STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1960 - 004

Voordracht in de serie
"Elementaire onderwerpen vanuit hoger standpunt belicht"

Dr. W. Verdenius

27 april 1960

Splitsing in kwadraten en de meetkunde der getallen

1960

The Mathematical Centre at Amsterdam, founded the 11th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government trough the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1960-004

Voordracht in de serie
"Elementaire onderwerpen vanuit hoger standpunt belicht"

door

Dr W. Verdenius

27 april 1960

Splitsing in kwadraten en de meetkunde der getallen

1. De vraag welke getallen te schrijven zijn als de som van twee of vier kwadraten van gehele getallen is reeds oud. (Zie Dickson [2].) Volgens sommige historici gaat de geschiedenis terug tot Diophantus van Alexandrië ($\pm$ 250). Wel is het zeker dat in het begin van de 17^{e} eeuw deze problemen de aandacht hebben van de mathematici. Uit die tijd stammen de volgende stellingen, toen nog als vermoedens geopperd:
Stelling 1. Een natuurlijk getal $n = \prod p_i^{\alpha_i}$ is dan en slechts dan te schrijven als de som van twee kwadraten van gehele getallen, als α_i even is voor elke i, waarvoor $p_i \equiv 3 \pmod 4$.
Stelling 2. Elk natuurlijk getal is te schrijven als de som van vier kwadraten van gehele getallen.

Tot degenen die deze stellingen formuleerden behoort Albert Girard (1635), een leerling van Simon Stevin.

Pas in de 18^{e} eeuw gelukte het deze stellingen te bewijzen. Na vele vergeefse pogingen gelukte het aan Euler (1749) stelling I te bewijzen. Naderhand volgde Lagrange (1770) met het bewijs van stelling II. Van de vele bewijzen die in latere tijd gegeven zijn willen we er een in deze voordracht bespreken.

2. Het is niet moeilijk om in te zien, dat niet ieder getal te schrijven is als de som van twee kwadraten. Het kwadraat van een even getal is een viervoud en het kwadraat van een oneven getal is een viervoud +1, zodat de som van twee kwadraten geen viervoud +3 kan zijn.

Om verder te komen leiden we eerst een hulpstelling af uit de theorie van de kwadraatresten, waarvan vooreerst slechts een helft

benut wordt.

Hulpstelling 1. De congruentie $x^2+1 \equiv 0 \pmod p$ is voor oneven p dan en slechts dan oplosbaar, als $p \equiv 1 \pmod 4$.
Bewijs: Stel $a^2+1 \equiv 0 \pmod p$. Dan is $p \nmid a$ en $a^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod p$. Volgens de stelling van Fermat is ook $a^{p-1} \equiv 1 \pmod p$. Dus is $\frac{p-1}{2}$ even, of $p \equiv 1 \pmod 4$. Dat omgekeerd $x^2+1 \equiv 0 \pmod p$ voor $p \equiv 1 \pmod 4$ een oplossing bezit, leiden we af uit de stelling van Wilson, die leert dat voor elk priemgetal geldt

$$(p-1)! \equiv -1 \pmod p.$$

Verminderen we in het linker lid de factoren $\frac{1}{2}(p+1),\ldots,p-1$ met p, dan vinden we

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

waaruit volgt dat $\left(\frac{p-1}{2}\right)!$ een oplossing is.

We tonen nu aan dat de in stelling 1 genoemde voorwaarden nodig is. Stel dat geldt

$$n = a^2+b^2,$$

met gehele a en b. Stel verder p/n en $p \equiv 3 \pmod 4$. Dan is

$$a^2+b^2 \equiv 0 \pmod p.$$

Is $p \nmid a$, dan kunnen we een geheel getal c bepalen, zodat $ac \equiv 1 \pmod p$. Blijkbaar is dan dus ook

$$1 + (bc)^2 \equiv 0 \pmod p,$$

hetgeen volgens hulpstelling 1 onmogelijk is. Dus p/a. Evenzo p/b. Dus p^2/n. Op

$$np^{-2} = (ap^{-1})^2 + bp^{-1})^2$$

kan nu dezelfde redenering worden toegepast. Zo doorgaande blijkt, dat de exacte macht van p, die op n deelbaar is, even is.

3. Bij de bewijzen van de stelling 1 en 2 kan men in de leerboeken der elementaire getallentheorie in de regel drie stappen onderscheiden.

