stichting
mathematisch
centrum

MC

AFDELING ZUIVERE WISKUNDE ZC 78/71 JUNI

H.G. MEIJER
CURSUS GETALTHEORIE 1970-1971

2e boerhaavestraat 49 amsterdam

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

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

Inhoud

Inleiding		1
Hoofdstuk I	: Deelbaarheid	5
Hoofdstuk II	: Congruenties	13
Hoofdstuk III	: Arithmetische functies	28
Hoofdstuk IV	: Grootteorde van arithmetische functies	44
Hoofdstuk V	: Priemgetallen	53
Hoofdstuk VI	: Voorstelling van een natuurlijk getal als som van kwadraten	64
Hoofdstuk VII	: Approximatie van reële getallen met rationale getallen	75
Hoofdstuk VIII	: Gelijkverdeling	90
Bibliographie		101
Correcties en aanvullingen		102

CURSUS GETALTHEORIE

door

Dr. H.G. MEIJER.

Inleiding

Getaltheorie - door sommige wiskundigen zoals Euler (1707-1783) als de koningin van de wiskunde beschouwd - heeft het voordeel boven de meeste andere takken van de wiskunde, dat het mogelijk is niet-triviale getaltheoretische problemen zo eenvoudig te formuleren, dat ze ook door niet-wiskundigen te begrijpen zijn. De oplossing van deze problemen is daarentegen meestal verre van eenvoudig en is vaak aanleiding tot de ontwikkeling van geheel nieuwe takken van de wiskunde. Op deze wijze heeft de getaltheorie steeds de ontwikkeling van andere gebieden van de wiskunde gestimuleerd, in het bijzonder de compleze functietheorie en de algebra. We geven hier twee voorbeelden van getaltheoretische problemen die een belangrijke invloed op de ontwikkeling van de wiskunde hebben gehad:

1e) de verdeling van de priemgetallen, 2e) de laatste stelling van Fermat.

Verdeling van priemgetallen

Een geheel getal $p > 1$, dat niet het product is van twee andere positieve gehele getallen, beide kleiner dan p, heet een priemgetal. Bij het bestuderen van de rij van priemgetallen

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, ...

vallen twee dingen op.

1e) Een grote onregelmatigheid wanneer we de verdeling gedetailleerd beschouwen. Zo kan men eenvoudig aantonen dat er gaten van willekeurige lengte tussen opeenvolgende priemgetallen voorkomen. (Zie hoofdstuk I). Anderzijds komen er ook priemgetaltweelingen voor; dat zijn paren van priemgetallen p en q met $q = p+2$, zoals 11, 13; 29, 31; 41, 43. Men vermoedt dat er oneindig veel van deze priemgetaltweelingen bestaan; dit is evenwel nooit bewezen.

2) Een grote regelmatigheid in de "gemiddelde" verdeling. De dichtheid van de priemgetallen neemt geleidelijk af. Zo komen er in de eerste vijf blokken van 1000 opeenvolgende getallen (1-1000, 1001-2000, enz.) resp. 168, 135, 127, 120 en 119 priemgetallen voor en in de laatste vijf blokken van 1000 opeenvolgende getallen voor 10^7 resp. 62, 58, 67, 64, 53.
Zij $\pi(x)$ het aantal priemgetallen $\leq x$.
Legendre (1752-1833) en Gauss (1777-1855) vermoedden reeds dat

$$(1) \qquad \pi(x) \sim \frac{x}{\log x}$$

d.w.z. dat

$$\lim_{x\to\infty} \pi(x) \frac{\log x}{x} = 1.$$

Tchebycheff (1821-1894) was de eerste die een resultaat in deze richting verkreeg. Hij bewees in 1851-1852 dat er positieve constanten c_1 en c_2 bestaan, $c_1 \leq 1 \leq c_2$ zodat

$$c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x} \qquad \text{voor } x \geq 2.$$

