Over het aantal oplossingen van het stelsel $x\sb {1\sp 2}+x\sb {2\sp 2}+x\sb {3\sp 2}=n$, $x\sb 1=x\sb 2+x\sb 3=m$

OVER HET AANTAL OPLOSSINGEN VAN HET STELSEL $x_1^2 + x_2^2 + x_3^2 = n$, $x_1 + x_2 + x_3 = m$ [1]

DOOR

N. G. DE BRUIJN

(Den Haag).

Door H. D. KLOOSTERMAN [2]) is beschouwd het stelsel diophantische vergelijkingen

$$x_1^2 + \ldots + x_s^2 = n,\ x_1 + \ldots + x_s = m. \quad . \quad . \quad (1)$$

In de gevallen $s = 3$, 5 en 7 bewees hij met behulp van analytische methoden exacte formules voor het aantal oplossingen $r_s(n, m)$ van het stelsel (1) bij gegeven geheele getallen n en m [3]). We zullen hier laten zien, dat zijn formule in het geval $s = 3$ elementair [4]) en wel zeer eenvoudig bewezen kan worden. De gevolgde methode biedt voor andere waarden van s echter geenerlei vooruitzichten.

Zij ω een primitieve wortel van de vergelijking $x^3 = 1$,

---

[1]) De inhoud van dit artikel werd in een brief d.d. 25-11-1941 door den schr. aan dr. KLOOSTERMAN medegedeeld.

[2]) Simultane Darstellung zweier ganzen Zahlen als einer Summe von ganzen Zahlen und deren Quadratsumme, Math. Ann. **118** (1942) blz. 319—364.

[3]) Door P. BRONKHORST (diss. Groningen 1943) zijn inmiddels de veel moeilijker gevallen $s = 6$ en $s = 8$ behandeld.

[4]) Zooals KLOOSTERMAN in een „Zusatz bei der Korrektur'' bij de onder [2]) genoemde verhandeling opmerkte, kan het stelsel (1) door eliminatie worden teruggevoerd op één enkele kwadratische vergelijking met homogeen linkerlid in $s - 1$ veranderlijken, die nog aan bepaalde congruentievoorwaarden moeten voldoen. Het behoeft dus geen verwondering te wekken, dat er voor $s - 1 = 2$ een elementair bewijs mogelijk is. Daar bij het hierboven gegeven bewijs de symmetrie niet verloren gaat, en de daarbij ingevoerde geometrische interpretatie het zeer overzichtelijk maakt, kwam publicatie ons desondanks gewenscht voor.

$C(\omega)$ het door ω voortgebrachte algebraïsche getallenlichaam. De ring der geheele getallen uit $C(\omega)$ is hoofdideaalring met basis $(1, \omega)$; we stellen haar door $C[\omega]$ voor. De discriminant van $C(\omega)$ is $\Delta = -3$, het aantal eenheden bedraagt 6.

In het volgende beteekent k steeds een *reëel* (niet noodzakelijk geheel) getal. We zetten

$$F(0) = \tfrac{1}{6}$$
$$F(k) = \sum_{d/k} \left(\frac{\Delta}{d}\right) \quad \text{als } k = 1, 2, \ldots,$$
$$F(k) = 0 \text{ als } k \neq 0, 1, 2, \ldots;$$

hierin stelt $\left(\frac{\Delta}{d}\right)$ het symbool van KRONECKER voor.

Volgens de reciprociteitswet [5]) is dit laatste gelijk aan het LEGENDRE-symbool $\left(\frac{d}{3}\right)$.

Daar $\left(\frac{d}{3}\right) = 0$ voor $3/d$ is voor geheele k

$$F(k) = \sum_{d/k} \left(\frac{d}{3}\right) = \sum_{d/3k} \left(\frac{d}{3}\right) = F(3k). \quad . \quad . \quad . \quad (2)$$

Nu geldt de (voor $k \neq 1, 2, 3, \ldots$ triviale)

Hulpstelling 1 [6]). *Het aantal oplossingen van* $\alpha \in C[\omega]$, $N(\alpha) = k$ *bedraagt* $6F(k)$.

Is vervolgens $\mathfrak{p}$ het priemideaal $(1 - \omega)$ in $C[\omega]$, dan is $\mathfrak{p}^2 = (1 - 2\omega + \omega^2) = (3)$ en $N(\mathfrak{p}) = 3$. Er zijn dus 3 restklassen mod $\mathfrak{p}$, met representanten $\beta_0 = 0$, $\beta_1 = 1$, $\beta_2 = 2$. Stellen we het aantal oplossingen van $\alpha \in C[\omega]$, $N(\alpha) = k$, $\alpha \equiv \beta_i(\mathfrak{p})$ door $G_i(k)$ voor, dan geldt

Hulpstelling 2. *Is* $k \equiv 0 \ (3)$, *dan* $G_0(k) = 6F(k)$; $G_1(k) = G_2(k) = 0$.

Is $k \not\equiv 0 \ (3)$, *dan* $G_0(k) = 0$; $G_1(k) = G_2(k) = 3F(k)$.

---

[5]) Zie bijv. LANDAU, Vorlesungen über Zahlentheorie, Leipzig 1927 Bd. I Satz 98.

[6]) Zij bijv. LANDAU loc. cit. [5]) Bd. III Satz 882. Opgemerkt zij, dat deze stelling gemakkelijk onafhankelijk van de algemeene algebraïsche getallentheorie kan worden bewezen naar analogie van de overeenkomstige stelling bij de geheele getallen van GAUSZ.

