Wie vermoedde Artin?

Bert van Dijk en Alex Vonk
Begeleider: Dr. P. Moree

Samenvatting

In 1927 uitte Emil Artin het vermoeden dat kwadraatvrije getallen $q \in \mathbb{Q}$ primitieve wortel waren voor oneindig veel priemgetallen. Hooley bewees dit vermoeden in 1967 onder aanname van de Gegeneraliseerde Riemann Hypothese. Was Artin de eerste die dit vermoeden had? Gauss uitte eerder een vermoeden over het getal 10 als primitieve wortel voor oneindig veel priemgetallen. Chebyshev bewijst dat 2 een primitieve wortel is voor priemgetallen van de vorm $4q + 1$, waar q ook een priemgetal is. Wertheim gebruikt dit resultaat om aan te tonen dat 3, 5, 7, 10, 11 primitieve wortels zijn voor soortgelijke priemgetallen. Ten slotte kijken we naar de vraag, hoe groot deze speciale groepen priemgetallen zijn.

Inhoudsopgave

Hoofdstuk 1

Inleiding

Tijdens de cursus Algebra 2A maak je kennis met het begrip primitieve wortel. Je gebruikt ze om te rekenen met eindige, cyclische groepen en leert dat het voortbrengers zijn. Ook leer je in te zien, dat in een eindige groep er meerdere primitieve wortels kunnen zijn. Primitieve wortels worden dus vanuit het licht van de eindige, cyclische groepen bekeken.
Wat wij in dit verslag gaan doen is het omgekeerde. Wij gaan eindige, cyclische groepen bekijken vanuit het licht van de primitieve wortels. Een belangrijk vermoeden, geuit door Emil Artin (1898-1962), over het aantal groepen waarvoor een bepaald getal een primitieve wortel is, is heden bekend onder de naam het Vermoeden van Artin. Wij zullen uitleggen wat dit vermoeden inhoudt en ons tevens afvragen: waren er al eerder wiskundigen bezig met deze vraag of was Artin de eerste die een uitspraak als deze deed.
In eerste instantie (Hoofdstuk 2) zullen we kijken naar specifieke gevallen van het Vermoeden. Om deze specifieke gevallen te kunnen bewijzen zullen we eerst wat, voor een lagerejaars student nieuwe, terminologie invoeren. In het volgende hoofdstuk (Hoofdstuk 3) zullen we het Vermoeden van Artin formuleren en uiteindelijk de link leggen met de voorgaande specifieke gevallen in Hoofdstuk 4. Hier gaan we proberen om in een van de gevallen na te gaan of hiermee echt een specifiek geval van het Vermoeden is geformuleerd.

Hoofdstuk 2

Begrippen en bewezen vermoedens

2.1 Notatie

Het onderzoek naar Artins vermoeden, is een onderzoek in de getaltheorie. Om deze discussie te volgen zijn enkele basisbegrippen noodzakelijk. De discussie gaat over priemgetallen, getallen alleen deelbaar door zichzelf of 1. Priemgetallen worden aangegeven met de letters p en q en leven in de verzameling van de natuurlijke getallen $\mathbb{N} = \{1, 2, 3, \ldots\}$ Maar wanneer we met priemgetallen rekenen kijken we naar de verzameling van de gehele getallen $\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$. Fixeer een priemgetal p, dan kan er een equivalentierelatie gelegd worden op de gehele getallen $\mathbb{Z}$ door twee getallen a en b equivalent te noemen als geldt:

$$a = xp + b, \text{ voor zekere } x \in \mathbb{Z}.$$

We noteren dit als $a \equiv b \pmod{p}$. In het geval dat er getalvoorbeelden worden gebruikt korten, we dit in tot $a \equiv b\,(p)$.
Neem van elke equivalentieklasse een representant $n \in \{0, 1, \ldots, p-1\}$. Dat dit mogelijk is, is intuïtief duidelijk [5]. Deze representanten heten de kleinste residuen modulo p en de equivalentieklassen worden wel genoteerd als $\{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$. Een bekend gegeven uit de groepentheorie stelt dat de verzameling getallen $\{n|(n, m) = 1,\ n, m \in \mathbb{Z}\}$ een groep onder vermenigvuldiging vormt ((n, m) duidt hier de grootste gemene deler van n en m aan). Deze groep wordt genoteerd als $(\mathbb{Z}/m\mathbb{Z})^*$. De cardinaliteit van deze groep wordt aangeduid met de Euler totiënt-functie: $\varphi(m)$. In het geval dat $m = p$ een priemgetal is, geldt dat deze verzameling bestaat uit de equivalentieklassen niet gelijk aan $\{\overline{0}\}$, dus $\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$. Een stelling die het gevolg

is van de Kleine Stelling van Fermat (zie vgl. (2.3)), zegt dat deze groep cyclisch is, dat wil zeggen: er is een element g zodat $\{\overline{g}, \overline{g}^2, \ldots, \overline{g}^{p-2}, \overline{g}^{p-1}\}$ alle elementen van de groep bevat. Het element g heet een primitieve wortel voor p. g heet niet *de* primitieve wortel voor p, omdat er vaak nog meer zijn. Er zijn in totaal namelijk $\varphi(p-1)$ primitieve wortels. De primitieve wortels zijn precies die getallen a^j, zo dat j relatief priem is met $p-1$ en de hoeveelheid hiervan komt dus overeen met de Euler totiënt.

