bewijzen

Eerst wordt het vermoeden bewezen voor stapgrootte $k = \sqrt{2}$. Hoe dit bewezen is, zal ik hier in eigen woorden reproduceren en toelichten, aan de hand van figuur 8. Neem een vierkant met hoekpunten $\{0,\ 65+65i,\ 130,\ 65-65i\}$ (de keuze voor deze hoekpunten zal ik later toelichten), en beschouw verzameling S van Gaussische gehelen binnen dit vierkant. Kleur alle punten $x \in S$ rood, dan en slechts dan als geldt $\text{ggd}(x, 65+65i) = 1$

Figuur 8: Visuele weergave periodiciteit in het Gaussische vlak. Het zwarte vierkant rechts heeft hoekpunten $\{0, 65+65i, 130, 65-65i\}$[15].



en verbind iedere twee punten met een rode lijn dan en slechts dan als ze hooguit $\sqrt{2}$ uit elkaar liggen. Voor alle punten $y \in S$ die **niet** rood zijn geldt $\text{ggd}(y, 65+65i) > 1$. Dit betekent dat de niet-rode punten ofwel niet priem zijn, ofwel een priemdeler zijn van $65+65i$ (want met stelling 3.15 op pagina 14 weten we dat ook Gaussische gehelen een unieke priemontbinding hebben). Als we het deel dat afgebakend wordt door rode lijnen waarin $2+2i$ ligt blauw kleuren, zien we dat er een gracht ligt, breder dan $\sqrt{2}$, waarover niet gestapt kan worden, omdat dit slechts samengestelde getallen (en priemdelers) bevat. Uiteraard bevat het blauwe gedeelte ook priemdelers van $65+65i$, maar deze priemdelers zijn allen kleiner dan $65+65i$. Gezien het patroon in S periodiek is (want het hangt af van congruentie van getallen modulo $65+65i$), komen we verderop in het vlak in de problemen, omdat daar de blauwe stukken geen priemdelers van $65+65i$ meer bevatten (dus alleen nog maar samengestelde getallen). Het aantal punten in S is dan een bovengrens voor het aantal stappen met grootte $\sqrt{2}$ dat gezet kan worden voor op een samengesteld getal moet worden gestapt.

[15] Afbeelding van [GS, p.290].

Getalkeuze

Om dit te bewijzen voor stapgrootte $k = 2$, wordt hetzelfde trucje toegepast, echter met een andere verzameling S. In het artikel wordt gekozen voor een vierkant met hoekpunten $\{0,\ 7113990,\ 7113990 + 7113990i,\ 7113990i\}$, met de toevoeging dat dit een kleiner vierkant mag zijn, maar dat met meer data simpelweg makkelijker te programmeren is. Dit getal lijkt op het eerste gezicht vrij willekeurig (er zijn 'logischere' grote getallen dan 7113990), maar de keuze voor dit getal heeft vermoedelijk te maken met de priemontbinding ervan. Zoals eerder gezegd is ook $65 + 65i$ tot op zekere hoogte willekeurig en dit heeft dezelfde reden. Ontbonden in priemen krijgen we $65 + 65i = (1 + i)(2 + i)(2 - i)(3 + 2i)(3 - 2i)$, ofwel $65 + 65i$ is opgebouwd uit de drie kleinste priemgetallen (geassocieerden niet meegerekend). Als je een getal opbouwt uit meer priemgetallen, dan krijg je ook meer getallen in de volledige verzameling Gaussische gehelen die een grootste gemene deler met dat getal hebben dat groter is dan 1. Je filtert dus ook alle veelvouden (en dus samengestelde getallen) van deze Gaussische priemdelers uit. In ons vierkant met de hoekpunten gerelateerd aan $77113990 + 7113990i$, filteren we zelfs alle veelvouden van 2, 3, $2 \pm i$, $3 \pm 2i$, $4 \pm i$, $5 \pm 2i$ en $6 \pm i$ uit: de eerste 7 priemgetallen (geassocieerden niet meegerekend). Met zoveel mogelijk Gaussische priemdelers, krijgen we zo veel mogelijk samengestelde getallen waarover niet gelopen kan worden.

