STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZC 20

Colloquim getallentheorie.

S.C.van Veen.

1952

ZC 20

Colloquium Getallentheorie.

1951/52

MATHEMATISCH CENTRUM,
2e Boerhaavestraat 49,
A M S T E R D A M .

Colloquium
G E T A L L E N T H E O R I E

o.l.v. Prof. Dr. S.C. van Veen.

1e Voordracht, 10 October 1951. 52

Analytische getallentheorie.

De stelling van Dirichlet over de priemgetallen in een rekenkundige reeks.
(Litt. Landau: Zahlentheorie I p. 79 - p. 97).

Algemene beschouwingen.
In 1837 is door Dirichlet het eerste strenge bewijs geleverd van de stelling:
In een rekenkundige reeks, waarvan het verschil en de eerste term onderling ondeelbaar zijn, komen oneindig veel priemgetallen voor. (Dirichlet, Abh. Berl. Akad. 1837). De juistheid van deze stelling was reeds lang vermoed (Gauss, Legendre). Het is duidelijk dat in de reeks

$$u_n = a + nv$$

de voorwaarde $(a,v) = 1$ (a ond. ondeelb. met v) noodzakelijk is, opdat er priemgetallen in deze reeks kunnen voorkomen. Of deze voorwaarde voldoende is, zelfs om te bewijzen, dat er in deze rij ten minste 1 priemgetal voorkomt, is bij algemene a en v tot nu toe met elememtaire hulpmiddelen niet gelukt. Wel zijn bijzondere gevallen elementair bewezen, o.a.

$$u_n = 6n - 1, 4n - 1, mn \pm 1$$

(vgl. Pólya-Szegö, Aufg, und Lehrsätze II p. 134). Lejeune Dirichlet heeft de stelling volledig en streng bewezen, maar dit bewijs vereist diepgaande en verfijnde analytische hulpmiddelen.
Wij beschouwen de rekenkundige reeks

$$u_n = l + nk \quad (l,k) = 1.$$

In laatste instantie komt het bewijs van Dirichlet neer op het bewijs, dat

$$\sum_{p \equiv l} \frac{\log p}{p^s} \longrightarrow \infty \qquad \text{als } s \longrightarrow 1. \tag{1}$$

(p doorloopt de priemgetallen $\equiv l \pmod h$). Hieruit volgt n.l.; dat deze som niet leeg kan zijn, en ook niet slechts een eindig aantal termen kan bevatten. (Er is hier nog meer bewezen dan nodig is, want ook bij

oneindig vele termen zou nog $\sum_{p \equiv \ell} \frac{\log p}{p^s} \to$ begrensde waarde kunnen zijn).

Het bewijs van (1) wordt teruggebracht tot de beschouwing van de reeks

$$\sum_{a \equiv \ell} \frac{\Lambda(a)}{a^s}$$

waarin a alle positieve gehele getallen $\equiv \ell \pmod k$ doorloopt.
Hierin stelt

$$\Lambda(a)$$

het symbool van Dirichlet voor, gedefinieerd door

$$\Lambda(a) = \begin{cases} \log p \text{ voor } a = p^c & c \geq 1 \\ 0 \text{ voor alle andere } a > 0 \end{cases}$$

dus

$$\sum_{a \equiv \ell} \frac{\Lambda(a)}{a^s} = \sum_{p \equiv \ell} \frac{\log p}{p^s} + \sum_{p^2 \equiv \ell} \frac{\log p}{p^{2s}} \sum_{p^3 \equiv \ell} \frac{\log p}{p^{3s}} + \ldots$$

Neem s reëel > 1.

$$\sum_{p^2 \equiv \ell} \frac{\log p}{p^{2s}} + \sum_{p^3 \equiv \ell} \frac{\log p}{p^{3s}} < \sum_{p} \log p \left\{ \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \ldots \right\}$$

$$< \sum_{p \infty} \log p \left\{ \frac{1}{p^2} + \frac{1}{p^3} + \ldots \right\} = \sum_{p} \frac{\log p}{p(p-1)} < \sum_{a \neq 1}^{\infty} \frac{\log a}{a(a-1)}$$

$$< \sum_{a=1} \frac{2 \log a}{a^2} \quad \text{(begrensd !)}$$

Het is dus voldoende, als bewezen wordt :

$$\sum_{a \equiv \ell} \frac{\Lambda(a)}{a^s} \to \infty \quad \text{voor} \quad s \to 1. \tag{B}$$

De som in (B) wordt in verband gebracht met de reeks:

$$\sum_{a=1}^{\infty} \frac{\chi(a)}{a^s}$$

waarin de rekenkundige functie $\chi(a)$ aan verschillende eisen moet voldoen, waarvan de voornaamste is

$$\chi(a) = 0 \tag{C}$$

als a en k een deler gemeen hebben, dus $(a,k) > 1$.
De functies $\chi(a)$, die in de beschouwingen van Dirichlet een hoofdrol spelen, heten de karakters van Dirichlet.
Dirichlet stelt alle karakters $\chi(a)$ op, welke behoren bij vast gegeven k. Dit geschiedt met behulp van de primitieve wortels modulo p^ℓ $(\ell > 1)$
Met deze beschouwingen zullen wij onze systematische behandeling beginnen. Om de bovengenoemde karakters $\chi(a)$ te kunnen definiëren, is het nodig de theorie der primitieve wortels (mod n) te kennen.

§1. Primitieve wortels (mod n).

Definitie: m geheel > 0, $(a,m) = 1$.
Men zegt: a behoort tot de exponent f (mod m), als
$a^f \equiv 1 \pmod m$; en $a^k \not\equiv 1 \pmod m$ voor $1 \leqslant k < f$,
m.a.w. f is de kleinste exponent > 0 waarvoor $a^f \equiv 1 \pmod m$ wordt.
f bestaat zeker, omdat $a^{\varphi(m)} \equiv 1$ (Fermat-Euler).

Stelling 1: Als a tot f behoort, dan is voor $b_1 \geqslant 0$, $b_2 \geqslant 0$
$a^{b_1} \equiv a^{b_2} \pmod m \rightleftarrows b_1 \equiv b_2 \pmod f$.
i.h.b.: 1) $a^0, a^1, \ldots a^{f-1}$ zijn incongruent (mod m)
2) $a^b \equiv 1 \pmod m \rightleftarrows f \mid b$ (d.i. f deelbaar op b).
3) $f \mid \varphi(m)$ (Fermat-Euler)

Bewijs: 1) Neem aan $b_2 \geqslant b_1 \geqslant 0$
$a^{b_1} \equiv a^{b_2} \pmod m \rightarrow a^{b_2 - b_1} \equiv 1 \pmod m$
$b_2 - b_1 = qf + r$, $q \geqslant 0$, $0 \leqslant r < f$,
dus
$1 \equiv a^{b_2 - b_1} \equiv a^{qf + r} \equiv a^r \pmod m \rightarrow r = 0$, $f \mid b_2 - b_1$.
2) $b_2 - b_1 = qf \rightarrow a^{b_2} \equiv a^{b_1 + qf} \equiv a^{b_1} \pmod m$

Stelling 2: q is een priemgetal, $l > 0$, $q^l \mid p-1$.
Dan is er een a, die tot $q^l \pmod p$ behoort.

Bewijs: Het aantal wortels van de congruentie $x^{\frac{p-1}{q}} \equiv 1 \pmod p$ is hoogstens gelijk aan de graad, dus aantal wortels
$\leqslant \frac{p-1}{q} \leqslant \frac{p-1}{2} \leqslant p-2$ (omdat $p \geqslant 2$).
Er bestaat dus zeker ten minste één c, $1 \leqslant c \leqslant p-1$ met
$c^{\frac{p-1}{q}} \not\equiv 1 \pmod p$.
Stel $a = c^{\frac{p-1}{q^l}}$
$a^{q^l} = c^{p-1} \equiv 1 \pmod p$.
Als a tot f behoort $\rightarrow f \mid q^l$, dus als $f \neq q^l$ moet $f \mid q^{l-1}$
dus $a^{q^{l-1}} \equiv c^{\frac{p-1}{q}} \equiv 1 \pmod p$ (tegenspraak), dus $\underline{f = q^l}$.

Stelling 3: Er is altijd ten minste 1 getal g, dat tot p-1 (mod p) behoo
(p is altijd priem).

Bewijs: 1) Als $p = 2$, dan voldoet $g = 1$.
2) Als $p > 2$ is, ontbinden wij p - 1 in priemfactoren

$$p-1 = \prod_{n=1}^{r} p_n^{l_n}$$

Voor $r = 1$ zie stelling 2.
Voor $r > 1$ kiezen wij op grond van stelling 2 voor iedere $n = 1, 2, \ldots r$ een a_n, behorende bij $p_n^{l_n}$.

Dan bewijzen wij :

$g = \prod_{n=1}^{r} a_n$ behoort bij $\underline{p-1}$.

Stel g behoort bij f. $f \mid p-1$. Als $f \neq p-1 \rightarrow$ zonder beperking $f \mid \frac{p-1}{p_1}$

$1 \equiv g^{\frac{p-1}{p}} \equiv a_1^{\frac{p-1}{p}} \prod_{n=2} a_n^{\frac{p-1}{p}} \equiv a_1^{\frac{p-1}{p}}$ (want $p_n^{l_n} \mid \frac{p-1}{p_1}$ $(n = 2,3\ldots r)$

Dus $p_1^{l_1} \mid \frac{p-1}{p_1}$ (st. 2) <u>tegenspraak</u>.

<u>Definitie</u>: Iedere g, behorende bij p-1 (mod p) heet <u>primitieve</u> wortel (mod p).

De machten $g^0, g^1, \ldots g^{p-2}$ stellen alle gereduceerde restklassen voor.

<u>Stelling 4</u>: $p > 2$, $l > 0$. Er is een g, die tot $\varphi(p^l)$ (mod p^l) behoort.

<u>Bewijs</u>: Voor $l = 1$ zie stelling 3, dus verder $l > 1$.

Stel g is primitieve wortel mod p. Dan is g zo te bepalen, dat

$$g^{p-1} \not\equiv 1 \pmod{p^2}$$

want als de primitieve wortel g zou voldoen aan $g^{p-1} \not\equiv 1 \pmod{p^2}$ dan voldoet de primitieve wortel <u>g+p</u> aan

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 + (p-1)g^{p-2}p \not\equiv 1 \pmod{p^2}.$$

Wij zullen nu bewijzen, dat iedere g, die voldoet aan $g^{p-1} \not\equiv 1 \pmod{p^2}$ tot $\varphi(p^l) = p^{l-1}(p-1)$ behoort.

<u>Volledige inductie</u>: Als $g^{p^{l-2}(p-1)} = 1 + h_l p^{l-1}$. $p \nmid h_l$ (zeker waar voor $l = 2$, Fermat en keuze van g), dan is

$$g^{p^{l-1}(p-1)} = (1+h_l p^{l-1})^p = 1 + p^l \left\{ h_l + h_l^2 \frac{p-1}{2} p^{l-1} + mp^{2l-3} \right\}$$

$$= 1 + h_{l+1} p^l \qquad p \nmid h_{l+1}$$

wanneer g tot f (mod p^l) behoort $\longrightarrow f \mid p^{l-1}(p-1)$.

g behoort tot p-1 (mod p), dus $g^f \equiv 1 \pmod{p}$ met $p-1 \mid f$, waaruit volgt: $f = p^m(p-1)$, $0 \leq m \leq l-1$. Als dus $f \neq p^{l-1}(p-1)$ is, dan is $f \mid p^{l-2}(p-1)$ dus $g^{p^{l-2}(p-1)} \not\equiv 1 \pmod{p^l}$. <u>Tegenspraak !</u>

Op deze wijze is het bestaan aangetoond van ten minste 1 getal g bij iedere modulus p^l ($p > 2$, $l > 0$) met de eigenschap, dat alle machten

$$g^m \quad (1 \leq m \leq p^{l-1}(p-1) = \varphi(p^l)$$

twee aan twee incongruent mod p^l zijn. Ze zijn bovendien alle ondeelbaar door p. Zij vormen dus een gereduceerd restsysteem mod p^l.

Het <u>even</u> priemgetal 2 gedraagt zich, zoals in de meeste dergelijke gevallen, afwijkend. Hier is geen enkel getal g aanwezig met de eigenschap, dat alle machten

$$g^m (1 \leq m \leq 2^{l-1} = \varphi(2^l))$$

twee aan twee incongruent mod p^l zijn, wanneer $l \geq 3$ is. (voor $l = 1$ en 2 voldoet het getal $g = 3$).

Voor <u>ieder</u> oneven geheel getal g geldt echter de stelling:

$$g^{\frac{1}{2}\varphi(2^l)} = g^{2^{l-2}} \equiv 1 \pmod{2^l}.$$

Deze stelling geldt inderdaad voor $l = 3$, $g^2 = (4m \pm 1)^2 \equiv 1 \pmod{2^3}$.

<u>Inductie</u>: Aangenomen de stelling geldt voor een willekeurige exponent $l \geqslant 3$ dus

$$g^{2^{l-2}} \equiv 1 \pmod{2^l} \text{ of } g^{2^{l-2}} = 1 + h.2^l$$

dan geeft kwadratering:

$$g^{2^{l-1}} = 1 + h.2^{l+1} + h^2.2^{2l} \equiv 1 \pmod{2^{l+1}}.$$

Er is dus geen primitieve wortel mod 2^l.
Er zijn wellicht getallen, die behoren bij de exponent $\frac{1}{2}\varphi(2^l)$. Zijn er inderdaad zulke ?
Ja !

<u>Stelling 5</u>: Voor $l > 2$ behoort <u>5</u> tot $\frac{1}{2}\varphi(2^l) = 2^{l-2} \pmod{2^l}$

<u>Bewijs</u>: Voor $l = 3$ is $5 \equiv 5 \bmod 8$
$5^2 \equiv 1 \bmod 8$.
Neem aan, dat de stelling geldt voor zekere $l \geqslant 3$ dus :

$$5^{2^{l-3}} = 1 + h_l 2^{l-1} \qquad 2 \nmid h_l$$

dan is

$$5^{2^{l-2}} = (1 + h_l 2^{l-1})^2 = 1+2^l(h_l+2^{l-1}h_l) = 1+h_{l+1}2^l \qquad 2 \nmid h_{l+1}$$

dus:
$5^{2^{l-3}} \not\equiv 1 \pmod{2^l}$, $5^{2^{l-2}} \equiv 1 \pmod{2^l}$
Als 5 tot f behoort, dan

$$f \nmid 2^{l-3}, \quad f \mid 2^{l-2} \qquad \text{dus } f = 2^{l-2} \qquad \text{w.t.b.w.}$$

De getallen $5^m (1 \leqslant m \leqslant 2^{l-2})$ behoren dus tot $\frac{1}{2}\varphi(2^l)$ restklassen mod 2^l.
De getallen $5^1, 5^2, \ldots 5^{2^{l-2}}$ (a)
zijn dus twee aan twee incongruent mod 2^l. Evenzo zijn de getallen
$-5^1, -5^2, \ldots -5^{2^{l-2}}$ (b)
twee aan twee incongruent mod 2^l.
Alle getallen van de 1^e soort zijn $\equiv 1 \pmod 4$
die van de 2^e soort $\equiv -1 \pmod 4$.
De getallen uit de beide rijen (a) en (b) vormen dus samen een gereduceerd restsysteem (mod 2^l).

MATHEMATISCH CENTRUM,
2e Boerhaavestraat 49,
A M S T E R D A M .

Colloquium
G E T A L L E N T H E O R I E

o.l.v. Prof. Dr S.C. van Veen.
2e Voordracht, 24 October 1951.

Analytische getallentheorie II.

Uit de laatste opmerking in de vorige syllabus volgt de stelling:

Stelling 6: Voor $l > 2$ voldoet ieder oneven getal a voor een bepaalde waarde van b aan de congruentie

$$a \equiv (-1)^{\frac{a-1}{2}} \; 5^b \pmod{2^l} \quad b \geqslant 0.$$

Deze congruentie geldt voor een bepaalde waarde van b uit een bepaalde restklasse mod 2^{l-2}.

§2. Karakters.

We zullen nu zien, hoe met behulp van de primitieve wortels de vroeger vermelde karakters van Dirichlet kunnen worden gedefinieerd.

In deze paragraaf stelt $k > 0$ een vast gegeven geheel getal voor (het verschil uit de rekenkundige reeks: $u_n = 1 + nk$). Het aantal getallen $< k$ en onderling ondeelbaar met k, dus $\varphi(k)$, wordt verder h gesteld. Wij zullen nu nagaan of er getallentheoretische functies bestaan, die aan de volgende eisen voldoen. Getallentheoretische functies zijn functies, die alleen bepaald worden voor gehele waarden van hun argument.

Definitie: Een getallentheoretische functie $\chi(a)$ heet karakter mod k, als deze voldoet aan de volgende 4 eisen:

I $\chi(a) = 0$ voor $(a,k) > 1$ (voornaamste eis),

II $\chi(1) \neq 0$, dus $\chi(a)$ niet steeds $= 0$,

III $\chi(a_1.a_2) = \chi(a_1).\chi(a_2)$ voor $(a_1,k) = 1$, $(a_2k) = 1$
(dus wegens I geldt deze multiplicatieve eigenschap voor gehele waarden van a_1, a_2),

IV $\chi(a_1) = \chi(a_2)$ voor $a_1 \equiv a_2 \pmod{k}$, $(a_1,k) = 1$
(dus wegens I altijd voor $a_1 \equiv a_2 \pmod{k}$).

Voorbeeld: Voor $k = 4$ voldoet aan deze eisen:
voor $a \equiv 0 \pmod 4$: $\chi(a) = 0$,

$a \equiv 1 \pmod 4$ $\chi(a) = 1$,
$a \equiv 2$ " $\chi(a) = 0$,
$a \equiv 3$ (") $\chi(a) = -1$,

Uit bovenstaande 4 eisen zijn reeds verschillende eigenschappen en stellingen voor de karakters (mod k) af te leiden.

Stelling 7: Voor ieder karakter is $\chi(1) = 1$.

Bewijs: III $\rightarrow \chi(1) = \chi(1.1) = \chi(1)\cdot\chi(1)$, dus wegens II $\rightarrow \chi(1) = 1$.

Stelling 8: Als $(a,k) = 1$, dan is:
$\{\chi(a)\}^k = 1$, m.a.w. $\chi(a)$ is een k^{de} machtswortel uit de eenheid en $|\chi(a)| = 1$, dus $\chi(a) \neq 0$.

Bewijs: $a^h \equiv 1 \pmod k$ (Fermat - Euler)
$\{\chi(a)\}^h = \chi(a^h) = \chi(1) = 1$.

Stelling 9: Bij iedere gehele k behoren een eindig aantal karakters, en wel minstens 1.

Bewijs: Volgens stelling 8 behoren bij iedere a uit $1 \leq a \leq k$ de karakters $\chi(a)$ tot een eindige waardevoorraad, n.l. 0 of een h^{de}-machtswortel uit de eenheid. Wegens IV geldt ditzelfde voor alle waarden van a. Dat het aantal karakters minstens 1 bedraagt, volgt uit het feit, dat

$$\chi(a) = \begin{matrix} 0 \text{ voor } (a,k) > 1 \\ 1 \text{ voor } (a,k) = 1 \end{matrix} \qquad (1)$$

aan alle eisen I ... IV voldoet.

Het speciale in I genoemde karakter wordt hoofdkarakter genoemd, en voorgesteld door $\chi_0(a)$.

In het algemeen zullen karakters complexe getallen zijn.

Onmiddelijk duidelijk is:

Stelling 10: Als $\chi(a)$ een karakter is, dan is ook het toegevoegd complexe getal $\overline{\chi}(a)$ een karakter.

Bewijs: De voorwaarden I ... IV zijn vervuld.

Stelling 11:
$$\sum_a \chi(a) = \begin{matrix} h \text{ voor } \chi_0 \\ 0 \text{ in alle andere gevallen.} \end{matrix}$$

Hierin betekent $\sum_a$, dat a een positief volledig restsysteem (mod k) doorloopt.

Bewijs:
Voor χ_0 is $\sum_a \chi(a) = \sum_{(a,k)\equiv 1} 1 = h$.

Wanneer er nog andere dan hoofdkarakters bestaan (dit zal later blijken), dan sluit dit in, dat er een getal $b > 0$ moet bestaan met

$$(b,k) = 1, \qquad \chi(b) \neq 1.$$

Met a doorloopt ook ba een volledig restsysteem, dus

$$S = \sum_a \chi(a) = \sum_a \chi(ba) = \sum_a \chi(b)\chi(a) = \chi(b) \sum_a \chi(a) = S\chi(b)$$

dus

$$S(1 - \chi(b)) = 0 \quad \rightarrow \quad S = 0.$$

Stelling 12: Met $\chi_1(a)$ en $\chi_2(a)$ is ook $\chi_1(a)\chi_2(a)$ een karakter, i.h.b. $\chi^2(a)$, $\chi^3(a)$ etc. zijn karakters.