2.2 Het Legendre symbool

Bekijk de vergelijking:

$$x^2 \equiv n \pmod{p}. \tag{2.1}$$

We zeggen dat n een kwadratisch residu is als er een x is die deze vergelijking oplost voor die n. We noteren dit als $n\mathbf{R}p$. Als n niet aan de vergelijking voldoet, dan noteren we $n\overline{\mathbf{R}}p$.

Voorbeeld 2.1 ($p = 7$**)** *Voor $p = 7$ zijn er de kwadratische residuen:*

$$1^2 \equiv 1\,(7), 2^2 \equiv 4\,(7) \text{ en } 3^2 \equiv 2\,(7).$$

We hebben de drie relaties $1\mathbf{R}7$, $2\mathbf{R}7$ *en* $4\mathbf{R}7$.

Wat opvalt als we naar dit voorbeeld kijken, is dat de helft van de getallen een kwadratisch residu is. In het algemeen blijkt dit ook zo te zijn:

Lemma 2.2 *Voor p een oneven priem zijn er precies $\frac{(p-1)}{2}$ kwadratische residuen en even zoveel niet-kwadratische residuen.*

Bewijs: Het is duidelijk dat er ten hoogste $\frac{(p-1)}{2}$ kwadratische residuen zijn, omdat zowel x^2 als $(-x)^2$ hetzelfde residu geven. Het zijn er ook minstens zoveel. De multiplicatieve groep $(\mathbb{Z}/p\mathbb{Z})^*$ heeft zoals gezegd een primitieve wortel g. De machten van g geven dan alle elementen uit de groep $\{g,\ g^2, \ldots,\ g^{p-1}\} = (\mathbb{Z}/p\mathbb{Z})^*$. En precies de helft van deze rij is duidelijk een kwadraat van een ander element. □

Met het begrip van de kwadratische residuen is het mogelijk om uitspraken te doen over "het primitieve wortel zijn" van bepaalde gehele getallen voor groepen priemgetallen. Het begrip Legendresymbool speelt hierin een cruciale rol.

Definitie 2.3 *Het Legendresymbool* $\left(\frac{n}{p}\right)$ *wordt gedefinieerd als*

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \textit{als } n \equiv 0 \pmod{p}, \\ 1 & \textit{als } n\mathbf{R}p \textit{ en} \\ -1 & \textit{als } n\overline{\mathbf{R}}p \end{cases}$$

Lemma 2.4 (Criterium van Euler) *Zij p een oneven priemgetal. Dan geldt voor alle n:*

$$\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod{p}. \tag{2.2}$$

Zo op het eerste oog is niet duidelijk of dit wel goed gedefinieerd is. Komt er bijvoorbeeld wel altijd ± 1 uit deze vergelijking?
De kleine stelling van Fermat zegt dat:

$$n^{p-1} \equiv 1 \pmod{p} \qquad \text{als } p \nmid n. \tag{2.3}$$

Omdat geldt:

$$n^{p-1} - 1 \;=\; (n^{(p-1)/2} - 1)(n^{(p-1)/2} + 1) \;\equiv 0 \pmod{p}, \tag{2.4}$$

geldt er inderdaad dat:

$$n^{(p-1)/2} \;\equiv\; \pm 1 \pmod{p}. \tag{2.5}$$

Wanneer n een kwadraat is, dus van de vorm x^2 voor zekere x, geldt $n^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$. □

2.3 Rekenregels voor het Legendre symbool

De volgende rekenregels worden veelvuldig gebruikt:

$$\left(\frac{mn}{p}\right) \;=\; \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \tag{2.6}$$

$$\left(\frac{n+p}{p}\right) \;=\; \left(\frac{n}{p}\right) \tag{2.7}$$

$$\left(\frac{-1}{p}\right) \;=\; (-1)^{(p-1)/2} \;=\; \begin{cases} 1 & \textit{als } p \equiv 1\,(4) \\ -1 & \textit{als } p \equiv 3\,(4) \end{cases} \tag{2.8}$$

$$\left(\frac{2}{p}\right) \;=\; (-1)^{(p^2-1)/8} = \begin{cases} 1 & \textit{als } p \equiv \pm 1\,(8) \\ -1 & \textit{als } p \equiv \pm 3\,(8) \end{cases} \tag{2.9}$$

Naast deze rekenregels die in veel bewijzen gebruikt kunnen worden, wordt de volgende misschien nog wel het meest toegepast:

Lemma 2.5 (Kwadratische wederkerigheid) *Voor oneven priemgetallen p en q, $p \neq q$ geldt:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \tag{2.10}$$

Deze formules en rekenregels vormen een goede basis om wat klassieke stellingen te bewijzen.

