stichting
mathematisch
centrum

MC

AFDELING ZUIVERE WISKUNDE ZN 73/77 APRIL

H.W. LENSTRA JR.

EUCLIDISCHE GETALLENLICHAMEN

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O).

AMS(MOS) subject classification scheme (1970): 12A45, 13F10, 01A55

Euclidische getallenlichamen

door

H.W. Lenstra jr.

SAMENVATTING

Dit rapport beoogt een algemeen wiskundig publiek een indruk te geven van het door de titel aangegeven vakgebied, van de historische achtergrond waartegen men het zien kan, en van de bewijstechnieken die erin gehanteerd worden. De tekst is overgenomen uit het gelijknamige proefschrift van de auteur (Universiteit van Amsterdam, 1977).

TREFWOORDEN: *euclidische algoritme, algebraïsche getallenlichamen*

Euclidische getallenlichamen

The story of "Fermat's Last Theorem" has been told so often that it hardly bears retelling

H.M. Edwards

N'y a-t-il pas là une lacune à remplir?

J. Liouville

Euclides van Alexandrië	~ -300
Diophantus van Alexandrië	~ 250
Pierre de Fermat	1601-1665
Leonhard Euler	1707-1783
Joseph Louis Lagrange	1736-1813
Carl Friedrich Gauss	1777-1855
Augustin Louis Cauchy	1789-1857
Gabriel Lamé	1795-1870
Carl Gustav Jacob Jacobi	1804-1851
Peter Gustav Lejeune Dirichlet	1805-1859
Joseph Liouville	1809-1882
Ernst Eduard Kummer	1810-1893
Pierre Laurent Wantzel	1814-1848
Gotthold Eisenstein	1823-1852
Leopold Kronecker	1823-1891
Bernhard Riemann	1826-1866
Adolf Hurwitz	1859-1919
Kurt Hensel	1861-1941
Hermann Minkowski	1864-1909
Harry Schultz Vandiver	1882-1973
Emil Artin	1898-1962
Harold Davenport	1907-1969
Theodore Samuel Motzkin	1908-1970

Euclidische getallenlichamen

1. De laatste stelling van Fermat

Op 1 maart 1847 had de Franse wiskundige LAMÉ, lid van de Parijse *Académie des Sciences*, een opzienbarende mededeling voor zijn mede-academici: hij zou erin geslaagd zijn de *laatste stelling van Fermat* te bewijzen, die zegt dat er geen positieve gehele getallen x, y en z zijn met

$$x^n + y^n = z^n$$

als n een geheel getal groter dan twee is. Voor n gelijk aan twee zijn er vele oplossingen:

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2, \quad 8^2 + 15^2 = 17^2,$$

de zogenaamde *Pythagoreïsche drietallen*. Dat er voor hogere n niet zulke drietallen te vinden zijn had de zeventiende-eeuwse Franse jurist FERMAT in de kantlijn van zijn exemplaar van DIOPHANTUS' *Arithmetica* geschreven, met de toevoeging dat hij er een wonderbaarlijk bewijs voor had waar de marge echter te klein voor was:

> "Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."

Alle andere stellingen die FERMAT op een dergelijke manier had medegedeeld waren anno 1847 inderdaad bewezen; alleen deze, de *laatste*, was over.

LAMÉ schreef het idee van zijn bewijs toe aan LIOUVILLE. Het bestond eruit, te werken met getallen van de vorm

$$(1) \qquad a_0 + a_1\zeta + \ldots + a_{n-1}\zeta^{n-1}, \qquad a_0, a_1, \ldots, a_{n-1} \text{ geheel},$$

waar ζ een complex getal met de eigenschappen $\zeta^n = 1$, $\zeta \neq 1$ is. Hierbij nam LAMÉ aan dat n een oneven priemgetal is, hetgeen, naar men al enige tijd wist, geen essentiële beperking is bij het bewijs van FERMAT's laatste stelling. Met behulp van deze getallen laat $x^n + y^n$ zich in n factoren splitsen:

$$x^n + y^n = (x + y)(x + \zeta y)\ldots(x + \zeta^{n-1}y)$$

en FERMAT's vergelijking krijgt dan de gedaante

$$(2) \qquad (x + y)(x + \zeta y)\ldots(x + \zeta^{n-1} y) = z^n.$$

Hierop paste LAMÉ de volgende uitspraak toe, een klassiek hulpmiddel uit de theorie der *diophantische vergelijkingen*:

(3) is het product van twee onderling ondeelbare getallen een n-de macht, dan is elk van deze getallen een n-de macht.

De geldigheid van deze uitspraak, voor positieve gehele getallen, ziet men onmiddellijk in door de getallen in priemfactoren te ontbinden en de bijdrage van elk priemgetal afzonderlijk te onderzoeken.

LAMÉ nam aan dat (3) ook waar is voor getallen van de vorm (1), en met behulp van een redenering die hier weinig ter zake doet kwam hij tot de conclusie dat (2) alleen mogelijk is als een van de getallen x, y, z nul is. Hieruit volgt dan de juistheid van FERMAT's laatste stelling.

Na LAMÉ richtte LIOUVILLE zich tot de vergadering. Het hem toegeschreven idee de complexe getallen (1) te beschouwen had, zo zei hij, niets nieuws, men kon ze al aantreffen in het werk van EULER, LAGRANGE, GAUSS en JACOBI. Bovendien, aldus LIOUVILLE, scheen het hem toe dat LAMÉ stilzwijgend aannam dat de stelling van de eenduidige ontbinding in priemfactoren ook geldt voor de getallen (1). En het was bij deze gelegenheid dat LIOUVILLE de enkele pagina's eerder aangehaalde woorden uitte.

De vraag waar FERMAT's laatste stelling aldus aanleiding toe gaf is wellicht interessanter dan FERMAT's laatste stelling zelf:

(4) geldt de stelling van de eenduidige ontbinding in priemfactoren ook voor getallen van het type (1)?

In deze paragraaf houden we ons voornamelijk bezig met de methoden die LIOUVILLEs tijdgenoten ter beantwoording van deze vraag toepasten.

Een tweede moeilijkheid waar LAMÉ door LIOUVILLE op gewezen werd betreft het bestaan van *delers van 1*: getallen die het getal 1 delen, of *eenheden*, zoals ze tegenwoordig heten. Dat deze een rol spelen bij beweringen als (3) blijkt uit het voorbeeld

$$-4 \cdot -9 = 6^2.$$

De beide factoren -4 en -9 zijn onderling ondeelbaar, hun product is een

kwadraat, maar toch zijn -4 en -9 zelf geen kwadraten van gehele getallen. Wel zijn ze elk een eenheid, namelijk -1, maal een kwadraat.

Bij getallen van de vorm (1) komen veel meer eenheden voor. Uit

$$(\zeta + \zeta^{n-1})\cdot(\zeta + \zeta^5 + \zeta^9 + \ldots + \zeta^{2n-1}) = 1 \qquad (n \text{ oneven}, \ n > 1)$$

blijkt bijvoorbeeld dat beide factoren in het linkerlid eenheden zijn. Eigenschappen van deelbaarheid door $\zeta + \zeta^{n-1}$ spelen een belangrijke rol in LAMÉ's bewijs. Maar dit getal deelt 1, dus ook elk ander getal, en deze opmerking doet LAMÉ's argumenten alle geldigheid verliezen, zelfs als men eenduidigheid van priemfactorontbinding aanneemt.

We staan hier niet langer stil bij het bestaan van eenheden. De verdere ontwikkeling heeft geleerd dat vragen over dit onderwerp lastiger te beantwoorden zijn dan vragen omtrent eenduidigheid van factorisatie. Opmerkelijk is overigens dat het besef, dat behalve eigenschappen van priemfactorontbinding tevens eigenschappen van eenheden bekend moeten zijn voor men een conclusie als in (3) kan trekken, ook hedentendage nog geen gemeengoed is bij schrijvers van leerboeken over de getallentheorie.

Twee weken na het exposé van LAMÉ kwam WANTZEL met een methode om LIOUVILLEs vraag te beantwoorden. Deze WANTZEL genoot tot aan het begin van deze eeuw enige faam wegens een vereenvoudigd bewijs van de onoplosbaarheid van vijfdegraads-vergelijkingen dat hij geleverd heeft. Tevens heeft hij de eerste gepubliceerde bewijzen van de onmogelijkheid van de driedeling van de hoek en de verdubbeling van de kubus op zijn naam staan. Door zijn vroege dood heeft hij aan de verwachtingen die men van hem had niet kunnen beantwoorden, en tegenwoordig is hij geheel vergeten.

WANTZELs idee komt op het volgende neer. Laat n een willekeurig geheel getal ≥ 3 zijn, en laat ζ een primitieve wortel van $\zeta^n = 1$ zijn, bijvoorbeeld $\zeta = e^{2\pi i/n}$. Om te bewijzen, zo betoogde WANTZEL, dat de getallen (1) de eigenschap van eenduidige factorisatie hebben, is het voldoende een substituut te vinden voor de van de gewone gehele getallen bekende *deling met rest*: dan kan men namelijk de tot EUCLIDES teruggaande argumenten herhalen die leiden tot de gewenste stelling van de eenduidige ontbinding in priemfactoren.

Om te illustreren hoe hij zo'n substituut vindt beschouwde WANTZEL eerst het geval $n = 4$. In dit geval zijn de getallen (1) juist de getallen $a + b\sqrt{-1}$, met a en b geheel, en de *norm* van zo'n getal definieert men door

$$N(a + b\sqrt{-1}) = (a + b\sqrt{-1})\cdot(a - b\sqrt{-1}) = a^2 + b^2.$$

Wil men nu $a + b\sqrt{-1}$ door $c + d\sqrt{-1}$ delen, met c en d niet beide nul, dan merkt men op dat

$$\frac{a + b\sqrt{-1}}{c + d\sqrt{-1}} = t + u\sqrt{-1}$$

met

$$t = (ac + bd)/(c^2 + d^2), \qquad u = (bc - ad)/(c^2 + d^2).$$

Dit betekent niet dat de deling opgaat, want t en u hoeven niet geheel te zijn. Maar we kunnen t en u wel benaderen met gehele getallen t', u':

$$t = t' + v, \qquad u = u' + w$$

met

$$|v| \leq \frac{1}{2}, \qquad |w| \leq \frac{1}{2}.$$

Dan geldt

$$a + b\sqrt{-1} = (t' + u'\sqrt{-1})\cdot(c + d\sqrt{-1}) + (v + w\sqrt{-1})\cdot(c + d\sqrt{-1}).$$

Schrijven we $r = vc - wd$, $s = vd + wc$ dan levert dit

$$a + b\sqrt{-1} = (t' + u'\sqrt{-1})\cdot(c + d\sqrt{-1}) + (r + s\sqrt{-1}). \tag{5}$$

Men kan $t' + u'\sqrt{-1}$ en $r + s\sqrt{-1}$ dus opvatten als *quotiënt* en *rest* van $a + b\sqrt{-1}$ bij deling door $c + d\sqrt{-1}$. Dat r en s geheel zijn volgt direct uit (5).