Riemann (1826-1866) bracht in een belangrijk artikel uit 1859 het probleem van de priemgetalverdeling in verband met de eigenschappen van de functie $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$, met complexe variabele s. Dit stimuleerde de ontwikkeling van de complexe functietheorie en in het bijzonder de studie van de gehele functies.
Hiermee bewezen tenslotte Hadamard (1865-1963) en de la Vallée Poussin (1866-1962) onafhankelijk van elkaar in 1896 de geldigheid van (1). Deze relatie staat nu bekend als de priemgetalstelling.
Een andere zeer interessante vraag uit het artikel van Riemann van 1859 is tot op heden onopgelost gebleven: liggen alle niet-triviale nulpunten van $\zeta(s)$ op de lijn Re $s = \frac{1}{2}$? Dit probleem staat bekend als de Riemann-hypothese. Bestudering van dit probleem heeft een grote invloed op de huidige ontwikkeling van de wiskunde.

Laatste stelling van Fermat

In 1637 beweerde Fermat (1601-1665) in een aantekening in de kantlijn van een uitgave van de werken van Diophantos, dat hij een schitterend bewijs had voor de volgende bewering:
de vergelijking

$$x^n + y^n = z^n \quad , \quad n \text{ geheel, } n > 2$$

heeft geen oplossing in positieve gehele getallen x, y en z.
Men is er echter later nooit in geslaagd dit te bewijzen, zodat Fermat zich vermoedelijk vergist heeft. De bewering is nu bewezen voor $2 < n < \pm 4002$. Dit probleem heeft grote invloed gehad op de ontwikkeling van de wiskunde, in het bijzonder op de theorie van de algebraïsche getallen en zodoende op de algebra.

Men kan de getaltheorie onderverdelen in verschillende elkaar gedeeltelijk overlappende gebieden zoals o.a.

a) multiplicatieve getaltheorie, die problemen samenhangende met de vermenigvuldiging bestudeert; in het bijzonder de verdeling van priemgetallen.

b) additieve getaltheorie, die optelproblemen behandelt, zoals de vraag hoe een getal te schrijven is als som van bepaalde andere getallen.

c) Diophantische vergelijkingen; dat zijn vergelijkingen in gehele getallen zoals de bovengenoemde "stelling" van Fermat. De naam komt van de Griekse wiskundige Diophantos van Alexandrie (3e - 4e eeuw na Chr.) die als eerste dit soort problemen bestudeerde.

d) analytische getaltheorie, die gebruik maakt van methoden uit de analyse, in het bijzonder uit de complexe functietheorie; zie de priemgetalstelling.

e) algebraïsche getaltheorie, die gebruik maakt van de algebra.

In deze cursus zullen we eerst de belangrijkste stellingen uit de elementaire getaltheorie bespreken en daarna enkele onderwerpen uit de analytische getaltheorie behandelen.

Notaties

Z : verzameling van de gehele getallen.
Q : verzameling van de rationale getallen.
R : verzameling van de reële getallen.
C : verzameling van de complexe getallen.

Literatuur bij inleiding

(Voor nadere gegevens over de genoemde boeken zie de bibliographie achter in de syllabus).

E. Grosswald: Topics from the theory of numbers, Part I.

W.J. LeVeque: Topics in number theory, volume I, Chapter 1.

Hoofdstuk I: Deelbaarheid

Definitie 1. Zij $a \in Z$, $b \in Z$ en $b \neq 0$. Het getal a heet deelbaar door b als er een $c \in Z$ bestaat zodat $bc = a$. Men zegt in dit geval ook b is een deler van a, b deelt a en a is een veelvoud van b.

Notaties.

$b \mid a$ betekent b is een deler van a.
$b \nmid a$ betekent b is geen deler van a.

Gevolgen.

1. Is $a \in Z$ $a \neq 0$ dan geldt $1 \mid a$ en $a \mid a$; is $b \in Z$ $b \neq 0$ en $b \mid a$ met $b \neq 1$, $b \neq a$ dan heet b wel een echte deler van a.
2. Zijn $a > 0$ en $b > 0$ gehele getallen en $b \mid a$ dan is $1 \leq b \leq a$.
3. Zijn a, b en $c \neq 0$ gehele getallen, dan volgt uit $c \mid a$, $c \mid b$ dat $c \mid ma+nb$ voor alle $m \in Z$, $n \in Z$.