Stelling 2.6 (Chebyshev, 1849) *Laat q een priem zijn, zodat $p = 4q + 1$ priem is. Dan is 2 een primitieve wortel modulo p.*

Bewijs: De stelling van Lagrange geeft ons dat de orde van 2 een deler van $p - 1 = 4q$ moet zijn. Dit geeft als mogelijke ordes: $\{1, 2, 4, q, 2q, 4q\}$.

1. $\mathrm{ord}_p(2) = 1$, dan $2^1 = 2 \equiv 1 \pmod{p}$, maar $p = 4q + 1$, dus minstens gelijk aan 13.

2. $\mathrm{ord}_p(2) = 2$, dan $2^2 = 4 \equiv 1 \pmod{p}$, dus valt ook af vanwege $p \geq 13$.

3. $\mathrm{ord}_p(2) = 4$, dan $2^4 = 16 \equiv 1 \pmod{p}$, dit kan alleen als $p = 3$ of $p = 5$, dus deze orde valt ook af.

4. $\mathrm{ord}_p(2) = 2q$, we laten hier tevens zien dat $\mathrm{ord}_p(2) \neq q$, want als $\mathrm{ord}_p(2) \neq 2$ of $2q$, dan $\mathrm{ord}_p(2) \neq q$. Dus zeg $\mathrm{ord}_p(2) = 2q$, dan:

   $$2^{2q} \equiv 2^{(p-1)/2} \pmod{p},$$

   wegens $p = 4q + 1$ is $2q = \frac{p-1}{2}$. Volgens de rekenregels met het Legendresymbool is dit gelijk aan:

   $$\left(\frac{2}{p}\right) \overset{2.9}{\equiv} (-1)^{(p^2-1)/8}.$$

   Omdat q een oneven priem is, dus van de vorm $2k+1$, voor een $k \in \mathbb{N}$, geldt er:

   $$p = 4q + 1 = 4(2k + 1) + 1 = 8k + 5 \equiv -3 \pmod{8}$$

   En dus uiteindelijk volgens de rekenregels met het Legendresymbool:

   $$2^{2q} \equiv -1 \pmod{p}$$

De orde van 2 is gelijk aan $4q$, 2 is dus een primitieve wortel voor p. $\square$

In een later hoofdstuk zal de vraag bekeken worden hoeveel priemgetallen van de vorm $p = 4q + 1$ met q een priem bestaan.

2.4 7 doet ook mee...

Het resultaat van Chebyshev leidt tot de vraag of we soortgelijke uitspraken ook voor andere gehele getallen kunnen doen. Werk van Wertheim [15] geeft soortgelijke resultaten voor priemgetallen van de vorm $p = 4q + 1$, waar q een priem is. Er geldt telkens $k \in \mathbb{N} \cup \{0\}$:

$n = 3$ is een primitieve wortel, behalve voor $p = 13$.
$n = 5$ is een primitieve wortel als $q = 10k + 3, 9$, behalve voor 13.
$n = 6$ is *geen* primitieve wortel voor genoemde p, behalve voor $p = 13$.
$n = 7$ is een primitieve wortel als $q = 14k + 1, 3, 11$.
$n = 10$ is een primitieve wortel als $q = 10k + 7$.
$n = 11$ is een primitieve wortel als $q = 22k + 3, 5, 7, 15, 21$.

We zullen de uitspraak voor $n = 7$ bewijzen.

Stelling 2.7 (Wertheim, 1895) *Het getal 7 is een primitieve wortel voor priemgetallen p van de vorm $p = 4q+1$, waar $q = 14k+1, 3, 11$ een priemgetal is, met $k \in \mathbb{Z}$.*

Bewijs: De mogelijke ordes van 7 zijn weer de delers van $p-1$: $\{1, 2, 4, q, 2q, 4q\}$ Voor de gevallen 1 en 2 is makkelijk na te gaan, dat dit niet de ordes kunnen zijn. Voor de mogelijke orde 4 krijgen we:

$$7^4 = 2401 \equiv 1\,(p) \Rightarrow p|2400 \Rightarrow p = 2,\; p = 3 \text{ of } p = 5.$$