Bewijs: I tot IV zijn vervuld.
In stelling 9 is bewezen, dat het aantal verschillende karakters (mod k) eindig is. Noem dit aantal voorlopig c. (Later zal worden bewezen, dat c = h).

Stelling 13: Doorloopt $\chi(a)$ de rij van alle c verschillende karakters

$$\chi_1(a),\ \chi_2(a),\ \ldots\ \chi_c(a) \qquad (A)$$

en is $\chi_m(a)$ een willekeurig exemplaar uit deze rij, dan is de rij

$$\chi_m(a)\chi_1(a),\ \chi_m(a)\chi_2(a),\ \ldots,\ \chi_m(a)\chi_c(a) \qquad (B)$$

op de volgorde na gelijk aan de rij (A), m.a.w. met $\chi(a)$ doorloopt $\chi(a)\chi_m(a)$ de rij van alle karakters.

Bewijs: De exemplaren uit (B) zijn alle verschillend voor (a,k) = 1 want uit

$$\chi_m(a)\chi_{l_1}(a) = \chi_m(a)\chi_{l_2}(a)$$

volgt, wegens $\chi_m(a) \neq 0$ (st.8)

$$\chi_{l_1}(a) = \chi_{l_2}(a), \text{ dus } l_1 = l_2.$$

Vanzelfsprekend geldt dit ook als (a,k) > 1 is.
De c functies $\chi_m(a)\chi_l(a)$ (l = 1, 2, ... c) zijn alle karakters (st. 12). Zij vormen dus c <u>verschillende</u> karakters, dus <u>alle</u> karakters.

Nu komt de belangrijkste stelling over de karakters, waarin de karakters worden geconstrueerd. In de voorgaande stellingen was niets nodig uit § 1. In deze stelling wordt het in § 1 behandelde apparaat der primitieve wortels in volle omvang toegepast.

Stelling 14: Voor iedere d > 0 met (d,k) = 1

$$d \not\equiv 1 \pmod{k}$$

bestaat een karakter $\chi(d) \neq 1$.

Bewijs: Wegens $d \not\equiv 1 \pmod{k}$ bestaat er

$$p^l \mid k \quad p > 2 \quad l > 0$$

of

$$2^l \mid k \qquad l > 0$$

zodat

$$d \not\equiv 1 \pmod{p^l} \text{ of } \pmod{2^l}.$$

a) Beschouw eerst $d \not\equiv 1 \pmod{p^l}$ $p > 2$, $l > 0$, $p^l \mid k$, dus $p \nmid d$ (wegens (d,k) = 1).

<u>Neem nu een primitieve wortel g(mod p^l) (st. 4).</u>

Wanneer a een getal is met (a,k) = 1, dus $p \nmid a$, dan is er een bepaald getal $b \geq 0$, zodat

$a \equiv g^b \pmod{p^l}$.

Wij zullen nu bewijzen, dat

$$\chi(a) = e^{\frac{2\pi i.b}{p^{l-1}(p-1)}}$$

een karakter is ($p^{l-1}(p-1) = \varphi(p^l)$).

Want:

II $\chi(1) = 1$, wegens $b = 0$.

III Als $(a_1,k) = 1$, $(a_2,k) = 1$ en b_1 en b_2 worden bepaald door

$a_1 \equiv g^{b_1}$; $a_2 \equiv g^{b_2} \pmod{p^l}$

dan is

$a_1 a_2 \equiv g^{b_1+b_2} \pmod{p^l}$ en $\chi(a_1 a_2) = e^{\frac{2\pi i(b_1+b_2)}{\varphi(p^l)}}$

$= \chi(a_1).\chi(a_2)$

IV geldt vanzelfsprekend, want $a_1 \equiv a_2 \pmod{k} \rightarrow a_1 \equiv a_2 \pmod{p^l}$

dus $b_1 = b_2$.

Tenslotte is er, wegens $d \not\equiv 1 \pmod{p^l}$ en $p \nmid d$ een getal r te bepalen, zodat

$d \equiv g^r \pmod{p^l}$, $\varphi(p^l) \nmid r$

$$\chi(d) = e^{\frac{2\pi ir}{\varphi(p^l)}} \neq 1. \quad \text{w.t.b.w.}$$

b) Stel $d \not\equiv 1 \pmod{2^l}$, $l > 0$ $2^l \mid k$, dus $l > 1$ (want k even, dus d oneven, dus $d \equiv 1 \pmod 2$).

Dit geval wordt weer gesplitst in: b_1) $d \equiv 1 \pmod{2^2}$

b_2) $d \equiv -1 \pmod{2^2}$.

b_1) $d \equiv 1 \pmod{2^2}$ dus $l > 2$.

Volgens stelling 6 geldt voor iedere a met $(a,k) = 1$ dus $(a,2) = 1$

$$a \equiv (-1)^{\frac{a-1}{2}} 5^b \pmod{2^l}$$

voor een bepaalde $b \geq 0$.

Nu is $\chi(a) = e^{\frac{2\pi ib}{2^{l-2}}}$ een karakter, want:

II $\chi(1) = 1$, omdat $b = 0$,

III voor $(a_1,k) = 1$, $(a_2,k) = 1$ bestaan bij a_1 en a_2 <u>bepaalde</u> getallen b_1 em b_2 met

$$a_1 \equiv (-1)^{\frac{a_1-1}{2}} 5^{b_1}, \pmod{2^l},$$

$$a_2 \equiv (-1)^{\frac{a_2-1}{2}} 5^{b_2}$$

dus

$$a_1 a_2 \equiv (-1)^{\frac{a_1 a_2-1}{2}} 5^{b_1+b_2} \pmod{2^l}$$

want

$(a_1-1)(a_2-1)$
is een viervoud.
Dus
$$\chi(a_1a_2) = e^{\frac{2\pi i(b_1+b_2)}{2^{l-2}}} = \chi(a_1)\,\chi(a_2).$$

IV geldt vanzelfsprekend: $a_1 \equiv a_2 \pmod{k} \rightarrow a_1 \equiv a_2 \pmod{2^l}$.
Tenslotte is wegens
$d \not\equiv 1 \pmod{2^l}$ met $d \equiv 1 \pmod 4$
$d \equiv 5^r \pmod{2^l}$ en $2^{l-2} \nmid r$
$$\chi(d) = e^{\frac{2\pi ir}{2^{l-2}}} \neq 1.$$
$b_2)d \equiv -1 \pmod 4$. Dan is $\chi(a) = (-1)^{\frac{a-1}{2}}$ een karakter voor $(a,k) = 1$, want

II $\chi(1) = 1$.
III $\chi(a_1a_2) = (-1)^{\frac{a_1a_2-1}{2}} = (-1)^{\frac{a_1-1}{2} + \frac{a_2-1}{2}} = \chi(a_1)\,\chi(a_2)$.
IV vanzelfsprekend, omdat $4 \mid k$.

Tenslotte is
$$\chi(d) = -1 \neq 1.$$

MATHEMATISCH CENTRUM
2de Boerhaavestr. 49
A m s t e r d a m O.

Colloquium

G E T A L L E N T H E O R I E

c.l.v. Prof.Dr S.C.van Veen.
3de Voordracht, 7 November 1951.

Analytische getallentheorie III.

Stelling 15: Wanneer bij gegeven vaste $a>0$ over alle c karakters wordt wordt gesommeerd, dan is

$$\sum_{\chi} \chi(a) = \begin{cases} c & \text{voor } a \equiv 1 \pmod k \\ 0 & \text{"} \quad a \not\equiv 1 \pmod k \end{cases}$$

Bewijs: 1) Als $a \equiv 1 \pmod k$ bestaat de som uit c termen ieder 1.
2) Als $(a,k)>1$, zijn alle termen nul (volgens def.)
3) Als $(a,k)=1$, $a \not\equiv 1$ is, dan kan in verband met stelling 14 een karakter χ_1 worden gekozen met $\chi_1(a) \neq 1$.

Dan is

$$\eta = \sum_{\chi} \chi(a) = \sum \chi(a)\cdot\chi_1(a) \ (\text{st } 13) = \chi_1(a) \sum_{\chi} \chi(a) = \chi_1(a)\cdot\eta$$

dus $(\chi_1(a)-1)\eta = 0$ dus $\eta = 0$

Stelling 16: c=h Er zijn dus precies h= $\varphi(k)$ karakters mod k.

Bewijs: Beschouw de dubbelsom $\sum_{\chi,a} \chi(a)$, waarin a een positief volledig restsysteem mod k doorloopt, terwijl χ alle h karakters doorloopt.

$$\sum_{a,\chi} \chi(a) = \sum_{a} \sum_{\chi} \chi(a) = \overbrace{c+0+\ldots\ldots\ldots\ldots\ldots 0}^{\text{k termen}} = c \ (\text{st. } 15)$$

$$\sum_{a,\chi} \chi(a) = \sum_{\chi} \sum_{a} \chi(a) = h+0+\ldots\ldots\ldots\ldots\ldots 0 = h \ (\text{st. } 11).$$

Stelling 17: $(l,k)=1$, $l>0$, $a>0$

Dan is

$$\sum_{\chi} \frac{1}{\chi(l)} \chi(a) = \begin{cases} h & \text{voor } a \equiv l \pmod k \\ 0 & \text{"} \quad a \not\equiv l \pmod k. \end{cases}$$

Wegens $\overline{\chi}(l)\cdot\chi(l)=1$ kan men ook schrijven:

$$\sum_{\chi} \overline{\chi}(l)\cdot\chi(a) = \begin{cases} h & \text{voor } a \equiv l \pmod k \\ 0 & \text{"} \quad a \not\equiv l \pmod k. \end{cases}$$

Bewijs: $j>0$ bepaald uit $jl \equiv 1 \pmod k$ (mogelijk wegens $(l,k)=1$).

$$\chi(j)\chi(l) = \chi(jl) = 1 \qquad \chi(l) = \frac{1}{\chi(j)}$$

$$\sum_{\chi} \frac{1}{\chi(l)}\chi(a) \sum_{\chi} \chi(j)\chi(a) = \sum_{\chi} \chi(ja) = \begin{cases} h & \text{voor } ja \equiv 1 \text{ of } a \equiv l \pmod k \\ 0 & \text{in de andere gevallen (st.15).} \end{cases}$$

Hiermede is de algemene theorie der karakters voltooid, en men kan

gerust de ingewikkelde structuur daarvan, benevens de theorie der primitieve wortels vergeten, als men maar in gedachte houdt de eenvoudige eigenschappen, speciaal die van de stellingen 15, 16 en 17. Voor de verdere beschouwing is het van belang, de karakters in 3 soorten te verdelen.

Definitie:

Men noemt een karakter van de eerste soort, als het een hoofdkarakter is (zie onder bewijs stelling 9).

Men noemt een karakter van de tweede soort als het reëel, maar niet hoofdkarakter is, dus steeds 0, 1 of -1, waarbij -1 werkelijk moet voorkomen.

Men noemt een karakter van de derde soort, wanneer $\chi(a)$ niet voor voor alle waarden van a reëel is

Voorbeelden: k=4

$$\left.\begin{array}{ll} \chi(a)=0 & \text{voor } a\equiv 0 \pmod 4 \\ \chi(a)=1 & \text{"} \quad a\equiv 1 \ (\ \text{"}\ ) \\ \chi(a)=0 & \text{"} \quad a\equiv 2 \ (\ \text{"}\ ) \\ \chi(a)=-1 & \text{"} \quad a\equiv 3 \ (\ \text{"}\ ) \end{array}\right\} \text{2de soort.}$$

k=5

$$\left.\begin{array}{ll} \chi(a)=0 & \text{voor } a\equiv 0 \pmod 5 \\ \chi(a)=1 & \text{"} \quad a\equiv 1 \ (\ \text{"}\ ) \\ \chi(a)=1 & \text{"} \quad a\equiv 2 \ (\ \text{"}\ ) \\ \chi(a)=-1 & \text{"} \quad a\equiv 3 \ (\ \text{"}\ ) \\ \chi(a)=-1 & \text{"} \quad a\equiv 4 \ (\ \text{"}\ ). \end{array}\right\} \text{3de soort.}$$

Na deze "elementaire" voorbereidingen begint het eigenlijke analytische gedeelte, het voornaamste.

Theorie der L-reeksen.

Onder L-reeksen verstaat men reeksen van de gedaante

$$\sum_{a=1}^{\infty} \frac{\chi(a)}{a^s}$$

(speciale reeksen van Dirichlet)

Hierin stelt s een gegeven complex getal voor.

Stelling 18: Voor ieder van de h karakters mod k is de reeks

$$\sum_{a=1}^{\infty} \frac{\chi(a)}{a^s} = L(s,\chi)$$

absoluut convergent voor $s>1$. (Dus s reëel in dit geval.)

Bewijs: $|\chi(a)| \leq 1$, dus $\left|\frac{\chi(a)}{a^s}\right| \leq \frac{1}{a^s}$,

dus absoluut convergent wegens convergentie van $\sum_{a=1}^{\infty} \frac{1}{a^s}$.

Stelling 19: Als χ niet hoofdkarakter is (dus van 2de of 3de soort), dan is voor $v \geq u \geq 1$:

$$\left| \sum_{a=u}^{v} \chi(a) \right| \leq \tfrac{1}{2} h$$

Bewijs: Volgens stelling 11 is $\sum_{a} \chi(a)=0$ bij sommatie over volledig restsysteem.

In $\sum_{a=u}^{v} \chi(a)$ behoeft men slechts het grootst mogelijke aantal volledige restsystemen er af te nemen, of eventueel te completeren tot het naast-grotere aantal volledige restsystemen. Men houdt dan een aantal termen over, of mer komt een aantal te kort, dat in beide gevallen $\leq \frac{h}{2}$ is.

MATHEMATISCH CENTRUM,
2de Boerhaavestr. 49,
A m s t e r d a m (O).

Colloquium

G E T A L L E N T H E O R I E

o.l.v. Prof. Dr S.C. van Veen.
4de Voordracht, 21 November 1951.

Analytische getallentheorie IV.

Stelling 20: $v > u$ γ_a willekeurig complex voor $u \leqslant a \leqslant v$.

$$\sum_{a=u}^{w} \gamma_a = R(w) \quad (u \leqslant w \leqslant v). \quad \max_{u \leqslant w \leqslant v} |R(w)| = \nu$$

$$\varepsilon_u \geqslant \varepsilon_{u+1} \geqslant \cdots \geqslant \varepsilon_v > 0$$

Dan is:

$$\left| \sum_{n=u}^{v} \varepsilon_n \gamma_n \right| \leqslant \varepsilon_u \nu$$

Bewijs: Een lege som als R(u-1) betekent 0.

$$\sum_{n=u}^{v} \varepsilon_n \gamma_n = \sum_{n=u}^{v} \varepsilon_n \{ R(n) - R(n-1) \} = \sum_{n=u}^{v} \varepsilon_n R(n) - \sum_{n=u-1}^{v-1} \varepsilon_{n+1} R(n)$$

$$= \sum_{n=u}^{v-1} (\varepsilon_n - \varepsilon_{n+1}) R(n) + \varepsilon_v R(v) \text{ dus } \left| \sum_{n=u}^{v} \varepsilon_n \gamma_n \right| \leqslant \nu \left(\sum_{n=0}^{v-1} (\varepsilon_n - \varepsilon_{n+1}) + \varepsilon_v \right) =$$

$$\leqslant \varepsilon_u \nu$$

Stelling 21: Als χ geen hoofdkarakter is, convergent de reeks $L(s,\chi)$ gelijkmatig voor $s \geqslant 1$.

Bewijs: $\left| \sum_{n=u}^{v} \frac{\chi(n)}{n^s} \right| \leqslant \frac{1}{u^s} \max_{u \leqslant w \leqslant v} \left| \sum_{n=u}^{w} \chi(n) \right| \leqslant \frac{h}{2} \frac{1}{u^s} \leqslant \frac{h}{2u}$. $(s \geqslant 1)$.

dus $\left| \sum_{n=u}^{v} \frac{\chi(n)}{n^s} \right| < \sigma$ voor $v \geqslant u \geqslant u_o(\sigma) = \frac{h}{2\sigma}$ (onafhankelijk van s).

Stelling 22: 1) $\sum_{n=1}^{\infty} \frac{\chi(n) \log n}{n^s}$ convergeert absoluut voor $s > 1$ en gelijkmatig voor $s > 1+\varepsilon$ ($\varepsilon > 0$ willekeurig)

2) voor $s > 1$ is

$$L'(s,\chi) = -\sum_{n=1}^{\infty} \frac{\chi(n) \log n}{n^s}.$$

Bewijs: 1) voor $s > 1 + \varepsilon$ is $\left| \frac{\chi(n) \log n}{n^s} \right| \leqslant \frac{\log n}{n^{1+\varepsilon}}$ en $\sum_{n=1}^{\infty} \frac{\log n}{n^{1+\varepsilon}}$ convergeert.

2) is vanzelfsprekend.

Stelling 23. Als χ geen hoofdkarakter is, convergeert $\sum_{n=1}^{\infty} \frac{\chi(n) \log n}{n^s}$ gelijkmatig voor $s \geqslant 1$, en $|\text{som}| \leqslant h$.

Bewijs:

a Neem $s \geqslant 1$. $\frac{d}{d\xi}\ \frac{\log \xi}{\xi^s} = \frac{1 - s \log \xi}{\xi^{s+1}} < 0$ voor $\xi > e^{\frac{1}{s}}$

dus zeker voor $\xi \geqslant 3$, dus voor $v \geqslant u \geqslant 3$ is

$$\left| \sum_{n=u}^{v} \frac{\chi(n) \log n}{n^s} \right| \leqslant \frac{h}{2}\ \frac{\log u}{u^s} \leqslant \frac{h}{2}\ \frac{\log u}{u} \text{ (gelijkmatig convergent).}$$

b Neem $u=3$, $v \to \infty$. $\left| \sum_{n=4}^{\infty} \frac{\chi(n) \log n}{n^s} \right| \leqslant \frac{\log 2}{2} + \frac{h}{2}\ \frac{\log 3}{3} < \frac{1}{2} + \frac{h}{2} < h.$

Definitie: De arithmetische functie $\mu(n)$ (Symbool van Möbius), wordt gedefinieerd door:

$$\mu(n) = \begin{cases} 1 \text{ voor } n = 1 \\ (-1)^k \text{ als } n \text{ het product van } k \text{ verschillende priemgetallen is.} \\ 0 \text{ in de andere gevallen, dus als } n \text{ tenminste door het quadraat van 1 priemgetal deelbaar is.} \end{cases}$$

Stelling 24: $|\mu(n)| \leqslant 1$.

Bewijs volgt onmiddellijk uit de definitie.

Van groot belang is de volgende eigenschap van $\mu(n)$, waarop het voornaamste gebruik van deze arithmetische functie berust.

Stelling 25: $\sum_{d \mid n} \mu(d) = \begin{cases} 1 \text{ voor } n = 1 \\ 0 \text{ voor } n > 1. \end{cases}$

(In deze som doorloopt d dus alle delers van n).

Bewijs: 1) voor $n = 1$ is $\sum_{d \mid n} \mu(d) = \mu(1) = 1$.

2) Neem $n > 1$, $n = p_1^{k_1} p_2^{k_2} \ldots . p_m^{k_m}$ (kanonische ontbinding).

Volgens de definitie zullen de enige van nul verschillende grootheden $\mu(d)$ behoren bij de delers van $p_1 . p_2 \ldots . p_m$.

1^o. voor ieder van de m delers $p_1, p_2, \ldots p_m$ is $\mu(d) = -1$.

2^o. voor ieder van de $\binom{m}{2}$ delers $p_k p_l$ $\mu(d) = (-1)^2$.

etc.

Dus: $\sum_{d \mid n} \mu(d) = 1 + \binom{m}{1}(-1) + \binom{m}{2}(-1)^2 + \ldots \binom{m}{m}(-1)^m = (1-1)^m = 0$, want $m > 0$.

Wij beschouwen nu de reeks $\sum_{n=1}^{\infty} \frac{\chi(n) \mu(n)}{n^s}$, welke zal blijken, ten nauwste met $L(s, \chi)$ samen te hangen (zie Stelling 27).

Ten eerste geldt hiervoor:

Stelling 26: $\sum_{n=1}^{\infty} \frac{\chi(n) \mu(n)}{n^s}$ convergent absoluut voor $s > 1$.

Bewijs: $\left| \frac{\chi(n) \mu(n)}{n^s} \right| \leqslant \frac{1}{n^s}$.

Stelling 27: Voor $s > 1$ is:

$$L(s, \chi) \cdot \sum_{n=1}^{\infty} \frac{\chi(n) \mu(n)}{n^s} = 1, \text{ dus } L(s, \chi) \neq 0.$$

Bewijs: Wegens de absolute convergentie van beide reeksen is

$$\sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} \cdot \sum_{n=1}^{\infty} \frac{\chi(n)\mu(n)}{n^s} = \sum_{k=1}^{\infty} \sum_{mn=k}^{\infty} \frac{\chi(m).\chi(n)\mu(n)}{(mn)^s}$$

$$= \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s} \cdot \sum_{n|k} \mu(n) = \frac{\chi(1)}{1} = 1 \text{ (st. 25).}$$

Dus:

$$\sum_{n=1}^{\infty} \frac{\chi(n)\mu(n)}{n^s} = \frac{1}{L(s,\chi)} .$$

Met behulp van het voorafgaande is het nu gemakkelijk een fundamentele identiteit te bewijzen, waardoor verband wordt gelegd tussen de priemgetallen en de functie $L(s,\chi)$.