Definitie 2. Een geheel getal $p > 1$ heet priemgetal, als p geen echte delers bezit. Een geheel getal $n > 1$ dat geen priemgetal is, heet samengesteld.

Stelling 1. Ieder geheel getal $n > 1$ is te schrijven als product van priemfactoren.

Bewijs. Is n priem dan is n het product van 1 factor. Is n samengesteld dan is $n = n_1 n_2$ met $1 < n_1 < n$, $1 < n_2 < n$. Is n_1 en (of) n_2 samengesteld, dan is deze nog verder te splitsen. Dit proces loopt na een eindig aantal stappen af.

Definitie 3. Is $n \in Z$, $n > 1$ en is

$$(1) \qquad n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$$

met $p_1, p_2, \ldots, p_k$ priemgetallen, $a_i > 0$ $(i = 1,2,\ldots,k)$ en is $p_1 < p_2 < \ldots < p_k$, dan heet (1) de kanonieke ontbinding van n.

Stelling 2. (hoofdstelling van de rekenkunde)
Is $n \in Z$, $n > 1$, dan is de kanonieke ontbinding eenduidig.

Stelling 2 is minder vanzelfsprekend dan hij in eerste instante lijkt, zoals het volgende voorbeeld aantoont.

Voorbeeld. Zij E de verzameling van de positieve even getallen. We merken op dat het product van twee even getallen steeds weer een even getal is. Een getal uit E noemen we E-priemgetal als het niet te schrijven is als product van twee andere getallen uit E. E-priemgetallen zijn dan bijvoorbeeld 2, 6, 10 en 30. Nu is $60 = 2.30 = 6.10$ zodat 60 op twee verschillende manieren als product van E-priemgetallen te schrijven is. In de verzameling E is de ontbinding in E-priemgetallen dus niet eenduidig. Voor andere voorbeelden zie Niven, Zuckerman pag. 11-13 en Grosswald pag. 28-30.

Voor het bewijs van stelling 2 zullen we een aantal stellingen afleiden, die ook op zich zelf interessant zijn.

Stelling 3. (delingsalgorithme).
Zijn $a \in Z$, $b \in Z$ met $a > 0$ dan bestaan er precies één $q \in Z$ en één $r \in Z$ zodat

$$b = qa + r \ , \quad 0 \leq r \leq a \ .$$

Bewijs. Beschouw de veelvouden van a: na, $n = 0, \pm 1, \pm 2, \ldots$. Er is precies één $q \in Z$ met

$$qa \leq b < (q+1)a \ ,$$

zodat $b = qa + r$ met $0 \leq r < a$.
(Bij toepassing van het delingsalgorithme noemt men r vaak de rest.)

Definitie 4. Een moduul S is een verzameling getallen met de eigenschap dat als $a \in S$ en $b \in S$ dan ook $a-b \in S$.

Opmerkingen.

1. Een triviaal moduul is $S = \{0\}$.
2. Een moduul hoeft niet uit gehele getallen te bestaan.
3. Is $a \neq 0$ en $a \in S$ dan volgt uit de definitie direct $0 \in S$, $-a \in S$, $2a \in S$ en algemeen $na \in S$ voor alle $n \in Z$.
4. Zijn $a \in S$ en $b \in S$ dan is $xa+yb \in S$ voor alle $x \in Z$, $y \in Z$.

Stelling 4. Is $S \neq \{0\}$ een moduul bestaande uit gehele getallen, dan bestaat S juist uit de veelvouden van een zeker positief getal d: $S = \{nd \mid n \in Z\}$.

Bewijs. Zij d het kleinste positieve getal uit S. Volgens opmerking 3 is dan $\{nd \mid n \in Z\} \subset S$. Zij nu b een willekeurig element uit S. Volgens stelling 3 geldt $b = qd + r$ met $0 \leq r < d$. Daar $b \in S$, $qd \in S$ is volgens definitie 4 ook $r = b-qd \in S$. Daar $0 \leq r < d$ en d het kleinste positieve getal uit S is, volgt $r = 0$, zodat $b = qd$. Hieruit volgt het gestelde.