Het priemgetal p is dus duidelijk niet van de voorgeschreven vorm. Wederom geldt dat de orde q uitgesloten kan worden, door te bewijzen dat $2q$ geen orde van 7 kan zijn. Stel dat de orde van 7 gelijk is aan $2q$. Dan geldt:

$$7^{2q}\,(p) \equiv 7^{(p-1)/2} \overset{2.2}{\equiv} \left(\frac{7}{p}\right) \overset{2.5}{=} \left(\frac{p}{7}\right).$$

De laatste gelijkheid is waar wegens de kwadratische wederkerigheidswet, namelijk:

$$\left(\frac{7}{p}\right)\left(\frac{p}{7}\right) = (-1)^{(p-1)(7-1)/4} = (-1)^{\frac{3}{2}(p-1)} = (-1)^{6q} = 1,$$

dus $\left(\frac{p}{7}\right) = \left(\frac{7}{p}\right)$. Het eerste deel van deze vergelijking is gelijk aan:

$$\left(\frac{p}{7}\right) = \left(\frac{4q+1}{7}\right) = \begin{cases} \left(\frac{4(14k+1)+1}{7}\right) & = \left(\frac{56k+5}{7}\right) & = \left(\frac{5}{7}\right) \\ \left(\frac{4(14k+3)+1}{7}\right) & = \left(\frac{56k+13}{7}\right) & = \left(\frac{6}{7}\right) \\ \left(\frac{4(14k+11)+1}{7}\right) & = \left(\frac{56k+45}{7}\right) & = \left(\frac{3}{7}\right) \end{cases} \qquad (2.11)$$

Uit voorbeeld 2.1 is bekend dat $3\overline{\mathbf{R}}7$, $5\overline{\mathbf{R}}7$ en $6\overline{\mathbf{R}}7$, dus $\left(\frac{p}{7}\right) = -1$ en dus $\mathrm{ord}_p 7 \neq 2q$. De orde van 7 moet dus gelijk zijn aan $4q$. $\square$

Hoofdstuk 3

Het vermoeden van Artin

3.1 Breuken met Gauss

Een natuurlijke vraag om te stellen met betrekking tot het voorgaande is of de priemgetallen van de vorm $p = 4q + 1$, waar q een priemgetal is, oneindig vaak voorkomen. In het bijzonder voor $q = 14k + 1, 3, 11$. In dat geval zijn de getallen 2 en 7 namelijk oneindig vaak primitieve wortel. In zijn *Disquisitiones Arithmeticae* [5] uit Gauss het vermoeden dat 10 oneindig vaak een primitieve wortel is voor priemgetallen p. Wat dit vermoeden eigenlijk zegt, is dat de decimaalontwikkeling van $\frac{1}{p}$ oneindig vaak maximale lengte, namelijk $p - 1$, heeft.

Voorbeeld 3.1 *Voor $p = 3$: $\frac{1}{3} = 0.333\ldots$ De periode is gelijk aan 1. Deze waarneming is gelijk aan het waarnemen dat $10 \equiv 1\,(3)$.*
Voor $p = 7$: $\frac{1}{7} = 0.1428571\ldots$ De periode is hier gelijk aan $6 (= p - 1)$. In dit geval is $10 \equiv 3\,(7)$ en 3 is net als 5 een primitieve wortel voor 7.

Het vermoeden van Gauss kan worden gegeneraliseerd naar een vermoeden dat bekend staat als Artins primitieve wortel vermoeden.

3.2 Het vermoeden van Artin

Vermoeden 3.2 (Artins vermoeden, 1927) *Voor $a \in \mathbb{Z}$, $a \neq -1$ en geen kwadraat, geldt dat a een primitieve wortel is voor oneindig veel priemgetallen.*

De voorwaarden in het vermoeden zijn noodzakelijk, -1 heeft namelijk altijd orde ≤ 2, en als n een kwadraat, dan geldt: $x^2 = n$ voor zekere x en

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

Het vermoeden is zoals de naam al aangeeft nog niet bewezen. Onder aanname van de Gegeneraliseerde Riemann Hypothese is Artins vermoeden bewezen door Hooley in 1967. In de appendix wordt de Riemann hypothese toegelicht. Daar wordt ook vertelt dat er voor de Riemann Hypothese nog geen sluitend bewijs is gevonden, en dus is het Vermoeden van Artin ook nog niet sluitend bewezen. De gegeneraliseerde vorm is hierop een uitbreiding. Met Artins kwalitatieve vermoeden kwam ook een kwantificering, hiervoor is het noodzakelijk enkele eigenschappen van priemgetallen nader te bekijken.