6.5 Vardi

Ilan Vardi gebruikt in zijn artikel [V] een heel andere methode om meer te ontdekken over de wandeling. Hij gebruikt de zogenaamde 'percolatietheorie', wat eigenlijk neerkomt op de vraag: stel dat er vloeistof wordt gegoten op poreus materiaal, kan deze vloeistof dan van ruimte naar ruimte de andere kant van het materiaal bereiken? Zie [Wi] voor een korte uitleg en bij interesse zie [SA] voor een uitgebreidere introductie in percolatietheorie. Percolatietheorie valt onder kansrekening, wat buiten het bestek van deze scriptie ligt. Ik heb er daarom voor gekozen om slechts kort en globaal uit te leggen hoe Vardi percolatietheorie toepast op ons probleem en tot welke conclusie hij gekomen is. Lees [V] voor het volledige bewijs.

Percolatietheorie

Vardi noemt kort de term *bond percolation* voor het onderzoeken van de kans dat een vloeistof door een vaste substantie zal sijpelen, als deze substantie met een bepaalde kansverdeling smalle dan wel bredere doorgangen heeft. Bewezen is dat hiervoor een kritieke kans bestaat waarvoor de vloeistof door de substantie zal sijpelen. De volgende term die genoemd wordt is *site percolation*, waar hetzelfde wordt onderzocht, maar dan heeft de substantie met een bepaalde kansverdeling al dan niet open doorgangen. Een doorgang is gesloten als twee punten verbonden zijn en dat is het geval als twee punten hooguit afstand k hebben ten opzichte van elkaar. Een limiet van dit probleem wordt gegeven door het *Poisson blob model*, waarbij cirkels met straal $k/2$ worden getekend en gekeken wordt naar het al dan niet overlappen van de schijven. In het geval van ons probleem wordt nu gekeken naar een oneindig component van overlappende schijven rond Gaussische priemen. Hiervoor is de dichtheid van Gaussische priemen van belang, waarvoor een model wordt opgesteld aan de hand van Cramérs model van priemgetallen (het gedrag van niet-Gaussische priemgetallen in het reële vlak). Met deze modellen komt Vardi tot een kritieke waarde voor de stapgrootte die nodig is om de wandeling te voltooien.

Algemene conclusie

In dit artikel stelt Vardi dat met percolatietheorie voorspeld kan worden dat wanneer Gaussische gehelen ver genoeg van elkaar liggen, een wandeling over deze gehelen naar oneindig niet bestaat. Ook kan bewezen worden dat Gaussische priemen willekeurig kleine dichtheid hebben als we ver genoeg van de oorsprong zitten, dus dat een wandeling over Gaussische priemgetallen niet bestaat.

6.6 Gethner, Wagon en Wick

In het artikel [GWW] wordt gesteld dat, om te bewijzen dat de wandeling niet bestaat, het afdoende is om vast te stellen dat een 'gracht' om de oorsprong van breedte k bestaat voor ieder willekeurig getal k. Dit is nog niet gedaan en lijkt ook geen makkelijk vraagstuk. Het verhaal bestaat uit twee delen: in het eerste deel zetten de auteurs een stap verder in het onderzoek dat Jordan en Rabung hebben opgezet, waarbij zij komen tot een

stapgrootte van $\sqrt{26}$. Het verschil met Jordan en Rabung is dat Gethner, Wagon en Wick de Gaussische priemgetallen én de afstand tussen de priemen hebben laten genereren door mathematica, terwijl Jordan en Rabung slechts de Gaussische priemen hebben laten genereren door IBM 360, maar de afstanden ertussen met de hand hebben uitgezocht. In het tweede deel van het artikel van Gethner, Wagon en Wick formuleren zij een bewijs voor de stelling dat een wandeling naar oneindig over Gaussische priemen niet bestaat als deze over één lijn wordt gemaakt.