Om de naam *rest* te verdienen, en - niet te vergeten - om EUCLIDES' argumenten te laten opgaan, moet $r + s\sqrt{-1}$ voorts *kleiner* zijn dan het getal $c + d\sqrt{-1}$ waardoor gedeeld wordt. Hierbij meten we de grootte met behulp van de norm. En inderdaad geldt

$$\begin{aligned} N(r + s\sqrt{-1}) &= (r + s\sqrt{-1})(r - s\sqrt{-1}) \\ &= (v + w\sqrt{-1})(c + d\sqrt{-1})(v - w\sqrt{-1})(c - d\sqrt{-1}) \\ &= (v^2 + w^2)\cdot N(c + d\sqrt{-1}) \\ &\leq ((\tfrac{1}{2})^2 + (\tfrac{1}{2})^2)\cdot N(c + d\sqrt{-1}) \\ &< N(c + d\sqrt{-1}). \end{aligned}$$

Tot zover het geval $n = 4$. Wat WANTZEL bewees formuleert men tegenwoordig door te zeggen dat de getallen $a + b\sqrt{-1}$, met a en b geheel, een *euclidische ring* vormen ten opzichte van de norm. De al vaker genoemde argumenten van EUCLIDES tonen aan dat in een euclidische ring de stelling van de eenduidige ontbinding in priemfactoren geldt.

Als tweede voorbeeld behandelde WANTZEL het geval $n = 3$. Dan geldt $\zeta^2 = -1 - \zeta$, dus de getallen (1) zijn te schrijven als $a + b\zeta$, met a en b geheel. De norm - *module*, in WANTZELs terminologie - wordt nu gedefinieerd door

$$N(a + b\zeta) = (a + b\zeta)\cdot(a + b\zeta^2) = a^2 - ab + b^2.$$

Op geheel analoge wijze vindt men bij deling van $a + b\zeta$ door $c + d\zeta$ nu

$$a + b\zeta = (t' + u'\zeta)\cdot(c + d\zeta) + (r + s\zeta)$$

met t', u', r, s geheel en

$$r + s\zeta = (v + w\zeta)\cdot(c + d\zeta)$$
$$|v| \leq \frac{1}{2}, \qquad |w| \leq \frac{1}{2}.$$

Dat de rest $r + s\zeta$ zijn naam verdient is weer eenvoudig te controleren:

$$N(r + s\zeta) = (v^2 - vw + w^2)\cdot N(c + d\zeta)$$
$$\leq \frac{3}{4}\cdot N(c + d\zeta) < N(c + d\zeta).$$

Hiermee is het geval $n = 3$ afgehandeld. Voor algemene n gaf WANTZEL minder details:

> "On voit facilement que le même mode de démonstration s'applique aux nombres complexes de forme plus compliquée qui dépendent des racines de $r^n = 1$ pour n quelconque. Il suffira d'établir que le module de l'expression
>
> $$\alpha + \beta r + \gamma r^2 + \ldots + \mu r^{n-1}$$
>
> est toujours moindre que 1 quand $\alpha, \beta, \gamma, \ldots, \mu$ sont compris entre 0 et 1; ce qui se vérifie de plusieurs manières."

Onder *module* (norm) van de uitdrukking

$$(6) \qquad u_0 + u_1\zeta + \ldots + u_{n-1}\zeta^{n-1}, \qquad u_0, u_1, \ldots, u_{n-1} \text{ reëel},$$

moet men hier het product verstaan van de getallen die men uit (6) krijgt door ζ de primitieve wortels van $\zeta^n = 1$ te laten doorlopen. In deze context heet een wortel ζ van $\zeta^n = 1$ *primitief* als er geen m is met $\zeta^m = 1$ en $0 < m < n$. Men kan bewijzen dat, als $u_0, u_1, \ldots, u_{n-1}$ gehele getallen zijn, de norm een geheel getal ≥ 0 is, dat alleen gelijk aan nul is als de uitdrukking (6) zelf nul is.

Het opmerkelijke van WANTZELs bewering is dat zij niet eens geldig is in het door hemzelf als voorbeeld gepresenteerde geval $n = 4$. Niemand zal toch kunnen volhouden dat de norm

$$N(v + w\sqrt{-1}) = v^2 + w^2$$

kleiner dan 1 is als v en w beide tussen 0 en 1 liggen. Maar zelfs als we $\alpha, \beta, \gamma, \ldots, \mu$ alle tussen $-\frac{1}{2}$ en $+\frac{1}{2}$ nemen is WANTZELs uitspraak, voor algemene n, onhoudbaar, zoals CAUCHY met een tegenvoorbeeld zou laten zien.

Al op de eerste maart, de dag van LAMÉ's aankondiging, had CAUCHY met kennelijk vertrouwen in LAMÉ's benadering een deel van de nog te behalen eer voor zich opgeëist. Hij had, zo zei hij, enkele maanden eerder de Academie een methode meegedeeld die mogelijk tot een bewijs van FERMAT's laatste stelling zou leiden.

> "Détourné par d'autres travaux, M. Cauchy n'a pas eu le temps de s'assurer si cette conjecture était fondée."

De serie mededelingen die CAUCHY nu in de *Comptes Rendus* van de Academie deed verschijnen zijn voornamelijk gewijd aan pogingen LIOUVILLEs vraag (4) bevestigend te beantwoorden. Bovendien leidde hij, hierop vooruitlopend, onder aanname van de eenduidige factorontbinding een aantal eigenschappen van de getallen (1) af die hem van pas leken te komen bij het bewijs van FERMAT's stelling. Op deze eigenschappen gaan we hier om uit het vervolg begrijpelijke redenen niet verder in. In ieder geval is de gangbare opvatting dat CAUCHY de stelling van de eenduidige ontbinding in priemfactoren voor de getallen (1) als een vanzelfsprekendheid aannam volkomen onjuist.

CAUCHY begon ermee WANTZEL op de vingers te tikken. Diens analyse van het geval $n = 4$ zou al te vinden zijn bij DIRICHLET; en inderdaad gaan deze argumenten ook op voor $n = 3$,

> "mais une objection s'élève contre le passage où il assure qu'on peut

aisément étendre le même mode de démonstration aux nombres complexes de forme plus compliquée qui dépendent des racines de l'équation binôme

$$x^n = 1,$$

n étant un nombre entier quelconque."

Vervolgens gaf CAUCHY een serie tegenvoorbeelden tegen WANTZELs eerder aangehaalde bewering, en hij concludeerde:

"On voit, par ce qui précède, que la théorie générale des nombres complexes est encore à établir."

Enkele maanden lang hield CAUCHY zich met dit probleem bezig, en hij bereikte slechts partiële resultaten. Hij toonde aan dat de getallen (1) inderdaad een euclidische ring vormen in de gevallen

$$n = 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15.$$

CAUCHY zag hier kennelijk over het hoofd dat voor oneven k de getallen (1) voor $n = k$ samenvallen met die voor $n = 2k$; de primitieve wortels van $\zeta^{2k} = 1$ zijn dan namelijk juist de tegengestelden van die van $\zeta^k = 1$. Hoe dan ook, CAUCHY's resultaat is correct. Zijn bewijs waarschijnlijk niet, hoewel dat door het schetsmatige karakter ervan moeilijk is vast te stellen.

Behalve dit resultaat voor kleine n vond CAUCHY analytische argumenten die hem ervan overtuigden dat ook voor grote n - groter dan 10, laten we zeggen - de getallen (1) een euclidische ring vormen, maar ondanks herhaalde pogingen kon hij het bewijs niet sluitend krijgen.

De verklaring voor CAUCHY's falen kwam, per post, uit Duitsland. Hoe Duitsland en Frankrijk zich in wiskundig opzicht onderling verhielden kan men opmaken uit onderstaande passage, ontleend aan een door KUMMER in 1847 geschreven bespreking van het eerste deel van JACOBI's *Mathematische Werke*. Na de lof van GAUSS, JACOBI en DIRICHLET te hebben gezongen schrijft KUMMER:

"Wir könnten nach diesen noch eine treffliche Reihe deutscher Mathematiker aufführen, welche das neu erwachte Leben entweder mit anfachen halfen, oder von demselben beseelt wurden, aber die Hauptmacht und der Principat, welchen Deutschland in dieser Wissenschaft jetzt behauptet, liegt allein in den genannten drei Namen Gauss, Jacobi und Dirichlet. In Frankreich lebt jetzt nur einer, welcher diesen an die Seite gestellt werden kann, nämlich Cauchy, dessen ausserordentlich productiver Geist

> in den elementarsten, sowie in den sublimsten Sphären der Mathematik neues schafft, und in allem, was er unternimmt, einen Fortschritt der Erkenntniss bewirkt. Wenn wir nun in den Mathematikern ersten Ranges das entschiedene Übergewicht über die Franzosen haben, da uns drei Sterne erster Grösse glänzen, jenen nur einer, so können wir ihnen gern zugestehen, dass sie unter den mathematischen Sternen zweiter und dritter Grösse mehr ausgezeichnete Namen nachzuweisen haben, als wir, und dass dieses Übergewicht weiter hinab bis zu den teleskopischen Sternen, selbst bis zu denen sechszehnter Grösse immer mehr zunimmt."

In deze situatie is het weinig verwonderlijk dat het antwoord op de vraag die men zich in Parijs stelde in Duitsland al enige tijd bekend was. Op 28 april 1847 schreef KUMMER aan LIOUVILLE:

> "Quant à la proposition élémentaire pour ces nombres complexes, *qu'un nombre complexe composé ne peut être décomposé en facteurs premiers que d'une seule manière*, (...) je puis vous assurer qu'*elle n'a pas lieu généralement* tant qu'il s'agit de nombres complexes de la forme $\alpha_0 + \alpha_1 r + \alpha_2 r^2 + \ldots + \alpha_{n-1} r^{n-1}$, mais qu'on peut la sauver en introduisant un nouveau genre de nombres complexes, que j'ai appelé *nombre complexe idéal*."

CAUCHY's reactie:

> "Si M. Kummer a fait faire à la question quelques pas de plus, si même il était parvenu à lever tous les obstacles, j'applaudirais le premier au succès de ses efforts; car ce que nous devons surtout désirer, c'est que les travaux de tous les amis de la science concourent à faire connaître et à propager la vérité."

In een van de volgende *Comptes Rendus* bewijst CAUCHY, in navolging van KUMMER, dat voor $n = 23$ de getallen (1) niet de eigenschap van de eenduidige ontbinding in priemfactoren hebben. Hiermee besluiten we ons relaas van de wederwaardigheden van de Parijse Academie in het eerste halfjaar van 1847. Voor meer bijzonderheden raadplege men de *Comptes Rendus de l'Académie des Sciences*, vol. 24, 1847.

In Duitsland had zich enkele jaren eerder een analoge ontwikkeling op iets minder overzichtelijke wijze voltrokken.