Eerst worden de volgende identiteiten genoemd:

$$(a_1^2+a_2^2)(b_1^2+b_2^2) = (a_1b_1+a_2b_2)^2 + (a_1b_2-a_2b_1)^2,$$
$$(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2) =$$
$$(a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2 + (a_1b_2-a_2b_1+a_3b_4-a_4b_3)^2 +$$
$$(a_1b_3-a_3b_1+a_2b_4-a_4b_2)^2 + (a_1b_4-a_4b_1+a_2b_3-a_3b_2)^2 .$$

Omdat

$$p^2 = p^2+0^2 = p^2+0^2+0^2+0^2$$

en

$$2 = 1^2+1^2 = 1^2+1^2+0^2+0^2,$$

blijkt dat het voldoende is stelling 1 te bewijzen voor de priemgetallen $\equiv 1 \pmod 4$ en stelling 2 voor de oneven priemgetallen.

In de tweede stap worden dan respectievelijk de volgende lemma's bewezen:

1. Als $p \equiv 1 \pmod 4$ bestaat er een positief veelvoud van p, dat gelijk is aan de som van twee kwadraten.
2. Als p oneven is bestaat er een positief veelvoud van p, dat gelijk is aan de som van vier kwadraten.

In de derde stap wordt tenslotte aangetoond, dat het mogelijk is het genoemde veelvoud van p gelijk aan p te nemen.

Uiteraard komen varianten op deze grondgedachte voor. Zo kan reeds in de tweede stap getracht worden het betrokken veelvoud klein te houden, zodat de derde stap minder moeite kost, soms zelfs geheel overbodig wordt. Zo gebruikt T. Nagell [4] een hulpstelling van Axel Thue (1917)-Arnold Scholz (1920), die we de volgende vorm geven:

Hulpstelling 2. Stel s en t zijn positieve getallen, a is een geheel en m een natuurlijk getal, terwijl $st > m$. Er bestaan dan twee gehele getallen x en y, niet beide 0, zodat

$$x \equiv ay \pmod m,$$
$$|x| < s \text{ en } |y| < t.$$

Het verband van deze hulpstelling en stelling 1 blijkt als volgt: Voor m nemen we het priemgetal waarvoor de stelling bewezen zal worden. Voor a een der oplossingen van $x^2+1 \equiv 0 \pmod p$. Verder $s = t = [\sqrt{p}]+ 1$. We vinden dus gehele x en y, niet beide 0, met

$$x \equiv ay \pmod p,$$
$$|x| < \sqrt{p} \text{ en } |y| < \sqrt{p}.$$

Deze voldoen dus ook aan

$$x^2+y^2 \equiv 0 \pmod{p}$$

en

$$0 < x^2+y^2 < 2p.$$

Dit houdt echter in

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

In dit bewijs lukt het dus zelfs de derde stap geheel te ontgaan.

Van de hulpstelling van Thue bestaat een generalisatie, afkomstig van Brauer-Reynolds, die het mogelijk maakt ook in het geval van stelling 2 het bewijs te bekorten. Zie LeVeque [3].

In onze toepassing van hulpstelling 2 treedt de puntverzameling

$$|x| < \sqrt{p},\ |y| < \sqrt{p}$$

op. De speciale vorm, een vierkant met (0,0) tot middelpunt en zijden evenwijdig aan de coördinaatassen is voor ons niet essentieel. Van belang is slechts, dat eruit volgt

$$x^2+y^2 < 2p.$$

Het is evenwel mogelijk zich meteen te baseren op deze laatste verzameling en daar het bewijs te brengen. Daartoe gaan we eerst enkele stellingen uit de meetkunde der getallen afleiden.

4. Als uitgangspunt nemen we de volgende stelling van Minkowski (1896):

Stelling 3. Elke begrensde convexe verzameling S van de n-dimensionale euclidische ruimte R_n, met middelpunt in de oorsprong en inhoud $> 2^n$, bevat behalve de oorsprong nog minstens één ander punt met gehele coördinaten.

Bewijs: Stel S bevat geen ander punt met gehele coördinaten. Laat S_Q de verzameling zijn die uit S ontstaat door vermenigvuldiging met $\frac{1}{2}$ vanuit O. Laat S_P de verzameling zijn die uit S_Q ontstaat door de verschuiving, die O in P doet overgaan. Hierbij is P een punt met gehele coördinaten.