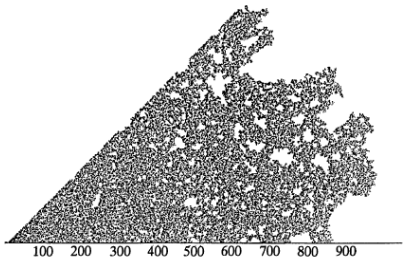
Grachten genereren en weergeven

Stapgrootte in het component	Verst gelegen bereikte punt	Grootste afstand afgelegd	Totaal aantal Gaussische priemen in het component
1	$2+i$	2,23	2
$\sqrt{2}$	$11+4i$	11,70	14
2	$42+17i$	45,31	92
$\sqrt{8}$	$84+41i$	93,47	380
$\sqrt{10}$	$976+311i$	1024,35	31221
4	$3297+2780i$	4312,61	347638
$\sqrt{18}$	$8174+6981i$	10749,4	2386129
$\sqrt{20}$	$109677+64268i$	127120	eindig
$\sqrt{26}$		≤ 5586757	eindig

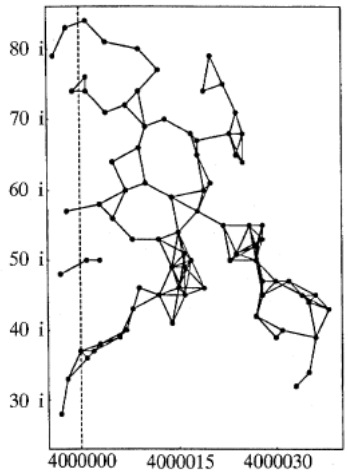
Tabel 1: Data van wandelingen met verschillende stapgroottes, gegenereerd met behulp van Mathematica. Er is een bovengrens vastgesteld voor de afstand die kan worden afgelegd met stapgrootte $\sqrt{26}$, waarvoor 9631177 Gaussische priemen zijn onderzocht.

De auteurs hebben visualisaties gemaakt van de ligging van de Gaussische priemgetallen en ze hebben de verst gelegen punten die bereikt kunnen worden met bepaalde stapgroottes gegenereerd. Ook de grootte van de wandeling met een bepaalde stapgrootte (dus het aantal bewandelde Gaussische priemen) kan hiermee worden weergegeven. Het genereren van deze gegevens gaat per niveau, waarbij steeds wordt gekeken naar de omliggende priemgetallen van een priemgetal op het huidige niveau en met welke stapgrootte deze bereikt kunnen worden. In tabel 1 zijn de gegevens weergegeven. Een visualisatie van de ligging van de Gaussische priemgetallen in het $\sqrt{10}$-component in het eerste octant is weergegeven in figuur 9. Omdat het verstgelegen punt van het $\sqrt{26}$-component niet wordt weergegeven in de tabel, hebben de auteurs op het gebied waarin dit punt ligt inge-

Figuur 9: Visuele weergave van het $\sqrt{10}$-component in het eerste octant. Onderstaande as is de reële as (imaginaire as is niet weergegeven), de zwarte stippen zijn (31121) Gaussische priemgetallen[17].



zoomd en in figuur 10 laten zien dat de wandeling in dat gebied doodloopt. Zij concluderen vervolgens dat een eindig component met stapgrootte $\sqrt{32}$ hoogstwaarschijnlijk bestaat, maar dat het aantonen hiervan nauwelijks de moeite waard is: men kan beter zoeken naar een rechtvaardiging van het vermoeden dat willekeurig grote grachten bestaan.



Figuur 10: Visualisatie van de paden die doodlopen. De punten zijn verbonden dan en slechts dan als ze $\sqrt{26}$ of minder uit elkaar liggen[19].

[17] Afbeelding van [GWW, p.330].
[19] Afbeelding van [GWW, p.332].

Geen wandeling over een rechte lijn

Als stap in de richting van een bewijs dat een wandeling naar oneindig over Gaussische priemen niet bestaat, hebben de auteurs een bewijs geformuleerd voor de volgende stelling:

Stelling 6.5. *Zij L een lijn die minstens twee verschillende Gaussische priemgetallen bevat en zij k een positief geheel getal. Dan bestaat er een Gaussisch geheel w op deze lijn zodanig dat alle Gaussische gehelen met een afstand k of minder van w samengesteld zijn.*

Voor het bewijs hiervan is nog een aantal getaltheoretische stellingen en resultaten nodig. De auteurs beginnen met het noemen en bewijzen van het volgende lemma:

Lemma 6.6. *Zij L een lijn die minstens twee verschillende Gaussische gehelen bevat. Dan bestaan er Gaussische gehelen $m \neq 0$ en b zodanig dat het reële en het imaginaire deel van m relatief priem zijn (hebben grootste gemene deler 1) en het Gaussische getal z ligt op deze lijn dan en slechts dan als er een geheel getal x bestaat waarvoor $z = mx + b$.*