Stelling 28: Voor $s > 1$ is

$$\frac{1}{L(s,\chi)} = \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right).$$

(in het product worden de factoren gerangschikt naar toenemende p, p doorloopt de rij der priemgetallen).

Deze identiteit is de uitbreiding van de productformule van Euler voor de reciproke ζ-functie

$$\prod_{p} \left(1 - \frac{1}{p^s}\right) = \frac{1}{\zeta(s)} \text{ voor } s > 1.$$

Bewijs: Door uitwerking van het product in de volgende uitkomst vindt men voor iedere $\xi > 1$

$$\prod_{p \leq \xi} \left(1 - \frac{\chi(p)}{p^s}\right) = \sum_{n=1}^{\infty}{}' \frac{\chi(n)\mu(n)}{n^s}$$

waar in de som $\sum'$ van het rechterlid n de rij van alle natuurlijke getallen doorloopt, die niet deelbaar zijn door een $p > \xi$.

Dus evenzo geldt:

$$\prod_{p \leq \xi} \left(1 - \frac{\chi(p)}{p^s}\right) = \sum_{n=1}^{\xi} \frac{\chi(n)\mu(n)}{n^s} + \sum_{n > \xi}{}' \frac{\chi(n)\mu(n)}{n^s}$$

(in de eerste som rechts doorloopt n alle natuurlijke getallen $1 \leq n \leq \xi$).

Voor $\xi \to \infty$ $\quad \sum_{n=1}^{\xi} \frac{\chi(n)\mu(n)}{n^s} \to \frac{1}{L(s,\chi)}$.

Verder is: $\left| \sum_{n < \xi}{}' \frac{\chi(n)\mu(n)}{n^s} \right| \leq \sum_{n > \xi} \frac{1}{n^s} \to 0$ voor $\xi \to \infty$

Stelling 29: Voor $s > 1$ is

$$\sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s} = -\frac{L'(s,\chi)}{L(s,\chi)}$$

Hierin stelt $\Lambda(n)$ het vroeger vermelde symbool van Dirichlet voor n.l.

$$\Lambda(n) = \begin{cases} \log p \text{ voor } n = p^k (k \geq 1) \\ 0 \text{ voor alle andere } n > 0 \end{cases}$$

De rij in het linkerlid convergeert dan absoluut voor $s > 1$.
(wegens $|\chi(n)\Lambda(n)| \leq \log n$.)

Bewijs:

Als $m = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ dan is

$$\sum_{n \mid m} \Lambda(m) = \sum_{w_1=1}^{k_1} \Lambda(p_1^{w_1}) + \sum_{w_2=1}^{k_2} \Lambda(p_2^{w_2}) + \ldots$$

$$+ \sum_{w_r=1}^{k_r} \Lambda(p_r^{w_r}) = k_1 \log p_1 + k_2 \log p_2 + \ldots k_r \log p_r = \log m.$$

Voor $s > 1$ is: $L(s,\chi) \cdot \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s} = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s} =$

$$= \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{\chi(mn)}{(mn)^s} \cdot \Lambda(n) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s} \cdot \sum_{n \mid k} \Lambda(n) = \sum_{k=1}^{\infty} \frac{\chi(k) \log k}{k^s} =$$

$$= - L'(s,k).$$

MATHEMATISCH CENTRUM,
Boerhaavestr. 49,
Amsterdam (O).

Colloquium

G E T A L L E N T H E O R I E

o.l.v. Prof. Dr S.C. van Veen.
5de Voordracht, 19 December 1951.

Analytische getallentheorie V.

Stelling 30: Voor $s \to 1$ (van rechts) is

$$-\frac{L'(s, \chi_0)}{L(s, \chi_0)} \to \infty$$

Bewijs: In stelling 29 is bewezen, dat voor $s > 1$:

$$\frac{L'(s, \chi)}{L(s, \chi)} = \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s}.$$

Wij nu voor χ een hoofdkarakter χ_0, dus $\chi(n)=+1$ voor $(n,k)=1$
$\chi(n)= 0$ voor $(n,k)\neq 1$
dan vinden wij:

$$\frac{L'(s,\chi_0)}{L(s,\chi_0)} = \sum_{\substack{n=1 \\ (n,k)=1}}^{\infty} \frac{\Lambda(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} - \sum_{p|k} \sum_{m=1}^{\infty} \frac{\log p}{p^{ms}} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} - \sum_{p|k} \frac{\log p}{p^s-1}.$$

De laatste som bestaat uit een eindig aantal termen, die ieder voor $s \to 1$ tot een eindige grenswaarde naderen. Men behoeft dus slechts aan te tonen, dat

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \to \infty \text{ voor } s \to 1.$$

Daartoe passen wij stelling 29 toe voor $k = 1$.
Dus $\chi(n) = 1$ voor alle waarden van n. $(= \chi_0(n))$.

$$L(s, \chi) = \frac{1}{\prod_p (1 - \frac{1}{p^s})} = \frac{1}{\zeta(s)} \qquad (s > 1) \qquad \text{(stelling 28)}.$$

Dus

$$-\frac{L'(s, \chi)}{L(s, \chi)} = \frac{\sum_{n=1}^{\infty} \frac{\log n}{n^s}}{\sum_{n=1}^{\infty} \frac{1}{n^s}}$$

$$\sum_{n=1}^{\infty} \frac{1}{n^s} > \int_1^{\infty} \frac{dn}{n^s} = \frac{1}{s-1} \to \infty \text{ voor } s \to + 1.$$

Voor $s > 1$ is $\sum_{n=1}^{\infty} \frac{\log n}{n^s} \geqslant \sum_{n=g}^{\infty} \frac{\log n}{n^s} > \log g \sum_{n=g}^{\infty} \frac{1}{n^s} =$

$$= \log g \left(\sum_{n=1}^{\infty} \frac{1}{n^s} - \sum_{n=1}^{n=g-1} \frac{1}{n^s} \right)$$

waarin g een willekeurig geheel getal > 1 voorstelt.

Dus

$$\frac{L'(s,\chi)}{L(s,\chi)} > \log g \left(1 - \frac{\sum_{n=1}^{g-1} \frac{1}{n^s}}{\sum_{n=1}^{\infty} \frac{1}{n^s}}\right) > \tfrac{1}{2} \log g$$

als s dicht genoeg bij 1 ligt,

$$\left(\text{want } 1 - \frac{\sum_{n=1}^{g-1}}{\sum_{n=1}^{\infty}} > 1 - \frac{g}{\frac{1}{s-1}} = 1 - g(s-1),\right)$$

Voor willekeurig groot gekozen g is

$1-g(s-1) > \frac{1}{2}$ als $\quad 1 < s < 1 + \frac{1}{2g}$)

Stelling 31: Voor $0 < \eta < 1$, φ willekeurig reëel is

$$(1-\eta)^3 \left|1-\eta e^{\varphi i}\right|^4 \left|1-\eta e^{2\varphi i}\right|^2 < 1.$$

Bewijs: Het linkerlid is

$$g = (1-\eta)^3 (1-\eta e^{\varphi i})^2 (1-\eta e^{-\varphi i})^2 (1-\eta e^{2\varphi i})(1-\eta e^{-2i\varphi})$$

$$\log g = -\sum_{k=1}^{\infty} \frac{\eta^k}{k} \left\{3+2(e^{k\varphi i} + e^{-k\varphi i}) + (e^{2k\varphi i} + e^{-2k\varphi i})\right\}$$

$$= -\sum_{k=1}^{\infty} \frac{\eta^k}{k} (3+4\cos k\varphi + 2\cos 2k\varphi) = -\sum_{k=1}^{\infty} \frac{\eta^k}{k} (2\cos k\varphi + 1)^2 < 0.$$

Stelling 32: Voor $s > 1$ is

$$\left\{L(s,\chi_0)\right\}^3 \cdot \left|L(s,\chi)\right|^4 \left|L(s,\chi^2)\right|^2 \geqslant 1.$$

Bewijs: In stelling 31 wordt gesteld voor $p \nmid k$.

$$e^{\varphi i} = \chi(p); \quad \eta = \frac{1}{p^s}.$$

Dus

$$\left(1-\frac{\chi_0(p)}{p^s}\right)^3 \left|1-\frac{\chi(p)}{p^s}\right|^4 \left|1-\frac{\chi^2(p)}{p^s}\right|^2 < 1.$$

Voor $p \mid k$ krijgen wij voor het linkerlid = 1

Dus voor alle p is linkerlid $\leqslant 1$.

Dus

$$\prod_p \left(1-\frac{\chi_0(p)}{p^s}\right)^{-3} \left|1-\frac{\chi(p)}{p^s}\right|^{-4} \left|1-\frac{\chi^2(p)}{p^s}\right|^{-2} =$$

$$\left\{L(s,\chi_0)\right\}^3 \left|L(s,\chi)\right|^4 \left|L(s,\chi^2)\right|^2 \geqslant 1.$$

Nu komen de beide hoofdstellingen, die de oplossing van het probleem voltooien. De eerste is vrij eenvoudig te bewijzen. Beide stellingen betreffen het geval s = 1.

Stelling 33. Voor ieder karakter van de derde soort is

$$L(1,\chi) \neq 0.$$

Bewijs: χ^2 is een karakter, maar geen hoofdkarakter, want dan zou χ steeds +1, -1 of nul zijn, dus reëel. Volgens bewijs stelling 21 is dus ($u = 1$, $v \to \infty$) voor $s \geq 1$.

$$\left| L(s, \chi^2) \right| \leq \frac{h}{2} < h.$$

Voor $1 < s < 2$ is $L(s, \chi_0) = \sum_{\substack{n=1 \\ (n,k)=1}}^{\infty} \frac{1}{n^s} \leq \sum_{n=1}^{\infty} \frac{1}{n^2} < 1 + \frac{1}{s-1} = \frac{s}{s-1} < \frac{2}{s-1}$.

Volgens de ongelijkheid uit stelling 32 is dus

$$\left| L(s, \chi) \right| \geq \frac{1}{\left\{ L(s, \chi_0) \right\}^{3/4}} \cdot \frac{1}{\left| L(s, \chi^2) \right|^{1/2}} > \frac{(s-1)^{3/4}}{2^{3/4}} \cdot \frac{1}{\sqrt{h}} > \frac{(s-1)^{3/4}}{2\sqrt{h}}$$

$L'(\xi, \chi)$ is continu voor $\xi \geq 1$. (stelling 23) dus

$$\int_1^s L'(\xi, \chi)\, d\xi = L(s, \chi) - L(1, \chi).$$

Dus

$$\left| L(s, \chi) - L(1, \chi) \right| < h(s-1). \text{ voor } s > 1.$$

Neem nu aan, dat $L(1, \chi) = 0$

Dan is voor alle s uit het gebied $1 < s < 2$:

$$\frac{(s-1)^{3/4}}{2\sqrt{h}} < \left| L(s, \chi) \right| < h(s-1).$$

cf

$$(s-1)^{1/4} > \frac{1}{2h^{3/2}} \quad , \quad s > 1 + \frac{1}{16h^6}.$$

Hier komen wij tot een tegenstrijdigheid.

Conclusie $L(1, \chi) \neq 0$.

Tenslotte krijgen wij de hoofdstelling, waarvan het bewijs het diepst verborgen ligt, n.l.

Stelling 34: Voor ieder karakter van de 2^e soort is

$$L(1, \chi) \neq 0.$$

(Opmerking: Uit stelling 28 weten wij reeds $L(s, \chi) \geq 0$ voor $s > 1$ De reeks is continu voor $s \geq 1$ (stelling 21) dus $L(1, \chi) \geq 0$)

Bewijs: Voor een vereenvoudiging van de bewijsmethode is door Mertens ingevoerd de getallentheoretische functie

$$f(n) = \sum_{d|n} \chi(d).$$

(Mertens: Crelle's Journal 1894. p. 169-184).

Voor $1 \geq 0$ is

$$f(p^l) = 1+\chi(p)+\ldots+\chi(p^l) = \begin{cases} 1++\ 0\ +\ldots+\ 0\ =\ 1 \text{ voor } \chi(p) = 0 \\ 1\ +\ 1\ +\ldots+\ 1 \geq 1 \text{ voor } \chi(p) = 1 \\ 1\ -\ 1\ +\ldots(-1)^l = \begin{cases} 0 \text{ voor } \chi(p) = -1,\ 2 \nmid l \\ 1 \text{ voor } \chi(p) = -1,\ 2 \mid l \end{cases} \end{cases}$$

dus: $f(p^l) \geq \begin{cases} 0 & \text{steeds} \\ 1 & \text{voor } 2 \mid l \end{cases}$ (1)

Voor $a_1 > 0, a_2 > 0, (a_1, a_2) = 1$ ontstaan alle positieve $d \mid a_1 a_2$ door vermenigvuldiging van de positieve $d_1 \mid a_1$ met de positieve $d_2 \mid a_2$.
Dus

$$f(a_1 a_2) = \sum_{d \mid a_1 a_2} \chi(d) = \sum_{\substack{d_1 \mid a_1 \\ d_2 \mid a_2}} \chi(d_1 d_2) = \sum_{d_1 \mid a_1} \chi(d_1) \sum_{d_2 \mid a_2} \chi(d_2) =$$

$$= f(a_1)\, f(a_2).$$

Dus $f(a)$ is multiplicatief. Wegens (1) is dus:

$$f(a) \geq \begin{cases} 0 \text{ steeds} \\ 1 \text{ bij kwadratische } a. \end{cases} \qquad (2)$$

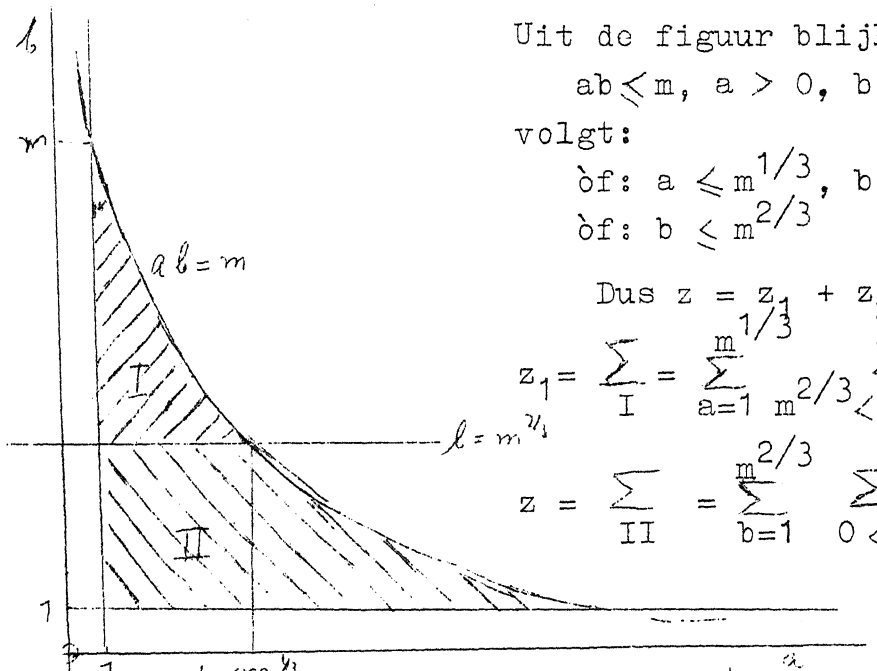
$$S(\chi) = \sum_{n=1}^{x} \chi(n) < \frac{h}{2}.$$

Stel $m = (4h)^6$

$$z = \sum_{n=1}^{m} 2(m-n) f(n) = \sum_{\substack{ab \leq m \\ a>0,\, b>0}} 2(m-ab)\, \chi(b).$$

Uit (2) volgt:

$$z \geq \sum_{b=1}^{\sqrt{m}} 2(m-b^2) \geq \sum_{b=1}^{\frac{1}{2}\sqrt{m}} 2(m-b^2) \geq \sum_{b=1}^{\frac{1}{2}\sqrt{m}} 2\left(m-\frac{m}{4}\right) = \frac{3}{4} m^{3/2} = \frac{3}{4}(4h)^9.$$



Uit de figuur blijkt, dat uit

$ab \leq m,\ a > 0,\ b > 0,$

volgt:

òf: $a \leq m^{1/3},\ b > m^{2/3}$ (gebied I)

òf: $b \leq m^{2/3}$ (gebied II).

Dus $z = z_1 + z_2$ waarin:

$$z_1 = \sum_{I} = \sum_{a=1}^{m^{1/3}} \sum_{m^{2/3} < b < \frac{m}{b}} 2(m-ab)\, \chi(b)$$

$$z = \sum_{II} = \sum_{b=1}^{m^{2/3}} \sum_{0 < a \leq \frac{m}{b}} 2(m-ab)\, \chi(b).$$

Hierin is $\left| \sum_{m^{2/3} < b < \frac{m}{b}} 2(m-ab)\, \chi(b) \right| < 2m.$ Max $\left| \sum \chi_b \right| \leq 2m \frac{h}{2}$

(zie stelling 20)

Dus

$$z_1 \leq \sum_{a=1}^{m^{1/3}} mh = m^{4/3} h.$$

Verder is:

$$z_2 = \sum_{b=1}^{m^{2/3}} \chi(b) \sum_{0<a\leq \frac{m}{b}} (2m - 2ab).$$

Hierin is:

$$\sum_{0<a\leq \frac{m}{b}} (2m-2ab) = 2m\left[\frac{m}{b}\right] - b\left[\frac{m}{b}\right]\left(\left[\frac{m}{b}\right]+1\right)$$

$$= 2m\left(\frac{m}{b} - \Theta\right) - b\left\{\left(\frac{m}{b} - \Theta\right)^2 + \frac{m}{b} - \Theta\right\} \qquad (0\leq \Theta < 1)$$

$$= \frac{m^2}{b} - m + b(\Theta - \Theta^2) \leq \frac{m^2}{b} - m + \frac{b}{4}.$$

Dus

$$z_2 \leq m^2\left\{L(1,\chi) - \sum_{b=m^{2/3}+1} \frac{\chi(b)}{b}\right\} + m\,\frac{h}{2} + \frac{1}{4}m^{4/3}$$

Hierin is $\left|\sum_{b=m^{2/3}+1} \frac{\chi(b)}{b}\right| < \frac{1}{m^{2/3}} \cdot \frac{h}{2}$ (stelling 20).

Dus:

$$z_2 < m^2 L(1,\chi) + m^{4/3}\frac{h}{2} + m^{4/3}\frac{h}{2} + m^{4/3}\frac{h}{4} = m^2L(1,\chi) + \frac{5}{4}m^{4/3}h$$

Dus

$$z = z_1 + z_2 < m^2L(1,\chi) + \frac{9}{4}m^{4/3}h < m^2L(1,\chi) + \frac{9}{16}(4h)^9$$

of

$$\frac{3}{4}(4h)^9 < z < \frac{9}{16}(4h)^9 + m^2L(1,\chi).$$

of:

$$m^2L(1,\chi) > \frac{3}{16}(4h)^9 > 0 \qquad \text{w.t.b.w.}$$

Ten slotte nog een kleinigheidje.

<u>Stelling 35</u>: Voor ieder karakter van de 2^e en 3^e soort is

$$\frac{L'(s,\chi)}{L(s,\chi)} \qquad \text{voor } s \geq 1 \text{ begrensd.}$$

<u>Bewijs</u>: $L(s,\chi)$ is continu voor $s \geq 1$. (stelling 21)

" $\neq 0$ voor $1 < s < 2$ (stelling 27)

" $\neq 0$ voor $s = 1$ (stelling 33 en 34)

Dus $\frac{1}{L(s,\chi)}$ is begrensd voor $1 \leq s \leq 2$,

en ook voor $s > 2$ (stelling 26 en 27)

Ook is: $L'(s,\chi)$ begrensd voor $s \geq 1$ (stelling 23)

Dus:

$$\frac{L'(s,\chi)}{L(s,\chi)} \text{ begrensd voor } s \geq 1.$$

MATHEMATISCH CENTRUM,
2de Boerhaavestr. 49,
A m s t e r d a m (O).

Colloquium

G E T A L L E N T H E O R I E

o.l.v. Prof. Dr S.C. van Veen.
6de Voordracht, 16 Januari 1952.

Analytische getallentheorie VI.

Bewijs van de stelling van Dirichlet.

Wij hebben in stelling 29 bewezen voor $s>1$:

$$\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s} .$$

Vrijwel onmiddellijk volgt hieruit:

Stelling 36: Voor $(m,k) = 1$, $m>0$, $s>1$ is

$$-\frac{1}{h}\sum_{\chi}\frac{1}{\chi(m)}\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n\equiv m}\frac{\Lambda(n)}{n^s} . \qquad (1)$$

(In de rechtersom wordt gesommeerd over alle $n \equiv m \pmod k$ in opklimmende volgorde).