We tonen nu eerst aan, dat de verzamelingen S_P disjunct zijn. Hadden twee van deze verzamelingen een punt gemeen, dan zou wegens de regelmaat van de verdeling, S_Q een punt gemeen hebben met bijv. S_R. Laat dit gemeenschappelijke punt X zijn. Voltooi nu het parallelogram OXQY en laat X' het spiegelpunt zijn van Y t.o.v. O.

Zij tenslotte M het snijpunt der diagonalen van OXQY. Wegens de symmetrie en de convexiteit van S is nu

$$X \in S_Q \Rightarrow X' \in S_O \Rightarrow \left.\begin{matrix} Y \in S_O \\ X \in S_O \end{matrix}\right\} \Rightarrow M \in S_O \Rightarrow Q \in S,$$

hetgeen strijdt met ons uitgangspunt.

We hebben nu rond ieder punt met gehele coördinaten een verzameling S_P, met volume $V > 1$, terwijl geen twee van die verzamelingen een punt gemeen hebben. Beschouw nu alle S_P, waarbij de coördinaten $x_1,\ldots,x_n$ van P voldoen aan

$$0 \leqslant x_i < N \quad (i = 1,\ldots,n),$$

waarbij N een natuurlijk getal is. Hun aantal is N^n en hun totale inhoud is N^nV. De gehele figuur ligt binnen een kubus

$$-k \leqslant x_i < N+k \quad (i = 1,\ldots,n),$$

waarin k een constante voorstelt bepaald door de begrensde afmetingen van S. Vergelijken we de inhouden, dan vinden we

$$N^nV \leqslant (N+2k)^n.$$

Delen we hierin beide leden door N^n en laten dan N naderen tot ∞, dan volgt $V \leqslant 1$, terwijl uit het gegeven volgt $V > 1$. Hiermede is het bewijs voltooid.

We onderwerpen nu de figuur van stelling 3 aan een niet-singuliere lineaire transformatie

$$y_i = \sum_{k=1}^{n} \alpha_{ik} x_k \quad (i = 1,\ldots,n).$$

De beeldpunten $(y_1,\ldots,y_n)$ van de punten $(x_1,\ldots,x_n)$ met gehele coördinaten noemen we roosterpunten. We stellen $|\det \alpha_{ik}| = \Delta$, de determinant van het rooster. Als de verzameling S overgaat in T, is T opnieuw convex en symmetrisch en omgekeerd. Verder is

$$V(T) = \int_T \cdots \int dy_1 \ldots dy_n = \Delta \int_S \cdots \int dx_1 \ldots dx_n = \Delta V(S).$$

We kunnen dus de volgende stelling uitspreken:

Stelling 4. Is R een rooster gelegen in R_n met determinant Δ en T een convexe verzameling met middelpunt in de oorsprong O en

inhoud $> 2^n\Delta$, dan bevat T behalve 0 nog minstens één roosterpunt.

5. Bij onze toepassingen van stelling 4 maken we gebruik van speciale roosters. Deze leiden we in met de volgende stelling.

Stelling 5. Stel r, n en $m_1,\ldots,m_r$ zijn natuurlijke getallen en a_{ik} is voor $i = 1,\ldots,r$; $k = 1,\ldots,n$ een geheel getal. De oplossingen $(x_1,\ldots,x_n)$ van het stelsel congruenties

$$\sum_{k=1}^{n} a_{ik}x_k \equiv 0 \pmod{m_i} \quad (i = 1,\ldots,r)$$

vormen een rooster met determinant $\leqslant m_1\ldots m_r$.

Bewijs: Zij eerst r = 1. Het gaat nu om de oplossingen van

$$a_1x_1 + \ldots + a_nx_n \equiv 0 \pmod{m}.$$

Stel $a_i = da_i'$ $(i = 1,\ldots,r)$ en $m = dm'$, waarin $d = (a_1,\ldots,a_n,m)$. Voor de congruentie laat zich nu schrijven

$$a_1'x_1 + \ldots + a_n'x_n \equiv 0 \pmod{m'}.$$

Minstens een der coëfficiënten $a_1',\ldots,a_n'$ heeft nu met m' geen factor > 1 gemeen. Laat dit a_1' zijn. Als b zo gekozen wordt, dat $a_1'b \equiv 1 \pmod{m}$, zijn de oplossingen van onze congruentie

$$\begin{cases} x_1 = m'y_1 - a_2'by_2 - \ldots - a_n'by_n \\ x_i = y_i \quad (i = 2,\ldots,n) . \end{cases}$$

Dit is een rooster met determinant $m' \leqslant m$. Met volledige inductie naar r laat zich het bewijs gemakkelijk voltooien als $r > 1$.