Dat men zich in Duitsland interesseerde voor getallen van de vorm (1)

kwam niet voort uit de wens FERMAT's laatste stelling te bewijzen - hoewel men zich van een mogelijke toepassing in deze richting wel bewust was - maar uit het probleem de *kwadratische reciprociteitswet* van GAUSS (1801) te generaliseren. De kwadratische reciprociteitswet zegt, dat als p en q twee verschillende oneven priemgetallen zijn, de beide congruenties

$$x^2 \equiv p \bmod q$$
$$y^2 \equiv q \bmod p$$

òfwel allebei oplosbaar zijn in gehele x en y, òfwel allebei onoplosbaar, behalve als p en q beide 3 modulo 4 zijn, in welk geval één van beide congruenties oplosbaar is en de andere onoplosbaar. De vraag rees deze wet te generaliseren voor hogere machten dan de tweede.

GAUSS zelf liet in 1832 zien dat men, om een dergelijke wet voor vierde machten adequaat te kunnen formuleren, de getallen (1) voor $n = 4$ nodig heeft. JACOBI gaf in 1836 een eenvoudig bewijs van de door GAUSS uitgesproken stelling, en was tevens in staat een derdemachts-reciprociteitswet te bewijzen, gebruik makende van de getallen (1) voor $n = 3$. Zijn resultaten suggereerden dat men zich voor hogere n allereerst de volgende vraag moest stellen:

(7) is elk priemgetal p dat 1 modulo n is te schrijven als norm van een getal (1)?

Voor $n = 4$ en $n = 3$ was dit bekend, en voor $n = 5$, 8 en 12 beantwoordde JACOBI deze vraag bevestigend in 1839, zonder evenwel het bewijs te publiceren.

In de ontwikkeling in Duitsland nam (7) de plaats in die in Frankrijk door LIOUVILLEs vraag (4) zou worden ingenomen. Beide kwesties hangen ten nauwste samen: indien men eenduidigheid van priemfactorontbinding voor de getallen (1) aanneemt, blijkt het niet lastig te zijn te bewijzen dat de eigenschap in (7) inderdaad geldt. Dat, omgekeerd, een bevestigend antwoord op (7) eenduidigheid van factorisatie impliceert lag buiten bereik van de toen bestaande middelen, maar het lijdt geen twijfel dat JACOBI en, enkele jaren later, EISENSTEIN inzagen dat dit zo moest zijn.

KUMMER waarschijnlijk niet: die legde in 1844 aan de Berlijnse Academie een manuscript voor waarin hij meende bewezen te hebben dat voor alle n het antwoord op (7) *ja* luidt. Zijn redenering berustte niet op eenduidige factorisatie, maar bevatte een andere fout. In elk geval kwam KUMMER, moge-

lijk op aanwijzing van JACOBI, tijdig tot de ontdekking dat (7) onjuist is voor $n = 23$, en het foutieve bewijs is nooit in druk verschenen.

Het schijnt dat dit incident, na een mondelinge overlevering van 66 jaar, in 1910 in een rede van HENSEL de vorm heeft gekregen waarin het nu aan de mathematische wereld bekend is: KUMMER zou een bewijs van FERMAT's laatste stelling gevonden menen te hebben, maar er door DIRICHLET op gewezen zijn dat het berustte op de onbewezen aanname van eenduidige priemfactorisatie. Indien dit overigens slecht gedocumenteerde verhaal op een andere gebeurtenis dan de boven vermelde slaat zou KUMMER zich tweemaal op vrijwel dezelfde wijze vergist hebben, hetgeen moeilijk aan te nemen is. Men raadplege hierover het aan het eind van deze paragraaf genoemde artikel van H.M. EDWARDS.

Niet uit het veld geslagen - zo gaat het verhaal, nu wel betrouwbaar, verder - wist KUMMER in 1845 tot een bevredigende theorie te komen door het invoeren van *ideale complexe getallen*, vergelijk zijn eerder geciteerde brief aan LIOUVILLE. En in maart 1847, juist toen men zich in Parijs het hoofd brak over eenduidige factorisatie, kwam KUMMER op het idee zijn *ideaaltheorie* op FERMAT's laatste stelling toe te passen. Uit zijn correspondentie met KRONECKER krijgen we de indruk dat hij niets beters te doen vond; en als hij zijn resultaten aan de Berlijnse Academie meedeelt schrijft hij:

> "Der Fermatsche Satz ist (...) mehr ein Curiosum als ein Hauptpunkt der Wissenschaft, (...)."

KUMMER was in staat FERMAT's laatste stelling voor een grote, waarschijnlijk oneindige klasse priemgetallen n te bewijzen. Of deze klasse priemgetallen inderdaad oneindig is, zoals KUMMER aanvankelijk beweerde, is onbekend. Zijn methoden en latere verfijningen ervan, met name van VANDIVER afkomstig, hebben enkele jaren geleden WAGSTAFF in staat gesteld met behulp van een electronische computer FERMAT's laatste stelling te bewijzen voor alle $n < 100000$. Het algemene geval blijft onbewezen. Vermeldenswaard is ten slotte een opmerking van KNUTH, die het in zijn *The Art of Computer Programming* gehanteerde systeem om vraagstukken te waarderen illustreert met de volgende opgave:

> "[*M50*] Prove that when n is an integer, $n > 2$, the equation $x^n + y^n = z^n$ has no solution in positive integers, x, y, z."

Bij de *Answers to Exercises* vindt men:

"(*Note:* One of the men who read a preliminary draft of the manuscript for this book reported that he had discovered a truly remarkable proof, which the margin of his copy was too small to contain.)"

We zullen niet verder stilstaan bij FERMAT's stelling, en evenmin bij het onderwerp waar KUMMER zijn theorie voor geschapen had: de n-de machts reciprociteitswetten die hij in later jaren bewees, en die hij zelf veel hoger schatte dan de resultaten betreffende FERMAT's stelling waar hij zijn tegenwoordige roem aan dankt. Vergelijk zijn woorden uit 1850:

"(...) ist es mir gelungen die allgemeinen Reciprocitätsgesetze für beliebig hohe Potenzreste zu entdecken, welche nach dem gegenwärtigen Stande der Zahlentheorie als die Hauptaufgabe und die Spitze dieser Wissenschaft anzusehen sind."

In plaats daarvan keren we terug tot een betrekkelijk ondergeschikt punt waar KUMMER in 1844 enige aandacht aan geschonken heeft.

Zoals we gezien hebben luidt voor $n = 23$ het antwoord op beide vragen (4) en (7) *neen*, en het bewijs dat men hiervan gaf was niet moeilijk: met behulp van de *perioden van GAUSS* toonde men aan dat $p = 47$ geen norm van een getal van de vorm (1), met $n = 23$, kan zijn. KUMMER, die eerst alleen het geval dat n priem is beschouwde, stelde zich de vraag: is $n = 23$ het eerste voorbeeld? Voor $n = 5, 7, 11, 13, 17, 19$ kwam hij door berekeningen tot de ontdekking dat inderdaad elk priemgetal $p \equiv 1 \bmod n$ dat kleiner dan 1000 is de norm van een getal (1) is. Maar hoe dit voor alle priemgetallen $p \equiv 1 \bmod n$ te bewijzen? KUMMER merkte op dat het voldoende is eenduidigheid van factorisatie aan te tonen, en hiertoe greep hij naar de methode die ook WANTZEL zou toepassen: de euclidische delingsalgorithme.

Uit de samenvatting die we van WANTZELs redenering gegeven hebben is duidelijk dat het probleem erop neerkomt een willekeurige uitdrukking

$$u_0 + u_1\zeta + \ldots + u_{n-1}\zeta^{n-1}, \qquad u_0, u_1, \ldots, u_{n-1} \text{ rationaal},$$

zodanig te benaderen met een getal

$$u_0' + u_1'\zeta + \ldots + u_{n-1}'\zeta^{n-1}, \qquad u_0', u_1', \ldots, u_{n-1}' \text{ geheel},$$

dat het verschil

$$(u_0 - u_0') + (u_1 - u_1')\zeta + \ldots + (u_{n-1} - u_{n-1}')\zeta^{n-1}$$

een norm heeft die kleiner dan 1 is.

Dit probleem loste KUMMER voor $n = 5$ op, in een brief aan KRONECKER gedateerd 2 october 1844. Een vereenvoudigd bewijs dat hij enkele dagen later vond is als volgt te reconstrueren.

De norm van $f(\zeta) = u_0 + u_1\zeta + u_2\zeta^2 + u_3\zeta^3 + u_4\zeta^4$ was gedefinieerd door

$$N(f(\zeta)) = f(\zeta)\cdot f(\zeta^2)\cdot f(\zeta^3)\cdot f(\zeta^4).$$

Hierbij geldt $\overline{f(\zeta)} = f(\zeta^4)$ en $\overline{f(\zeta^2)} = f(\zeta^3)$, dus $f(\zeta)f(\zeta^4)$ en $f(\zeta^2)f(\zeta^3)$ zijn reële getallen ≥ 0. De ongelijkheid tussen het meetkundig en het rekenkundig gemiddelde levert nu

$$\sqrt{N(f(\zeta))} \leq \frac{1}{2}(f(\zeta)\cdot f(\zeta^4) + f(\zeta^2)\cdot f(\zeta^3)).$$

Uit een eenvoudige berekening volgt dat het rechterlid gelijk is aan:

$$\frac{1}{4}\cdot \sum_{0\leq i<j\leq 4} (u_i - u_j)^2.$$

Om het probleem voor $n = 5$ op te lossen is het dus voldoende de volgende bewering te bewijzen, waarbij we $v_i = u_i - u_i'$ zetten:

(8) bij elke keuze van vijf reële getallen u_0, u_1, u_2, u_3, u_4 is het mogelijk reële getallen v_0, v_1, v_2, v_3, v_4 te vinden zodanig dat

(9) $\qquad u_i - v_i$ geheel is, voor $i = 0, 1, 2, 3, 4,$

en

(10) $$\sum_{0\leq i<j\leq 4} (v_i - v_j)^2 < 4.$$

Een nuttige ongelijkheid bij het bewijs is

$$\sum_{0\leq i<j\leq 4} (v_i - v_j)^2 = 5\cdot \sum_{i=0}^{4} (v_i - v)^2 - \Big(\sum_{i=0}^{4} (v_i - v)\Big)^2 \leq 5\cdot \sum_{i=0}^{4} (v_i - v)^2$$

voor willekeurige reële v.

We kiezen nu de v_i zó dat (9) geldt, en $0 \leq v_i < 1$. Dan volgt met $v = \frac{1}{2}$ uit bovenstaande ongelijkheid:

$$\sum_{0\leq i<j\leq 4} (v_i - v_j)^2 \leq 5\cdot((\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2) = 6\tfrac{1}{4},$$

hetgeen niet goed genoeg is om (10) te bewijzen. Om een beter resultaat te verkrijgen merken we op dat we mogen aannemen dat er k en ℓ, $0 \leq k < \ell \leq 4$,

zijn met $|v_k - v_\ell| \leq \frac{1}{5}$. Dit is evident als de v_i alle in een interval van lengte $\leq \frac{4}{5}$ liggen, en als dit interval langer is (maar < 1), dan trekken we van de grootste v_i één af. Dan blijft (9) gelden.