3.3 Over de verdeling van priemgetallen

Gauss bekeek in 1792 tabellen met priemgetallen en toen viel hem iets op in de verdeling. Telling van het aantal priemgetallen kleiner dan x, genoteerd $\pi(x)$, suggereerde dat:

$$\pi(x) := \{p \,|\, p \leq x, p \text{ priem}\} \sim \frac{x}{\log x}. \tag{3.1}$$

Deze vergelijking zegt dat $\pi(x)$ asymptotisch nadert tot $\frac{x}{\log x}$. Ruim een eeuw later werd dit bewezen door Hadamard en De la Valleé Poussin. Zij bewezen een iets sterkere stelling als de volgende stelling:

Stelling 3.3 (Priemgetalstelling) *Zij $\pi(x)$ als hierboven, dan geldt:*

$$\lim_{x\to\infty} \frac{\pi(x) \cdot \log x}{x} = 1. \tag{3.2}$$

Deze stelling was al vermoed door Chebyshev, die wel wist aan te tonen dat als de limiet in (3.2) bestaat, deze gelijk moet zijn aan 1 en tevens dat voor x groot genoeg de volgende ongelijkheid geldt:

$$\frac{7}{8} < \frac{\pi(x) \cdot \log x}{x} < \frac{9}{8}. \tag{3.3}$$

Pierre Dusart [4] liet zelfs zien dat voor $x > 598$:

$$1 + \frac{0,992}{\log x} \leq \frac{\pi(x) \cdot \log x}{x} \leq 1 + \frac{1,2762}{\log x}. \tag{3.4}$$

We kunnen voor x de kans $\mathbb{P}_x(a)$ dat a een priemgetal is definiëren als:

$$\mathbb{P}_x(a) = \frac{\pi(x)}{x} = \frac{1}{\log x} \text{ (op den duur)}. \tag{3.5}$$

Met deze kansdefinitie kunnen we de verwachting van het aantal priemgetallen kleiner dan x uitrekenen:

$$E(\pi(x)) \sim \sum_{2 \leq n \leq x} \frac{1}{\log n}. \tag{3.6}$$

Deze vergelijking is niet intuïtief, en vereist daarom wat uitleg. De verwachtingswaarde van een stochast, hier $\pi(x)$, is gelijk $\mathbb{P}(uitkomst) \cdot uitkomst$, in dit geval is de uitkomst 1 als p een priem en 0 als p geen priem is. De kans op een priem p is gelijk aan $\frac{1}{\log p}$. Het tweede deel van de vergelijking is ingegeven door de analyse en wordt aangeduid als $Li(x)$. Dus $\pi(x) \approx Li(x)$. Het blijkt dat $Li(x)$ een betere benadering geeft dan $\frac{x}{\log x}$. Meer over $Li(x)$ in het volgende hoofdstuk.

3.4 Meer Artin voor je geld

Volgens het vermoeden van Artin zijn er oneindig veel priemen waarvoor een bepaalde a een primitieve wortel is. Artin heeft ook een uitspraak gedaan over hoe snel de cardinaliteit van de verzameling van priemgetallen waarvoor a een primitieve wortel is oneindig groot wordt. We formuleren hier het Vermoeden van Artin in de kwantitatieve vorm:

Vermoeden 3.4 (Artin) *Laat $N_a(x)$ het aantal priemgetallen zijn waar voor a een primitieve wortel is en die niet groter zijn dan x. Zij h het grootste gehele getal, zodat $a = a_0^h$ met $a_0 \in \mathbb{Q}$. Dan hebben we als x naar oneindig gaat:*

$$N_a(x) = \prod_{q \nmid h} \left(1 - \frac{1}{q(q-1)}\right) \prod_{q \mid h} \left(1 - \frac{1}{q(q-1)}\right) \frac{x}{\log x} + o\left(\frac{x}{\log x}\right), \tag{3.7}$$

waarbij het product loopt over alle priemen q.

Numerieke resultaten van D. en E. Lehmer suggereerden echter dat Vermoeden (3.4) niet altijd correct is. Het bleek dat Artin een aantal gebeurtenissen als onafhankelijk had gedacht, iets waarop hij na een intensieve briefwisseling met de Lehmer's terugkwam. Onder aanname van de gegeneraliseerde Riemann Hypothese bewees Hooley [9] een kwantitatieve versie van het Artin vermoeden. Het blijkt dat onder deze aanname (3.7) correct is als

$$a_0 \not\equiv 1 (\text{mod } 4) \tag{3.8}$$

en incorrect anders. Het heeft uiteindelijk meer dan 30 jaar geduurd voor er een juiste formulering van de kwantitatieve vorm van Artin's vermoeden kwam.