Bewijs. Uit $\alpha \equiv 0(\mathfrak{p})$ volgt $N(\alpha) \equiv 0(3)$ en omgekeerd, dus

$$\text{voor } k \not\equiv 0 \ (3) \text{ is } G_0(k) = 0,$$
$$\text{voor } k \equiv 0 \ (3) \text{ is } G_1(k) = G_2(k) = 0.$$

Volgens hulpst. 1 is verder $G_0(k) + G_1(k) + G_2(k) = 6F(k)$. Tenslotte is steeds $G_1(k) = G_2(k)$, daar de door β_1 resp. β_2 gerepresenteerde restklassen eenheden bevatten. Het gestelde is nu onmiddellijk duidelijk.

We voeren vervolgens een meetkundige terminologie in. Bij $a > 0$ verstaan we onder $L(a)$ een rooster in het platte vlak, dat congruent is met de verzameling der punten $a\alpha$ ($\alpha \in C[\omega]$) in het complexe vlak. Gelijkzijdige driehoeken met zijde a, waarvan de hoekpunten in punten van $L(a)$ vallen, noemen we elementaire driehoeken van het rooster. Nu geldt

Hulpstelling 3. *Het aantal punten van* $L(a)$ *met afstand* $\sqrt{k}$ *tot een vast punt* O *van* $L(a)$ *bedraagt* $6F(ka^{-2})$.

Het aantal punten van $L(a)$ *met afstand* $\sqrt{k}$ *tot het middelpunt* O_1 *van een vasten elementairen driehoek bedraagt* $G_1(3ka^{-2})$.

Dit laatste ziet men in, door de punten van het rooster $L\left(\frac{a}{\sqrt{3}}\right)$, dat ontstaat door de middelpunten van alle elementaire driehoeken aan $L(a)$ toe te voegen, af te beelden op $C[\omega]$ ($O_1 \rightarrow 0$). De punten van $L(a)$ correspondeeren dan met één der restklassen β_1 of β_2 mod $\mathfrak{p}$.

We kunnen nu bewijzen:

Stelling [7]. *Is bij geheele* n *en* m $r_3(n, m)$ *het aantal oplossingen van het stelsel* (1), *en is* $N = \frac{1}{2}(3n - m^2)$; $\alpha_N = 6$ *als* $N \equiv 0$ (3), $\alpha_N = 3$ *als* $N \not\equiv 0$ (3), *dan is*

$$r_3(n, m) = \alpha_N F(N). \quad \ldots\ldots \quad (3)$$

Voor $N \not\equiv 0$ (1) is dus steeds $r_3(n, m) = 0$.

Bewijs. Het vlak $x_1 + x_2 + x_3 = m$ snijdt het door de punten (x_1, x_2, x_3) met geheele coördinaten gevormde kubische rooster volgens een rooster $L(\sqrt{2})$. De projectie van $(0, 0, 0)$

---

[7]) Loc. cit. [2]) Hauptsatz III blz. 362.

op dat vlak bevindt zich in een hoekpunt resp. middelpunt van een elementairen driehoek van dat rooster, al naar gelang $m \equiv 0 \ (3)$ resp. $m \not\equiv 0 \ (3)$ is. De bol met straal $\sqrt{n}$ en middelpunt in (0, 0, 0) snijdt dat vlak volgens een cirkel met straal $\sqrt{n - \frac{m^2}{3}} = \sqrt{\frac{2}{3}\mathrm{N}}$. Hulpst. 3 levert:

$$\text{Is } m \equiv 0 \ (3), \text{ dan } r_3(n, m) = 6\mathrm{F}\left(\frac{\mathrm{N}}{3}\right); \quad \ldots \quad (4)$$

$$\text{is } m \not\equiv 0(3), \text{ dan } r_3\,(n, m) = \mathrm{G}_1(\mathrm{N}). \quad \ldots \quad (5)$$

We onderscheiden nu drie gevallen:

Is $\mathrm{N} \equiv 0 \ (3)$, dan is wegens $m^2 = 3n - 2\mathrm{N}$ ook $m \equiv 0 \ (3)$, dus $r_3(m, n) = 6\mathrm{F}\left(\frac{\mathrm{N}}{3}\right)$. Volgens (2) is dat hetzelfde als $\alpha_\mathrm{N}\mathrm{F}(\mathrm{N})$.

Is N niet geheel, dan is $\mathrm{F}\left(\frac{\mathrm{N}}{3}\right) = 0$ en volgens hulpst. 2 ook $\mathrm{G}_1(\mathrm{N}) = 0$, zoodat (4) en (5) opleveren $r_3(n, m) = 0$. Daar ook $\mathrm{F}(\mathrm{N}) = 0$ is, is (3) weer juist.

Is N geheel, doch niet $\equiv 0(3)$, dan is, daar $m^2 = 3n - 2\mathrm{N}$, ook $m \not\equiv 0 \ (3)$. Volgens (5) geldt dus $r_3(n, m) = \mathrm{G}_1(\mathrm{N})$. Hulpst. 2 levert hiervoor de waarde $3\mathrm{F}(\mathrm{N}) = \alpha_\mathrm{N}\mathrm{F}(\mathrm{N})$.

(Ingekomen 24-6-'43).