Nemen we voor v het gemiddelde van v_k en v_ℓ, dan geldt $|v_k - v| \leq \frac{1}{10}$, $|v_\ell - v| \leq \frac{1}{10}$. Bij de overige v_i tellen we nu, zo nodig, $+1$ of -1 op om te bereiken dat $|v_i - v| \leq \frac{1}{2}$. Dan vinden we

$$\sum_{0\leq i<j\leq 4} (v_i - v_j)^2 \leq 5\cdot((\tfrac{1}{10})^2 + (\tfrac{1}{10})^2 + (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2) = 3{,}85 < 4$$

waarmee (10) is aangetoond. De getallen (1) vormen voor $n = 5$ dus een euclidische ring.

KUMMER beweerde het geval $n = 7$ evenzo te kunnen behandelen. Hiertoe zou men voor gegeven $u_0, u_1, \ldots, u_6$ getallen $v_0, v_1, \ldots, v_6$ moeten kunnen vinden met $u_i - v_i$ geheel $(i = 0, 1, \ldots, 6)$ en

$$(11) \qquad \sum_{0\leq i<j\leq 6} (v_i - v_j)^2 < 6.$$

Het voor $n = 5$ gegeven argument leidt nu slechts tot

$$\sum_{0\leq i<j\leq 6} (v_i - v_j)^2 \leq 8\tfrac{23}{28}.$$

Dat het toch denkbaar is dat KUMMER (11) bewezen kan hebben blijkt als men nagaat wat voor n getallen, in plaats van vijf of zeven, het best mogelijke resultaat is. Men vindt dan (zie [13]):

$$\sum_{0\leq i<j<n} (v_i - v_j)^2 \leq \frac{n^2 - 1}{12}$$

waarbij het gelijkheidsteken bijvoorbeeld nodig is als $u_i = i/n$, voor $i = 0, 1, \ldots, n-1$. In het bijzonder kan < 4 in (10) vervangen worden door ≤ 2, en < 6 in (11) door ≤ 4. Voor $n = 11$ vindt men ≤ 10, en afgezien van een kleine moeilijkheid met het gelijkheidsteken is dit juist toereikend om te bewijzen dat ook voor $n = 11$ de getallen (1) een euclidische ring vormen, een resultaat dat KUMMER niet opmerkte. De gevallen $n = 13$, 17 en 19 blijven met deze methode onbeslist.

Toen KUMMER eenmaal zijn ideaaltheorie ontwikkeld had verdween de kwestie die ons hier bezighoudt uit het centrum van de toenmalige belangstelling. We gaan hier niet verder in op de geschiedenis van het onderwerp maar beperken ons tot een korte bespreking van de resultaten zoals die nu bekend zijn.

Enkele jaren geleden hebben MASLEY en MONTGOMERY, zie [15], alle getallen n bepaald waarvoor de getallen (1), met ζ een primitieve wortel van

$\zeta^n = 1$, de eigenschap van de eenduidige ontbinding in priemfactoren hebben. Zoals we bij de bespreking van CAUCHY's resultaten gezien hebben mogen we ons beperken tot het geval n niet 2 modulo 4 is. Voor dergelijke n geldt, dat het antwoord op (4) *ja* is dan en slechts dan als n een van de volgende dertig waarden aanneemt:

(12) 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.

Het moeilijke deel van deze stelling is de *slechts dan*-kant: het bewijs dat voor alle andere waarden van n, $n \not\equiv 2 \bmod 4$, het antwoord op (4) *neen* is. Het bewijs van de *dan*-kant is een routine-zaak als men door MINKOWSKI ontwikkelde methoden toepast, en het begrip *euclidische ring* speelt hierbij geheel geen rol.

Voor dertien van de dertig waarden (12) is bekend dat de getallen (1) een euclidische ring vormen ten opzichte van de norm. Dit zijn

(13) 1, 3, 4, 5, 7, 8, 9, 11, 12, 15, 16, 20, 24.

De overige zeventien waarden schijnen nooit onderzocht te zijn, met uitzondering van $n = 32$. In dit geval geldt de euclidische eigenschap niet: is ζ een primitieve wortel van $\zeta^{32} = 1$, dan is het onmogelijk $1 + (1 + \zeta)^5$ zodanig te delen door $(1 + \zeta)^6$ dat de rest een norm heeft die kleiner is dan $N((1 + \zeta)^6) = 64$.

De getallen (13) zijn precies alle n, $n \not\equiv 2 \bmod 4$, waarvoor geldt $\phi(n) \leq 10$. Hier duidt $\phi(n)$ het aantal getallen m met $1 \leq m \leq n$ aan dat onderling ondeelbaar is met n. Het is gemakkelijk in te zien dat $\phi(n)$ precies het aantal primitieve wortels van $\zeta^n = 1$ is. Bovendien blijkt $\phi(n)$ juist het kleinste getal d te zijn met de eigenschap dat alle getallen (1) zich al laten schrijven als

$$a_0 + a_1\zeta + \ldots + a_{d-1}\zeta^{d-1}, \qquad a_0, a_1, \ldots, a_{d-1} \text{ geheel.}$$

Men kan $\phi(n)$ dus opvatten als maat voor het *aantal* getallen (1), en de dertien gevallen (13) zien als de dertien eenvoudigste.

Dat men voor $n = 1$ een euclidische ring krijgt werd opgemerkt door EUCLIDES. Het geval $n = 4$ vindt men bij GAUSS [9, pp. 117-118] en DIRICHLET [6, vol. I, pp. 540-541]. Dat $n = 3$ geheel analoog ging was algemeen bekend, maar vóór WANTZEL [3, pp. 430-434] scheen niemand het de moeite

waard te vinden het op te schrijven. Het is ook te vinden bij GAUSS' nagelaten papieren [9, pp. 391-393]. Het geval $n = 5$ werd voor het eerst gepubliceerd door OUSPENSKY [17], enkele jaren voor KUMMERs bewijs verscheen. EISENSTEIN [8, vol. II, pp. 585-595] handelde het geval $n = 8$ af, zie ook [12] en [14]. Een opmerking van hem [8, vol. II, p. 793] doet vermoeden dat hij ook op de hoogte was van het geval $n = 12$ maar een eerder dan 1972 gepubliceerd bewijs, zie [12], heb ik niet kunnen vinden; zie ook [14]. Voor $n = 7, 9, 11, 15, 20$ vindt men bewijzen in [13]. Een lang bewijs - één uur rekentijd op een UNIVAC 1108 - voor het geval $n = 16$ werd gevonden door OJALA [16]. Het geval $n = 24$, tenslotte, kan behandeld worden met behulp van eigenschappen van de Weylgroep E_8, maar de bijzonderheden zijn nog niet gepubliceerd.

Literatuur bij §1.

1. F. CAJORI, Pierre Laurent Wantzel, *Bull. Amer. Math. Soc.* 24 (1918), 339-347.
2. A. CAUCHY, *Oeuvres complètes*, sér. 1, tome X, Gauthier-Villars, Parijs 1897.
3. *Comptes Rendus de l'Académie des Sciences* 24 (1847).
4. L.E. DICKSON, *History of the theory of numbers*, vol. II, Ch. XXVI, Chelsea, New York 1952 (herdruk).
5. L.E. DICKSON et al., *Algebraic numbers*, Chelsea, Bronx, z.j. (herdruk).
6. G. LEJEUNE DIRICHLET, *Werke*, Chelsea, Bronx 1969 (herdruk).
7. H.M. EDWARDS, The background of Kummer's proof of Fermat's last theorem for regular primes, *Arch. History Exact Sci.* 14 (1975), 219-236.
8. G. EISENSTEIN, *Mathematische Werke*, Chelsea, New York 1975.
9. C.F. GAUSS, *Werke*, Zweiter Band, Göttingen 1876.
10. C.G.J. JACOBI, *Gesammelte Werke*, Sechster Band, Chelsea, New York 1969 (herdruk).
11. E.E. KUMMER, *Collected papers*, Springer, Berlijn 1975.
12. R.B. LAKEIN, Euclid's algorithm in complex quartic fields, *Acta Arith.* 20 (1972), 393-400.
13. H.W. LENSTRA, JR., Euclid's algorithm in cyclotomic fields, *J. London Math. Soc.* (2) 10 (1975), 457-465.
14. J.M. MASLEY, On euclidean rings of integers in cyclotomic fields, *J. Reine Angew. Math.* 272 (1975), 45-48.
15. J.M. MASLEY, H.L. MONTGOMERY, Cyclotomic fields with unique factorization, *J. Reine Angew. Math.* 286/287 (1976), 248-256.
16. T. OJALA, Euclid's algorithm in the cyclotomic field $\mathbb{Q}(\zeta_{16})$, te verschijnen.
17. J. OUSPENSKY, Note sur les nombres entiers dépendant d'une racine cinquième de l'unité, *Math. Ann.* 66 (1909), 109-112. Vgl. *Jbuch Fortschr. Math.* 37 (1906), 241.
18. H.J.S. SMITH, *Report on the theory of numbers*, Chelsea, Bronx 1965 (herdruk).
19. S.S. WAGSTAFF, JR., Fermat's last theorem is true for all exponents less than 58150, *Notices Amer. Math. Soc.* 22 (1975), A-507.
20. A. WEIL, La cyclotomie jadis et naguère, *Sém. Bourbaki* (1973/74), exp. 452, *Lect. Notes Math.* 431, Springer, Berlijn 1975.

Euclidische getallenlichamen
2. Een methode van Hurwitz

Het in de vorige paragraaf beschouwde probleem laat zich direct generaliseren voor algemenere getallenlichamen. Laat

$$g = X^n + q_{n-1}X^{n-1} + \ldots + q_1X + q_0$$

een irreducibel polynoom met rationale coëfficiënten zijn, γ een nulpunt van g, en K het door γ voortgebrachte lichaam. Elk element ξ van K laat zich eenduidig schrijven als

$$(1) \qquad p_0 + p_1\gamma + \ldots + p_{n-1}\gamma^{n-1}, \qquad p_0, p_1, \ldots, p_{n-1} \text{ rationaal.}$$

De *norm* $N(\xi)$ van ξ is per definitie de absolute waarde van het product van de getallen (1), waar γ de complexe nulpunten van g doorloopt. Kennelijk geldt $N(\xi\eta) = N(\xi)N(\eta)$ voor alle ξ en η in K, en men kan bewijzen dat $N(\xi)$ een *rationaal* getal is dat alleen nul is als $\xi = 0$.