Bewijs. Zij z_1, z_2 twee verschillende Gaussische gehelen op lijn L. Laat $b = z_1$ en $m_0 = z_2 - z_1$ en zij d de grootste gemene delers van het imaginaire en het reële deel van m_0, laat dan $m = m_0/d = u + vi$. Dan is $\text{ggd}(u, v) = 1$ (dit is een stelling, onder andere gegeven in [Beu, 3.3.2]) en ieder punt op de lijn is van de vorm $mx + b$ met $x \in \mathbb{R}$. Neem namelijk z_1, z_2 zoals bovengenoemd, dan bestaat er een x_1 waarvoor $z_1 = b$, namelijk $x_1 = 0$, en een x_2 zodanig dat $m_0 = z_1 - z_2$. We krijgen $m_0 = mx_2 + b - b = mx_2$ en dus geldt $x_2 = d$. Gezien lijn L een rechte lijn is en we twee punten op deze lijn hebben gevonden die inderdaad te schrijven zijn als $z = mx + b$, geldt dit voor ieder punt op lijn L.
Zij z een willekeurig Gaussisch geheel getal op de lijn L. Dan bestaat er een reëel getal x zodanig dat $z = mx+b$. Nu moeten we nog laten zien dat x een geheel getal is. We weten dat $mx = ux+vxi = z-b$ en dat is een Gaussisch geheel getal, dus ux, vx zijn gehele getallen. Omdat $\text{ggd}(u, v) = 1$, bestaan er r en s geheel zodat $ur + vs = 1$ (dit is ook een stelling, terug te vinden in [Beu, 3.4.1]). Nu geldt dat $uxr + vxs = x$ en dus geldt dat x een geheel getal is, dus $z = mx + b$ is een Gaussisch geheel getal.

□

Het volgende dat nodig is voor het bewijs van stelling 6.5 is de Chinese Reststelling. Ik zal deze stelling noemen en toelichten.

Stelling 6.7 (Chinese reststelling)**.** *Zij a_i en m_i gehele getallen zodanig dat alle m_i paarsgewijs relatief priem zijn. Dan bestaat er een oplossing voor het stelsel congruenties*

$$X \equiv a_1 \pmod{m_1},\ X \equiv a_2 \pmod{m_2},\ \ldots,\ X \equiv a_s \pmod{m_s}.$$

Bovendien geldt als x de kleinste oplossing is voor het stelsel congruenties, dan worden alle oplossingen gegeven door $\{x + Mn \mid n \in \mathbb{Z}\}$ met $M = m_1 m_2 \cdots m_s$ en dus is de oplossing uniek modulo M.

Bovenstaande stelling is gegeven zoals hij ook in het artikel [GWW, p.333] is gegeven. De toelichting ervan kan waarschijnlijk het best met een voorbeeld gegeven worden.

Voorbeeld 6.8. *Bekijk het stelsel vergelijkingen*

$$X \equiv 1 \pmod{2},\ X \equiv 2 \pmod{3},\ \ldots,\ X \equiv 0 \pmod{5}.$$

De kleinste oplossing hiervan is 5 *en we zien inderdaad dat de overige oplossingen* (35, 65, 95, *etc*) *gegeven worden door $\{5 + 30n \mid n \in \mathbb{Z}\}$.*

De auteurs stellen dat de Chinese reststelling geldt voor Gaussische gehelen. Gezien het bewijs van stelling 6.5 vrij uitgebreid is besproken in het artikel, zal ik dit slechts beknopt reproduceren/toelichten. Hierin zal ik weglaten waarom bepaalde keuzes (mogen) worden gemaakt.
In het bewijs voor stelling 6.5 lijn L gedefinieerd met m en b als in lemma 6.6. Het bewijs is onderverdeeld in 3 situaties: m is reëel (dus L is horizontaal); m is imaginair en het reële deel van m is 0 (dus L is verticaal); m is imaginair en zowel het imaginaire als het reële deel van m zijn ongelijk aan 0. De eerste twee situaties worden op soortgelijke manier behandeld. Er wordt een geheel getal w op de lijn L geconstrueerd, zodanig dat voor iedere z op de lijn met afstand tot w kleiner dan een bepaalde k geldt dat z samengesteld is. Hiertoe wordt z_j gedefinieerd als de verzameling Gaussische gehelen met $|z_j| < k$ voor $j = 1, 2, ..., N$ en er wordt een stelsel congruenties $x \equiv a_j \pmod{b_j}$ gedefinieerd met de volgende eigenschappen:

- Alle a_j en b_j zijn gehele getallen;
- Iedere b_j is groter dan 1;

- Alle b_j zijn paarsgewijs relatief priem (dus ze hebben onderling allemaal een grootste gemene deler gelijk aan 1);
- $z_j + a_j$ niet relatief priem met b_j (dus $z_j + a_j$ en b_j hebben een grootste gemene deler, zeg q_j, groter dan 1).

Dat een stelsel dat aan deze eisen voldoet gedefinieerd kan worden, wordt bewezen in het artikel. Met de Chinese reststelling kan dan een oplossing gevonden worden gevonden voor dit stelsel, noem een oplossing w. Nu komt de truc:

$$\begin{aligned} w &\equiv a_j \pmod{b_j} \\ w + z_j &\equiv a_j + z_j \pmod{b_j} \\ w + z_j &\equiv 0 \pmod{q_j} \end{aligned}$$

Wat dus betekent dat q_j een deler is van $w + z_j$ en dus dat $w + z_j$ samengesteld is voor alle $j = 1, 2, ..., N$.

De derde situatie is ingewikkelder om te bewijzen. Kort gezegd wordt er wederom een stelsel congruenties opgesteld zodat de Chinese reststelling kan worden toegepast. Op soortgelijke manier als bovenstaand kan dan worden laten zien dat alle getallen op dezelfde lijn deelbare getallen zijn. Ik ben tot hier gekomen met het reproduceren van dit bewijs, zie het artikel [GWW] voor het volledige bewijs.

7 Waarom is dit een lastig probleem?

We hebben besproken wat het Gaussische grachtenprobleem inhoudt en welke onderzoeken ernaar gedaan zijn, maar toch kun je je afvragen: waarom is dit probleem zo moeilijk op te lossen? Laten we eens kijken naar de verschillen en overeenkomsten tussen het algebraïsche grachtenprobleem en het Gaussische grachtenprobleem, wellicht brengt ons dat tot inzichten.
Op de reële as hoeven we slechts op zoek te gaan naar een gat tussen twee priemgetallen in één dimensie; in het Gaussische vlak moeten we in twee dimensies kijken. Op de reële as zetten we een stap verder richting oneindig als we een priemgetal verder lopen, in het Gaussische vlak is dat niet zo. Sterker nog, soms is het nuttig om een stap terug te zetten. Kijk nog eens naar figuur 3 op pagina 17 en bedenk dat we met stapgrootte 2 aan het wandelen zijn. Stel dat we geen stap terug zouden kunnen zetten, dan kunnen we stranden op $10 + 9i$, waar vandaan we een stap zouden moeten zetten van breedte $\sqrt{10}$ om naar $13 + 10i$ te komen. Als we terugstappen op $10 + 7i$, dan kunnen we via $11 + 9i$ schuin naar boven weer een stuk verder lopen: volgens tabel 1 op pagina 33 tot $42 + 17i$. De grachten zijn dus ook nog eens niet netjes rond met een gelijke straal rond de hele oorsprong, maar ze hebben een vreemde vorm die alleen te vinden is door per stapsteen te kijken naar de ligging van de volgende stapsteen.
Een belangrijk verband tussen de reële priemgetallen en Gaussische priemgetallen is een resultaat dat we hebben ontdekt tijdens het formuleren van het bewijs van stelling 3.8 op pagina 15: ieder Gaussish priemgetal is een deler van een positief reëel priemgetal p. Deze p is uniek.