Bewijs: Volgens stelling 29 en stelling 19 is:

$$-\sum_{\chi}\frac{1}{\chi(m)}\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\chi}\frac{1}{\chi(m)}\sum_{n=1}^{\infty}\frac{\chi(n)\Lambda(n)}{n^s} =$$

$$= \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}\sum_{\chi}\frac{1}{\chi(m)}\chi(n) = \sum_{n\equiv m}\frac{\Lambda(n)}{n^s} . h, \qquad \text{w.t.b.w.}$$

Hieruit volgt direct het bewijs der slotstelling.

Stelling 37: Wanneer $(m,k)= 1$, zijn er oneindig vele priemgetallen

$$p \equiv m \pmod k .$$

Bewijs: Wij kunnen zonder enige beperking nemen $m > 0$.

Beschouw de uitkomst (1) uit stelling 36

$$-\frac{1}{h}\sum_{\chi}\frac{1}{\chi(m)}\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n\equiv m}\frac{\Lambda(n)}{n^s} .$$

Het rechterlid (dus het linkerlid) is reëel voor reële s. Laat nu s tot 1 naderen en beschouw het linkerlid.

De term met χ_0 dus

$$-\frac{1}{h}\frac{1}{\chi_0(m)}\frac{L'(s,\chi_0)}{L(s,\chi_0)} = -\frac{1}{h}\frac{L'(s,\chi_0)}{L(s,\chi_0)} \to \infty \quad \text{(Stelling 30).}$$

De overige h-1 termen van het linkerlid van (1) blijven begrensd voor $s \to 1$. (Stelling 35).

Dus ook het rechterlid $\sum_{n \equiv m} \frac{\Lambda(n)}{n^s} \to \infty$ voor $s \to 1$.

$$\sum_{n \equiv m} \frac{\Lambda(n)}{n^s} = \sum_{p \equiv m} \frac{\log p}{p^s} + \sum_{\substack{p,r \\ r>1 \\ p^r \equiv m}} \frac{\log p}{p^{rs}} \to \infty \qquad (2)$$

De laatste som, met $r > 1$ blijft <u>begrensd</u> als $s \to 1$, want voor $s > 1$ is:

$$\sum_{\substack{p,r \\ r>1 \\ p^r \equiv m}} \frac{\log p}{p^{rs}} < \sum_{\substack{p,r \\ r>1}} \frac{\log p}{p^r} = \sum_{p} \frac{\log p}{p(p-1)} \leqslant \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)}$$

$$= \sum_{n=2}^{\infty} \log n \left(\frac{1}{n-1} - \frac{1}{n} \right) = \sum_{n=1}^{\infty} \left(\frac{\log(n+1)}{n} - \frac{\log n}{n} \right)$$

$$= \sum_{n=1}^{\infty} \frac{\log\left(1+\frac{1}{n}\right)}{n} < \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Dus de eerste term van het 2e lid van (2)

$$\sum_{p \equiv m} \frac{\log p}{p^s} \to \infty \qquad \text{voor } s \to 1.$$

m.a.w. deze som kan <u>niet</u> leeg zijn, of een <u>eindig</u> aantal termen bevatten.

<u>Het aantal priemgetallen $p \equiv m \pmod k$ is oneindig groot als $(m,k) = 1$</u>.

Wij willen deze beschouwingen besluiten met enige aanvullende opmerkingen, zonder bewijs (dat komt eventueel later).

De stelling van Dirichlet levert slechts een kwalitatieve uitkomst, die als zodanig de uitbreiding is van het resultaat van Euclides dat het aantal priemgetallen in de natuurlijke getallenrij oneindig is (speciaal geval van Dirichlet m=k=1).

De la Vallée - Poussin en Hadamard hebben gelijktijdig in 1896 het asymptotisch bedrag van het aantal priemgetallen in de reeks $n \equiv m \pmod k$, $(k,m) = 1$ bepaald en gevonden.

$$\lim_{x \to \infty} \frac{\Pi(x)}{\frac{x}{\log x}} = \frac{1}{\varphi(k)} = \frac{1}{h}.$$

als $\Pi(x)$ het aantal priemgetallen in de reeks $n \equiv m \pmod k$ voorstelt (vgl. Ch de la Vallée - Poussin, Recherches analytiques sur la théorie des nombres premiers en général. Deuxième partie: Les fonctions de Dirichlet et les nombres premiers de la forme linéaire $MX + N$.

Ann. de la Soc. scientifique de Bruxelles, Bd 20, deel 2, p. 185-256 1896).

Bij de gelegenheid van zijn bewijs van de stelling van de priemgetallen in een rekenkundige reeks heeft Dirichlet het volgende vermoeden uitgesproken, maar niet bewezen.

Voor $(m_1,k) = 1, (m_2,k) = 1$ is

$$\lim_{x\to\infty} \frac{\Pi_{m_1}(x)}{\Pi_{m_2}(x)} = 1$$

als $\Pi_{m_1}(x)$ resp. $\Pi_{m_2}(x)$ het aantal priemgetallen in de reeksen $n \equiv m_1$, $n \equiv m_2 \pmod k$ voorstelt.

MATHEMATISCH CENTRUM,
2de Boerhaavestr. 49,
A M S T E R D A M - O.

Colloquium

G E T A L L E N T H E O R I E

o.l.v. Prof. Dr S.C. van Veen.
7 de Voordracht, 30 Januari 1952.

De stelling van Vinogradow over het probleem van Waring.

Spreker: Dr W. Verdenius.

Litt.: E. Landau, Ueber einige neuere Fortschritte der additiven Zahlentheorie. (Camb. Tracts no 35)

§ 1. Inleiding.

Waring vermoedde in 1770 (Meditationes Algebraicae p. 204 - 205), dat aan ieder natuurlijk getal k een getal s = s(k) is toe te voegen, zodat ieder natuurlijk getal n te schrijven is als

$$n = \sum_{h=1}^{s} m_h^k + \text{met } m_h \geqslant 0.$$

Het kleinste getal s(k) met deze eigenschap wordt in de litteratuur aangeduid met g(k).

Dit vermoeden werd pas in 1909 door Hilbert bewezen. (Math. Annalen, 67 (1909) p. 281 - 300). Reeds eerder was het door anderen voor $1 \leqslant k \leqslant 9$ en voor k = 10 bewezen. Ik noem daarvan:

Het geval k = 1 is triviaal; g(1) = 1.
Lagrange bewees reeds in 1770, dat g(2) = 4.
Liouville toonde in 1859 aan, dat $g(4) \leqslant 53$. Thans is bekend, dat $19 \leqslant g(4) \leqslant 35$.
Maillet bewees in 1895, dat $g(3) \leqslant 21$. Wieferich verscherpte dit in 1909 tot g(3) = 9 (aangevuld door Kempner in 1912). Alle genoemde bewijzen maken gebruik van zekere identiteiten. In vele gevallen moet men bovendien, wil men de grens voor g(k) klein houden, de stelling voor een groot aantal getallen numeriek controleren.

In verband hiermede zal het duidelijk zijn, dat het wenselijk is ook een onderzoek in te stellen naar het kleinste getal s = G(k) zodat ieder voldoend groot natuurlijk getal n in de gedaante (1) geschreven kan worden. Men is dan minder afhankelijk van de gedragingen van één enkel speciaal getal, terwijl uit het bewijs dat G(k) eindig is tevens de stelling van Hilbert volgt. Het blijkt, dat voor $k > 2$ geldt $G(k) < g(k)$; zo is b.v. thans bekend G(3) = 7 (Linnik 1943) en G(4) = 16 (Davenport 1939).

Deze laatste resultaten zijn evenwel bereikt met geheel andere methoden, waarbij de analytische hulpmiddelen op de voorgrond treden. De stoot hiertoe gaven Hardy en Littlewood in 1920 met een serie artikelen: Some problems on "partitio numerorum". Een van hun eerste resultaten is

$$G(k) \leqslant (k-2)2^{k-1} + 5 = G^*(k).$$

Bovendien leiden ze een asymptotische formule af voor het aantal oplossingen $L(n)$ van (1) als $s = G^*(k)$. In hun resultaat komt een gecompliceerde reeks $\mathfrak{S}(k,n)$ voor, die bekend staat als de singuliere reeks ("singular series"). Ook wordt hij wel aangeduid als de arithmetische factor, omdat hij alleen afhangt van rekenkundige eigenschappen van k en n. In §2 en 3 komt $\mathfrak{S}$ uitvoerig ter sprake. Daar zal bewezen worden, dat er een constante $c_1(k) > 0$ bestaat, zodat $\mathfrak{S}(n) > c_1$. Bij vele analoge onderzoekingen schuilt hierin de grootste moeilijkheid.

Het uitgangspunt van deze onderzoekingen is hierbij

$$L(n) = \sum_{m_1=0}^{n^{\frac{1}{k}}} \cdots \sum_{m_s=0}^{n^{\frac{1}{k}}} \int_0^1 e^{2\pi i\alpha(m_1^k + \ldots + m_s^k - n)}\, d\alpha .$$

Het bewijs berust nu hierop, dat van de integratieweg slechts die gedeelten van belang zijn, die dicht bij een onvereenvoudigbare breuk met kleine noemer liggen (de z.g. "major arcs"), terwijl de overige gedeelten (de z.g. "minor arcs") een bijdrage leveren, die in de restterm kan worden opgenomen,

In 1934 gelukt het Vinogradow een veel scherpere grens te vinden, n.l.

$$G(k) \leqslant 6k \log k + c_2 k,$$

waarin c_2 een niet ter zake doende positieve constante is. Het bewijs berust op vrijwel dezelfde principes als dat van Hardy en Littlewood. Wij zullen in deze serie voordrachten deze stelling bewijzen voor het geval $k > 3$, op de wijze als Heilbronn en Landau het vereenvoudigd hebben.

Naderhand is deze methode ook zeer vruchtbaar gebleken bij het onderzoek van analoge problemen. Dit is o.m. gebeurd door Van der Corput en Loo Keng Hua (± 1939). Een merkwaardig resultaat bereikten Dickson, Pillae e.a. ten aanzien van de functie g(k) met behulp van deze methode. Zij leidde tenslotte tot de mogelijkheid om g(k) te berekenen voor $k > 5$.

§ 2. Stellingen over eenheidswortels.

Enkele afspraken:

Kleine latijnse letters behalve e en i stellen gehele getallen voor;

p, p_1 enz. zijn priemgetallen;

c_1, c_2 enz. stellen geschikt gekozen positieve constanten voor, resp.

positieve functies van de achter c genoemde variabelen;
$k \geqslant 3$.

Definitie 1: Voor ieder getal α stellen we $e(\alpha) = e^{2\pi i\alpha}$.
Definitie 2: Voor iedere onvereenvoudigbare breuk $\frac{a}{q}$ stellen we

$$S(\frac{a}{q}, k) = \sum_{m}{}_1 \quad e(\frac{a}{q} m^k),$$

waarin $\sum_1$ uitgestrekt wordt over de getallen m van een willekeurig volledig restsysteem modulo q. Omdat $(m+q)^k \equiv m^k$ is S onafhankelijk van de keuze van het restsysteem.
In deze paragraaf zullen we bewijzen

$$\left|S(\frac{a}{q}, k)\right| \leqslant c_3(k)\ q^{1-\frac{1}{k}};$$

Stelling 1: Voor $l > 1$ is

$$(x+yp^{l-1})^k \equiv x^k + kx^{k-1}p^{l-1} \pmod{p^l}.$$

Bewijs: Rechts staan de eerste twee termen van de binomiaalontwikkeling van het linkerlid. Alle volgende termen zijn deelbaar door p^l, omdat voor $h > 1$ geldt $h(l-1) \geqslant 2(l-1) \geqslant l$.
Stelling 2: Als t het aantal factoren p van k voorstelt $k = k_o p^t$ (dus $p \nmid k_o$) en $l > k$ is, geldt

$$(x + yp^{l-1-t})^k \equiv x^k + k_o x^{k-1} yp^{l-1} \pmod{p^l}.$$

Opmerking: $l - 1 - t \geqslant k - t \geqslant 2^t - t > 0$.

Bewijs: Het geval $t = 0$ is een speciaal geval van stelling 1. Zij dus verder $t > 0$. Voor $k = 4$, $p = 2$ krijgen we $t = 2$ en $l \geqslant 5$. Dan is

$$(x + yp^{l-1-t})^k = (x + y2^{l-3})^4 =$$

$$x^4 + x^3y2^{l-1} + 3x^2y^2 2^{2l-5} + xy^3 2^{3l-5} + y^4 2^{4l-12} \equiv$$

$$x^4 + x^3y2^{l-1} = x^k + k_o x^{k-1} yp^{l-1} \pmod{p^l}.$$

Er resteert nog het bewijs voor $k \neq 4$, $t > 0$.
Uit de binomiaalontwikkeling van het linkerlid blijkt, dat we kunnen volstaan met te bewijzen $2(l-1-t) \geqslant l$, dus dat $k \geqslant 2t+1$. Dit blijkt aldus:
1). Voor $p > 2$ is $k \geqslant p^t \geqslant 3^t \geqslant 2^t+1$.
2). Voor $p = 2$ en $t = 1$ of 2 is $k \geqslant 6 > 2t+1$.
3). Voor $p = 2$ en $t > 2$ is $k \geqslant 2^t > 2^t+1$.
Stelling 3: Voor $(a,p) = 1$ en $p \nmid k$, $l > 1$ of $p \mid k$, $l > k$ geldt

$$\sum_{\substack{z=0 \\ p \nmid z}}^{p^l-1} e\left(\frac{a}{p^l} z^k\right) = 0.$$

Bewijs: Zij t weer het aantal factoren p van k en $k = k_o p^t$.

Als $p \nmid x$, $0 \leqslant x \leqslant p^{l-1-t} - 1$ en $0 \leqslant y \leqslant p^{t+1} - 1$ vormen de getallen

$$x + y\, p^{l-1-t}$$

juist het systeem van de getallen z waarover gesommeerd moet worden. Voor de in de stelling genoemde som $\sum_z$ is dus

$$\sum_z = \sum_{x,y} e\left(\frac{a}{p^l} (x + y\, p^{l-1-t})^k\right).$$

Uit stelling 1, resp. 2 volgt nu

$$\sum_z = \sum_x e\left(\frac{a}{p^l} x^k\right) \sum_y e\left(\frac{a}{p} k_o\, x^{k-1} y\right).$$

Omdat $p \nmid a k_o x^{k-1}$ is $\sum_y = 0$, want er wordt gesommeerd over een aantal volledige restsystemen modulo p. Dus is $\sum_z = 0$.

Stelling 4: Zij $(a,p) = 1$ en $l > k$. Dan is

$$S\left(\frac{a}{p^l}\right) = p^{k-1}\, S\left(\frac{a}{p^{l-k}}\right).$$

Bewijs: $S\left(\frac{a}{p^l}\right) = \sum_{z=0}^{p^l-1} e\left(\frac{a}{p^l} z^k\right) = \sum_{\substack{z=0 \\ p \mid z}}^{p^l-1} e\left(\frac{a}{p^l} z^k\right)$ (stelling 3)

$$= \sum_{u=0}^{p^{l-1}-1} e\left(\frac{a}{p^l}(up)^k\right) = \sum_{u=0}^{p^{l-1}-1} e\left(\frac{a}{p^{l-k}} u^k\right) = p^{k-1}\, S\left(\frac{a}{p^{l-k}}\right),$$

want in deze laatste som doorloopt u juist p^{k-1} volledige restsystemen modulo p^{l-k}.

Stelling 5: Zij $(a,p) = 1$, $p \nmid k$, $2 \leqslant l \leqslant k$. Dan is

$$S\left(\frac{a}{p^l}\right) = p^{l-1}.$$

Bewijs: Uit $p \nmid k$, $l > 1$ volgt volgens stelling 3

$$S\left(\frac{a}{p^l}\right) = \sum_{z=0}^{p^l-1} e\left(\frac{a}{p^l} z^k\right) = \sum_{\substack{z=0 \\ p \mid z}}^{p^l-1} e\left(\frac{a}{p^l} z^k\right) = \sum_{u=0}^{p^{l-1}-1} e(a p^{k-l} u^k) = p^{l-1}.$$

Stelling 6: Zij $p > 2$, g primitieve wortel modulo p (dus $g^0, g^1, \ldots, g^{p-1}$ stellen alle gereduceerde restklassen modulo p voor). De volgende $(k, p-1)$ getallentheoretische functies $\chi_m(h)$, $0 \leqslant m < (k, p-1)$ zijn verschillende karakters modulo p:

$$\chi_m(h) = \begin{cases} 0 \text{ voor } p \mid h \\ e\left(\frac{mx}{(k,p-1)}\right) \text{ voor } p \nmid h; \text{ waarbij } x \text{ bepaald is door} \\ h \equiv g^x \pmod p,\ 0 \leq x < p-1. \end{cases}$$

($\chi_0(h)$ is ook nu het hoofdkarakter)

Bewijs: De vier eisen, die aan een karakter gesteld zijn (zie pag. 6) zijn vervuld; I, II, IV zijn duidelijk, en III geldt, omdat uit

$$a_1 \equiv g^{x_1},\ a_2 \equiv g^{x_2},\ x_1 \geq 0,\ x_2 \geq 0$$

volgt $a_1 a_2 \equiv g^{x_1+x_2} \pmod p$, zodat aan $a_1 a_2$ is toegevoegd $x_1 + x_2$ of $x_1 + x_2 - (p-1)$. Dat de karakters verschillen blijkt uit het feit, dat de m getallen $\chi_m(g) = e\left(\frac{m}{(k,p-1)}\right)$ verschillen.

Stelling 7: Zij $p > 2$, $h > 0$. Dan is

$$\sum_{m=0}^{(k,p-1)-1} \chi_m(h) = \begin{cases} (k,p-1) \text{ als } p \nmid h \text{ en } h \text{ een } k\text{-de machtsrest} \\ \text{mod } p \text{ is;} \\ 0 \text{ in de overige gevallen.} \end{cases}$$

Bewijs: Zij g een primitieve wortel mod p en laat voor $p \nmid h$ gelden $g^x \equiv h \pmod p$. Volgens de in stelling 6 gegeven definitie is dus

$$\sum_m \chi_m(h) = \begin{cases} 0 \text{ als } p \mid h; \\ \sum_m e\left(\frac{mx}{(k,p-1)}\right) \text{ als } p \nmid h. \end{cases}$$

Deze laatste som is gelijk aan $(k,p-1)$ als $(k,p-1) \mid x$ en anders is ze nul. We moeten dus nog aantonen, dat h, met $p \nmid h$, dan en alleen dan een k-de machtsrest is als $(k,p-1) \mid x$. Om na te gaan wanneer $h \equiv y^k \pmod p$ oplosbaar is naar y, kunnen we $y \equiv g^z \pmod p$ stellen en nagaan wanneer $g^x \equiv g^{zk} \pmod p$ oplosbaar is naar z. Daarvoor is nodig en voldoende, dat $x \equiv zk \pmod{(p-1)}$ oplosbaar is naar z. Dit is dan en alleen dan mogelijk als $(k,p-1) \mid x$.

Stelling 8: Zij $p > 2$. Doorloopt h de getallen van 1 tot en met p-1, dan doorloopt h^k modulo p alle klassen k-de machtsresten $\not\equiv 0 \pmod p$ en wel iedere klasse $(k,p-1)$ maal.

Bewijs: 1). Dat iedere klasse voorkomt is duidelijk.

2). Zij $d = (k,p-1)$. Eenvoudig is in te zien, dat iedere wortel van $x^k \equiv 1 \pmod p$ tevens voldoet aan $x^d \equiv 1 \pmod p$ en omgekeerd, omdat volgens Fermat geldt $x^{p-1} \equiv 1 \pmod p$.

Stel nu $x^{p-1} - 1 = (x^d - 1)\, f(x)$,

dan is $f(x) = x^{p-1-d} + x^{p-1-2d} + \ldots + x^d + 1$.

Nu heeft $x^{p-1}-1 \equiv 0 \pmod p$ juist p-1 wortels en $g(x) \equiv 0 \pmod p$ hoogstens p-1-d. Dus heeft $x^d-1 \equiv 0$ minstens d wortels, dus juist d. De congruentie $x^k \equiv 1 \pmod p$ heeft dus ook d wortels. Bijgevolg heeft ook $z^k \equiv (xk_1)^k \equiv h_o{}^k \pmod p$ voor iedere $h_o \not\equiv 0 \pmod p$ juist d wortels in z.