Hoofdstuk 4

Chebyshev priemgetallen

Met het vermoeden van Artin in het achterhoofd kunnen we onszelf de vraag stellen hoeveel priemgetallen er bestaan in de gevallen van Wertheim en Chebyshev. Intuïtief is het duidelijk, dat er in het geval van Chebyshev meer priemgetallen zijn dan in de gevallen van Wertheim.
Een van de stellingen die Dirichlet bewezen heeft (zie [1]) zegt, dat er oneindig veel priemgetallen zitten in de verzameling $\{4n+1|n \in \mathbb{N}\}$. Laten we nu het aantal priemgetallen p bekijken van de vorm $p = 4q + 1$ met q priem, dus de verzameling priemen in $\{4q+1|q \in \mathcal{P}\}$. Uit de Priemgetalstelling (3.2) volgt, dat de kans dat p priem is gelijk is aan $\frac{1}{\log p}$ en de kans dat q priem is gelijk is aan $\frac{1}{\log q}$. Het is niet duidelijk of deze twee gebeurtenissen onafhankelijk zijn. Het is daarom niet direct duidelijk dat de kans dat p priem is van de vorm $p = 4q + 1$, met q priem gelijk is aan $\frac{1}{\log p} \cdot \frac{1}{\log q} = \frac{1}{\log 4q+1} \cdot \frac{1}{\log q}$, omdat de onafhankelijkheid van deze gebeurtenissen niet direct vaststaat.

4.1 Priemgetallen tellen

We verwachten dat het aantal priemgetallen $\leq x$ benadert wordt door:

$$\sum_{2 \leq n \leq x} \frac{1}{\log n}. \tag{4.1}$$

Stel dat we de onafhankelijkheid aannemen. Dan vinden we, dat het aantal priemgetallen in de stelling van Chebyshev gelijk is aan:

$$\sum_{2 \leq n \leq x} \frac{1}{\log n} \cdot \frac{1}{\log 4n+1}. \tag{4.2}$$

Gaan we nu alle priemen van deze vorm proberen te bepalen, dan vinden we dus dat het aantal van de priemen van die vorm gelijk is aan:

$$\lim_{x\to\infty} \sum_{2\leq n\leq x} \frac{1}{\log 4n+1} \cdot \frac{1}{\log n}. \tag{4.3}$$

Laten we het eindige geval bekijken, dus we laten de limiet achterwege en later de limiet hiervan naar oneindig bekijken:

$$\sum_{2\leq n\leq x} \frac{1}{\log n} \cdot \frac{1}{\log 4n+1}. \tag{4.4}$$

Analyse leert ons, dat dit assymptotisch gelijk is aan:

$$\int_2^x \left(\frac{1}{\log t} \cdot \frac{1}{\log 4t+1} \right) dt. \tag{4.5}$$

Vervolgens is deze integraal weer assymptotisch gelijk aan:

$$\int_2^x \left(\frac{1}{\log t} \cdot \frac{1}{\log t} \right) dt \tag{4.6}$$

Partieel integreren betekent:

$$\int f \cdot G dx = F \cdot G - \int F \cdot g dx. \tag{4.7}$$

Nemen we nu:

$$f = 1 \ en \ G = \frac{1}{(\log t)^2}, \tag{4.8}$$

dan is $F \cdot g$ gelijk aan:

$$F \cdot g = \int \frac{2}{(\log t)^3}. \tag{4.9}$$

En dus vinden we dat (4.5) gelijk is aan:

$$\left[\frac{1}{(\log t)^2} \right]_2^x - \int_2^x \frac{2}{(\log t)^3} dt. \tag{4.10}$$

Dit is ongeveer gelijk aan:

$$\frac{x}{(\log x)^2} + O\left(\frac{x}{(\log x)^3} \right). \tag{4.11}$$

Ook kunnen we een andere strategie proberen toe te passen om het aantal priemgetallen te tellen.

4.2 Zeeftheorie

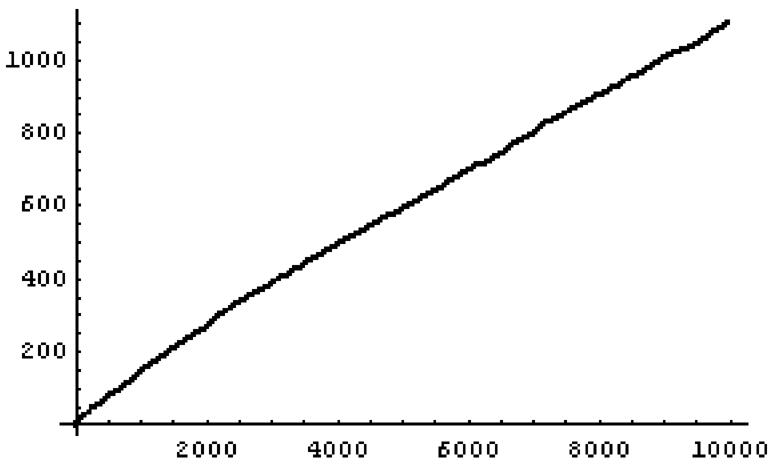
Zeeftheorie is een bepaald soort strategie waarmee we priemgetallen kunnen bepalen. De eenvoudigste en verreweg bekendste tactiek is de Zeef van Erastostenes. Bij deze techniek zet je alle getallen op een rij en dan begin je met alle tweevouden weg te strepen. Als je hiermee klaar bent ga je alle veelvouden wegstrepen van het eerste getal dat nog niet is weggestreept. Dit getal is dan een priemgetal. We kunnen dan ook de priemgetallen tellen. Voor voldoende grote x kunnen we nu met zeeftheorie stellen, dat (4.5) kleiner is dan:

$$\frac{Cx}{(\log x)^2}, \text{ voor een constante C.} \tag{4.12}$$

Voor een $C > 0$ geldt dat voor $x \to \infty$ dit ook naar oneindig gaat. De bovengrens is dus onbegrensd.
Voor de eerste n priemen q hebben we uitgerekend hoeveel $4q + 1$ ook priem zijn:

n	$\#\{4q + 1 \text{ priem}\}$	ratio
10	3	0.33
100	21	0.21
1000	145	0.15
10000	1108	0.111
100000	9314	0.0931
1000000	78676	0.079

Zetten we het aantal priemgetallen als in de stelling van Chebyshev in een grafiek tegen het aantal priemgetallen dan is er een stijgende lijn te zien. De snelheid waarmee de lijn stijgt neemt echter wel af.



Met deze kennis kunnen we C benaderen, omdat

$$C = \frac{(\log(n^e priem))^2}{n^e priem} \cdot \#\{4q + 1 \ priem\}. \tag{4.13}$$

n	C
10	1.17
100	1.54
1000	1.48
10000	1.41
100000	1.42
1000000	1.39

We verwachten dus, dat C naar een waarde van ongeveer 1.40 convergeert. Onder aanname van bepaalde vermoedens kan bewezen worden dat deze waarde convergeert naar de zogenaamde priemtweeling constante die ongeveer de waarde 1.32 heeft (zie [13]). Nemen we dus C kleiner als deze waarde, dan hebben we een ondergrens van (4.5) gevonden en kunnen we dus concluderen dat er oneindig veel priemgetallen in het geval van de stelling van Chebyshev bestaan.
De stelling van Chebyshev geeft dat 2 een primitieve wortel is voor priemgetallen van de vorm $4q+1$, waar q een priemgetal is. Aannemelijk is gemaakt dat het aantal priemgetallen van deze vorm kleiner dan x in ieder geval groter is dan $\frac{x}{(\log x)^2}$, omdat we verwachten dat $C \approx 1.40$. Omdat dit niet wil convergeren maar divergeert naar ∞ is hiermee Artin voor het speciale geval $a = 2$ aannemelijk gemaakt. Voor dit ene geval heeft Chebyshev dus al een aanzet gegeven tot het Vermoeden van Artin, maar nog niet volledig geformuleerd. Ook omdat Chebyshev er zelf niet bij kon vertellen of er oneindig veel priemgetallen van de vorm uit zijn stelling zijn.
Gelijksoortige argumenten in combinatie met Wertheim's werk (zie sectie 2.4), suggereren dat Artin's vermoeden ook correct is voor $a = 3, 5, 7, 10$ en 11. Dus ook Wertheim had al met Artin's vermoeden kunnen komen, maar hiervoor zijn geen geschreven of gedrukte aanwijzingen.

Bibliografie

[1] T.M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag New York (1976)

[2] E. Artin, *The collected works of Emil Artin*, (Eds.) S. Lang, J. T. Tate, Addison-Wesley (1965)

[3] P.L. Chebyshev, *Theorie der Congruenzen:(Elemente der Zahlentheorie)*, Chelsea pub. 1972

[4] P. Dusart, The kth prime is greater than $k(ln\ k + ln\ ln\ k - 1)$ for $k > 2$, *Math. Comp.* **68:225** (1999),411-415.

[5] C.F. Gauss, *Disquisitiones Arithmeticae*; vertaald door Arthur A. Clarke, New Haven University Press (1966)

[6] J.R. Goldman, *The Queen of Mathematics*, A.K. Peters Ltd. (1997)

[7] M. Goossens, F. Mittelback en A. Samarin, *The LaTeX Companion*, Addison-Wesley (1994)

[8] A. Heck, *Learning LaTeX by Doing*, Amstel Institute (2002)

[9] C. Hooley, *On Artinś conjecture*, J. reine Angew. Math. 226 (1967), 209-220

[10] M. Křížek, F. Luca, L. Somer, *17 Lectures on Fermat Numbers*, Springer-Verlag New York (2001)

[11] F. Lemmermeyer, *Reciprocity Laws, From Euler to Eisenstein*, Springer-Verlag (1991)

[12] Pieter Moree, *Artin's primitive root conjecture-a survey*, http://staff.science.uva.nl/∼ moree/varia.htm

[13] P. Stevenhagen, *priemgetallen*, te vinden op http://turing.sccience.uva.nl/∼psh/pub/

[14] E.W. Weisstein, *The CRC Concise Encyclopedia of Mathematics* , CRC Press (1999)

[15] G. Wertheim, Primitiven Wurzeln der Primzahlen von der Form $2^x q^\lambda + 1$, in welcher $q = 1$ oder eine ungerade Primzahl ist, *Acta Math.* **20** (1895),143-152.