Definitie 5. Zijn $a \in Z$, $b \in Z$ en a en b niet beide 0, dan is de grootste gemene deler van a en b het grootste positieve getal dat zowel a als b deelt; notatie (a,b). Is $(a,b) = 1$ dan heten a en b relatief priem.

Opmerking.

5. Is $a \in Z$, $a \neq 0$ dan is $(0,a) = |a|$.

Stelling 5. Zijn $a \in Z$, $b \in Z$ en a en b niet beide 0, dan bestaat het moduul $S = \{ax+by \mid x \in Z, y \in Z\}$ uit alle veelvouden van $d = (a,b)$.

Bewijs. We merken allereerst op dat S inderdaad een moduul is. Volgens stelling 4 is dus $S = \{nc\}$ voor zekere $c \in Z$, $c > 0$. Daar $a \in S$ en $b \in S$ volgt $c \mid a$ en $c \mid b$. Volgens definitie 5 is $d = (a,b)$ de grootste gemeenschappelijke deler van a en b zodat $c \leq d$.
Anderzijds volgt uit $d \mid a$ en $d \mid b$ dat $d \mid ax+by$ voor alle $x \in Z$ en $y \in Z$ (gevolg 3). Daar $c = ax_0 + by_0$ voor zekere $x_0 \in Z$, $y_0 \in Z$ volgt $d \mid c$ zodat $d \leq c$ (gevolg 1). Hiermee is bewezen $c = d$.

Uit stelling 5 volgen direct de volgende twee stellingen.

Stelling 6. Zijn $a \in Z$, $b \in Z$ en a en b niet beide 0, dan bestaan er $x \in Z$, $y \in Z$ met

$$xa + yb = (a,b) .$$

Stelling 7. Zijn $a \in Z$, $b \in Z$, $n \in Z$ en a en b niet beide 0, dan is de vergelijking

$$ax + by = n$$

dan en slechts dan oplosbaar met gehele x en y als $(a,b) \mid n$.

Stelling 8. (1e stelling van Euclides).
Zijn $p \in Z$, $a \in Z$, $b \in Z$ en p priemgetal dan volgt uit $p \mid ab$ dat $p \mid a$ of $p \mid b$.

Bewijs. Stel $p \nmid a$ dan is $(p,a) = 1$. Volgens stelling 6 zijn er dan $x \in Z$, $y \in Z$ met

$$xp + ya = 1 .$$

Hieruit volg $xpb + yab = b$.
Daar $p \mid xpb$ en volgens het gegeven $p \mid ab$ zodat $p \mid yab$ volgt $p \mid b$. q.e.d.

Uit stelling 8 volgt

Stelling 8a. Zijn $p \in Z$, $a_i \in Z$ $(i = 1,2,\ldots,n)$ en p priemgetal dan volgt uit $p \mid a_1 a_2 \ldots a_n$ dat p minstens één van de getallen $a_1, a_2, \ldots, a_n$ deelt.

Bewijs stelling 2.
Stel dat een geheel getal $n > 1$ twee verschillende kanonieke ontbindingen heeft:

$$(2) \qquad p_1^{a_1} \ldots p_r^{a_r} = q_1^{b_1} \ldots q_k^{b_k} .$$

Daar p_1 het linkerlid deelt, deelt p_1 het rechterlid. Volgens stelling 8a is dan één van de priemgetallen $q_1, \ldots, q_k$ gelijk aan p_1. Op deze

wijze ziet men direct in dat iedere p_i $(i = 1,\ldots,r)$ gelijk moet zijn aan een q_j $(j = 1,\ldots,k)$ en omgekeerd iedere q_j gelijk moet zijn aan een p_i. Dan is (2) te schrijven als

$$p_1^{a_1} \cdots p_r^{a_r} = p_1^{c_1} \cdots p_r^{c_r} .$$

Stel nu dat $a_1 > c_1$ dan volgt na delen door $p_1^{c_1}$

$$p_1^{a_1-c_1} p_2^{a_2} \cdots p_r^{a_r} = p_2^{c_2} \cdots p_r^{c_r} .$$

Nu is het linkerlid deelbaar door p_1 en het rechterlid niet, wat onmogelijk is. Dus is $a_1 = c_1$. Op dezelfde wijze volgt $a_i = c_i$ $(i=2,\ldots,r)$. Voor een ander bewijs van stelling 2 zie Hardy, Wright p. 21 of Niven, Zuckerman p. 14.