Stelling 9: Stel $\chi(h)$ is niet-hoofdkarakter modulo p. Dan is voor (a,p) = 1

$$\left| \sum_{h=1}^{p-1} \chi(h)\, e\left(\frac{ah}{p}\right) \right| = \sqrt{p}\,.$$

Bewijs:

$$\left| \sum_{h=1}^{p-1} \chi(h)\, e\left(\frac{ah}{p}\right) \right|^2 = \sum_{h=1}^{p-1} \chi(h)\, e\left(\frac{ah}{p}\right) \sum_{j=1}^{p-1} \overline{\chi}(j)\, e\left(-\frac{ah}{p}\right) =$$

$$= \sum_{h=1}^{p-1} \chi(h)\, e\left(\frac{ah}{p}\right) \sum_{l=1}^{p-1} \overline{\chi}(hl)\, e\left(-\frac{ahl}{p}\right) =$$

$$= \sum_{l=1}^{p-1} \overline{\chi}(l) \sum_{h=1}^{p-1} e\left(\frac{ah(1-l)}{p}\right) = \sum_{l=1}^{p-1} \chi(l) \sum_{h=0}^{p-1} e\left(\frac{ah(1-l)}{p}\right) =$$

$$= \overline{\chi}(1)\, p = p.$$

Stelling 10: Zij $p > 2$ en (a,p) = 1. Dan is

$$\left| S\left(\frac{a}{p}, k\right) \right| < k\sqrt{p}\,.$$

Bewijs: Stel r doorloopt alle k-de machtsresten met $0 < r < p$. Dan is

$$S\left(\frac{a}{p}, k\right) = \sum_{h=0}^{p-1} e\left(\frac{a}{p} h^k\right) = 1 + \sum_{h=1}^{p-1} e\left(\frac{a}{p} h^k\right) =$$

$$= 1 + (k, p-1) \sum_{r} e\left(\frac{a}{p} r\right) \quad \text{(stelling 8)}$$

$$= 1 + \sum_{h=1}^{p-1} e\left(\frac{a}{p} h\right) \sum_{m=0}^{(k,p-1)-1} \chi_m(h) \quad \text{(stelling 7)}$$

$$= \sum_{h=1}^{p-1} e\left(\frac{a}{p} h\right) \sum_{m=1}^{(k,p-1)-1} \chi_m(h) \quad (\chi_o \text{ is het hoofdkarakter})$$

Volgens stelling 9 is dus

$$\left| S\left(\frac{a}{p}, k\right) \right| \leq \sum_{m=1}^{(k,p-1)-1} \sqrt{p} = ((k,p-1)-1)\sqrt{p} < k\sqrt{p}\,.$$

MATHEMATISCH CENTRUM,
2de Boerhaavestr. 49,
A m s t e r d a m (O)

Colloquium

G E T A L L E N T H E O R I E

o.l.v. Prof. Dr S.C. van Veen.
8e Voordracht, 13 Februari 1952.

De stelling van Vinogradow over het probleem van Waring II.

Spreker: Dr W. Verdenius.

We gaan nu met behulp van de stellingen 4,5 en 10 aantonen:

Stelling 11. Zij $l > 0$ en $(a,p)=1$. Dan is

$$\left|S\left(\frac{a}{p^l},k\right)\right| \leqslant \begin{cases} p^{l(1-\frac{1}{k})} & \text{als } p \geqslant k^6; \\ kp^{l(1-\frac{1}{k})} & \text{steeds.} \end{cases}$$

Bewijs: Stel $l = kq + r$, waarin $1 \leqslant r \leqslant k$ is. Door q maal stelling 4 toe te passen blijkt

$$S\left(\frac{a}{p^l}\right) = p^{q(k-1)} S\left(\frac{a}{p^r}\right).$$

Omdat $p^{q(k-1)} p^{r(1-\frac{1}{k})} = p^{l(1-\frac{1}{k})}$ mogen we z.d.a.t.s. verderop aannemen, dat $1 \leqslant l \leqslant k$.

We onderscheiden nu vier gevallen:

1) $p \nmid k$, dus $p \leqslant k < k^6$. Dan is

$$\left|S\left(\frac{a}{p^l}\right)\right| \leqslant p^l \leqslant p p^{l(1-\frac{1}{k})} \leqslant k p^{l(1-\frac{1}{k})}.$$

2) $p \nmid k$, $2 \leqslant l \leqslant k$. Volgens stelling 5 is

$$S\left(\frac{a}{p^l}\right) = p^{l-1} \leqslant p^{l(1-\frac{1}{k})}.$$

3) $p \nmid k$, $p > 2$, $l=1$. Volgens stelling 10 is

$$\left|S\left(\frac{a}{p^l}\right)\right| = \left|S\left(\frac{a}{p}\right)\right| < k\sqrt{p} = k\, p^{1-\frac{1}{k}}\, p^{\frac{1}{k}-\frac{1}{2}} \leqslant k\, p^{1-\frac{1}{k}}\, p^{-\frac{1}{6}} \leqslant$$

$$\leqslant \begin{cases} k\, p^{l(1-\frac{1}{k})} & \text{steeds;} \\ p^{l(1-\frac{1}{k})} & \text{als } p \geqslant k^6. \end{cases}$$

4) $p \nmid k$, $p = 2$, $l = 1$. Dan is

$$S\left(\frac{a}{p^l}\right) = S\left(\tfrac{1}{2}\right) = e\left(\tfrac{1}{2}\right) + e(1) = 0.$$

Stelling 12. Zij $q_1 > 0$, $q_2 > 0$, $(q_1,q_2) = (a_1,q_1) = (a_2,q_2) = 1$. Dan is

$$S\left(\frac{a_1}{q_1},k\right) S\left(\frac{a_2}{q_2},k\right) = S\left(\frac{a_1}{q_1} + \frac{a_2}{q_2},k\right).$$

Bewijs: Doorlopen h_1 en h_2 opvolgend volledige restsystemen mod q_1 en q_2, dan doorloopt $h_1q_2 + h_2q_1$ een volledig restsysteem mod q_1q_2. Dus is

$$S(\frac{a_1}{q_1} + \frac{a_2}{q_2}) = \sum_{h_1=1}^{q_1} \sum_{h_2=1}^{q_2} e((\frac{a_1}{q_1} + \frac{a_2}{q_2})(h_1q_2 + h_2q_1)^k) =$$

$$= \sum_{h_1=1}^{q_1} \sum_{h_2=1}^{q_2} e((\frac{a_1}{q_1} + \frac{a_2}{q_2})((h_1q_2)^k + (h_2q_1)^k) =$$

$$= \sum_{h_1=1}^{q_1} \sum_{h_2=1}^{q_2} e(\frac{a_1}{q_1}(h_1q_2)^k)\, e(\frac{a_2}{q_2}(h_2q_1)^k) = S(\frac{a_1}{q_1})\, S(\frac{a_2}{q_2}).$$

Stelling 13. Als $(a,q) = 1$ is $|S(\frac{a}{q},k)| \leqslant c_3(k)q^{1-\frac{1}{k}}$.

Bewijs: Zij $q = p_1^{l_1} \ldots p_r^{l_r}$ de ontbinding van q in priemfactoren. Omdat $(a,q)=1$ is het mogelijk r onvereenvoudigbare breuken $\frac{a_1}{p_1^{l_1}}, \ldots, \frac{a_r}{p_r^{l_r}}$ te vinden, zodat $\frac{a}{q} = \sum_{\rho=1}^{r} \frac{a_\rho}{p_\rho^{l_\rho}}$.

Uit stelling 12 en 11 volgt dus

$$|S(\frac{a}{q})| = \prod_{\rho=1}^{r} |S(\frac{a_\rho}{p_\rho^{l_\rho}})| \leqslant \prod_{\substack{\rho=1 \\ p_\rho \leqslant k^6}}^{r} k \prod_{\rho=1}^{r} p_\rho^{l_\rho(1-\frac{1}{k})} \leqslant c_3(k)q^{1-\frac{1}{k}}.$$

§ 3. De arithmetische factor of singuliere reeks.

Het getal s stelt een natuurlijk getal voor.

Definitie 3. Voor iedere $q > 0$ stellen we

$$A(q,n,k,s) = A(q,n) = q^{-s} \sum\nolimits_{a}{}_{2}\, S^s(\frac{a}{q},k)\, e(-\frac{a}{q}n),$$

waarin $\sum_2$ uitgestrekt wordt over de getallen a van een willekeurig gereduceerd restsysteem mod q.

Omdat $S(\frac{a}{q}) = S(\frac{a+q}{q})$ en $e(-\frac{a}{q}n) = e(-\frac{a+q}{q}n)$ is $A(q,n)$ onafhankelijk van de keuze van het gereduceerde restsysteem.

Definitie 4. Onder voorbehoud van convergentie stellen we

$$\mathfrak{S}(n,k,s,) = \mathfrak{S}(n) = \sum_{q=1}^{\infty} A(q,n,k,s).$$

In deze paragraaf zullen we o.m. aantonen dat $\mathfrak{S}(n)$ reëel is en dat voor $s \geqslant 4k$ geldt:

$$\mathfrak{S}(n,k,s) \geqslant \frac{1}{c_4(k,s)}.$$

Stelling 14. Voor $q > 0$ is $|A(q,n,k,s)| \leqslant c_5(k,s)q^{1-\frac{s}{k}}$.

Bewijs. Uit stelling 13 blijkt

$$|A(q,n)| \leqslant q^{1-s}\, c_3{}^{s}(k)q^{s(1-\frac{1}{k})} = c_5(k,s)q^{1-\frac{s}{k}}.$$

Stelling 15. De reeks $\sum_{q=1}^{\infty} |A(q,n)|$ is voor $s > 2k$ convergent.

Bewijs: De reeks $\sum_{q=1}^{\infty} c_5(k,s)q^{1-\frac{s}{k}}$ is convergent en volgens stelling 14 een majorante van $\sum_{q=1}^{\infty} |A(q,n)|$.

Stelling 16. Zij $q_1 > 0$, $q_2 > 0$, $(q_1,q_2) = 1$. Dan is

$$A(q_1,n)\, A(q_2,n) = A(q_1q_2,n).$$

Bewijs: Doorlopen a_1 en a_2 opvolgend gereduceerde restsystemen mod q_1 en q_2, dan doorloopt $a_1q_2 + a_2q_1$ een gereduceerd restsysteem mod q_1q_2. Dus is volgens stelling 12

$$A(q_1q_2,n) = (q_1q_2)^{-s} \sum_{\substack{a_1=1 \\ (a_1,q_1)=1}}^{q_1} \sum_{\substack{a_2=1 \\ (a_2,q_2)=1}}^{q_2} S^s\left(\frac{a_1q_2+a_2q_1}{q_1q_2}\right) e\left(-\frac{a_1q_2+a_2q_1}{q_1q_2}\, n\right) =$$

$$= A(q_1,n)\, A(q_2,n).$$

Stelling 17. Zij $s > 2k$. Dan is

$$\zeta^s(n) = \prod_p \sum_{h=0}^{\infty} A(p^h,n).$$

Bewijs. Omdat $s > 2k$ is $\sum_{h=0}^{\infty} A(p^h,n)$ voor elke p absoluut convergent. (Stelling 15). In verband met stelling 16 is dus voor iedere $N > 2$

$$\prod_{p \leqslant N} \sum_{h=0}^{\infty} A(p^h,n) = \sum_{q=1}^{N} H(q,n) + \sum_{q}{}_3 H(q,n),$$

waarin $\sum_3$ uitgestrekt wordt over alle $q > N$, die geen priemfactoren $> N$ bevatten. Uit stelling 15 volgt verder

$$\lim_{N \to \infty} \sum_3 H(q,n) = 0 \quad .$$

Uit deze beide relaties volgt de stelling.

Stelling 18. Zij $l \geqslant 0$ en $N(p^l,n,k,s)$ het aantal incongruente oplossingen $(h_1,\ldots,h_s)$ van $h_1^{\,k} + \ldots + h_s^{\,k} \equiv n \pmod{p^l}$.

Dan is

$$p^{l(1-s)} N(p^l,n,k,s) = \sum_{h=0}^{l} A(p^h,n).$$

Bewijs. We merken eerst op

$$p^l N(p^l,n) = \sum_{a=1}^{p^l} \sum_{h_1=1}^{p^l} \cdots \sum_{h_s=1}^{p^l} e\left(\frac{a}{p^l}(h_1^k+\ldots+h_s^k-n)\right).$$

Voor l=0 is de stelling triviaal, want N(1,n)=1=A(1,n).

Zij nu $l>0$. Dan is dus

$$p^{l(1-s)}\, N(p^l,n) = A(p^l,n) +$$

$$+ p^{-ls+s} \sum_{a=1}^{p^{l-1}} \sum_{h_1=1}^{p^{l-1}} \cdots \sum_{h_s=1}^{p^{l-1}} e\left(\frac{a}{p^{l-1}}(h_1^k+\ldots+h_s^k-n)\right) =$$

$$= A(p^l,n) + p^{(l-1)(1-s)}\, N(p^{l-1},n).$$

Met behulp van volledige inductie naar l blijkt dus de juistheid van deze stelling.

Thans is ons probleem dus teruggebracht tot het onderzoek van het aantal oplossingen van de congruentie

$$h_1^k+\ldots+h_s^k \equiv n \pmod{p^l}.$$

Met de grote priemgetallen kunnen we nu het reëel zijn van de factoren van $\mathfrak{J}$ vaststaat (gevolg van stelling 18) reeds heel eenvoudig afrekenen:

Stelling 19. Voor $s>2k$ is

$$\sum_{h=0}^{\infty} A(p^h,n) > 1 - c_6(k,s)p^{1-\frac{s}{k}}.$$

Bewijs. Uit stelling 14 volgt

$$\sum_{h=0}^{\infty} A(p^h,n) \geqslant A(1,n) - \sum_{h=1}^{\infty} \left|A(p^h,n)\right| \geqslant$$

$$\geqslant 1 - \sum_{h=1}^{\infty} c_5(k,s)p^{h(1-\frac{s}{k})} = 1 - \frac{c_5(k,s)}{p^{\frac{s}{k}-1}-1} \geqslant 1 - 2c_5(k,s)p^{1-\frac{s}{k}}.$$

MATHEMATISCH CENTRUM,
2de Boerhaavestr. 49,
A m s t e r d a m (O)

Colloquium

G E T A L L E N T H E O R I E

o.l.v. Prof.Dr S.C. van Veen.

9e Voordracht, 27 Februari 1952.

De stelling van Vinogradow over het probleem van Waring III.

Spreker: Dr W. Verdenius

We gaan nu stellingen afleiden over het aantal oplossingen $N(p^l,n)$ bedoeld in stelling 18. Het geval p=2 moet ook nu afzonderlijk behandeld worden.

Stelling 20. Zij $p > 2$, $s \geqslant 2k$, $k = p^t k_0$, $p \nmid k_0$. Dan bezit de congruentie

$$\sum_{h=1}^{s-1} x_h^k \equiv n \pmod{p^{t+1}}$$

minstens één oplossing $(x_1,\ldots,x_{s-1})$.

Bewijs. Het geval $n \equiv 0 \pmod{p^{t+1}}$ is triviaal: $x_h = 0 (h=1,\ldots,s-1)$ voldoet. We nemen nu verderop aan dat $n \not\equiv 0 \pmod{p^{t+1}}$.

We verdelen de getallen $1,2,\ldots,p^{t+1}-1$ in klassen, waarbij we twee getallen n_1 en n_2 in dezelfde klasse opnemen $(n_1 \sim n_2)$ als er een x te vinden is, zodat geldt

(1)..... $\quad x^k n_1 \equiv n_2 \pmod{p^{t+1}}$ en $p \nmid x$.

Dit begrip geeft inderdaad een klasseindeling:

1) $n \sim n$, want aan $x^k n \equiv n$, $p \nmid x$ voldoet x=1.

2) Uit $n_1 \sim n_2$ volgt het bestaan van een x met (1). Bij deze x is een y te vinden met $xy \equiv 1 \pmod{p^{t+1}}$, $p \nmid y$. Nu is dus

$$n_1 \equiv (xy)^k n_2 \equiv y^k n_2 \pmod{p^{t+1}}.$$ Dus is $n_2 \sim n_1$.

3) Uit $n_1 \sim n_2$ en $n_2 \sim n_3$ volgt het bestaan van een x met (1) en een y met $y^k n_2 \equiv n_3 \pmod{p^{t+1}}$, $p \nmid y$. Dus geldt

$$(xy)^k n_1 \equiv y^k n_2 \equiv n_3 \pmod{p^{t+1}}, \quad p \nmid xy.$$

Dus is $n_1 \sim n_3$.

We willen nu het aantal van deze klassen bepalen. We merken eerst op, dat alle elementen van dezelfde klasse evenveel factoren p bevatten. Dit blijkt uit (1) omdat geen der te beschouwen elementen meer dan t factoren p bevat. We tellen eerst het aantal elementen van iedere klasse.

Zij n_1 een getal uit het systeem $(1,\ldots,p^{t+1}-1)$ dat juist d factoren p bevat. We vragen nu naar het aantal getallen n_2 uit dit systeem dat ook juist de factoren p bevat en waarvoor (1) een oplossing x bezit. Stel $n_1 = n_1' p^d$ en $n_2 = n_2' p^d$. We mogen nu evengoed het aantal getallen n_2' bepalen, met $1 \leqslant n_2 \leqslant p^{t+1-d}-1$ en waarbij een x te vinden is, zodat

$$x^k n_1' \equiv n_2' \pmod{p^{t+1-d}}, \quad p \nmid x.$$

Zij nu g primitieve wortel mod p^{t+1-d}. Stel

$$x \equiv g^y,\ n_1' \equiv g^{m_1} \text{ en } n_2' \equiv g^{m_2} (\text{mod } p^{t+1-d}).$$

We mogen dus ook nagaan hoeveel getallen m_2 er zijn met

$$0 \leqslant m_2 < \varphi(p^{t+1-d}) = p^{t-d}(p-1)$$

en waarbij een y te vinden is, zodat

$$ky + m_1 \equiv m_2 (\text{mod } p^{t-d}(p-1)).$$

Dit laatste is vervuld als m_2 in een bepaalde restklasse mod $(k, p^{t-d}(p-1))$ ligt. Het gezochte aantal is dus

$$\frac{p^{t-d}(p-1)}{(k, p^{t-d}(p-1))} = \frac{p-1}{(k_0, p-1)}.$$

Onder de getallen $1, \ldots, p^{t+1}-1$ bevinden zich $p^{t-d}(p-1)$ getallen die juist d factoren p bevatten. Het aantal klassen waarvan de elementen juist d factoren p bevatten is dus $p^{t-d}(k_0, p-1)$. Het totale aantal klassen r is dus

$$r = \sum_{d=0}^{t} p^{t-d}(k_0, p-1) = (k_0, p-1)\frac{p^{t+1}-1}{p-1} < \frac{p^{t+1}}{p-1} k_0 =$$

$$= \frac{p}{p-1} k \leqslant \frac{3}{2} k < 2k.$$

Zij nu v(n) het kleinste getal v, waarvoor

$$\sum_{h=1}^{v} x_h^k \equiv n (\text{mod } p^{t+1})$$

ten minste één oplossing $(x_1, \ldots, x_v)$ bezit. Als $n_1 \sim n_2$ is voor geschikte keuze van x de relatie (1) vervuld, dus volgt uit het bestaan van een oplossing van

$$\sum_{h=1}^{m} x_h^k \equiv n_1 (\text{mod } p^{t+1}) \text{ dat ook } \sum_{h=1}^{m} x_h^k \equiv n_2 (\text{mod } p^{t+1})$$

een oplossing bezit en omgekeerd. v(n) hangt dus alleen van de klasse af, waarin n ligt. v(n) neemt dus hoogstens 2k-1 verschillende waarden aan.

Uit v(1) = 1 en $v(n+1) \leqslant v(n)+1$ volgt dus dat

$$v(n) \leqslant 2k-1 \quad \text{voor } 1 \leqslant n \leqslant p^{t+1}-1.$$

Hieruit volgt de stelling.

<u>Stelling 21</u>. Zij $p > 2$, $k = p^t k_0, p \nmid k_0, l \geqslant t+1$, $a \equiv 1 (\text{mod } p^{t+1})$. Dan is er een x met $x^k \equiv a (\text{mod } p^l)$.

<u>Bewijs</u>: Stel g is primitieve wortel mod p^u voor iedere $u > 0$. (Het bestaan hiervan blijkt uit het bewijs van stelling 4 op pag. 4). Omdat $a \equiv 1 (\text{mod } p^{t+1})$ is $p \nmid a$. Stel $a \equiv g^z (\text{mod } p^l)$. Dus is zeker $g^z \equiv 1 (\text{mod } p^{t+1})$, dus $z \equiv 0 (\text{mod } p^t(p-1))$.

De congruentie $z \equiv vk(p-1) (\text{mod } p^{l-1}(p-1))$ zal nu een oplossing v en dus ook een oplossing $v \geqslant 0$ bezitten, omdat

$$(k(p-1), p^{l-1}(p-1)) = p^t(p-1).$$

Dus zal gelden $g^z \equiv (g^{v(p-1)})^k \pmod{p^l}$,
zodat $x = g^{v(p-1)}$ gekozen kan worden.