Stelling 7.1. *Ieder Gaussisch priemgetal γ is een deler van precies één positief reëel priemgetal p (geassocieerden van γ worden niet gezien als andere Gaussische priemgetallen dan γ).*

Bewijs. We weten dat γ een deler is van $N(\gamma)$ en dat de norm een reëel geheel getal is. Als $N(\gamma)$ priem in $\mathbb{Z}$, dan zijn we klaar. Stel dat $N(\gamma)$ samengesteld is in $\mathbb{Z}$, dan geldt wegens unieke priemfactorisatie in $\mathbb{Z}$ dat $N(\gamma) = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ en dus is γ een deler van p_1 of p_2 of ...of p_r (zie stelling 3.15 op pagina 14), dus γ deelt ten minste één reëel priemgetal p.
Stel nu γ deelt zowel p als p'. Dan geldt dat γ een deler is van $xp - yp'$ en die kunnen we met de juiste keuze van x en y gelijk stellen aan 1 (zie voor uitleg van deze aanname [Beu, h.14]). Nu staat er echter dat γ een deler is van 1 en dat is natuurlijk een tegenspraak. Dus p is uniek. □

We weten nu dat er minstens zoveel reële priemgetallen zijn als Gaussische priemgetallen (geassocieerden niet meegerekend, maar dit probleem wordt opgelost doordat we slechts kijken in het eerste octant van het Gaussische vlak). Dit maakt het niet makkelijker, omdat je nu zou verwachten dat als de dichtheid van reële priemgetallen niet afdoende is om een wandeling naar oneindig mogelijk te maken, dat de dichtheid van Gaussische priemgetallen waarvan er minder bestaan dat al helemaal niet zou zijn. Echter is dan geen rekening gehouden met de ligging van de Gaussische priemgetallen, dus die conclusie mag niet zo snel worden getrokken. Een ander onopgelost probleem dat zowel in [Guy, A8] als in [GWW, p.329] wordt aangehaald, heeft te maken met deze ligging.

Vermoeden 7.2. $\lim_{n\to\infty}(\sqrt{p_{n+1}} - \sqrt{p_n}) = 0$ *met* p_n *het* n*-de (reële) priemgetal.*

Gaussische priemgetallen in het eerste octant (dus van de vorm $a + bi$, met $a, b \geq 0$ en $a > b$) zijn altijd van de vorm $a^2 + b^2 = p$ met p een reëel priemgetal (zie stelling 3.8 op pagina 12). Stel nu a_1+b_1i met $a_1^2+b_1^2 = p_1$ en a_2+b_2i met $a_2^2+b_2^2 = p_2$ Gaussische priemgetallen, dan zijn de afstanden van deze priemgetallen tot de oorsprong respectievelijk gelijk aan $\sqrt{a_1^2 + b_1^2} = \sqrt{p_1}$ en $\sqrt{a_2^2 + b_2^2} = \sqrt{p_2}$. Deze afstanden tot de oorsprong komen dus steeds dichter bij elkaar te liggen als de priemgetallen zich verder richting oneindig in het Gaussische vlak bevinden. Het is nu onmogelijk om ver in het Gaussische vlak een cirkelvormige gracht te vinden om de oorsprong heen en het bestaan van een wandeling naar oneindig over de priemgetallen met begrensde staplengte wordt waarschijnlijker.
Tot slot zijn vraagstukken over priemgetallen vaker lastig op te lossen. De eigenschap 'priem' zegt slechts iets over deelbaarheid van getallen door 'welk ander getal ook'. Dit maakt het ongrijpbaar en zegt weinig over de afstand tussen twee getallen die niet deelbaar zijn door andere getallen.

8 Een oneindige zoektocht naar een oneindige wandeling

Over de reële as kan niet met begrensde staplengte over alleen priemgetallen naar oneindig worden gelopen. De vraag of een wandeling naar oneindig met begrensde stapgrootte bestaat in het Gaussische vlak als alleen Gaussische priemgetallen als stapstenen mogen worden gebruikt, is tot op heden een onopgelost probleem en noemen we 'het Gaussische grachtenprobleem'. Een oplossing van het probleem kan worden gevonden als bewezen wordt dat voor iedere willekeurige stapgrootte k een gracht rond de oorsprong bestaat die groter is dan deze k.