Binnen K beschouwen we nu een ring R die zich, ruw gesproken, ten opzichte van K gedraagt als de ring der gehele getallen ten opzichte van het lichaam der rationale getallen. Preciezer gesproken houdt dit twee eisen in. Ten eerste moet van elk element ξ van K een veelvoud $m\xi$ in R liggen, met m geheel, $m > 0$. In de tweede plaats verlangen we dat er elementen $\theta_0, \theta_1, \ldots, \theta_{d-1}$ in K zijn zodanig dat een element ξ van K in R ligt dan en slechts dan als het te schrijven is in de vorm

$$(2) \qquad \xi = a_0\theta_0 + a_1\theta_1 + \ldots + a_{d-1}\theta_{d-1}, \qquad a_0, a_1, \ldots, a_{d-1} \text{ geheel.}$$

Men kan bewijzen dat als zulke $\theta_0, \theta_1, \ldots, \theta_{d-1}$ bestaan ze ook zo te kiezen zijn dat $d = n$; dan is de voorstelling (2) bovendien eenduidig. Opdat R een ring vormt moeten de getallen θ_i de eigenschap hebben dat alle producten $\theta_i\theta_j$ weer van de vorm (2) zijn. We zullen bovendien steeds aannemen dat 1 tot R behoort.

Ringen R die aan de zojuist beschreven voorwaarden voldoen zijn steeds te vinden. Nemen we bijvoorbeeld aan dat de coëfficiënten q_i van g *geheel* zijn - en dit kan men bereiken door zo nodig γ door een geschikt veelvoud $m\gamma$ te vervangen - dan kunnen we $d = n$, $\theta_i = \gamma^i$ nemen. De elementen van R zien er dan evenzo uit als de getallen (1) uit de vorige paragraaf:

(3) $\quad a_0 + a_1\gamma + \ldots a_{n-1}\gamma^{n-1}, \qquad a_0, a_1, \ldots, a_{n-1}$ geheel.

Men kan bewijzen dat de vereniging R_0 van alle ringen R die aan onze eisen voldoen zelf ook een ring is die deze eigenschappen heeft. Men noemt R_0 wel de ring van *algebraïsche gehele getallen* in K.

De ring R heet *euclidisch ten opzichte van de norm*, of kortweg *norm-euclidisch*, als het voor elk tweetal elementen α en β uit R, met $\beta \neq 0$, mogelijk is een quotiënt κ en een rest ρ te vinden, beide tot R behorend, zodanig dat

$$\alpha = \kappa\beta + \rho$$

$$N(\rho) < N(\beta).$$

Hierbij merken we op dat $N(\beta)$ steeds *geheel* is als β tot R behoort. Voor β uit R, ongelijk aan nul, blijkt men namelijk $N(\beta)$ te kunnen interpreteren als het aantal *restklassen* modulo β, d.w.z. het grootste aantal elementen $\rho_1, \rho_2, \ldots, \rho_m$ dat in R te vinden is met de eigenschap dat geen van de verschillen $\rho_i - \rho_j$ $(i \neq j)$ in R deelbaar is door β.

We noemen het lichaam K *euclidisch* als R_0 norm-euclidisch is. Het blijkt overigens dat R_0 de enige R is die norm-euclidisch kan zijn.

De voornaamste motivatie voor deze definitie is dezelfde als in de vorige paragraaf:

(4) als R norm-euclidisch is, geldt de stelling van de eenduidigheid van ontbinding in priemfactoren in R.

Dit wordt weer bewezen met de argumenten van EUCLIDES.

Dat de omkering van (4) niet geldt hebben we in de vorige paragraaf gezien aan het geval $n = 32$. Een eenvoudiger voorbeeld verkrijgt men door de getallen $a + b\sqrt{14}$, met a en b geheel, of de getallen $\frac{1}{2}(a + b\sqrt{-19})$, met a en b geheel, $a - b$ even, te beschouwen.

Hoe te bepalen of R norm-euclidisch is? Schrijven we $\xi = \alpha/\beta$ dan vinden we uit de definitie:

> R is norm-euclidisch dan en slechts dan als er voor elke ξ uit K een κ uit R te vinden is met $N(\xi - \kappa) < 1$.

Dit kunnen we gebruiken om het probleem meetkundig te formuleren.

Het polynoom g heeft n complexe nulpunten, waarvan er, laten we zeggen, r reëel zijn: $\gamma_1, \gamma_2, \ldots, \gamma_r$. De overige $n - r$ nulpunten

vallen in een aantal, zeg s, paren complex geconjugeerden uiteen. Kies uit elk paar één; dat geeft s nulpunten $\delta_1, \delta_2, \ldots, \delta_s$ van g, en er geldt $r + 2s = n$. We bedden het lichaam K nu in de n-dimensionale reële vectorruimte $\mathbb{R}^r \times \mathbb{C}^s$ in door een uitdrukking $f(\gamma) = p_0 + p_1\gamma + \ldots + p_{n-1}\gamma^{n-1}$ als in (1) af te beelden op

$$(f(\gamma_1), \ldots, f(\gamma_r), f(\delta_1), \ldots, f(\delta_s)).$$

Het blijkt dat K dicht komt te liggen in $\mathbb{R}^r \times \mathbb{C}^s$. Wegens

$$N(f(\gamma)) = \Big| \prod_{i=1}^{r} f(\gamma_i) \cdot \prod_{i=1}^{s} f(\delta_i) f(\overline{\delta_i}) \Big|$$

kunnen we het definitie-gebied van de norm N uitbreiden tot de hele ruimte $\mathbb{R}^r \times \mathbb{C}^s$ door

$$N((x_1, \ldots, x_r, y_1, \ldots, y_s)) = \Big| \prod_{i=1}^{r} x_i \cdot \prod_{i=1}^{s} y_i \overline{y}_i \Big|$$

met x_i reëel en y_i complex.

De ring R is onder de inbedding in $\mathbb{R}^r \times \mathbb{C}^s$ een *rooster* geworden, d.w.z., er is een *basis* $\theta_0, \theta_1, \ldots, \theta_{n-1}$ van $\mathbb{R}^r \times \mathbb{C}^s$ over de reële getallen zodanig dat de getallen van R precies de vectoren van de vorm

(5) $$a_0\theta_0 + a_1\theta_1 + \ldots a_{n-1}\theta_{n-1}, \qquad a_0, a_1, \ldots, a_{n-1} \text{ } \textit{geheel},$$

zijn. We zien:

(6) R is norm-euclidisch als elk element ξ van $\mathbb{R}^r \times \mathbb{C}^s$ te schrijven is als som van een element κ van R en een element dat behoort tot de verzameling

$$V = \{y \mid N(y) < 1\}.$$

De verzameling V is in het geval $r = 0$, $s = 1$ een open cirkelschijf met 0 als middelpunt. In het geval $r = 2$, $s = 0$ is V een onbegrensde verzameling in het platte vlak, begrensd door hyperbolen. In het algemeen is V een open verzameling die 0 bevat en alleen begrensd is als $r + s = 1$. Volgens (6) is het nu de vraag, of de translaties

$$\kappa + V, \qquad \kappa \text{ uit } R,$$

samen de hele ruimte overdekken. Om te zien of ξ tot een van deze translaties behoort, mogen we kennelijk vrijelijk elementen van R bij ξ op-

tellen; aangezien deze van de vorm (5) zijn, is het voldoende alleen ξ's te beschouwen die in het volgende parallellepipedum liggen:

$$(7) \qquad \{q_0\theta_0 + q_1\theta_1 + \ldots + q_{n-1}\theta_{n-1} \mid 0 \le q_0 < 1, \quad 0 \le q_1 < 1, \ \ldots, \ 0 \le q_{n-1} < 1\}.$$

Dit is een begrensde verzameling, en het is niet lastig in te zien dat, *als* deze overdekt wordt door de oneindig vele translaties $\kappa + V$, dit ook reeds geschiedt door een *eindig* aantal hiervan.

Als we er inderdaad in geslaagd zijn het parallellepipedum (7) te overdekken hebben we eigenlijk meer bewezen dan strikt nodig: om te bewijzen dat R norm-euclidisch is was het voldoende geweest alleen ξ uit K te beschouwen, hetgeen correspondeert met *rationale* $q_0, q_1, \ldots, q_{n-1}$ in (7). Indien de omkering van (6) gold zouden beide kwesties equivalent zijn; deze omkering is echter nooit bewezen, noch is een tegenvoorbeeld bekend. Men vergelijke hiermee een onbewezen vermoeden van BARNES en SWINNERTON-DYER [1, p. 313].

Nemen we de omkering van (6) als waar aan dan is de vraag of R euclidisch ten opzichte van de norm is beslisbaar. Immers, laat $\beta_1, \beta_2, \beta_3, \ldots$ een aftelling van alle elementen van R ongelijk aan nul zijn. Dan kan men voor $n = 1, 2, 3, \ldots$ achtereenvolgens controleren of aan de volgende twee voorwaarden voldaan is:

I_n: voor elke α uit R is er een ρ uit R met $\rho \equiv \alpha \bmod \beta_n$ en $N(\rho) < N(\beta_n)$;

II_n: het parallellepipedum (7) wordt niet overdekt door de $n+1$ translaties $V, \ \beta_1 + V, \ \beta_2 + V, \ \ldots, \ \beta_n + V$.

Indien aan een van beide voorwaarden niet voldaan is stopt men: is I_n niet vervuld dan is R niet norm-euclidisch, en is II_n niet vervuld dan is R wel norm-euclidisch. Als deze beslissingsprocedure niet termineert is voor alle n aan I_n en II_n voldaan. Dan is R norm-euclidisch, maar de translaties $\kappa + V$, met κ uit R, overdekken niet de hele ruimte $\mathbb{R}^r \times \mathbb{C}^s$, in tegenspraak met de omkering van (6) die we voor waar hadden aangenomen. Volledigheidshalve merken we op dat voor vaste n de vraag of I_n en II_n vervuld zijn beslisbaar is.

Dat de beslisbaarheid van de vraag of R norm-euclidisch is zonder onbewezen aannamen nog nooit is aangetoond is kenmerkend voor het gebrek aan algemene stellingen dat de theorie kent. Voorbeelden is het enige waar de

theorie rijk aan is, maar zelfs de meest voor de hand liggende vraag naar de grootte van deze rijkdom:

zijn er, op isomorfie na, oneindig veel euclidische K ?

blijft onbeantwoord. Het belangrijkste resultaat op dit gebied is een stelling van DAVENPORT, zie [2], die zegt dat er op isomorfie na slechts eindig veel euclidische lichamen zijn met $r + s \leq 2$. Met zijn methoden heeft men alle euclidische K met $n \leq 2$ kunnen bepalen. Tenslotte is er een eindigheidsstelling van HEILBRONN die betrekking heeft op speciale klassen van abelse lichamen, zie [5].

Er zijn, op isomorfie na, 311 verschillende euclidische K bekend. Onderstaande tabel, ontleend aan [7], geeft aan hoe deze lichamen verdeeld zijn ten opzichte van n en $r + s$.

$r+s$ \ n	1	2	3	4	5	6	7	8	9	10	totaal
1	1	5									6
2		16	52	32							100
3			57	11	12	28					108
4				9	10	25	23	24			91
5					1	2	0	0	0	1	4
6						2	0	0	0	0	2
totaal	1	21	109	52	23	57	23	24	0	1	311

Voor verwijzingen naar een deel van de onoverzienbare literatuur op dit gebied zie men [7].