Stelling 22. Zij $p > 2$, $s \geqslant 2k$, $k = p^t k_0$, $p \nmid k_0$. Voor $l \geqslant t+1$ is het aantal incongruente oplossingen $(x_1,\ldots,x_s)$ van

$$\sum_{h=1}^{s} x_h^{\,k} \equiv n \pmod{p^l}$$

ten minste $p^{(l-t-1)(s-1)}$.

Bewijs: De congruentie

$$\sum_{h=2}^{s} x_h^{\,k} \equiv n-1 \pmod{p^{t+1}}$$

bezit volgens stelling 20 ten minste één oplossing. Er zijn dus zeker $p^{(l-t-1)(s-1)}$ systemen $(x_2,\ldots,x_s)$, die voldoen aan

$$n - \sum_{h=2}^{s} x_h^{\,k} \equiv 1 \pmod{p^{t+1}} \text{ en } 1 \leqslant x_h \leqslant p^l (h=2,\ldots,s).$$

Volgens stelling 21 kunnen we bij ieder dergelijk systeem $(x_2,\ldots,x_s)$ het getal x_1 zo bepalen, dat

$$x_1^{\,k} \equiv n - \sum_{h=2}^{s} x_h^{\,k} \pmod{p^l}.$$

De aldus verkregen systemen $(x_1,\ldots,x_s)$ voldoen aan de gegeven congruentie

Stelling 23. Zij $k = 2^t k_0$, k_0 oneven, $l \geqslant t+2$ en $a \equiv 1 \pmod{2^{t+2}}$. Dan is er een x met $x^k \equiv a \pmod{2^l}$.

Bewijs. $a \equiv 1 \pmod 4$. Dus is de congruentie $a \equiv 5^z \pmod{2^l}$ oplosbaar naar z. (Stelling 6 pag. 6) Hiervoor is dus ook

$$1 \equiv 5^z \pmod{2^{t+2}}.$$

Omdat $z=0$ hieraan voldoet is $z \equiv 0 \pmod{2^t}$ (Stelling 6 pag. 6).
Omdat $(k, 2^{l-2}) = 2^t$ is de congruentie

$$z \equiv vk \pmod{2^{l-2}}$$

oplosbaar naar v en dus is er ook een oplossing $v \geqslant 0$. Dan is

$$(5^v)^k = 5^{vk} \equiv 5^z \equiv a \pmod{2^l},$$

want aan $5^z \equiv a \pmod{2^l}$ voldoen alle z van een bepaalde restklasse mod 2^{l-2} (stelling 6 pag. 6).

Stelling 24. Zij $s \geqslant 4k$, $k = 2^t k_0$, k_0 oneven. Voor $l \geqslant t+2$ is het aantal incongruente oplossingen $(x_1,\ldots,x_s)$ van

$$\sum_{h=1}^{s} x_h^{\,k} \equiv n \pmod{2^l}$$

tenminste $2^{(l-t-2)(s-1)}$

Bewijs: Stel $n-1 \equiv m \pmod{2^{t+2}}$ en $0 \leqslant m \leqslant 2^{t+2}-1 \leqslant 4k-1 \leqslant s-1$.
Omdat

$$\sum_{h=2}^{m+1} 1^k + \sum_{h=m+2}^{s} 0^k \equiv n-1 \pmod{2^{t+2}},$$

bezit

$$\sum_{h=2}^{s} x_h^{\,k} \equiv n-1 \pmod{2^{t+2}}$$

ten minste één oplossing $(x_2,\ldots,x_s)$.

Er zijn dus minstens $2^{(1-t-2)(s-1)}$ systemen $(x_2,\ldots,x_s)$, die voldoen aan $n - \sum_{h=2}^{s} x_h^k \equiv 1 \pmod{2^{t+2}}$ en $1 \leqslant x_h \leqslant 2^l (h = 2,\ldots,s)$. Volgens stelling 23 kunnen we bij elk dergelijk systeem $(x_2,\ldots,x_s)$ een x_1 bepalen met $x_1^k \equiv n - \sum_{h=2}^{s} x_h^k \pmod{z^l}$.

Alle aldus verkregen systemen $(x_1,\ldots,x_s)$ voldoen aan de gegeven congruentie.

Stelling 25. Zij $s \geqslant 4k$, $k = p^t k_0$, $p \nmid k_0$. Dan is

$$\sum_{h=0}^{\infty} A(p^l,n) \geqslant p^{(1-s)(t+2)}$$

Bewijs: Zij $l \geqslant t+2$. Volgens stelling 18 is

$$\sum_{h=0}^{\infty} A(p^h,n) = p^{l(1-s)}\, N(p^l,n),$$

waarin $N(p^l,n)$ het aantal incongruente oplossingen is van

$$\sum_{h=1}^{s} x_h^k \equiv n \pmod{p^l}.$$

Met behulp van stelling 22 $(p > 2)$ en 24 $(p = 2)$ blijkt hieruit dat

$$\sum_{h=0}^{l} A(p^h,n) \geqslant p^{l(1-s)+(1-t-2)(s-1)} = p^{(1-s)(t+2)}.$$

Hieruit volgt de bewering.

(Opm.: Dat we voor $p > 2$ scherpere grenzen tot onze beschikking hebben is voor ons doel van geen belang.)

Stelling 26. Voor $s \geqslant 4k$ is $\gamma(n,k,s) \geqslant \frac{1}{c_4(k,s)}$.

Bewijs: Met behulp van stelling 19 blijkt

$$\sum_{h=0}^{\infty} A(p^l,n) > 1 - c_6 p^{1-\frac{s}{k}} > 1 - \frac{c_6}{p^3} > 1 - \frac{1}{p^2}$$

als $p > c_6$ is. In verband met stelling 17 en 25 geeft dit

$$\gamma(n) \geqslant \prod_{p \leqslant c_6} p^{(1-s)(t+2)} \prod_{p > c_6} (1 - \frac{1}{p^2}) \geqslant \frac{1}{c_4},$$

wegens de convergentie van dit laatste product.

MATHEMATISCH CENTRUM,
2de Boerhaavestr. 49,
A M S T E R D A M - O.

Colloquium

G E T A L L E N T H E O R I E

o.l.v. Prof. Dr S.C. van Veen
11e Voordracht, 12 Maart 1952.

De stelling van Vinogradow over het probleem van Waring IV

Spreker: Dr W. Verdenius.

§ 4. Voorbereidende stellingen.

In deze § geven we enkele stellingen, die in het analytische deel van het bewijs gebruikt zullen worden.

Van fundamenteel belang is hierbij de Fareyverdeling van het interval $(0,1)$.

Definitie 5. Onder de Fareyrij F_n van de orde $n (n \geq 1)$ verstaan we de stijgende rij van onvereenvoudigbare breuken $\frac{a}{q}$ met

$$0 \leq \frac{a}{q} \leq 1 \text{ en } q \leq n.$$

Dus $\frac{a}{q}$ behoort tot F_n, als $0 \leq a \leq q \leq n$ en $(a,q) = 1$. Zo is F_5 de rij $\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{2}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}$.

Alles wat we nodig hebben omtrent F_n nemen we op in de volgende stelling:

Stelling 27. Als $\frac{a}{q}$ en $\frac{a'}{q'}$ twee opeenvolgende breuken zijn van F_n, is

$$a'q - aq' = 1 \text{ en } q + q' > n.$$

Bewijs: Omdat $(a, q) = 1$, is de vergelijking

$$qx - ay = 1$$

oplosbaar in gehele getallen x en y. Als (x_o, y_o) een oplossing is, dan worden alle oplossingen gegeven door $(x_o + ha, y_o + hq)$, waarbij h geheel is. We bepalen h zo, dat $n - q < y_o + hq \leq n$. We hebben nu een oplossing (x, y) gekregen met

$$(x,y) = 1, \quad 0 \leq n - q < y \leq n.$$

De breuk $\frac{x}{y}$ behoort dus tot F_n. Omdat

$$\frac{x}{y} = \frac{a}{q} + \frac{1}{qy} > \frac{a}{q},$$

komt $\frac{x}{y}$ na $\frac{a}{q}$ in F_n. Als het niet $\frac{a'}{q'}$ is, is $\frac{x}{y} > \frac{a'}{q'}$ en dus

$$\frac{x}{y} - \frac{a'}{q'} = \frac{xq' - ay'}{yq'} \geq \frac{1}{yq'},$$

terwijl

$$\frac{a'}{q'} - \frac{a}{q} = \frac{a'q - aq'}{qq'} \geq \frac{1}{qq'}.$$

Hieruit volgt

$$\frac{1}{yq} = \frac{x}{y} - \frac{a}{q} \geq \frac{1}{yq} + \frac{1}{qq'} = \frac{y+q}{yqq'} > \frac{n}{yqq'} \geq \frac{1}{yq},$$

hetgeen onmogelijk is. Dus is $\frac{x}{y} = \frac{a'}{q'}$, zodat $a'q - aq' = 1$.

Uit de ongelijkheid waarmee y vastgelegd is, volgt nu $q + q' > n$.

In het analytische deel van het bewijs treden verschillende grootheden op, die we nu in het kort samenvatten. We stellen N is geheel ≥ 6 en $P = N^{k^1}$. Op het interval $0 \leq \alpha \leq 1$ markeren we nu alle Fareybreuken met noemer $P^{k-\frac{1}{2}}$. We brengen vervolgens de medianten van twee opeenvolgende breuken aan, dus tussen $\frac{a}{q}$ en $\frac{a'}{q'}$ noteren we $\frac{a+q}{a'+q'}$. Volgens stelling 27 is dus

$$\frac{a+a'}{q+q'} - \frac{a}{q} = \frac{a'q - aq'}{q(q+q')} = \frac{1}{q(q+q')} \begin{cases} \geq \frac{1}{2q\ P^{k-\frac{1}{2}}} \\ \leq \frac{1}{q\ P^{k-\frac{1}{2}}}; \end{cases}$$

en evenzo

$$\frac{a'}{q'} - \frac{a+a'}{q+q'} = \frac{1}{q'(q+q')} \begin{cases} \geq \frac{1}{2q'\ P^{k-\frac{1}{2}}} \\ \leq \frac{1}{q'\ P^{k-\frac{1}{2}}}. \end{cases}$$

We veschuiven nu het interval van 0 tot de eerste mediante (ϑ) over de eenheid naar rechts. We laten nu de Fareybreuken weg en beschouwen alleen de medianten. Door deze punten wordt het interval $\vartheta \leq \alpha \leq 1 + \vartheta$ in deelintervallen verdeeld, die de gedaante

$$\alpha = \frac{a}{q} + \beta,$$

met $(a,q) = 1$, $1 \leq a \leq q \leq P^{k-\frac{1}{2}}$, $-\vartheta_1 \leq \beta \leq \vartheta_2$ hebben, waarin geldt

$$\frac{1}{2q\ P^{k-\frac{1}{2}}} \leq \begin{matrix} \vartheta_1 \\ \vartheta_2 \end{matrix} \leq \frac{1}{q\ P^{k-\frac{1}{2}}}.$$

Zeker is dus

$$|\beta| = \left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q\ P^{k-\frac{1}{2}}} \leq \frac{1}{q^2}.$$

De deelintervallen met $1 \leq q < P^{\frac{1}{2}}$ noemen we M ("Major arcs").en die met $P^{\frac{1}{2}} \leq q \leq P^{k-\frac{1}{2}}$ duiden we aan met m ("Minor arcs").

We voeren verder voor ieder natuurlijk getal l de verzameling H_l in bestaande uit de verzameling der natuurlijke getallen z, die te schrijven zijn als

$$z = \sum_{h=1}^{l} x_h^k \text{ met } x_h \geq 0 \quad (h = 1,\ldots,l).$$

Het aantal elementen van H_1, die $\leq Q$ zijn, noemen we $H_1(Q)$.

Voor s nemen we voortaan 4k; voor l zullen we later een geschikte keuze doen, afhankelijk van k.

We definiëren verder

$$T(\alpha) = T(\alpha,k,N) = \sum_{1\leq x\leq P} e(x^k\alpha),$$

$$R(\alpha) = R(\alpha,k,l,N) = \sum_{\substack{u\leq \frac{1}{4}P^k \\ u \text{ in } H_1}} e(u\alpha),$$

$$S(\alpha) = S(\alpha,k,l,N) = \sum_{1\leq y\leq P^{\frac{1}{2k}}} \sum_{\substack{u\leq \frac{1}{4}P^{k-\frac{1}{2}} \\ u \text{ in } H_1}} e(y^k u\alpha).$$

We geven nu een korte schets van het bewijs.

Het aantal oplossingen in gehele getallen $x_1,\ldots,x_s$, u_1, u_2, u_3, y, die voldoen aan

$$1 \leq x_h \leq P \qquad (h = 1,\ldots,s)$$

$$u_h \text{ in } H_1 \qquad u_h \leq \tfrac{1}{4}P^k \qquad (h = 1,2)$$

$$u_3 \text{ in } H_1 \qquad u_3 \leq \tfrac{1}{4}P^{k-\frac{1}{2}}$$

$$1 \leq y \leq P^{\frac{1}{2k}}$$

van

$$N = \sum_{h=1}^{s} x_h^k + u_1 + u_2 + y^k u_3$$

is gelijk aan

$$\int_0^1 e(-\alpha N)T^s(\alpha)R^2(\alpha)S(\alpha)d\alpha.$$

We leiden nu eerst een <u>ondergrens</u> G_M af voor $\mathrm{Re}\sum_M \int_M$ en daarna een <u>bovengrens</u> G_m af voor $\left|\mathrm{Re}\sum_m \int_m\right|$. Deze grenzen bepalen we zo scherp, dat voor geschikt gekozen l en voldoend grote N geldt

$$\int_0^1 = \mathrm{Re}\int_0^1 = \mathrm{Re}\sum_M \int_M + \mathrm{Re}\sum_m \int_m \geq G_M - G_m > 0.$$

De stelling van <u>Hilbert</u> is hiermee dan bewezen. Tevens vinden we (zie § 1) $G(k) \leq s + 31$. Deze laatste ongelijkheid zal de stelling van <u>Vinogradow</u> opleveren.

Om de ondergrens G_M te bereiken, maken we behalve van de stellingen 13, 14 en 26 gebruik van de volgende stelling:

<u>Stelling 28</u>. Zij $\tau_1 \leq \tau_2$. Voor $\tau_1 \leq \tau \leq \tau_2$ zij $0 \leq F(\tau) \leq B$, $0 \leq F'(\tau) \leq C$ en $0 \leq F''(\tau)$.

Dan is

$$\sum_{\tau_1 < t \le \tau_2} e^{iF(t)} - \int_{\tau_1}^{\tau_2} e^{iF(\tau)}\, d\tau \le 4(1 + B + BC).$$

Bewijs: We onderscheiden drie gevallen: I τ_1 en τ_2 geheel. Dan is

$$\left| \sum_{\tau_1 < t \le \tau_2} e^{iF(t)} - \int_{\tau_1}^{\tau_2} e^{iF(\tau)} d\tau \right| \le 1 + \left| \sum_{t=\tau_1}^{2} e^{iF(t)} - \tfrac{1}{2} e^{iF(\tau_1)} - \tfrac{1}{2} e^{iF(\tau_2)} - \int_{\tau_1}^{\tau_2} e^{iF(\tau)} d\tau \right| =$$

$$(1) \qquad = 1 + \left| \int_{\tau_1}^{\tau_2} (\tau - [\tau] - \tfrac{1}{2})\, F'(\tau)\, e^{iF(\tau)} d\tau \right|.$$

Voor iedere $\eta \le \xi$ is

$$\left| \int_{\eta}^{\xi} (\tau - [\tau] - \tfrac{1}{2}) d\tau \right| \le \frac{1}{8}.$$

Stellen we voor $\tau_1 \le \xi \le \tau_2$

$$\int_{\tau_1}^{\xi} (\tau - [\tau] - \tfrac{1}{2})\, F'(\tau)\, d\tau = \psi(\xi),$$

dan is volgens de tweede stelling van het gemiddelde

$$|\psi(\xi)| \le \frac{1}{8} C \text{ voor } \tau_1 \le \xi \le \tau_2.$$

Het rechterlid van (1) is dus

$$= 1 + \left| \psi(\tau_2)\, e^{iF(\tau_2)} - \int_{\tau_1}^{\tau_2} \psi(\tau)\, i\, e^{iF(\tau)}\, F'(\tau) d\tau \right| \le$$

$$\le 1 + \frac{1}{8} C + \int_{\tau_1}^{\tau_2} \frac{1}{8} C\, F'(\tau) d\tau = 1 + \frac{1}{8} C (1 + B) (< 4(1 + B + BC)).$$

II $[\tau_1] = [\tau_2]$. Dan is $\tau_2 - \tau_1 < 1$ en derhalve

$$\left| \sum_{\tau_1 < t \le \tau_2} e^{iF(t)} - \int_{\tau_1}^{\tau_2} e^{iF(\tau)} d\tau \right| = \left| \int_{\tau_1}^{\tau_2} e^{iF(\tau)} d\tau \right| < 1 < 4(1 + C + BC).$$

III $[\tau_1] < [\tau_2]$. Dan is volgens het bovenstaande

$$\left| \sum_{\tau_1 < t \le \tau_2} e^{iF(t)} - \int_{\tau_1}^{\tau_2} e^{iF(\tau)} d\tau \right| < \left| \sum_{[\tau_1]+1 < t \le [\tau_2]} e^{iF(t)} - \int_{[\tau_1]+1}^{[\tau_2]} e^{iF(\tau)} d\tau \right| + 3 \le$$

$$\le 1 + \frac{1}{8} C (1 + B) + 3 \le 4(1 + C + BC).$$

Om de bovengrens G_m te bereiken, bewijzen we de volgende drie hulpstellingen. Alleen stelling 31 zullen we later gebruiken.

Stelling 29. Stel $q > 1$, $(a,q) = 1$, α en γ reëel, $\left| \alpha - \frac{a}{q} \right| \le \frac{1}{q^2}$. Met $\{\beta\}$ wordt voor reële β de afstand van β tot het naastbijgelegen gehele getal bedoeld. Min $(q, \frac{1}{\alpha})$ stellen we gelijk aan q.

Dan is

$$\sum_{x=0}^{q-1} \mathrm{Min}\left(q, \frac{1}{\{\gamma + \alpha x\}}\right) < 8\, q \log q.$$

Bewijs: We kiezen m zodanig, dat

$$\left|\gamma - \frac{m}{q}\right| \leq \frac{1}{2q};$$

dan is voor $0 \leq x \leq q-1$

$$\left|\gamma + \alpha x - \frac{m + ax}{q}\right| = \left|\left(\gamma - \frac{m}{q}\right) + x\left(\alpha - \frac{a}{q}\right)\right| < \frac{1}{2q} + q\,\frac{1}{q^2} = \frac{3}{2q},$$

zodat $\gamma + \alpha x = \frac{m + ax + \theta(x)}{q}$ met $|\theta(x)| < \frac{3}{2}$.

$\{\beta\}$ heeft de periode 1; omdat $(a,q) = 1$, doorloopt $m + ax$ een volledig restsysteem mod q. Dus kunnen we

$$\{\gamma + \alpha x\} = \left\{\frac{y(x) + \theta(x)}{q}\right\}$$

stellen, waarin $y(x)$ voor $x = 0, \ldots, q-1$ de getallen $0, \ldots, q-1$ in een zekere volgorde doorloopt.

Wij redeneren nu als volgt

$$\sum_{x=0}^{q-1} \mathrm{Min}\left(q, \frac{1}{\{\gamma + \alpha x\}}\right) \leq \sum\nolimits_{x}{}_1\, q + \sum\nolimits_{x}{}_2 \frac{1}{\{\gamma + \alpha x\}},$$

waarbij we in $\sum_1$ die waarden van x nemen, waarvoor $\gamma + \alpha x$ dicht bij een geheel getal ligt en in $\sum_2$ de overige waarden van x. Voor ons doel is het voldoende om $\sum_2$ uit te strekken over die x, waarvoor geldt

(2) $\quad 3 \leq y(x) \leq q - 3.$

Om te bereiken, dat dit voorkomt, nemen we voorlopig aan $q \geq 6$. We strekken dus $\sum_1$ slechts uit over 5 waarden van x, zodat $\sum_{x}{}_1\, q = 5q$.

Voor de x met (2) geldt

$$\frac{y(x)}{2} \leq y(x) - \frac{3}{2} < y(x) + \theta(x) < y(x) + \frac{3}{2} \leq q - \frac{q - y(x)}{2},$$

dus is

$$\frac{y(x)}{2q} < \frac{y(x) + \theta(x)}{q} < 1 - \frac{q - y(x)}{2q},$$

zodat

$$\frac{1}{\{\gamma + \alpha x\}} < 2q\ \mathrm{Max}\left(\frac{1}{y(x)}, \frac{1}{q - y(x)}\right) < 2q\left(\frac{1}{y(x)} + \frac{1}{q - y(x)}\right).$$

Hieruit volgt

$$\sum\nolimits_{x}{}_2 \frac{1}{\{\gamma + \alpha x\}} < 2q \sum_{y=3}^{q-3} \left(\frac{1}{y} + \frac{1}{q - y}\right) < 4q \int_{\cdot}^{?} \frac{dy}{y} = 4q \log q.$$

Samen geeft dit

$$\sum_{x=0}^{q-1} \mathrm{Min}\left(q, \frac{1}{\{\gamma + \alpha x\}}\right) < 5q + 4q \log q < \left(\frac{5}{\log 6} + 4\right) q \log q < 8q \log q.$$

Voor $q < 6$ is het bewijs eenvoudig:

$$\sum_{x=0}^{q-1} \mathrm{Min}\left(q, \frac{1}{\{\gamma + \alpha x\}}\right) \leq 5q \leq 5q\,\frac{\log q}{\log 2} < 8q \log q.$$

Stelling 30. Stel $b - a \geq q > 1$, $(a,q) = 1$, α reëel en $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$.