De hulpstelling van Thue-Scholz kunnen we nu als volgt bewijzen: De oplossingen van $x \equiv ay \pmod{m}$ vormen een rooster met determinant $\leqslant m$. De verzameling $|x| < s, |y| < t$ is convex, heeft 0 tot middelpunt en zijn inhoud $= 4st > 2^2m$. De bewering volgt nu uit stelling 4.

6. Met de thans ontwikkelde hulpmiddelen geven we nu een bewijs van de stellingen 1 en 2, waarbij de eerste stap een trivialiteit wordt en de derde stap overbodig wordt.

Bewijs van stelling 1. Het is voldoende de stelling te bewijzen voor de natuurlijke getallen, die niet deelbaar zijn door een kwadraat > 1. Uit $n = x^2+y^2$ volgt immers $nn_1^2 = (xn_1)^2 + (yn_1)^2$.

Stel nu $n = p_1 \ldots p_r$, dan weten we $p_i \not\equiv 3 \pmod 4$. Er bestaan dan gehele getallen a_i, zodat

$$a_i^2 + 1 \equiv 0 \pmod{p_i} \quad (i = 1,\ldots,r).$$

Voor $p_i \equiv 1 \pmod 4$ volgt dit uit hulpstelling 1 en voor $p_i = 2$ voldoet $a_i = 1$.

We passen nu stelling 4 toe op het rooster

$$x \equiv a_i y \pmod{p_i} \quad (i = 1,\ldots,r).$$

Hiervan is de determinant $\Delta \leqslant n$. Voor T nemen we de cirkel

$$x^2 + y^2 < 2n.$$

Hiervan is het volume $V = 2\pi n > 2^2\Delta$. Er ligt dus in T een roosterpunt $(x,y) \neq (0,0)$. Hiervoor geldt

$$x^2 + y^2 \equiv (a_i^2+1)y^2 \equiv 0 \pmod{p_i} \quad (i = 1,\ldots,r),$$

dus zelfs $$x^2 + y^2 \equiv 0 \pmod n.$$

Omdat ook $$0 < x^2+y^2 < 2n,$$

is $$x^2 + y^2 = n.$$

Alvorens stelling 2 te bewijzen een hulpstelling.

Hulpstelling 3. Bij elk priemgetal p zijn twee gehele getallen a_p en b_p te vinden, zodat

$$a_p^2 + b_p^2 + 1 \equiv 0 \pmod p.$$

Bewijs: Voor $p = 2$ voldoen $a_p = 1$ en $b_p = 0$. Is p oneven, dan beschouwen we de tweemaal $\frac{1}{2}(p+1)$ getallen

$$\begin{array}{ll} h^2 & (0 \leqslant h \leqslant \frac{1}{2}(p-1)), \\ -k^2-1 & (0 \leqslant k \leqslant \frac{1}{2}(p-1)). \end{array}$$

Van elke rij behoren de getallen tot verschillende restklassen modulo p, want uit $h_1^2 \equiv h_2^2 \pmod p$ volgt hier $h_1 \equiv h_2 \pmod p$. Tezamen staan er p+1 getallen. Minstens een der getallen van de eerste rij is dus congruent met een der getallen van de tweede rij. Hieruit volgt het bestaan van a_p en b_p.

Bewijs van stelling 2. Wederom kunnen we ons beperken tot het geval dat n niet deelbaar is door een kwadraat > 1. Zij $n = p_1 \ldots p_r$.

We passen stelling 4 toe op het rooster:

$$\begin{cases} x_1 \equiv a_{p_i} x_3 + b_{p_i} x_4 \pmod{p_i}, \\ x_2 \equiv b_{p_i} x_3 - a_{p_i} x_4 \pmod{p_i}. \end{cases} \qquad (i = 1,\ldots,r)$$

Hiervan is de determinant $\Delta \leqslant n^2$. Voor T nemen we de vierdimensionale bol

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2n.$$

Hiervan is de inhoud $V = \frac{1}{2}\pi^2(2n)^2 = 2\pi^2 n^2 > 2^4 n^2 \geqslant 2^4\Delta$.