Definitie 6. Zijn $a \in Z$, $b \in Z$, $a \neq 0$, $b \neq 0$ dan is het kleinste gemene veelvoud van a en b het kleinste positieve getal dat zowel door a als door b deelbaar is; notatie $[a,b]$.

Stelling 9. Zij $a \in Z$, $b \in Z$ en $a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, $b = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$ met p_i priemgetal en $a_i \geq 0$, $b_i \geq 0$ dan is

$$(a,b) = \prod_{i=1}^{n} p_i^{\min(a_i,b_i)} , \quad [a,b] = \prod_{i=1}^{n} p_i^{\max(a_i,b_i)} .$$

Bewijs. Dit volgt direct uit stelling 2 en definities 5 en 6.

Gevolg.

4. Zijn $a \in Z$, $b \in Z$, $a \neq 0$, $b \neq 0$ dan is $(a,b)[a,b] = |ab|$.

Berekening (a,b). (algorithme van Euclides).
Zij $a \in Z$, $b \in Z$, $a \neq 0$ en $b > 0$ dan kan (a,b) berekend worden volgens stelling 9. Het is vaak eenvoudiger (a,b) te berekenen volgens het algorithme van Euclides dat berust op herhaalde toepassing van stelling 3 en de constatering dat $(b,a) = (b,a+bn)$ voor $n \in Z$. Dit laatste bewijzen we als volgt:

Zij $d = (a,b)$ en $g = (b,a+bn)$.
Uit $d|a$, $d|b$ volgt $d|b$, $d|a+bn$ (gevolg 3), zodat $d \leq g$ (definitie 5).
Uit $g|b$, $g|a+bn$ volgt $g|a$, $g|b$, zodat $g \leq d$.
Dus $d = g$.
Zij

$$\begin{aligned} a &= bq_1 + r_1 & 0 < r_1 < b \\ b &= r_1q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3 & 0 < r_3 < r_2 \\ &\cdots\cdots\cdots & \cdots\cdots \\ r_{j-2} &= r_{j-1}q_j + r_j & 0 < r_j < r_{j-1} \end{aligned}$$

Daar de rest r_j steeds kleiner wordt, breekt dit proces na een eindig aantal stappen af met

$$r_{j-1} = r_jq_{j+1} .$$

Nu is $(b,a) = (b,a-bq_1) = (b,r_1)$,

$(r_1,b) = (r_1,b-r_1q_2) = (r_1,r_2)$,

$(r_{j-1},r_{j-2}) = (r_{j-1},r_{j-2}-r_{j-1}q_j) = (r_{j-1}r_j) = r_j$.

Zodat $(a,b) = r_j$, de laatste restterm in bovenstaand schema. Deze berekening staat bekend als het algorithme van Euclides.

Stelling 10. (2e stelling van Euclides)
Er zijn oneindig veel priemgetallen.

Bewijs. Laten $2,3,5,\ldots,p$ de priemgetallen $\leq$ het priemgetal p zijn.
Zij q het getal

$$q = 2.3.5....p + 1 .$$

Dan is q niet deelbaar door de priemgetallen $2,3,5,\ldots,p$. Dus is q of zelf priem of deelbaar door een priemgetal groter dan p. Dit houdt in dat er bij ieder priemgetal p een groter priemgetal te vinden is. Voor twee andere bewijzen van stelling 10 zie Hardy, Wright p. 14, 16-17.