In de methoden waarmee deze 311 lichamen gevonden zijn is een grote diversiteit te onderscheiden. Voor een aantal elementaire bewijzen in het kwadratische geval ($n = 2$) raadplege men HARDY en WRIGHT [4, §14.7/8]. De meeste kubische voorbeelden ($n = 3$) zijn gevonden met behulp van een electronische computer; de gevolgde methode kan men beschouwen als een verfijning van de boven geschetste beslissingsprocedure.

Wij zullen hier een methode beschrijven die teruggaat op een idee van HURWITZ [6, pp. 236-243, pp. 471-474]. Deze baseert een tegenwoordig in onbruik geraakte opzet van de ideaaltheorie op de volgende variant van de

euclidische delingsalgorithme, geldig voor elke K en R:

(8) er is een geheel getal $m > 1$, zodanig dat er voor elke ξ uit K een κ uit R is, en een geheel getal j, $0 < j < m$, met

$$N(j\xi - \kappa) < 1.$$

Hier is m afhankelijk van R. Het is duidelijk dat R norm-euclidisch is dan en slechts dan als we $m = 2$ kunnen nemen.

We schetsen een bewijs van (8). Omdat de verzameling V uit (6) open is, kan men een open omgeving U van 0 in $\mathbb{R}^r \times \mathbb{C}^s$ kiezen zodat $U - U$ in V bevat is, d.w.z.:

(9) $\quad N(u - v) < 1 \quad$ voor alle u en v uit U.

Laat nu ξ een element van K zijn, en beschouw de translaties

$$i\xi + U, \qquad i = 1, 2, \ldots, m,$$

van U, waar m een nader te kiezen geheel getal > 1 is. Van elk element van $i\xi + U$ trekken we zódanig een element van R af dat het binnen het parallellepipedum (7) terechtkomt. Dit levert een verzameling, laten we zeggen $(i\xi + U)^*$, die geheel binnen (7) bevat is, en die hetzelfde volume als $(i\xi + U)$ bezit. Zou dit laatste namelijk niet het geval zijn, dan zouden er twee verschillende punten van $i\xi + U$ zijn, die op hetzelfde punt van (7) terechtkomen, dus een verschil hebben dat in R ligt; dit is wegens (9) echter onmogelijk.

Merken we verder op dat $i\xi + U$ en U kennelijk hetzelfde volume hebben, dan concluderen we dat we binnen (7) de m verzamelingen

(10) $\quad (\xi + U)^*, \ (2\xi + U)^*, \ \ldots, \ (m\xi + U)^*$

hebben, elk met een volume gelijk aan dat van U. Laat nu m zo gekozen zijn dat m maal het volume van U groter is dan het kennelijk eindige volume van het parallellepipedum (7); dit is een keuze die niet van ξ afhangt. Dan kunnen de verzamelingen (10) niet disjunct zijn, dus er zijn gehele getallen i en i', $1 \leq i < i' \leq m$, elementen u en v van U, en λ, λ' uit R zodat

$$i\xi + u - \lambda = i'\xi + v - \lambda'.$$

Met $\kappa = \lambda' - \lambda$ en $j = i' - i$ krijgen we

$$N(j\xi - \kappa) = N(i'\xi - \lambda' - i\xi + \lambda) = N(u - v) < 1,$$

en j is een geheel getal, $0 < j < m$. Hiermee is HURWITZ' stelling bewezen.

Om met dit bewijs een zo klein mogelijke waarde voor m te vinden moet men U natuurlijk zo groot mogelijk trachten te kiezen. Zelfs dan komt men echter in slechts enkele gevallen op de gewenste $m = 2$ uit. Met een kleine modificatie van HURWITZ' stelling is veel meer te bereiken. Beschouwen we in plaats van de verzamelingen $\xi + U$, $2\xi + U$, ..., $m\xi + U$ namelijk de verzamelingen $\omega_1\xi + U$, $\omega_2\xi + U$, ..., $\omega_m\xi + U$, waar $\omega_1, \omega_2, \ldots, \omega_m$ willekeurige elementen van K zijn, dan vinden we op geheel analoge wijze:

(11) er is een geheel getal $m > 1$, zodanig dat voor alle $\omega_1, \omega_2, \ldots, \omega_m$ en ξ uit K er een κ uit R is zodat

(12) $$N((\omega_i - \omega_j)\xi - \kappa) < 1$$

voor zekere i, j, $1 \leq i < j \leq m$.

Stel nu dat $\omega_1, \omega_2, \ldots, \omega_m$ zó gekozen kunnen worden dat alle verschillen $\omega_i - \omega_j$ $(i \neq j)$ *eenheden* zijn, d.w.z. een inverse hebben die tot R behoort. Dan geldt $N(\omega_i - \omega_j) = 1$, en uit (12) vindt men

$$N(\xi - \kappa\cdot(\omega_i - \omega_j)^{-1}) < 1.$$

Aangezien $\kappa\cdot(\omega_i - \omega_j)^{-1}$ een element van R is concluderen we dat R norm-euclidisch is. Met andere woorden:

(13) als R een *voldoende* aantal elementen bezit waarvan alle verschillen eenheden zijn is R euclidisch ten opzichte van de norm.

Als voorbeeld beschouwen we het lichaam K voortgebracht door een nulpunt γ van $g = X^5 - X^3 + X^2 - X - 1$, met $r = 3$, $s = 1$, en voor R nemen we de verzameling getallen (3). Het blijkt dat men, met U in het bovenstaande bewijs goed gekozen, op $m = 5$ uitkomt. Dus R is norm-euclidisch als er vijf elementen te vinden zijn waarvan alle verschillen eenheden zijn. We beweren dat we hiervoor kunnen nemen

$$0, \quad 1, \quad \gamma, \quad \frac{1}{1 - \gamma}, \quad \frac{\gamma - 1}{\gamma}.$$

Men controleert gemakkelijk dat deze bewering erop neerkomt dat γ, $\gamma - 1$

en $\gamma^2 - \gamma + 1$ alle drie eenheden zijn. En inderdaad, uit

$$\gamma^5 - \gamma^3 + \gamma^2 - \gamma - 1 = g(\gamma) = 0$$

volgt

$$\gamma\cdot(\gamma^4 - \gamma^2 + \gamma - 1) = 1$$
$$(\gamma - 1)\cdot(\gamma^4 + \gamma^3 + \gamma) = 1$$
$$(\gamma^2 - \gamma + 1)\cdot(\gamma^3 + \gamma^2 - \gamma - 1) = \gamma.$$

We concluderen dat K euclidisch is.

Voor meer voorbeelden verwijzen we naar [7]. Met deze methode laat zich ook een aantal van de in de vorige paragraaf genoemde ringen behandelen.

HURWITZ' stelling is tevens te gebruiken om een charmant resultaat van O'MEARA, zie [8], af te leiden, dat als volgt luidt:

(14) er is een element δ van R, ongelijk aan nul, zodanig dat de ring $T = R[\delta^{-1}]$ voortgebracht door R en de inverse van δ euclidisch is ten opzichte van de functie N_T gedefinieerd door

$$N_T(0) = 0$$
$$N_T(\beta) = \text{aantal restklassen van } T \text{ modulo } \beta$$

voor β uit T, $\beta \neq 0$.

Hier heet T euclidisch ten opzichte van N_T als voor alle α en β uit T, $\beta \neq 0$, er κ en ρ in T te vinden zijn met $\alpha = \kappa\beta + \rho$ en $N_T(\rho) < N_T(\beta)$. Voor het bewijs van O'MEARA's stelling blijkt het voldoende te zijn voor δ het product van alle getallen $\omega_i - \omega_j$, $1 \leq i < j \leq m$, te nemen, met m als boven en $\omega_1, \omega_2, \ldots, \omega_m$ willekeurige verschillende elementen van R.

We merken hierbij op dat het veel eenvoudiger is een δ te vinden zodat in $R[\delta^{-1}]$ de stelling van de eenduidige priemfactorontbinding geldt. In het geval $R = R_0$ kan men δ dan zelfs onderling ondeelbaar met een willekeurige ε uit R kiezen, $\varepsilon \neq 0$; d.w.z., zó dat $\lambda\delta + \mu\varepsilon = 1$ voor zekere λ, μ uit R. Of een dergelijke vrijheid van keuze ook in (14) bestaat is een onopgelost probleem.

De ringen $T = R[\delta^{-1}]$, met δ uit R, ongelijk aan nul, vertonen eigenschappen die in vele opzichten analoog zijn aan die van de ringen R zelf, en veel van wat we in deze paragraaf gezegd hebben laat zich met enige

aanpassingen ook voor ringen van het type T uitspreken. Naast $\mathbb{R}$ en $\mathbb{C}$ ziet men dan p-adische lichamen verschijnen. Zoals O'MEARA's stelling aantoont is er in deze uitgebreidere klasse ringen in elk geval geen gebrek aan voorbeelden van euclidische ringen. Het is wellicht een aantrekkelijk probleem de juiste generalisatie van de boven geciteerde stelling van DAVENPORT te vinden.

Literatuur bij §2.

1. E.S. BARNES, H.P.F. SWINNERTON-DYER, The inhomogeneous minima of binary quadratic forms (II), *Acta Math.* 88 (1952), 279-316
2. J.W.S. CASSELS, The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic forms, *Proc. Cambridge Philos. Soc.* 48 (1952), 72-86, 519-520.
3. H.J. GODWIN, Computations relating to cubic fields, pp. 225-229 in: A.O.L. ATKIN, B.J. BIRCH (eds), *Computers in number theory*, Academic Press, Londen 1971.
4. G.H. HARDY, E.M. WRIGHT, *An introduction to the theory of numbers*, vierde druk, Oxford University Press, Oxford 1960.
5. H. HEILBRONN, On Euclid's algorithm in cyclic fields, *Canad. J. Math.* 3 (1951), 257-268.
6. A. HURWITZ, *Mathematische Werke*, Zweiter Band, Birkhäuser, Bazel 1933.
7. H.W. LENSTRA, JR., Euclidean number fields of large degree, *Invent. Math.* (1977), te verschijnen.
8. O.T. O'MEARA, On the finite generation of linear groups over Hasse domains, *J. Reine Angew. Math.* 217 (1965), 79-108.

Euclidische getallenlichamen

3. Het vermoeden van Artin

In de voorgaande paragrafen hebben we, bij de deling met rest $\alpha = \kappa\beta + \rho$, steeds geëist dat ρ kleiner is dan β, gemeten met de norm:

$$N(\rho) < N(\beta).$$

In deze paragraaf gaan we na welke vrijheid we krijgen als we andere functies dan de norm toelaten.

