Radicals in arithmetic

Palenstijn, W.J.

Samenvatting

Dit proefschrift bestaat uit twee onafhankelijke delen. In het eerste deel, dat de Hoofdstukken 1 tot en met 6 beslaat, bouwen we een theorie op om *verstrengelde radicaaluitbreidingen* te beschrijven. Deze theorie gebruiken we om generalisaties te geven van een vermoeden van Artin over *primitieve wortels*.

Het tweede deel bestaat uit Hoofdstuk 7. In dit hoofdstuk beschrijven we het algoritme om alle zogeheten *ABC-drietallen* onder een gegeven grens te bepalen dat gebruikt is door het gedistribueerde online rekenproject ABC@home.

Om het vermoeden van Artin over primitieve wortels te begrijpen kijken we eerst naar de machten van 2. Dit is een snel groeiende rij:

$$2^1 = 2, 2^2 = 2 \times 2 = 4, 2^3 = 2 \times 2 \times 2 = 8, 2^4 = 16, 2^5 = 32, \text{enz.}$$

Als we de resten bij deling door het priemgetal 5 nemen van deze rij, dan raken we in een lus: 2, 4, 3 (8 geeft rest 3), 1 (16 geeft rest 1), 2, 4, 3, 1, enz. We zien dat we, op 0 na, alle mogelijke resten bij deling door 5 krijgen als macht van 2.

Als we hetzelfde doen met het priemgetal 7 in plaats van 5, is dit niet meer het geval. De machten van 2 geven wel nog steeds een lus, 2, 4, 1 (8 geeft rest 1), 2, 4, 1, enz., maar deze lus bevat niet meer alle mogelijke resten op 0 na. In het bijzonder zal een macht van 2 nooit rest 3, 5 of 6 hebben bij deling door 7.

Rekenen met resten na deling door 5 (of 7) noemen we rekenen *modulo* 5 (of 7). Omdat de machten van 2 modulo 5 alle resten op 0 na geven, heet 2 een *primitieve wortel* modulo 5. Zoals we gezien hebben is 2 juist geen primitieve wortel modulo 7, maar bijvoorbeeld 3 wel. We krijgen daarvoor de lus 3, $3^2 = 9$ geeft 2, $3^3 = 27$ geeft 6, en dan verder 4, 5, 1, 3, enz.

Als q een priemgetal groter dan 3 is, zijn er altijd meerdere primitieve wortels modulo q tussen 1 en q. Zo zijn modulo 5 de getallen 2 en 3 primitieve wortels, en modulo 7 hebben we 3 en 5.

Zij $x \neq 0$ een geheel getal. In 1927 formuleerde Artin een vermoeden over hoeveel priemgetallen q er zijn waarvoor x een primitieve wortel is modulo q.

Deze hoeveelheid is uitgedrukt als een zogeheten dichtheid van priemgetallen. We kijken voor een getal N welke fractie van de priemgetallen onder de N deze eigenschap heeft. Als we N dan onbeperkt laten groeien, is het mogelijk dat deze

fractie convergeert naar een getal d tussen 0 en 1. In die situatie zeggen we dat deze verzameling priemgetallen *dichtheid* d heeft.

De redenering achter het vermoeden van Artin is als volgt. Voor het gemak nemen we hier aan dat het gehele getal x geen macht is. Als x geen veelvoud van q is, dan vormen de machten van x modulo q altijd een lus waarvan de lengte een deler van $q-1$ is. Als we deze lengte l noemen, dan heet het quotient $\frac{q-1}{l}$ de *index* van de lus. Het getal x is nu een primitieve wortel modulo q dan en slechts dan als de index 1 is.

Een positief geheel getal is 1 precies als het geen priemdelers heeft. We kunnen dus zien of x een primitieve wortel is door voor elk priemgetal p te controleren of p een deler is van de index.