Het bewijs van stelling 10 geeft een eenvoudige methode om een ondergrens voor de functie $\pi(x)$ - het aantal priemgetallen $\leq x$ - af te leiden. Zij p_n het n^e priemgetal dan volgt uit het bovenstaande

$$p_{n+1} \leq 2.3.5...p_n+1 .$$

Hieruit is met inductie eenvoudig te bewijzen

$$p_n < 2^{2^n} .$$

Zij nu $e^{e^{n-1}} < x \leq e^{e^n}$.
Voor $n \geq 4$ geldt $e^{n-1} > 2^n$, zodat

$$\pi(x) \geq \pi(e^{e^{n-1}}) \geq \pi(2^{2^n}) \geq n \geq \log\log x .$$

Hoewel stelling 10 zeer eenvoudig te bewijzen is, is het bewijs van de volgende, daarmee verwante, stelling zeer moeilijk. We zullen deze stelling daarom hier alleen vermelden.

Stelling 11. (Dirichlet, 1837)
Zijn $a \in Z$, $b \in Z$, $a > 0$, $b \neq 0$, $(a,b) = 1$ dan zijn er oneindig veel priemgetallen van de vorm $an+b$ met $n \in Z$, $n > 0$.

Stelling 12.
Er zijn gaten van willekeurige lengte in de rij van priemgetallen, m.a.w. voor ieder natuurlijk getal k bestaan er k opeenvolgende samengestelde getallen.

Bewijs. Beschouw de k opeenvolgende getallen

$$(k+1)!+2,(k+1)!+3,...,(k+1)!+k,(k+1)!+k+1 .$$

Deze zijn alle samengesteld, want ze zijn deelbaar door respectievelijk $2,3,...,k,k+1$.

Literatuur bij hoofdstuk I.

E. Grosswald: Topics from the theory of numbers, Chapter 3.

G.H. Hardy, E.M. Wright: An introduction to the theory of numbers, Chapter I and II.

I. Niven, H.S. Zuckerman: An introduction to the theory of numbers, Chapter I.

Hoofdstuk II: Congruenties

Definitie 1. Zij a, b, m $\in$ Z en m $\geq$ 1. Als m $\mid$ a-b dan heet a congruent b modulo m; notatie $a \equiv b \pmod{m}$. Als m $\nmid$ a-b dan heet a niet congruent b modulo m; notatie $a \not\equiv b \pmod{m}$.
Uit de definitie volgt direkt:

Stelling 1. Zij a, a_1, b, b_1, k, m $\in$ Z en m $\geq$ 1.
Is $a \equiv a_1 \pmod{m}$ en $b \equiv b_1 \pmod{m}$, dan is

a) $a+b \equiv a_1+b_1 \pmod{m}$,

b) $ka \equiv ka_1 \pmod{m}$,

c) $ab \equiv a_1b_1 \pmod{m}$.

Gevolg 1. Zij m, u, u_1 $\in$ Z en m $\geq$ 1. Zij
$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ met $a_i \in Z$ $(i = 0,1,\ldots,n)$.
Is $u \equiv u_1 \pmod{m}$, dan is $f(u) \equiv f(u_1) \pmod{m}$.

Gevolg 2. (9-proef en 11-proef).
Zij g een getal dat uitgeschreven in cijfers de gedaante heeft
$g = g_ng_{n-1}\ldots g_0$ $(g_i \in 0,1,\ldots,9;\ i = 0,1,\ldots,n)$, dan is

$$g = g_n10^n + g_{n-1}10^{n-1} + \ldots + g_1.10 + g_0.$$

Volgens gevolg 1 met m = 9, u = 10, u_1 = 1 en

$f(x) = g_nx^n + g_{n-1}x^{n-1} + \ldots + g_0$ geldt dan

$$g = f(10) \equiv f(1) = g_n + g_{n-1} + \ldots + g_0 \pmod{9}.$$

Hieruit volgt dat g dan en slechts dan deelbaar is door 9 als de som van zijn cijfers $g_n + \ldots + g_0$ deelbaar is door 9.

---

syll. ZC 78, afl.3.