We vinden dus het bestaan van een roosterpunt $(x_1,x_2,x_3,x_4) \neq (0,0,0,0)$ met

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv (a_{p_i}^2 + b_{p_i}^2 + 1)(x_3^2 + x_4^2) \equiv 0 \pmod{p_i} \quad (i = 1,\ldots,r),$$

dus zelfs

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{n}.$$

Omdat ook $$0 < x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2n,$$

is $$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n.$$

Bovenstaand bewijs komt voor bij Cassels [1], die het ontleent aan een voordracht van Davenport (1947). Dezelfde grondgedachte is evenwel reeds aanwezig in een bewijs van Hermite (1853).

7. Het ligt voor de hand na te gaan wat er gebeurt als men zich baseert op een willekeurige positief definiete kwadratische vorm $ax^2 + bxy + cy^2$, in plaats van op $x^2 + y^2$. Men vindt dan de volgende stelling:

Stelling 6. Stel $ax^2 + bxy + cy^2$ is een positief definiete kwadratische vorm met gehele coëfficiënten. Stel verder dat n behoudens een kwadratische factor gelijk is aan het product van de priemgetallen $p_1,\ldots,p_r$ en dat de congruentie

$$x^2 + 4ac - b^2 \equiv 0 \pmod{4p_1\ldots p_r}$$

oplossingen bezit. Dan bestaan er gehele x en y en een natuurlijk getal λ, met

$$ax^2 + bxy + cy^2 = \lambda n$$
$$1 \leqslant \lambda < \frac{2}{\pi}\sqrt{4ac - b^2}\,.$$

Het speciale geval a = b = c = 1 geeft het volgende resultaat.

Stelling 7. Elk natuurlijk getal, dat behoudens een kwadratische factor te schrijven is als het product van 3 en/of priemgetallen $p \equiv 1 \pmod 6$ is te schrijven in de gedaante $x^2 + xy + y^2$.

Op grond van de theorie van de definiete kwadratische vormen is evenwel ook geen algemeen geldig resultaat met $\lambda = 1$ te verwachten. Onze methode geeft wel betere grenzen voor λ dan de hulpstelling van Thue-Scholz, maar anderzijds verdient vermelding dat ook scherpere grenzen bekend zijn.

Tot slot noemen we nog twee stellingen waarbij bovengenoemde methode van dienst kan zijn.

Stelling 8. Als a_1, a_2 en a_3 natuurlijke getallen zijn, die niet deelbaar zijn door een kwadraat >1, paarsgewijs geen factor gemeen hebben en waarvoor elk der congruenties

$$x^2 + a_2a_3 \equiv 0 \pmod{a_1},\ x^2 + a_1a_3 \equiv 0 \pmod{a_2},\ x^2 + a_1a_2 \equiv 0 \pmod{a_3}$$

oplossingen bezitten, heeft de vergelijking

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = a_1a_2a_3$$

een oplossing in gehele getallen x_1, x_2, x_3.

Stelling 9. Als a_1, a_2 en a_3 gehele getallen $\neq 0$ zijn, die niet alle hetzelfde teken hebben, niet deelbaar zijn door een kwadraat > 1 en paarsgewijs geen factor gemeen hebben, is nodig en voldoende opdat de vergelijking

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$$

een oplossing in gehele getallen $(x_1, x_2, x_3) \neq (0,0,0)$ bezit, dat elk der congruenties

$$x^2 + a_2a_3 \equiv 0 \pmod{a_1},\ x^2 + a_1a_3 \equiv 0 \pmod{a_2},\ x^2 + a_1a_2 \equiv 0 \pmod{a_3}$$

oplossingen bezitten.

Deze laatste eigenschap is van Legendre (1785). Er bestaat een uitgebreide literatuur over (zie Dickson [2]). Het hier bedoelde bewijs is te vinden in Cassels [1].

Literatuur:

[1] J.W.S. Cassels, An introduction to the geometry of numbers, Springer Verlag 1959.

[2] L.E. Dickson, History of the theory of numbers II, Wash. 1920.

[3] W.J. LeVeque, Topics in number theory I, Addison-Wesley Co, 1955.

[4] T. Nagell, Introduction to number theory, Wiley & Sons, 1950.