Laat p nu een priemgetal zijn. Artin heeft een getaltheoretisch argument gegeven om te bepalen voor hoeveel priemgetallen q, het priemgetal p geen deler is van deze index. Deze redenering staat in zijn geheel in Hoofdstuk 1 van dit proefschrift, en de kern van dit argument rust op het begrijpen van de structuur van de p-demachtswortels van x, zowel modulo q als binnen de complexe getallen. Het resultaat ervan is dat de dichtheid van de priemgetallen q waarvoor p geen deler van de index is, gelijk is aan

$$1 - \frac{1}{p(p-1)}.$$

Als we aannemen dat al deze voorwaarden onafhankelijk zijn van elkaar en we daarom al deze dichtheden met elkaar vermenigvuldigen, krijgen we het vermoeden dat de dichtheid van de priemgetallen q waarvoor x een primitieve wortel modulo q is, gelijk is aan het oneindige product

$$\prod_{p \text{ priem}} 1 - \frac{1}{p(p-1)} = \left(1 - \frac{1}{2 \cdot 1}\right)\left(1 - \frac{1}{3 \cdot 2}\right)\left(1 - \frac{1}{5 \cdot 4}\right) \cdots \approx 0,3739558\ldots$$

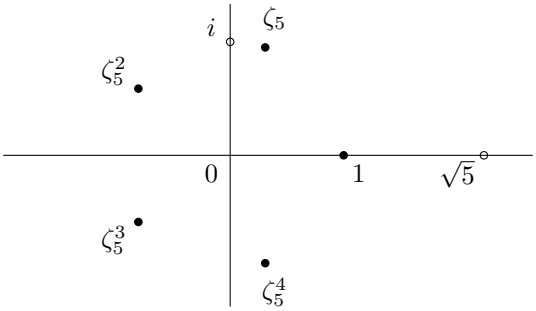
In de jaren '50 hebben Derrick en Emma Lehmer dit eerste vermoeden met een computer gecontroleerd voor de priemgetallen tot 20 000. Voor $x = 2$ bleek dit numerieke experiment goed overeen te komen met de formule hierboven, maar voor $x = 5$ leek de werkelijke dichtheid groter te zijn.

Artin realiseerde zich hierop dat voor $x = 5$ de voorwaarde voor $p = 2$ en $p = 5$ niet onafhankelijk zijn van elkaar. Dit komt door een onverwachte relatie tussen 2-demachtswortels van 5 en 5-demachtswortels van 1 binnen de complexe getallen. Binnen de reële getallen is er slechts een enkele 5-demachtswortel van 1 (namelijk 1 zelf), maar binnen de complexe getallen zijn het er 5, gegeven door

$$1, e^{2\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5}, e^{8\pi i/5}.$$

We schrijven vaak $\zeta_5 = e^{2\pi i/5}$. Met die notatie zijn de 5-demachtswortels van 1 gegeven door $1, \zeta_5, \zeta_5^2, \zeta_5^3$ en ζ_5^4.

Grafisch vormen deze 5 punten de hoekpunten van een regelmatige vijfhoek op de eenheidscirkel.



Het blijkt dat de wortel van 5 te schrijven is in termen van ζ_5:

$$\sqrt{5} = (\zeta_5 + \zeta_5^4) - (\zeta_5^2 + \zeta_5^3).$$

Immers, het is na te rekenen dat het kwadraat van de formule aan de rechterkant gelijk is aan 5. Een dergelijke onverwachte relatie tussen wortels (of radicalen) noemen we *verstrengeling van radicalen*.

Deze relaties zorgen voor een correctiefactor voor de dichtheid van priemgetallen $q \neq 5$ waarvoor 5 een primitieve wortel modulo q is. Dit door Artin aangepaste vermoeden is in 1967 bewezen door Hooley, onder de aanname van de zogeheten Gegeneraliseerde Riemann-Hypothese (GRH). Dit is een nog onbewezen diepe getaltheoretische hypothese die gevolgen heeft voor de nauwkeurigheid waarmee we de verdeling van de priemgetallen kunnen beschrijven. Hij wordt in het bewijs van het vermoeden van Artin gebruikt om het combineren van de oneindig veel condities bij priemgetallen p mogelijk te maken.

In Hoofdstuk 1 geven we een **generalisatie van het vermoeden van Artin naar getallenlichamen**. Onder aanname van GRH heeft de dichtheid in deze generalisatie dezelfde vorm van een oneindig product maal een rationale correctiefactor. Dit hoofdstuk vormt een opzichzelfstaand geheel.