Basil Gordon was de eerste wiskundige die in 1962 dit probleem voorlegde op het *International Congress of Mathematicians* in Stockholm en sindsdien zijn verschillende onderzoeken naar dit probleem gedaan. Jordan en Rabung zijn de eersten die in 1970 hun onderzoek hebben gepubliceerd. Zij hebben Gaussische priemgetallen laten genereren door een computerprogramma en hebben handmatig grachten gevonden van breedtes 2, $\sqrt{10}$ en 4. De volgende wiskundige die een artikel publiceerde over het probleem was Haugland, die de Gaussische gehelen vergeleek met Eisenstein-Jacobi gehelen en bewees dat een wandeling naar oneindig over Eisenstein-Jacobi priemgetallen met begrendse staplengte niet mogelijk is, dus dat het bestaan van een dergelijke wandeling over Gaussische priemgetallen onwaarschijnlijk is. Gethner en Stark hebben gebruik gemaakt van periodiciteit van deelbaarheid van getallen en daarmee hun vermoeden dat de wandeling niet bestaat versterkt. Vardi heeft percolatietheorie toegepast op het probleem en daarmee een ondergrens gesteld voor de stapgrootte waarmee een onbegrensde wandeling bestaat. Gethner, Wagon en Wick zijn de laatsten die een artikel hebben gepubliceerd over dit onderwerp, waarin zij hebben bewezen dat een dergelijke wandeling naar oneindig in het Gaussische vlak niet mogelijk is als deze over één lijn wordt gemaakt.
Al deze onderzoeken zijn versterkingen van vermoedens over het al dan niet bestaan van de wandeling, maar geen directe oplossing van het Gaussische grachtenprobleem.

De moeilijkheid van het oplossen van het probleem ligt hem grotendeels in het feit dat in iedere richting kan worden gelopen, in plaats van in één richting. Bovendien heeft de definitie van priemgetallen een ongrijpbaar karakter. Een ander onopgelost probleem over priemgetallen is het vermoeden dat de afstanden tot de oorsprong van twee verschillende Gaussische priem-

getallen (van de vorm $a + bi$, $a, b \neq 0$) die in het oneindige liggen, steeds dichter bij elkaar komen te liggen. Als dit het geval is, dan is het vinden van een perfect ronde gracht om de oorsprong heen onmogelijk, wat het bestaan van een wandeling naar oneindig met begrensde staplengte over Gaussische priemgetallen waarschijnlijker maakt.

De geschiedenis van het Gaussische grachtenprobleem is tot nog toe niet zo uitgebreid, maar gezien het mysterie dat nog altijd hangt rond dit probleem, lijkt het pad naar de oplossing van het probleem nog een oneindige wandeling.

Referenties

[A] Alladi, K. (2013). *Remembering Basil Gordon*. Laatst geraadpleegd op 3-1-2018, van http://www.ams.org/notices/201307/rnoti-p856.pdf.

[Ba] Babai, L., Pomerance, C., & Vértesi, P. (1998). The mathematics of Paul Erdös. *Notices of the AMS*, 45, 19-32.

[Beu] Beukers, F. (2015). *Getaltheorie: Een inleiding* (5e ed.). Amsterdam, Nederland: Epsilon Uitgaven.

[Bo] Boyer, C. B., & Merzbach, C. (2011). *A History of Mathematics* (3e ed.). Hoboken, New Jersey: John Wiley & Sons, Inc..

[G1] Gauss, C. F. (1801). *Disquisitiones Arithmeticae*. Leipzig, Duitsland: Gerhard Fleischer.

[G2] Gauss, C. F. (1832). *Theoria Residuorum Biquadraticorum: Commentatio Secunda*. Göttingen, Duitsland: Typis Dieterichianis.

[G2v] Ewald, W. (1999). *From Kant to Hilbert Volume 1: A Source Book in the Foundations of Mathematics* (Vol. 1, h. 7C). Ontleend aan http://web.a.ebscohost.com.proxy.library.uu.nl/ehost/ebookviewer/ebook/bmxlYmtfXzIxMTU4NV9fQU41?sid=5eb77f4f-6690-440e-b100-0ec208723bea@sessionmgr4009&vid=0&format=EB&rid=1

[Er] Erdös, P. (1949). On a new method in elementary number theory which leads to an elementary proof of the prime number theorem. *Proceedings of the National Academy of Sciences U.S.A*, 35, 374-384.

[Eu1] Euler, L. (1761). Theoremata circa residua ex divisione potestatum relicta. *Novi Commentarii academiae scientiarum Petropolitanae*, 7, 49-82. Ontleend aan http://eulerarchive.maa.org//index.html

[Eu2] Euler, L. (1783). Observationes circa divisionem quadratorum per numeros primos. *Opuscula Analtika*, 1, 64-84. Ontleend aan http://eulerarchive.maa.org//index.html

[GS] Gethner, E., & Stark, H. M. (1997). Periodic Gaussian Moats. *Experimental Mathamatics*, 6, 289-292.