Bijlage A

De Riemann Hypothese

Het Vermoeden van Artin is bewezen door Hooley [9] in 1967 onder aanname van de gegeneraliseerde Riemann hypothese. Voor ieder algebraisch getallenlichaam K, kan de zogenaamde Dedekind zetafunctie $\zeta_K(s)$ gedefinieerd worden. De gegeneraliseerde Riemann hypothese zegt nu dat alle nulpunten van deze functie in de kritieke strip $0 \leq \Re(s) \leq 1$, op de kritieke lijn $\Re(s) = \frac{1}{2}$ liggen. Wij zullen dit als voorbeeld uitwerken voor $K = \mathbb{Q}$. De Dedekind zetafunctie behorend bij $\mathbb{Q}$ is gelijk aan de zogenaamde Riemann zeta functie. Riemann onderzocht de zeta functie:

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}. \tag{A.1}$$

Deze functie is voor $x > 1$ goed gedefinieerd en convergeert naar een eindige waarde. Voor $x \leq 1$ divergeert de functie. Via een herschrijving van de bovenstaande som kan de link naar priemgetallen worden gelegd, hier is $x > 1$:

$$\begin{aligned}
(1 + \frac{1}{2^x} + \frac{1}{2^{2x}} + \frac{1}{3^x} + \ldots)(1 + \frac{1}{3^x} + \frac{1}{3^{2x}} + \ldots)(1 + \frac{1}{5^x} + \frac{1}{5^{2x}} + \ldots)(1 + \frac{1}{7^x} + \ldots \\
= 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{2^{2x}} + \frac{1}{5^x} + \frac{1}{2^x 3^x} + \frac{1}{7^x} + \frac{1}{2^{3x}} + \frac{1}{3^{2x}} + \frac{1}{2^x 5^x} + \ldots \\
= \sum_{n=1}^{\infty} \frac{1}{n^x}.
\end{aligned}$$

In het kort:

$$\prod_p (1 + \frac{1}{p^x} + \frac{1}{p^{2x}} + \frac{1}{p^{3x}} + \ldots) = \zeta(x). \tag{A.2}$$

Voor $x > 1$ kan de linkerkant nog eens worden herschreven. Dan geldt namelijk dat $|\frac{1}{p^x}| < 1$ en we schrijven:

$$\zeta(x) = \prod_p \frac{1}{1 - p^{-x}} \quad (x > 1). \tag{A.3}$$

Op het complexe vlak bekeken is de zeta functie zo volledig vastgelegd op het halfvlak rechts van de lijn $\Re(z) = 1$. Uit de complexe functietheorie volgt dat de functie analytisch is, en op maar één manier kan worden uitgebreid naar het gehele complexe vlak, met uitzondering van $z = 1$, waar een enkelvoudige pool is. Riemann ontdekte dat de analytische uitbreiding op de volgende manier kan worden beschreven:

$$\pi^{-\frac{1}{2}z}\Gamma(\frac{1}{2}z)\zeta(z) = \pi^{-\frac{1}{2}(1-z)}\Gamma(\frac{1}{2}(1-z))\zeta(1-z) \tag{A.4}$$

$\zeta(z)$ is hier afhankelijk van $\zeta(z-1)$. Zo'n soort verband wordt binnen de wiskunde een functionaalvergelijking genoemd. Ook de in de vergelijking voorkomende Gamma-functie $\Gamma(z)$ is zo'n vergelijking. Deze functie is een uitbreiding van $\Gamma(n) = (n-1)!$ naar het complexe vlak. Met de wetenschap dat $\Gamma(z) = \infty$ voor alle niet-positieve integers en nergens anders, kan snel worden gezien dat $\zeta(z) = 0$ in de punten $z = -2, -4, -6, \ldots$. Deze punten heten de triviale nulpunten van $\zeta(z)$. Er moeten alleen nog oneindig veel meer nulpunten zijn, en die liggen allemaal in de *kritieke strip* $0 \leq \Re(z) \leq 1$.

Vermoeden A.1 (Riemann, 1859) *De niet-triviale nulpunten van de zeta functie liggen op de lijn* $\Re(z) = \frac{1}{2}$.

Er is ook bekend dat tenminste $\frac{3}{5}$ van alle nulpunten in de kritieke strip $0 \leq \Re(s) \leq 1$ op de kritieke lijn liggen. Met computers is het vermoeden voor de eerste miljard nulpunten bewezen op het CWI in Amsterdam. Het wachten is op een sluitend bewijs.