In Hoofdstuk 2 bouwen we een theorie voor verstrengelde wortels op, los van getallenlichamen. De eenhedengroep van een lichaam heeft de eigenschap dat elke eindige ondergroep cyclisch is. Dit blijkt een essentiële eigenschap voor de theorie in dit proefschift. Laat daarom B een abelse groep zijn waarvan alle eindige ondergroepen cyclisch zijn, en G een pro-eindige groep die werkt op B. We schrijven B^G voor de ondergroep van B die invariant is onder de actie van G. Als B/B^G torsie is, dan noemen we B een Galois-radicaaluitbreiding van B^G. In Hoofdstuk 2 beschrijven we een aantal eigenschappen hiervan die sterk lijken op Galoistheorie van lichamen. Eén van de hoofdresultaten uit Hoofdstuk 2 is dat **het beeld van G in $\mathrm{Aut}_{B^G}(B)$ een normale ondergroep is, met een abels quotient** $\mathrm{Aut}_{B^G}(B)/\mathrm{im}(G)$. We noemen dit quotient de *verstrengelingsgroep* van de werking van G op B.

In Hoofdstuk 3 kijken we naar de verstrengelingsgroep van de maximale radicaaluitbreiding van de eenhedengroep van een lichaam K, met de werking van de absolute Galoisgroep van K. Deze noemen we de **absolute verstrengelingsgroep**.

In Hoofdstuk 4 beschrijven we expliciet verstrengelingsgroepen over $\mathbf{Q}$, en gebruiken dit om een algoritme te geven voor het berekenen van **de lichaamsgraad van radicaaluitbreidingen van Q**.

In Hoofdstuk 5 geven we een verdere generalisatie van het vermoeden van Artin over primitieve wortels. We kijken hier naar **bijna-primitieve wortels**, die niet noodzakelijk de gehele eenhedengroep van de maximale orde van een getallenlichaam modolo een priem voortbrengen, maar een ondergroep waarvan de index een gegeven geheel getal t deelt. Een andere generalisatie die we in dit hoofdstuk beschouwen is die van **hogere rang**, waar we een eindige verzameling $x_1, \ldots, x_k$ van niet-0 elementen van een lichaam K nemen, en de dichtheid bepalen van de priemen $\mathfrak{q}$ van K, met voor alle x_i de eigenschap $\mathrm{ord}_{\mathfrak{q}}(x_i) = 0$, waarvoor $x_1, \ldots, x_k$ samen $(\mathcal{O}_K/\mathfrak{q})^*$ voortbrengen.

De algemeenheid van de theorie uit Hoofdstuk 2 stelt ons in staat om in Hoofdstuk 6 ook een generalisatie van het vermoeden van Artin voor **tori van rang 1 over getallenlichamen** te geven. Dit zijn algebraïsche groepen die sterk lijken op de multiplicatieve groep $\mathbf{G}_{\mathrm{m}}$, waarover we in Hoofdstuk 1 en 5 gewerkt hebben. De eis dat een torus T over een lichaam K rang 1 heeft, zorgt er precies voor dat eindige ondergroepen van de groep van punten $T(K)$ cyclisch zijn, waardoor de theorie uit Hoofdstuk 2 van toepassing is.

Het tweede deel van dit proefschrift bestaat uit Hoofdstuk 7. In dit hoofdstuk beschrijven we een algoritme dat we gebruikt hebben in het gedistribueerde online rekenproject ABC@home om alle zogeheten *ABC-drietallen* te vinden kleiner dan 10^{18}. Een ABC-drietal is een drietal positieve gehele getallen (a, b, c) dat voldoet aan de volgende voorwaarden:

- $a + b = c$;
- $a \leq b$;
- a, b en c hebben geen gemeenschappelijke priemdelers, en
- het product van de priemdelers van abc is kleiner dan c.

Het product van de priemdelers van een positief geheel getal n noemen we het *radicaal* van n, en we schrijven dit als $\mathrm{rad}(n)$. De *kwaliteit* van een ABC-drietal wordt gegeven door het volgende quotient:

$$q = \frac{\log(c)}{\log(\mathrm{rad}(abc))}.$$

Deze ABC-drietallen vormen een centrale rol in het *ABC-vermoeden*, dat een uitspraak doet over het limietgedrag van de kwaliteit van ABC-drietallen. Het algoritme dat we beschrijven in dit hoofdstuk is in het kader van het ABC@home-project gebruikt met de hulp van vele vrijwilligers wereldwijd om alle ABC-drietallen kleiner dan 10^{18} te vinden. In Sectie 7.5 sluiten we dit proefschrift af met een aantal observaties over de 14 482 065 gevonden drietallen.