Dan is $\sum_{z=a+1}^{b} \text{Min}\left(q, \frac{1}{\{\alpha z\}}\right) < 16\,(b-a)\log q$.

Bewijs: We verdelen de gehele getallen $a+1, \ldots, b$ in de volgende groepen

$$a + hq + 1, \ldots, a + (h+1)q \quad \left(h = 0, \ldots, \left[\frac{b-a}{q}\right] - 1\right)$$

$$a + \left[\frac{b-a}{q}\right] q + 1, \ldots, b.$$

De te beschouwen som valt nu uiteen in $\left[\frac{b-a}{q}\right]$ of $\left[\frac{b-a}{q}\right] + 1$ deelsommen, waarvan de laatste hoogstens gelijk en de overigen gelijk aan een som in de zin van stelling 29 zijn. Dus is

$$\sum_{z=a+1}^{b} < \left(\frac{[b-a]}{q} + 1\right) 8q \log q \leq 16(b-a)\log q.$$

Stelling 31. (Vinogradow) Stel $z \geq q > 1$, $(a,q) = 1$, α reëel en $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$.

Dan is

$$\left|\sum_{x,y} e(xy\alpha)\right|^2 \leq 32\,XYZ \log q;$$

hierin wordt in $\sum_{x,y}$ het getal x uitgestrekt over X natuurlijke getallen $\leq q$ en y over Y verschillende natuurlijke getallen $\leq Z$.

Bewijs: Voor reële μ is steeds

$$\left|\sum_{x=1}^{q} e(x\mu)\right| \leq q$$

en als μ niet geheel is, geldt

$$\left|\sum_{x=1}^{q} e(\mu x)\right| = \left|\frac{e(\mu) - e(\mu(q+1))}{1 - e(\mu)}\right| \leq \left|\frac{2}{e(-\tfrac{1}{2}\mu) - e(\tfrac{1}{2}\mu)}\right| = \frac{1}{|\sin \pi\mu|} =$$

$$= \frac{1}{\sin(\pi\{\mu\})} \leq \frac{1}{\frac{2}{\pi}\pi\{\mu\}} < \frac{1}{\{\mu\}}.$$

Hieruit volgt in verband met de ongelijkheid van Cauchy-Schwarz (y' doorloopt dezelfde waarden als y in het voorafgaande).

$$\left|\sum_{x,y} e(xy\alpha)\right|^2 \leq \left(\sum_{x}\left|\sum_{y} e(xy\alpha)\right|\right)^2 \leq X\sum_{x}\left|\sum_{y} e(xy\alpha)\right|^2 \leq$$

$$\leq X\sum_{x=1}^{q}\left|\sum_{y} e(xy\alpha)\right|^2 = X\sum_{y,y'}\sum_{x=1}^{q} e(x(y-y')\alpha) \leq$$

$$\leq X\sum_{y,y'} \text{Min}\left(q, \frac{1}{\{\alpha(y-y')\}}\right).$$

Stel nu $y-y' = z$, dan is

$$-[Z] + 1 \leq z \leq [Z] - 1$$

en iedere z komt hoogstens Y maal als y-y' voor. Omdat

$$2[Z] - 1 \geq 2q - 1 > q$$

kunnen we stelling 30 toepassen bij de sommatie over z. Dit levert

$$\left|\sum_{x,y} e(xy\alpha)\right|^2 \leq XY \sum_{z=-[Z]+1}^{[Z]-1} \text{Min}\left(q, \frac{1}{\{\alpha z\}}\right) \leq 32\,XYZ \log q.$$

MATHEMATISCH CENTRUM,
2de Boerhaavestr. 49,
A M S T E R D A M - O.

Colloquium
G E T A L L E N T H E O R I E

o.l.v. Prof. Dr S.C. van Veen
11e[1] Voordracht, 26 Maart 1952

De stelling van Vinogradow over het probleem van Waring V

Spreker: Dr W. Verdenius.

§ 5. De "Major Arcs".

Aan de reeds op pag. 40 en 41 ingevoerde notaties - deze worden in het vervolg bij voortduring gebruikt - voegen we nog de volgende toe:

Voor reële β stellen we

$$U(\beta) = U(\beta,k,N) = \int_0^P e(\omega^k\beta)\,d\omega,$$

$$V(\beta) = V(\beta,k,N) = \frac{1}{k}\sum_{x=1}^{N} x^{\frac{1}{k}-1}\, e(x\beta).$$

Voor een natuurlijk getal n stellen we

$$D(n) = D(k,n,N) = \int_{-\frac{1}{2}}^{+\frac{1}{2}} e(-n\beta)V^s(\beta)\,d\beta.$$

Voorlopig stellen we ons ten doel om aan te tonen, dat voor $n < N$ geldt

$$(3)\qquad \left|\sum_{M} \int_{M} e(-n\alpha)T^s(\alpha)\,d\alpha - D(n)\Gamma(n)\right| < c_1(k)P^{3k-\frac{1}{2}}.$$

Verder zal blijken, dat voor $\frac{1}{4}N \leqq n < N$ geldt

$$D(n)\Gamma(n) > \frac{1}{c_8(k)}P^{3k}.$$

Voor voldoend grote N (d.w.z. groter dan een alleen van k afhankelijk getal) en iedere n met $\frac{1}{4}N \leqq n < N$ is dus

$$\left|\sum_{M} \int_{M} e(-n\alpha)T^s(\alpha)\,d\alpha\right| > \frac{1}{c_9(k)}P^{3k}.$$

Met behulp hiervan bepalen we tenslotte een voor voldoend grote N geldige bovengrens voor

$$\mathrm{Re}\sum_{M}\int_{M} e(-N\alpha)T^s(\alpha)R^2(\alpha)S(\alpha)\,d\alpha.$$

Om (3) te bereiken, brengen we $T(\alpha)$ eerst in verband met $U(\beta)$, daarna pas met $V(\beta)$. Door integratie over alle major arcs zullen we

1) De voordracht d.d. 12 Maart 1952 is abusievelijk eveneens als 11e voordracht aangekondigd. Dit moet zijn 10e voordracht.

voorlopig nog niet (3) vinden, maar een ongelijkheid, die uit (3) ontstaat door $\delta'(n)$ te vervangen voor $\sum_{q<\sqrt{P}} A(q,n)$. Evenwel zal blijken, dat de reeks $\delta'(n)$ voldoende snel convergeert om tot (3) te komen.

Stelling 32. Ligt α op de M(major arc) met bijbehorende breuk $\frac{a}{q}$, dan is

$$\left| T(\alpha) - q^{-1} S(\tfrac{a}{q}) U(\alpha - \tfrac{a}{q}) \right| < c_{10}(k) q.$$

Bewijs: Zij $\alpha = \frac{a}{q} + \beta$. We brengen $T(\alpha)$ in de gedaante $(\alpha = \frac{a}{q} + \beta)$

$$T(\alpha) = \sum_{r=1}^{q} \sum_{-\frac{r}{q} < t \leqq \frac{P-r}{q}} e((tq+r)^k(\tfrac{a}{q} + \beta)).$$

Dit kan omdat voor M geldt $q \leqq P$. Verder is

$$\frac{U(\beta)}{q} = \frac{1}{q}\int_0^P e(\omega^k \beta)\,d\omega = \int_{-\frac{r}{q}}^{\frac{P-r}{q}} e((\tau q+r)^k \beta)\,d\tau.$$

Hieruit volgt

$$T(\alpha) - q^{-1} S(\tfrac{a}{q}) U(\beta) =$$

$$= \sum_{r=1}^{q} e(\tfrac{a}{q} r^k) \left(\sum_{-\frac{r}{q} < t \leqq \frac{P-r}{q}} e((tq+r)^k \beta) - \int_{-\frac{r}{q}}^{\frac{P-r}{q}} e((\tau q+r)^k \beta)\,d\tau \right),$$

zodat

$$\left| T(\alpha) - q^{-1} S(\tfrac{a}{q}) U(\beta) \right| \leqq \sum_{r=1}^{q} \left| \sum_{-\frac{r}{q} < t \leqq \frac{P-r}{q}} e((tq+r)^k |\beta|) - \int_{-\frac{r}{q}}^{\frac{P-r}{q}} e((\tau q+r)^k |\beta|)\,d\tau \right|$$

Op de termen van de som $\sum_{r=1}^{q}$ in het rechterlid passen we stelling 28 toe. We kiezen

$$\tau_1 = -\frac{r}{q}, \quad \tau_2 = \frac{P-r}{q} \text{ en } F(\tau) = 2\pi(\tau q+r)^k |\beta|.$$

Voor $\tau_1 \leqq \tau \leqq \tau_2$ is dan

$$0 \leqq F(\tau) \leqq 2\pi P^k |\beta| \leqq 2\pi q^{-1} P^{\frac{1}{2}} \leqq 2\pi P^{\frac{1}{2}},$$

$$0 \leqq F'(\tau) \leqq 2\pi k q P^{k-1} |\beta| \leqq 2\pi k P^{-\frac{1}{2}},$$

$$0 \leqq F''(\tau).$$

We vinden dus

$$\left| T(\alpha) - q^{-1} S(\tfrac{a}{q}) U(\beta) \right| \leqq \sum_{r=1}^{q} 4(1 + 2\pi k P^{-\frac{1}{2}} + 4\pi^2 k^2) \leqq c_{10}(k) q.$$

Stelling 33. Ligt α op de M (major arc) met bijbehorende breuk $\frac{a}{q}$, dan is

$$\left| T(\alpha) - q^{-1} S(\tfrac{a}{q}) V(\alpha - \tfrac{a}{q}) \right| < c_{11}(k) q.$$

Bewijs: Omdat $\left| S(\tfrac{a}{q}) \right| \leqq q$, kunnen we op grond van stelling 32 volstaan met aan te tonen $(\beta = \alpha - \frac{a}{q})$

$$\left| U(\beta) - V(\beta) \right| < c_{12}(k).$$

Dit blijkt aldus

$$|U(\rho)-V(\rho)| = \left|\frac{1}{k}\int_0^N \lambda^{\frac{1}{k}-1} e(\rho\lambda)\,d\lambda - \frac{1}{k}\sum_{x=1}^{N} x^{\frac{1}{k}-1} e(\rho x)\right| \leqslant$$

$$\leqslant \frac{1}{k}\int_0^1 \lambda^{\frac{1}{k}-1}\,d\lambda + \frac{1}{2k} + \frac{1}{2k}N^{\frac{1}{k}-1} +$$

$$+\left|\frac{1}{k}\int_1^N \lambda^{\frac{1}{k}-1} e(\rho\lambda) - \frac{1}{k}\sum_{x=1}^{N} x^{\frac{1}{k}-1} e(\rho x) + \frac{1}{2k}e(\rho) + \frac{1}{2k}e(\rho N)N^{\frac{1}{k}-1}\right| \leqslant$$

$$\leqslant c_{13}(k) + \frac{1}{k}\left|\int_1^N (\lambda - [\lambda] - \tfrac{1}{2})\,d(\lambda^{\frac{1}{k}-1} e(\rho\lambda))\right| \leqslant$$

$$\leqslant c_{13}(k) + \frac{1}{2k}\int_1^N \left|2\pi\rho\, e(\rho\lambda)\lambda^{\frac{1}{k}-1} + e(\rho\lambda)(\tfrac{1}{k}-1)\lambda^{\frac{1}{k}-2}\right| d\lambda \leqslant$$

$$\leqslant c_{13}(k) + \frac{\pi}{k}|\rho|\int_1^N \lambda^{\frac{1}{k}-1}\,d\lambda + \int_1^N \lambda^{\frac{1}{k}-2}\,d\lambda \leqslant$$

$$\leqslant c_{14}(k) + \pi|\rho|\, N^{\frac{1}{k}} < c_{12}(k).$$

<u>Stelling 34.</u> Ligt α op de M (major arc) met bijbehorende breuk $\frac{a}{q}$, dan is

$$\left|T^s(\alpha) - q^{-s}S^s(\tfrac{a}{q})V^s(\alpha-\tfrac{a}{q})\right| < c_{15}(k)q^{-2}P^{4k-1}.$$

<u>Bewijs:</u> Uit

$$|u^s - v^s| = |u-v|\left|u^{s-1} + u^{s-2}v + \ldots + v^{s-1}\right| \leqslant s|u-v|\mathrm{Max}^{s-1}(|u|,|v|)$$

volgt ($\beta = \alpha - \frac{a}{q}$)

$$\left|T^s(\alpha) - q^{-s}S^s(\tfrac{a}{q})V^s(\beta)\right| \leqslant s\left|T(\alpha) - q^{-1}S(\tfrac{a}{q})V(\beta)\right|\mathrm{Max}^{s-1}(|T(\alpha)|, |q^{-1}S(\tfrac{a}{q})V(\beta)|).$$

Volgens stelling 33 is dus

$$(4)\quad \left|T^s(\alpha) - q^{-s}S^s(\tfrac{a}{q})V^s(\beta)\right| \leqslant c_{16}(k)q\,\mathrm{Max}^{s-1}(|T(\alpha)|, |q^{-1}S(\tfrac{a}{q})V(\beta)|).$$

Omdat

$$|V(\beta)| \leqslant \frac{1}{k}\sum_{x=1}^{N} x^{\frac{1}{k}-1} < \frac{1}{k}\int_1^N \lambda^{\frac{1}{k}-1}\,d\lambda = P,$$

volgt uit <u>stelling 13</u>

$$(5)\quad \left|q^{-1}S(\tfrac{a}{q})V(\beta)\right| \leqslant c_3(k)q^{-\frac{1}{k}}P.$$

Uit stelling 33 volgt dus

$$|T(\alpha)| \leqslant |T(\alpha) - q^{-1}S(\tfrac{a}{q})V(\beta)| + \left|q^{-1}S(\tfrac{a}{q})V(\beta)\right| \leqslant c_{11}(k)q + c_3(k)q^{-\frac{1}{k}}P.$$

Op M is $P > q^2$, dus $q^{-\frac{1}{k}}P > q^{2-\frac{1}{k}} > q$, zodat

$$(6)\quad |T(\alpha)| < (c_{11}(k) + c_3(k))q^{-\frac{1}{k}}P.$$

Uit (4), (5) en (6) volgt nu

$$\left|T^s(\alpha) - q^{-s}S^s(\tfrac{a}{q})V^s(\beta)\right| < c_{15}(k)q^{1-\frac{s-1}{k}}P^{s-1} < c_{15}(k)q^{-2}P^{4k-1}.$$

Stelling 35. Voor iedere M (major arc) en ieder natuurlijk getal n geldt

$$\left| \int_M e(-n\beta) V^s(\beta)\, d\beta - D(k,n) \right| \leqslant c_{17}(k) q P^{3k-\frac{1}{2}}.$$

Bewijs: Uit de definities (p. 40 en 45) blijkt

$$(7) \qquad \left| \int_M e(-n\beta) V^s(\beta)\, d\beta - D(n) \right| \leqslant \int_{-\frac{1}{2}}^{-\frac{1}{2}} |V^s(\beta)|\, d\beta + \int_{\frac{1}{2}}^{\frac{1}{2}} |V^s(\beta)|\, d\beta.$$

Om dit te benutten, bepalen we een bovengrens voor $|V(\beta)|$, waarbij $0 < |\beta| \leqslant \frac{1}{2}$. We merken eerst even op, dat $(a \leqq b)$

$$\left| \sum_{x=a}^{b} e(\beta x) \right| = \left| e(\beta a) \frac{e(\beta(b-a+1))-1}{e(\beta)-1} \right| \leqslant \frac{2}{\sin \pi |\beta|} \leqslant \frac{2}{\frac{2}{\pi} \pi |\beta|} = \frac{1}{|\beta|}.$$

We schrijven nu

$$V(\beta) = \frac{1}{k}\left(\sum_{x=1}^{Q} x^{\frac{1}{k}-1} e(\beta x) + \sum_{x=Q+1}^{N} x^{\frac{1}{k}-1} e(\beta x)\right) = \frac{1}{k}(\Sigma_1 + \Sigma_2),$$

waarin Q een straks te kiezen natuurlijk getal $\leqq N$ is.

Voor Σ_1 bepalen we een bovengrens als volgt

$$|\Sigma_1| \leqslant \sum_{x=1}^{Q} x^{\frac{1}{k}-1} < \int_0^Q \lambda^{\frac{1}{k}-1}\, d\lambda = k Q^{\frac{1}{k}}.$$

Σ_2 gaan we partieël sommeren (Abel). Wordt $S(Q) = 0$ en voor $Q+1 \leqq x < N$ gesteld $S(x) = \sum_{h=Q+1}^{x} e(\beta h)$, dan is

$$|\Sigma_2| = \left| \sum_{x=Q+1}^{N} x^{\frac{1}{k}-1} (S(x)-S(x-1)) \right| = \left| \sum_{x=Q+1}^{N} x^{\frac{1}{k}-1} S(x) - \sum_{x=Q}^{N=1} (x+1)^{\frac{1}{k}-1} S(x) \right| =$$

$$= \left| \sum_{x=Q+1}^{N-1} (x^{\frac{1}{k}-1} - (x+1)^{\frac{1}{k}-1}) S(x) + N^{\frac{1}{k}-1} S(N) \right| \leqslant$$

$$\leqslant \frac{1}{|\beta|} \sum_{x=Q+1}^{N-1} (x^{\frac{1}{k}-1} - (x+1)^{\frac{1}{k}-1}) + \frac{1}{|\beta|} N^{\frac{1}{k}-1} < \frac{1}{|\beta|} (Q+1)^{\frac{1}{k}-1}.$$

Derhalve is $|V(\beta)| < Q^{\frac{1}{k}} + \frac{1}{|\beta|}(Q+1)^{\frac{1}{k}-1}$. Kiezen we $Q = \left[\mathrm{Min}\left(\frac{1}{|\beta|}, N\right) \right]$, dan vinden we $|V(\beta)| < 2|\beta|^{\frac{1}{k}}$.

Gebruik makende van (7) en de op p. 40 genoemde grenzen voor ϑ_1 en ϑ_2 krijgen we

$$\left| \int_M e(-n\beta) V^s(\beta)\, d\beta - D(n) \right| \leqslant 2 \int_{\frac{1}{2qP^{k-\frac{1}{2}}}}^{\frac{1}{2}} 2^s |\beta|^{\frac{s}{k}}\, d\beta <$$

$$< 2^{4k+1} \int_{\frac{1}{2qP^{k-\frac{1}{2}}}}^{\infty} \beta^{-4}\, d\beta < c_{17}(k) q^3 P^{3k-1\frac{1}{2}} < c_{17}(k) q P^{3k-\frac{1}{2}}.$$

Stelling 36. Voor ieder natuurlijk getal n is

$$\left| \sum_{M} \int_{M} e(-n\alpha) T^s(\alpha) - D(k,n) \sum_{q \leq \sqrt{P}} A(q,n) \right| < c_{18}(k) P^{3k-\frac{1}{2}}.$$

Bewijs: De lengte van iedere M is $\leqq \frac{2}{qP^{k-\frac{1}{2}}}$ op iedere M is volgens stelling 34 ($\alpha = \frac{a}{q} + \beta$)

$$\left| e(-n\alpha) T^s(\alpha) - q^{-s} S^s(\tfrac{a}{q}) e(-\tfrac{an}{q}) e(-n\beta) V^s(\beta) \right| < c_{15}(k) q^{-2} P^{4k-1}.$$

Dus is voor iedere M

$$\left| \int_{M} e(-n\alpha) T^s(\alpha) d\alpha - q^{-s} S^s(\tfrac{a}{q}) e(-\tfrac{an}{q}) \int_{M} e(-n\beta) V^s(\beta) d\beta \right| <$$

$$< c_{19}(k) q^{-3} P^{3k-\frac{1}{2}}.$$

Uit stelling 13 en 35 volgt nu, dat voor iedere M geldt

$$\left| \int_{M} e(-n\alpha) T^s(\alpha) d\alpha - D(k,n) q^{-s} S^s(\tfrac{a}{q}) e(-\tfrac{an}{q}) \right| <$$

$$< c_{19}(k) q^{-3} P^{3k-\frac{1}{2}} + c_3^s(k) q^{-s} q^{s(1-\frac{1}{k})} c_{17}(k) q P^{3k-\frac{1}{2}} =$$

$$= c_{20}(k) q^{-3} P^{3k-\frac{1}{2}}.$$

Sommatie over M geeft (verg. pag. 32)

$$\left| \sum_{M} \int_{M} e(-n\alpha) T^s(\alpha) - D(k,n) \sum_{q \leq \sqrt{P}} A(q,n) \right| <$$

$$< c_{20}(k) P^{3k-\frac{1}{2}} \sum_{q \leq \sqrt{P}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} q^{-3} <$$

$$< c_{20}(k) P^{3k-\frac{1}{2}} \sum_{q=1}^{\infty} q^{-2} = c_{18}(k) P^{3k-\frac{1}{2}}.$$

MATHEMATISCH CENTRUM,
2de Boerhaavestr. 49,
A M S T E R D A M - O.