Laat T een commutatieve ring met 1, $1 \neq 0$, zonder nuldelers zijn. We zijn voornamelijk geïnteresseerd in ringen T van het type $R[\delta^{-1}]$, zie §2, (14). Deze ringen noemen we *getallenringen*. Zij ψ een afbeelding die aan elk element β van T ongelijk aan nul een niet-negatief geheel getal $\psi(\beta)$ toevoegt. We zeggen dat T *euclidisch ten opzichte van* ψ is, of dat ψ een *delingsalgorithme* op T is, als voor alle α en β uit T, $\beta \neq 0$, er κ en ρ in T bestaan met

$$(1) \qquad \begin{cases} \alpha = \kappa\beta + \rho \\ \rho = 0 \quad \text{of} \quad \psi(\rho) < \psi(\beta). \end{cases}$$

Indien een dergelijke ψ bestaat noemen we T *euclidisch*. Is T euclidisch, dan geldt in T de stelling van de eenduidige ontbinding in priemfactoren.

De tegenwoordige stand van zaken suggereert dat we hier voor getallenringen niet met een algemener begrip dan te voren te maken hebben:

(2) elke bekende euclidische getallenring T is euclidisch ten opzichte van de norm N_T gedefinieerd in §2, (14).

Maar (2) is waarschijnlijk eerder een blijk van onmacht dan een afspiegeling van de werkelijke situatie: er zijn oneindig veel getallenringen T waarin de stelling van de eenduidige priemfactorontbinding geldt die *niet* euclidisch ten opzichte van N_T zijn, maar zoals we zullen zien is er reden te veronderstellen dat deze T, op vier uitzonderingen na, *wel* euclidisch ten opzichte van een andere functie zijn.

De analyse waarop deze veronderstelling berust gaat uit van een gedachte van MOTZKIN, zie [6, 7]. Laat T, als boven, een commutatieve ring met 1, $1 \neq 0$, zonder nuldelers zijn. We trachten een functie ψ te definiëren die een delingsalgorithme op T is. Voor welke β uit T, $\beta \neq 0$, kunnen we

$\psi(\beta) = 0$ zetten? Voor zulke β is, in (1), het alternatief $\psi(\rho) < \psi(\beta)$ uitgesloten, dus we moeten hebben $\rho = 0$, en $\alpha = \kappa\beta$: elke α moet door β deelbaar zijn, d.w.z.: β is een eenheid. Definiëren we nu

$\psi(\beta) = 0$ als β een eenheid is

dan kunnen we, voor deze β en voor elke α uit T, inderdaad κ en ρ in T vinden waarvoor (1) geldt, nl. $\rho = 0$, $\kappa = \alpha\beta^{-1}$. Vervolgens vragen we ons af voor welke β we $\psi(\beta) = 1$ kunnen nemen. Voor dergelijke β is in (1), behalve $\rho = 0$, nu ook toegelaten $\psi(\rho) = 0$, d.w.z. ρ is een eenheid. Met andere woorden: elke α uit T die niet deelbaar door β is moet modulo β congruent zijn met een eenheid. Zetten we

$\psi(\beta) = 1$ als elke restklasse modulo β óf 0 óf een eenheid bevat

dan is weer aan (1) te voldoen voor alle α, β uit T met $\psi(\beta) \leq 1$. Algemeen kunnen we met inductie naar n definiëren

$$T_{-1} = \{0\}$$

$$T_n = \{\beta \mid \text{elke restklasse modulo } \beta \text{ bevat een element van } T_{n-1}\}$$

voor $n \geq 0$, en we kunnen nemen

(3) $\psi(\beta) = n$ als β tot T_n maar niet tot T_{n-1} behoort, $n \geq 0$.

De volgende stelling is nu eenvoudig te bewijzen.

(4) Als er een element van T is dat tot geen enkele T_n behoort is T niet euclidisch. Als daarentegen elk element van T tot een T_n behoort is T euclidisch ten opzichte van de door (3) gedefinieerde functie ψ. Bovendien is ψ dan de *kleinste* delingsalgorithme op T, d.w.z.

$$\psi(\beta) \leq \chi(\beta)$$

voor alle β uit T ongelijk aan nul en alle delingsalgorithmen χ op T.

Nemen we voor T de ring der gehele getallen dan vinden we uit bovenstaande constructie

$\psi(\beta) = 0$ voor $\beta = \pm 1$

$$\psi(\beta) = 1 \qquad \text{voor} \quad \beta = \pm 2, \pm 3,$$

en algemeen

$$\psi(\beta) = [\log |\beta| / \log 2], \qquad \beta \neq 0, \tag{5}$$

waarbij $[x]$ het grootste gehele getal $\leq x$ aangeeft.

Is T de polynoomring in één veranderlijke over een lichaam dan ziet men gemakkelijk in dat

$$\psi(\beta) = \text{graad}(\beta)$$

voor alle β uit T ongelijk aan nul.

Om te begrijpen hoe MOTZKINs algemene procedure werkt in het geval van de getallenringen waarin wij geïnteresseerd zijn moeten we allereerst informatie over de eenheden van zulke ringen hebben. Met behulp van de *eenhedenstelling van DIRICHLET* blijkt dan dat het boven gegeven voorbeeld van de gehele getallen niet typisch is: in de meeste gevallen heeft een getallenring oneindig veel eenheden. Beperken we ons tot getallenringen waarin de stelling van de eenduidige priemfactorontbinding geldt - want alleen deze kunnen euclidisch zijn - dan zijn er in feite slechts tien gevallen waarin het aantal eenheden eindig is: is γ een van de negen getallen

$$\frac{1}{2}(1 + \sqrt{-3}), \quad \sqrt{-1}, \quad \frac{1}{2}(1 + \sqrt{-7}), \quad \sqrt{-2}, \quad \frac{1}{2}(1 + \sqrt{-11}), \tag{6}$$

$$\frac{1}{2}(1 + \sqrt{-19}), \quad \frac{1}{2}(1 + \sqrt{-43}), \quad \frac{1}{2}(1 + \sqrt{-67}), \quad \frac{1}{2}(1 + \sqrt{-163}), \tag{7}$$

dan is de verzameling getallen $a + b\gamma$, met a en b geheel, zo'n ring, en het tiende voorbeeld is de ring der gehele getallen zelf. Vier van deze tien ringen, corresponderend met de waarden (7), zijn niet euclidisch. De overige zes zijn norm-euclidisch, en in de gevallen (6) laat ψ zich als volgt benaderen. Zet

$$c = 3, \ 2, \ \frac{7}{4}, \ \frac{4}{3}, \ \frac{11}{9}$$

voor de vijf waarden (6) van γ, respectievelijk, en definieer

$$\chi(a + b\gamma) = [\log N(a + b\gamma) / \log c],$$

voor a en b geheel, niet beide 0; vgl. (5). Dan is χ een delingsalgorithme, en χ heeft slechts een begrensd verschil met de kleinste delingsalgorithme ψ. Deze resultaten zijn te vinden in [8, 7, 4]. Voor een

precieze beschrijving van ψ in de gevallen $\gamma = \frac{1}{2}\cdot(1 + \sqrt{-3})$ en $\gamma = \sqrt{-1}$ zie men [4]. Een aantal open problemen betreffende de overige gevallen is te vinden in [3].

In de rest van deze paragraaf nemen we voor T een getallenring met oneindig veel eenheden, en we nemen aan dat in T de stelling van de eenduidige priemfactorontbinding geldt. Ons doel is de functie ψ te bepalen. We weten al, dat $\psi(\beta) = 1$ geldt dan en slechts dan als β de volgende eigenschap heeft:

(8) elke α uit T is òf deelbaar door β, òf modulo β congruent met een eenheid.

In het bijzonder heeft elke α uit T die niet door β deelbaar is geen factoren met β gemeen, als $\psi(\beta) = 1$, dus β moet een priemelement zijn; dit volgt ook uit (9). Geven we met P de verzameling priemelementen met eigenschap (8) aan dan hebben we kennelijk

$$\psi(\eta) \geq 2 \quad \text{voor elk priemelement } \eta \text{ van T dat niet tot P behoort.}$$

Hierbij zetten we gemakshalve $\psi(\eta) = \infty$ als η tot geen enkele T_n behoort. Passen we nu de algemene ongelijkheid

$$(9) \qquad \psi(\alpha_1\alpha_2) \geq \psi(\alpha_1) + \psi(\alpha_2) \qquad (\alpha_1\cdot\alpha_2 \neq 0)$$

(vgl. [7, prop. 12]) toe, dan vinden we het volgende resultaat. Is α een willekeurig element $\neq 0$ van T, met priemfactorontbinding

$$\alpha = \varepsilon\beta_1\beta_2\cdots\beta_v\eta_1\eta_2\cdots\eta_w$$

waar ε een eenheid is, $\beta_1, \ldots, \beta_v$ priemelementen uit P zijn, en $\eta_1, \ldots, \eta_w$ priemelementen die niet tot P behoren, dan

$$(10) \qquad \psi(\alpha) \geq v + 2w.$$

Er geldt nu:

(11) *Laat* T *een getallenring met oneindig veel eenheden zijn waarin de stelling van de eenduidige priemfactorontbinding geldt, en neem een aantal gegeneraliseerde RIEMANN-hypothesen aan. Dan is* T *euclidisch en geldt in (10) het gelijkheidsteken voor alle* α *uit* T *ongelijk aan nul.*

Dit is bewezen in [5]; vergelijk [9, 10].

Het bewijs van (11) berust op het feit dat, onder aanname van de RIEMANN-hypothesen, die we met *GRH* zullen aanduiden, de verzameling P *voldoende groot* is. Nemen we bijvoorbeeld de volgende uitspraak als waar aan:

(12) voor elk tweetal onderling ondeelbare elementen α en β uit T, met $\beta \neq 0$, is er een element van P dat modulo β congruent is met α.

Dan is (11) als volgt te bewijzen. Zij χ de functie gedefinieerd door het rechterlid van (10):

$$\chi(\alpha) = v + 2w, \qquad \text{voor } \alpha, v, w \text{ als boven.}$$

Het is kennelijk voldoende te bewijzen dat χ een delingsalgorithme op T is. Dus, gegeven α en β uit T, met $\beta \neq 0$, moeten we een ρ vinden met $\rho = 0$ of $\chi(\rho) < \chi(\beta)$, die modulo β congruent met α is.

Zonder verlies van algemeenheid mogen we α en β onderling ondeelbaar veronderstellen: we kunnen α en β anders beide door hun grootste gemene deler delen zonder het probleem te veranderen.

Als nu geldt $\chi(\beta) = 0$ dan is β een eenheid, en we kunnen $\rho = 0$ nemen. Indien we hebben $\chi(\beta) = 1$, dan behoort β tot P, dus volgens de definitie van P kunnen we een eenheid ρ kiezen die congruent met α modulo β is. Dan geldt inderdaad

$$\chi(\rho) = 0 < 1 = \chi(\beta).$$

Tenslotte, als $\chi(\beta) \geq 2$, dan kiezen we, gebruik makend van (12), een element ρ uit P dat modulo β congruent is met α, en voor deze ρ hebben we

$$\chi(\rho) = 1 < 2 \leq \chi(\beta),$$

zoals verlangd. Het rest ons slechts (12) te onderzoeken.