[GWW] Gethner, E., Wagon, S., & Wick, B. D. (1998). A Stroll Through the Gaussian Primes. *The American Mathematical Monthly*, 105, 327-337.

[Guy] Guy, R. K. (1994). *Unsolved Problems in Number Theory* (2e ed.). New York, New York: Springer-Verlag.

[HW] Hardy, G. H., & Wright, E. M. (1960). *An Introduction to the Theory of Numbers* (4e ed.). London, England: Oxford University Press.

[Ha] Haugland, J. K. (1995). En spasertur på komplekse primtall. *Normat*, 4, 168-170.

[JR] Jordan, J. H., & Rabung, J. R. (1970). A Conjecture of Paul Erdös Concerning Gaussian Primes. *Mathematics of Computation*, 24, 221-223.

[K] Katz, V. J., & Parshall, K. H. (2014). *Taming the Unknown : A History of Algebra from Antiquity to the Early Twentieth Century*. Ontleend aan https://ebookcentral.proquest.com/lib/uunl/reader.action?docID=1609399

[Le] Legendre, A. M. (1798). *Essai sur la Théorie des Nombres*. Parijs, Frankrijk: Duprat.

[M] Montgomery, H. L. (1994). *Ten lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*. Providence, Rhode Island: American Mathematical Society.

[SA] Stauffer, D., & Aharony, A. (1994). *Introduction to percolation theory* (2e ed.). Londen, Engeland: Taylor and Francis Ltd.

[SW] Stillwell, J. (2010). *Mathematics and Its History* (3e ed.). Ontleend aan https://link-springer-com.proxy.library.uu.nl/book/10.1007

[V] Vardi, I. (1998). Prime Percolation. *Experimental Mathematics*, 7, 275-289.

[Wag] Wagon, S. (1998). *Mathematica in Action* (2e ed.). New York, New York: Springer.

[WR] Weisstein, E. W. (1999). *Moat-Crossing Problem*. Laatst geraadpleegd op 23-12-2017, van http://mathworld.wolfram.com/Moat-CrossingProblem.html

[Wi] Wikipedia (2017). *Percolation Theory*. Laatst geraadpleegd op 23-12-2017, van https://en.wikipedia.org/wiki/Percolation_theory

Bijlage 1

Gaussian moat problem

Butter, T.L. (Tara)
Sent: Thursday, November 02, 2017 5:53 PM
To: rkg@ucalgary.ca
Cc: rkg@cpsc.ucalgary.ca

Dear Mr. Guy,

Please forgive me for adressing you so buntly. It is with great interest that I read your work and decided to look up your contact details on the internet. My name is Tara Butter and I am a mathematics student at Utrecht University in Holland. I am writing my bachelor thesis about the Gaussian moat problem an for this, I also read the part of the Gaussian primes in your book 'Unsolved problems in Number Theory' (second edition) on page 33-35. Something that caught my interest in reading (the few) different published references to the problem, is that there seems to be no agreement on who would have been the first mathematician to come up with the problem. In the article of Jordan and Rabung you mention in your book, the problem is assigned to Paul Erds and in a more recent article from Gethner, Wagon and Wick ('A Stroll Through the Gaussian Primes', 1998), it is stated that Paul Erdös did not come up with the idea and that he himself assigned it to Basil Gordon (the problem being posed on a congress in Stockholm in 1962). What I found interesting in your book, is that you assign it to nobody (or to Motzkin and Gordon), but do not mention the name of Erdös. Was there a reason for that? To whom did you assign the problem and how did you find out that Motzkin was also working on this problem (I tried to find an article of Motzkin about the Gaussian moat problem but could not find it)?

Hopefully you will find the time to answer this e-mail, I am looking forward to hearing from you.

Sincerely,

Tara Butter
Student at Utrecht University

Re: Gaussian moat problem

rkg [rkg@ucalgary.ca]
Sent: Monday, November 06, 2017 6:47 PM
To: Butter, T.L. (Tara)
Cc: rkg@cpsc.ucalgary.ca

Dear Tara Butter,
My recollection is that I first heard of the problem in conversations with Motzkin. R.