Colloquium
G E T A L L E N T H E O R I E

o.l.v. Prof. Dr S.C. van Veen
12e Voordracht, 9 April 1952

De stelling van Vinogradow over het probleem van Waring VI

Spreker: Dr W. Verdenius.

Om stelling 36 te kunnen benutten, moeten we eerst de functie $D(k,n,N)$ nader onderzoeken.

Stelling 37. I Voor ieder natuurlijk getal n geldt

$$D(k,n) < c_{21}(k)P^{3k}.$$

II Voor ieder natuurlijk getal $n \geqslant s$ met $\frac{1}{4}N \leqslant n < N$[1] geldt

$$D(k,n) > \frac{1}{c_{22}(k)} P^{3k}.$$

Bewijs: We brengen eerst $D(k,n)$ in een andere gedaante

$$D(k,n) = \int_{-\frac{1}{2}}^{+\frac{1}{2}} e(-n\beta)V^s(\beta)\,d\beta = \frac{1}{k^s}\int_{-\frac{1}{2}}^{+\frac{1}{2}} \sum_{x_1=1}^{N} \cdots \sum_{x_s=1}^{N} (x_1 \cdots x_s)^{\frac{1}{k}-1} e((-n+x_1+\ldots+x_s)\beta)\,d\beta =$$

$$(8) \qquad = \frac{1}{k^s} \sum_{\substack{x_1=1 \\ x_1+\ldots+x_s=n}}^{N} \cdots \sum_{x_s=1}^{N} (x_1 \cdots x_s)^{\frac{1}{k}-1}.$$

Zij $Q = \min(n,N)$. Bij de sommatie in (8) is $x_1+\ldots+x_s = n$. Ten minste een der x_i voldoet dus aan $x_i \geqslant \frac{n}{s} \geqslant \frac{Q}{s}$. Alle x_i voldoen aan $x_i \leqslant n$. Omdat ook $x_i \leqslant N$ is dus $x_i \leqslant Q$. Op grond van de symmetrie van (8) is dus

$$D(k,n) \leqslant \frac{s}{k^s} \sum_{x_1=1}^{Q} \cdots \sum_{x_{s-1}=1}^{Q} (x_1 \cdots x_{s-1}\,\frac{Q}{s})^{\frac{1}{k}-1} \leqslant c_{23}(k)Q^{\frac{1}{k}-1}\Big(\sum_{x=1}^{Q} x^{\frac{1}{k}-1}\Big)^{s-1} \leqslant$$

$$\leqslant c_{23}(k)Q^{\frac{1}{k}-1}(kQ^{\frac{1}{k}})^{s-1} = c_{21}(k)Q^{\frac{s}{k}-1} \leqslant c_{21}(k)N^3 = c_{21}(k)P^{3k},$$

waarmede I bewezen is.

Voor het bewijs van II merken we op, dat voor $n < N$ uit (8) volgt

---

1) De grenzen $\frac{1}{4}N$ en N zijn slechts in verband met de toepassing aldus gekozen en zijn niet de uiterste grenzen.

$$D(k,n) = \frac{1}{k^s} \sum_{\substack{x_1+\ldots+x_s=n \\ x_i>0}} (x_1 \ldots x_s)^{\frac{1}{k}-1} \quad 1)$$

Omdat voor positieve getallen het meetkundig gemiddelde niet groter is dan het rekenkundig gemiddelde, is

$$D(k,n) \geqslant \frac{1}{k^s} \sum_{\substack{x_1+\ldots+x_s=n \\ x_i>0}} \left(\frac{1}{s}(x_1+\ldots+x_s)\right)^{s(\frac{1}{k}-1)} \geqslant$$

$$\geqslant \frac{1}{c_{24}(k)} n^{s(\frac{1}{k}-1)} \sum_{\substack{x_1+\ldots+x_s=n \\ x_i>0}} 1 \geqslant \frac{1}{c_{24}(k)} n^{s(\frac{1}{k}-1)} \left[\frac{n}{s}\right]^{s-1}.$$

Omdat $n \geqslant s$ en $\geqslant \frac{1}{4}N$ is dus

$$D(k,n) \geqslant \frac{1}{2^{s-1}s^{s-1}c_{24}(k)} n^{\frac{s}{k}-1} > \frac{1}{c_{22}(k)} N^3 = \frac{1}{c_{22}(k)} P^{3k}.$$

Stelling 38. Voor ieder natturlijk getal n is

$$\left| \sum_{M} \int_{M} e(-n\alpha) T^s(\alpha) - D(k,n) \mathfrak{J}(k,n) \right| < c_{25}(k) P^{3k-\frac{1}{2}}.$$

Bewijs: In stelling 36 bewezen we voor ieder natuurlijk getal n

$$(9) \qquad \left| \sum_{M} \int_{M} e(-n\alpha) T^s(\alpha) - D(k,n) \sum_{q<\sqrt{P}} A(q,n) \right| < c_{18}(k) P^{3k-\frac{1}{2}}.$$

We moeten dit resultaat nu zo veranderen, dat $\sum_{q<\sqrt{P}} A(q,n)$ vervangen wordt door $\mathfrak{J}(k,n) = \sum_{q=1}^{\infty} A(q,n)$. Uit stelling 14 volgt

$$\left| \mathfrak{J}(n) - \sum_{q<\sqrt{P}} A(q,n) \right| \leqslant c_5(k) \sum_{q \geqslant \sqrt{P}} q^{1-\frac{s}{k}} = c_5(k) \sum_{q \geqslant \sqrt{P}} q^{-3} <$$

$$< c_{26}(k) P^{-1} < c_{26}(k) P^{-\frac{1}{2}}.$$

In verband met stelling 37 I vinden we dus

$$(10) \qquad \left| D(k,n) \sum_{q<\sqrt{P}} A(q,n) - D(k,n) \mathfrak{J}(k,n) \right| < c_{21}(k) c_{26}(k) P^{3k-\frac{1}{2}}.$$

Uit (9) en (10) volgt de bewering.

Stelling 39. Voor $N > c_{27}(k)$ en iedere n met $\frac{1}{4}N \leqslant n < N$ is

$$\mathrm{Re} \sum_{M} \int_{M} e(-n\alpha) T^s(\alpha)\, d\alpha > \frac{1}{c_{28}(k)} P^{3k}.$$

---

1) Als dus $n < N$ mogen we schrijven $D(k,n)$ i.p.v. $D(k,n,N)$. Daarom is reeds in het voorafgaande de afhankelijkheid van N niet steeds uitdrukkelijk vermeld.

Bewijs: Volgens stelling 37 is D(k,n) reëel en volgens stelling 26 is $\mathfrak{J}'(k,n)$ reëel. Uit stelling 38 volgt nu dat voor iedere n geldt

$$\left| \operatorname{Re} \sum_M \int_M e(-n\alpha) T^s(\alpha)\, d\alpha - D(\mathbf{k},n)\mathfrak{J}'(k,n) \right| < c_{25}(k) P^{3k-\frac{1}{2}}$$

en dus ook

$$\operatorname{Re} \sum_M \int_M e(-n\alpha) T^s(\alpha)\, d\alpha > D(k,n)\mathfrak{J}'(k,n) - c_{25}(k) P^{3k-\frac{1}{2}}.$$

In verband met stelling 26 en 37 II zien we dat voor $N \geqslant 4s$ en $\frac{1}{4}N \leqslant n < N$ geldt

$$\operatorname{Re} \sum_M \int_M e(-n\alpha) T^s(\alpha)\, d\alpha > \frac{1}{c_4(k) c_{22}(k)} P^{3k} - c_{25}(k) P^{3k-\frac{1}{2}} =$$

$$= \frac{P^{3k}}{c_{29}(k)} \left(1 - \frac{c_{30}(k)}{\sqrt{P}}\right) > \frac{P^{3k}}{2c_{29}(k)},$$

als bovendien $\sqrt{P} > 2c_{30}(k)$ of $N > (2c_{30}(k))^{2k}$ is. Hiermee is het bewijs geleverd.

Stelling 40. Voor $N > c_{27}(k)$ is

$$\operatorname{Re} \sum_M \int_M e(-N\alpha) T^s(\alpha) R^2(\alpha) S(\alpha)\, d\alpha > \frac{1}{c_{28}(k)} P^{3k} R'^2 S';$$

waarin R' en S' het aantal termen van $R(\alpha)$ resp. $S(\alpha)$ voorstellen.

Bewijs: We beginnen met op te merken (verg. p. 41)

$$e(-N\alpha) T^s(\alpha) R^2(\alpha) S(\alpha) = \sum_{u_1,u_2,y,u_3} e((u_1 + u_2 + y^k u_3 - N)\alpha) T^s(\alpha),$$

waarin u_1 en u_2 de R' getallen u van $R(\alpha)$ en y_3, u_3 de S' getallenparen y,u van $S(\alpha)$ doorlopen. Stellen we

$$n = N - u_1 - u_2 - y^k u_3,$$

dan geldt voor ieder systeem u_1, u_2, y, u_3 waarover gesommeerd wordt

$$N > n \geqslant N - \tfrac{1}{4}N - \tfrac{1}{4}N - \tfrac{1}{4}P^{\frac{1}{2}} P^{k-\frac{1}{2}} = \frac{N}{4}.$$

Is dus $N > c_{27}(k)$, dan is volgens stelling 39

$$\operatorname{Re} \sum_M \int_M e(-N\alpha) T^s(\alpha) R^2(\alpha) S(\alpha)\, d\alpha =$$

$$= \sum_{u_1,u_2,y,u_3} \operatorname{Re} \sum_M \int_M e(-n\alpha) T^s(\alpha)\, d\alpha > \frac{1}{c_{28}(k)} P^{3k} R'^2 S'.$$

MATHEMATISCH CENTRUM,
2de Boerhaavestr. 49,
Amsterdam O.

Colloquium
GETALLENTHEORIE
o.l.v. Prof. Dr S.C. van Veen
13e Voordracht, 28 Mei 1952

De stelling van Vinogradow over het probleem van Waring VII

Spreker: Dr W. Verdenius.

§ 6. De "Minor Arcs".

In deze paragraaf wordt de stelling van Vinogradow (stelling 31) toegepast.

Stelling 41. Op iedere m is

$$|S(\alpha)| < c_{31}(k)P^{\frac{k}{2}-\frac{1}{4}}\sqrt{S'\log P},$$

waarin S' het aantal termen van $S(\alpha)$ voorstelt.

Bewijs: Stel m behoort bij de Fareybreuk $\frac{a}{q}$. Dan is dus

$$\left|\alpha - \frac{a}{q}\right| \leqq \frac{1}{q^2}, \quad (a,q) = 1 \text{ en } P^{\frac{1}{2}} \leqq q \leqq P^{k-\frac{1}{2}}.$$

In de som die $S(\alpha)$ definieert, doorloopt y^k juist $\left[P^{\frac{1}{2k}}\right]$ verschillende natuurlijke getallen $\leqq P^{\frac{1}{2}}$, die dus alle $\leqq q$ zijn. Verder wordt u uitgestrekt over $S'\left[P^{\frac{1}{2}k}\right]^{-1}$ verschillende natuurlijke getallen $\leqq \frac{1}{4}P^{k-\frac{1}{2}}$.

Stelling 31 geeft

$$|S(\alpha)|^2 < 32\left[P^{\frac{1}{2k}}\right]S'\left[P^{\frac{1}{2k}}\right]^{-1}\tfrac{1}{4}P^{k-\frac{1}{2}}\log q.$$

Hieruit volgt de stelling omdat $q < P$.

Stelling 42.

$$\mathrm{Re}\sum_m \int_m e(-N\alpha)T^s(\alpha)R^2(\alpha)S(\alpha)d\alpha > -c_{31}(k)P^{\frac{9}{2}k-\frac{1}{4}}R'\sqrt{S'\log P},$$

als R' en S' het aantal termen van $R(\alpha)$, resp. $S(\alpha)$ voorstellen.

Bewijs: Uit de definitie van $T(\alpha)$ blijkt

$$|T(\alpha)| \leqq P.$$

Stelling 41 geeft dus

$$\left|\sum_m \int_m e(-N\alpha)T^s(\alpha)R^2(\alpha)S(\alpha)d\alpha\right| < c_{31}(k)P^{\frac{9}{2}k-\frac{1}{4}}\sqrt{S'\log P}\int_0^1 |R^2(\alpha)|d\alpha.$$

De hierin optredende integraal behandelen we even afzonderlijk

$$\int_0^1 |R^2(\alpha)|d\alpha = \sum_{\substack{u_1 \leqq \frac{1}{4}P^k \\ u_1 \text{ in } H_1}} \sum_{\substack{u_2 \leqq \frac{1}{4}P^k \\ u_2 \text{ in } H_1}} \int_C e((u_1-u_2)\alpha)d\alpha = R'.$$

Uit het voorgaande volgt de stelling door nog te bedenken, dat voor complexe getallen β geldt $\mathrm{Re}\,\beta \geqslant -|\beta|$.

§ 7. De stelling van Vinogradow.

R' en S' stellen weer het aantal termen voor van $R(\alpha)$, resp. $S(\alpha)$. We verenigen vooreerst de resultaten van § 5 en § 6.

Stelling 43. Voor $N > c_{27}(k)$ is

$$\mathrm{Re}\int_0^1 e(-N\alpha)T^s(\alpha)R^2(\alpha)S(\alpha)\,d\alpha > \frac{1}{c_{28}(k)}\,P^{3k}R'^2S'\left(1-c_{32}(k)\,\frac{P^{\frac{3}{2}k-\frac{1}{4}}\sqrt{\log P}}{R'\sqrt{S'}}\right).$$

Bewijs: Omdat

$$\mathrm{Re}\int_0^1 = \mathrm{Re}\sum_M \int_M + \mathrm{Re}\sum_m \int_m$$

geven stelling 40 en 42 de bewering als $c_{32}(k) = c_{31}(k)c_{28}(k)$ genomen wordt.

Indachtig aan ons doel - te bewijzen dat $\int_0^1 > 0$ - , hebben we nu nog een bovengrens nodig voor $R'\sqrt{S'}$. Hiervoor dient de volgende stelling:

Stelling 44. Zij $l > 1, Q \geqslant 1$. Dan is

$$H_l(Q) > \frac{1}{c_{33}(k,l)}\,Q^{1-(1-\frac{1}{k})^l}.$$

Bewijs: Voor $l = 1$ is

$$H_1(Q) = H_1(Q) = \left[Q^{\frac{1}{k}}\right] > \tfrac{1}{2}Q^{\frac{1}{k}} = \frac{1}{c_{34}}\,Q^{1-(1-\frac{1}{k})^1}.$$

Zij nu $l > 1$ en de bewering juist als we l door $l-1$ vervangen. We onderscheiden daarbij twee gevallen:

1) Zij $1 \leqq Q < 8^k$. Omdat 1 tot H_l behoort, is

$$H_l(Q) \geqslant 1 > \frac{1}{8^k}\,Q = \frac{1}{c_{35}(k)}\,Q \geqslant \frac{1}{c_{35}(k)}\,Q^{1-(1-\frac{1}{k})^l}.$$

2) Zij $Q \geqslant 8^k$. De getallen v^k+z, met

$$\tfrac{1}{2}Q^{\frac{1}{k}} \leqq v \leqq Q^{\frac{1}{k}} - 1,\quad z \leqq (\tfrac{1}{2}Q^{\frac{1}{k}})^{k-1},\quad z \text{ in } H_{l-1}$$

liggen in H_l; verder zijn ze $\leqq Q$ en verschillend, omdat

$$v^k < v^k + z \leqq v^k + v^{k-1} < (v+1)^k \leqq Q.$$

Dus is

$$H_l(Q) \geqslant ((Q^{\frac{1}{k}} - 1) - \tfrac{1}{2}Q^{\frac{1}{k}} - 1)H_{l-1}(\frac{1}{2^{k-1}}\,Q^{1-\frac{1}{k}}) \geqslant$$

$$\geqslant (\tfrac{1}{2}Q^{\frac{1}{k}} - 2)\,\frac{1}{c_{33}(k,l-1)}\,(\frac{1}{2^{k-1}}\,Q^{1-\frac{1}{k}})^{1-(1-\frac{1}{k})^{l-1}} \geqslant$$

$$\geqslant \tfrac{1}{4}Q^{\frac{1}{k}}\,\frac{1}{c_{33}(k,l-1)2^{k-1}}\,Q^{1-\frac{1}{k}-(1-\frac{1}{k})^l} = \frac{1}{c_{33}(k,l)}\,Q^{1-(1-\frac{1}{k})^l}.$$

In de nu volgende stellingen wordt $l = \left[k \log(6k^2)\right] + 1$ gesteld.

Stelling 45. Voor $N > c_{36}(k)$ is

$$\mathrm{Re}\int_0^1 e(-N\alpha)T^s(\alpha)R^2(\alpha)S(\alpha)\,d\alpha > 0.$$

Bewijs: Uit de definities van $R(\alpha)$ en $S(\alpha)$ blijkt

$$R'\sqrt{S'} = H_1(\tfrac{1}{4}P^k)\left(\left[P^{\frac{1}{2k}}\right] H_1(\tfrac{1}{4}P^{k-\frac{1}{2}})\right)^{\frac{1}{2}}.$$

Met behulp van stelling 44 volgt hieruit

$$R'\sqrt{S'} > \frac{1}{c_{37}(k)} P^{k(1-(1-\frac{1}{k})^l)+\frac{1}{4k}+\frac{1}{2}(k-\frac{1}{2})(1-(1-\frac{1}{k})^l)} =$$

$$= \frac{1}{c_{37}(k)} P^{\frac{3}{2}k-\frac{1}{4}+\frac{1}{4k}-(\frac{3}{2}k-\frac{1}{4})(1-\frac{1}{k})^l}.$$

Omdat

$$(1-\tfrac{1}{k})^l = e^{l\log(1-\frac{1}{k})} < e^{-\frac{l}{k}} < e^{-\log 6k^2} = \frac{1}{6k^2}$$

is dus

$$R'\sqrt{S'} > \frac{1}{c_{37}(k)} P^{\frac{3}{2}k-\frac{1}{4}+\frac{1}{4k}-\frac{1}{4k}+\frac{1}{24k^2}} = P^{\frac{3}{2}k-\frac{1}{4}+\frac{1}{24k^2}}.$$

Voor $N > c_{38}(k)$ is dus

$$c_{32}(k)\frac{P^{\frac{3}{2}k-\frac{1}{4}}\sqrt{\log P}}{R'\sqrt{S'}} < c_{39}(k)P^{-\frac{1}{4k^2}}\sqrt{\log P} < 1.$$

Dus is volgens stelling 43 voor $N > c_{36}(k) = \max(c_{27}(k), c_{38}(k))$ de stelling juist.

Stelling 46. $$G(k) \leqq 6k\log k + c_{40}k.$$

Bewijs: Uit de definities van $T(\alpha)$, $R(\alpha)$ en $S(\alpha)$ volgt, dat

$$\int_0^1 e(-N\alpha)T^s(\alpha)R^2(\alpha)S(\alpha)\,d\alpha$$

gelijk is aan het aantal A der oplossingen in natuurlijke getallen $x_1,\ldots,x_s$, u_1,u_2,u_3, y die voldoen aan

$$\begin{cases} N = x_1^k + \ldots + x_s^k + u_1 + u_2 + y^k u_3, \\ x_h \leqq P_1 \quad (h=1,\ldots,s), \\ y \leqq P^{\frac{1}{2k}}, \\ u_h \leqq \tfrac{1}{4}P^k \quad (h=1,2), \\ u_3 \leqq \tfrac{1}{4}P^{k-\frac{1}{2}}, \\ u_h \text{ in } H_1 \quad (h=1,2,3). \end{cases}$$

Dus is $\int_0^1 = \mathrm{Re}\int_0^1$, en volgt uit stelling 45 dat $A > 0$, als $N > c_{36}(k)$. A fortiori is dus dan ook het aantal oplossingen in niet-negatieve gehele getallen $x_1,\ldots,x_{s+3l}$ van

$$N = x_1^k + \ldots + x_{s+3l}^k$$

positief, dus ten minste één. Dus voldoet $G(k)$ (zie § 1) aan

$$G(k) \leqq s+3l = 4k+3\left[k\log(6k^2)\right] + 3 \leqq 6k\log k + c_{40}k.$$