We beschouwen een voorbeeld. Laat T de verzameling rationale getallen zijn waarvan de noemer een macht van 2 is. Dit is inderdaad een getallenring waarin de stelling van de eenduidige priemfactorontbinding geldt. De eenheden van T zijn precies de getallen $\pm 2^j$, met j geheel, en dit zijn er oneindig veel. Het is niet lastig in te zien dat de verzameling P in dit geval, op vermenigvuldiging met eenheden na, samenvalt met de verzameling oneven priemgetallen p met de volgende eigenschap:

(13) elk geheel getal a, $1 \leq a \leq p-1$, is modulo p congruent met een getal van de vorm $\pm 2^j$, met j geheel, $j \geq 0$.

Van de veertien oneven priemgetallen < 50 missen alleen 17, 31, 41 en 43 deze eigenschap. Maar hoewel men mag vermoeden dat (13) waar is voor meer dan de helft van alle priemgetallen - preciezer, 56,0933720... % -, is nog niet eens bewezen dat er *oneindig veel* zulke priemgetallen zijn, laat staan dat een eigenschap als (12) aangetoond is.

Laat men in (13) het ±-teken weg dan drukt men (13) wel uit door te zeggen dat 2 een *primitieve wortel* modulo p is. Dit roept een vermoeden van ARTIN uit 1927 in herinnering, dat uitspreekt dat voor elk geheel getal t, $|t| > 1$, de limiet

$$(14) \qquad \lim_{x \to \infty} \frac{\text{aantal priemgetallen } < x \text{ dat } t \text{ als primitieve wortel heeft}}{\text{aantal priemgetallen } < x}$$

bestaat. Tevens geeft het vermoeden een formule voor de waarde van deze limiet. Men kan zich de limiet voorstellen als het *percentage* priemgetallen met t als primitieve wortel. Het is duidelijk dat het aantal van zulke priemgetallen oneindig is als dit percentage positief is.

ARTINs vermoeden werd in 1967 door HOOLEY bewezen onder aanname van een reeks gegeneraliseerde RIEMANN-hypothesen, zie [2]. Indien wij ook bereid zijn onder een dergelijke aanname te werken blijven er, om (12) te bewijzen, drie vragen over. Ten eerste: laten ARTINs vermoeden en HOOLEY's bewijs zich generaliseren voor de verzameling P? Ten tweede: is het bij deze benadering mogelijk rekening te houden met de conditie dat de priemelementen tevens congruent met α modulo β moeten zijn? Ten derde: doet het geval zich niet voor dat de formule voor het percentage de waarde *nul* levert? In dat geval zou de betreffende verzameling namelijk leeg kunnen zijn.

Bij de eerste vraag staan we niet lang stil. ARTINs vermoeden laat inderdaad een voor de hand liggende generalisatie toe die een voorspelling doet omtrent het percentage priemelementen dat tot P behoort, en met HOOLEY's techniek laat deze generalisatie zich inderdaad bewijzen modulo GRH. Zie hiervoor [1]. We gaan hier niet in op de precieze betekenis van *percentage* in het geval van een algemene getallenring T.

Wat de tweede vraag betreft: zijn α en β onderling ondeelbare elementen van T, met $\beta \neq 0$, dan is de conditie

$$(15) \qquad \rho \equiv \alpha \bmod \beta$$

inderdaad vervuld voor een positief percentage van alle priemelementen ρ. Dit is een stelling die op DIRICHLET teruggaat. Maar (15) is, voor priemelementen ρ, niet onafhankelijk van de conditie

(16) ρ behoort tot P,

zoals we beneden aan een voorbeeld zullen zien. Wel blijkt het mogelijk met (15) rekening te houden in een nieuwe generalisatie van ARTINs vermoeden, waarvan het bewijs kan worden teruggevoerd op de vorige versie.

We blijven zitten met de derde vraag: is het mogelijk dat we, onder aanname van GRH, tot de ontdekking komen dat asymptotisch 0% van alle priemelementen aan beide condities (15) en (16) voldoet? In het geval van het originele vermoeden blijkt de voorspelde waarde voor de limiet (14) alleen 0 te zijn als t een kwadraat is. Voor P doet dit verschijnsel zich niet voor: het percentage priemelementen dat tot P behoort is positief, als de RIEMANN-hypothesen waar zijn. Onaangenaam is echter de ontdekking dat de conditie (15) in tegenspraak met (16) kan zijn. Voor ARTINs oorspronkelijke vermoeden is een dergelijk voorbeeld gemakkelijk te geven: de beide eisen

$p \equiv 1 \bmod 8$

2 is een primitieve wortel modulo p

zijn, voor priemgetallen p, onverenigbaar. Uit $p \equiv 1 \bmod 8$ is namelijk af te leiden dat 2 een kwadraat modulo p is, en dan kan het geen primitieve wortel zijn. Met wat meer moeite construeert men ook in het ons interesserende geval een voorbeeld:

(17) laat T bestaan uit de getallen

$$a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3, \qquad a_0, a_1, a_2, a_3 \text{ geheel},$$

met $\zeta^5 = 1$, $\zeta \neq 1$; dan bevat P geen element dat 1 modulo 4 is.

Het bewijs verloopt analoog: is ρ een priemelement, $\rho \equiv 1 \bmod 4$, dan volgt dat alle eenheden van T kwadraten modulo ρ zijn, waaruit men afleidt dat ρ niet tot P kan behoren.

We zien uit (17) dat (12) niet algemeen geldig is. Gelukkig hadden we, om het op (12) volgende bewijs van (11) te kunnen leveren, ook wel met

minder toegekund: hebben we, in dat bewijs, bijvoorbeeld $\chi(\beta) \geq 3$, dan hadden we volgens de bij (15) genoemde stelling een priemelement ρ kunnen nemen met $\rho \equiv \alpha \bmod \beta$, en dan had inderdaad

$$\chi(\rho) \leq 2 < 3 \leq \chi(\beta)$$

gegolden. Dus voor ons is het voldoende (12) te weten in het geval $\chi(\beta) = 2$. Helaas toont het bovengegeven voorbeeld aan dat zelfs dan (12) niet waar hoeft te zijn. Dit betekent bijna dat ook (11) niet waar is - bijna, want om $\chi(\rho) < \chi(\beta) = 2$ te bereiken mogen we voor ρ ook een eenheid nemen. Dus om (11) aan te tonen is het voldoende om de volgende afzwakking van (12) te bewijzen:

(18) voor elk tweetal onderling ondeelbare elementen α, β van T, met $\chi(\beta) = 2$, is er een ρ uit T met

$$\rho \equiv \alpha \bmod \beta$$

zodanig dat ρ een element van P of een eenheid van T is.

Bovendien is dit het uiterste waartoe we kunnen gaan: de geldigheid van (18), modulo GRH, is niet alleen voldoende, maar ook nodig voor (11). Het is dan ook een gelukkige omstandigheid dat de bezwaren die tegen (12) ingebracht konden worden in het geval van (18) niet meer geldig blijken te zijn, en dat (18) in feite een gevolg is van de genoemde generalisatie van ARTINs vermoeden.

We besluiten deze paragraaf met een korte bespreking van de plaats die de RIEMANN-hypothesen in het bewijs van (18) innemen.

Is ρ een priemelement van T, dan vormen de restklassen modulo ρ die 0 niet bevatten een eindige multiplicatieve groep, zeg G_ρ. De restklassen die eenheden van T bevatten vormen een ondergroep van G_ρ, die we H_ρ noemen. Kennelijk behoort ρ tot P dan en slechts dan als $G_\rho = H_\rho$, dus als we zetten

$$k_\rho = \text{index}(G_\rho : H_\rho)$$

dan geldt $P = \{\rho \mid k_\rho = 1\}$. Schrijven we

$$P_m = \{\rho \mid k_\rho \text{ heeft geen priemfactoren } \leq m\}$$

voor m positief geheel, dan hebben we

$$P = \bigcap_{m=1}^{\infty} P_m, \qquad P_1 \supset P_2 \supset P_3 \ldots .$$

Laten nu α, β zijn als in (18), en neem aan dat α modulo β niet congruent met een eenheid is. We zijn geïnteresseerd in de verzameling

$$V = \{\rho \mid \rho \equiv \alpha \bmod \beta, \text{ en } \rho \text{ behoort tot } P\}$$

die we natuurlijk kunnen schrijven als

$$(19) \qquad V = \bigcap_{m=1}^{\infty} V_m, \qquad V_1 \supset V_2 \supset V_3 \ldots$$

waar V_m bestaat uit de priemelementen $\rho \equiv \alpha \bmod \beta$ die tot P_m behoren. Zonder enige onbewezen aanname kan nu worden aangetoond dat voor elke m een positieve fractie, zeg δ_m, van alle priemelementen tot V_m behoort, met

$$\delta_1 \geq \delta_2 \geq \delta_3 \geq \ldots ,$$

en dat geldt

$$(20) \qquad \delta = \lim_{m\to\infty} \delta_m > 0.$$

De uit (19) en (20) plausibel lijkende veronderstelling, dat van alle priemelementen een positieve fractie, nl. δ, tot V behoort, zou (18) nu impliceren. Het is precies bij het bewijs van deze onderstelling dat de RIEMANN-hypothesen gebruikt worden. Dat juist deze hun intrede doen is wel te begrijpen: gegeneraliseerde RIEMANN-hypothesen doen een uitspraak over de restterm van de voor algebraïsche getallenlichamen gegeneraliseerde priemgetalstelling en, via het mechanisme waarmee de V_m geanalyseerd worden, ook over de restterm in de boven gedane asymptotische bewering dat van alle priemelementen een positieve fractie δ_m tot V_m behoort.

Literatuur bij §3.

1. G. COOKE, P.J. WEINBERGER, On the construction of division chains in algebraic number fields, with applications to SL_2, *Comm. Alg.* 3 (1975), 481-524.
2. C. HOOLEY, On Artin's conjecture, *J. Reine Angew. Math.* 225 (1967), 209-220.
3. D. LAZARD, On the minimal algorithm in rings of imaginary quadratic integers, te verschijnen.
4. H.W. LENSTRA, JR., *Lectures on euclidean rings*, Bielefeld 1974.
5. H.W. LENSTRA, JR., On Artin's conjecture and Euclid's algorithm in global fields, Rapport 77-03, Math. Inst., Univ. van Amsterdam 1977.
6. T. MOTZKIN, The euclidean algorithm, *Bull. Amer. Math. Soc.* 55 (1949), 1142-1146.
7. P. SAMUEL, About euclidean rings, *J. Algebra* 19 (1971), 282-301.
8. H.M. STARK, A complete determination of the complex quadratic fields of class-number one, *Mich. Math. J.* 14 (1967), 1-27.
9. C. QUEEN, Arithmetic euclidean rings, *Acta Arith.* 26 (1974), 105-113.
10. P.J. WEINBERGER, On euclidean rings of algebraic integers, *Proc. Symp. Pure Math.* 24 (*Analytic Number Theory*), 321-332, Amer. Math. Soc., 1973.