Analoog volgt met $m = 11$, $u = 10$, $u_1 = -1$ dat

$$g = f(10) \equiv f(-1) = (-1)^n g_n + (-1)^{n-1} g_{n-1} + \ldots + g_0 \pmod{11}$$

zodat g dan en slechts dan deelbaar is door 11 als zijn cijfers afwisselend opgeteld en afgetrokken een 11-voud leveren.

Opmerking 1.
Uit stelling 1 blijkt dat we congruenties kunnen optellen, aftrekken en vermenigvuldigen. We mogen ze echter niet delen zoals blijkt uit het volgende tegenvoorbeeld. Er geldt $2 \equiv 12 \pmod{10}$; echter $1 \not\equiv 6 \pmod{10}$. Bij deling geldt de volgende stelling.

Stelling 2. Zij $a, b, k, m \in Z$, $m \geq 1$ en $d = (k,m)$.
a) $ka \equiv kb \pmod{m} \longleftrightarrow a \equiv b \pmod{\frac{m}{d}}$.
b) Is $(k,m) = 1$, dan is $ka \equiv kb \pmod{m} \longleftrightarrow a \equiv b \pmod{m}$.

Bewijs. a) Zij $k = k_1 d$, $m = m_1 d$, zodat $(k_1, m_1) = 1$, dan is
$ka \equiv kb \pmod{m} \longleftrightarrow m \mid k(a-b) \longleftrightarrow m_1 \mid k_1(a-b)$ en daar $(k_1, m_1) = 1$ is dit aequivalent met $m_1 \mid a-b \longleftrightarrow a \equiv b \pmod{m_1}$.
b) Is een direct gevolg van a).

Restklassen.
De relatie $\equiv \pmod{m}$ is een aequivalentierelatie. Hierdoor wordt Z ingedeeld in aequivalentieklassen van onderling congruente elementen: de restklassen modulo m. Uiteraard liggen $0,1,2,\ldots,m-1$ in verschillende restklassen. Is $n \in Z$, dan is n te schrijven als $n = am+r$ voor zekere $a,r \in Z$ met $0 \leq r < m$. Ofwel $n \equiv r \pmod{m}$. Er zijn dus precies m restklassen modulo m; men noemt ze een volledig stelsel restklassen modulo m. Kiezen we uit iedere restklasse één element (representant) dan vormen de m gekozen elementen een volledig stelsel representanten modulo m. Zo is bijvoorbeeld 5,1,12,23,9 een volledig stelsel representanten modulo 5.

Een voor de hand liggende keuze voor een volledig stelsel representanten modulo m is de keuze 0,1,2,...,m-1.

Optellen van restklassen.

Zijn A en B twee restklassen modulo m. Is $a \in A$, $b \in B$ en laat $a + b$ in restklasse C liggen. Uit stelling 1a volgt nu dat als we in plaats van a en b twee andere elementen $a_1 \in A$, $b_1 \in B$, kiezen, dat dan $a_1 + b_1$ weer in C ligt. Dit stelt ons in staat op natuurlijke wijze een optelling in de verzameling restklassen te definieren : onder A + B verstaan we de restklasse waarin het element a + b ligt als $a \in A$, $b \in B$. Zij N de restklasse $N = \{n \mid n \equiv 0 \pmod{m}\}$, dan is N + A = A voor iedere restklasse A. N is het nulelement voor de optelling van de restklassen modulo m.

Zij A een restklasse en $a \in A$, dan zullen we onder -A verstaan de restklasse $-A = \{n \mid n \equiv -a \pmod{m}\}$ zodat A + (-A) = N. Verder schrijven we B - A voor B + (-A). Met deze definitie van optelling is de verzameling restklassen modulo m een additieve abelse groep.

Vermenigvuldiging van restklassen.

Op analoge wijze kunnen we op grond van stelling 1c een vermenigvuldiging van restklassen definieren: AB is de restklasse waarin ab ligt als $a \in A$, $b \in B$. Zij E de restklasse $E = \{n \mid n \equiv 1 \pmod{m}\}$ dan is AE = A voor alle restklassen A. E is het eenheidselement voor de vermenigvuldiging van restklassen modulo m.

Met deze definities van optelling en vermenigvuldiging is de verzameling van restklassen modulo m een ring. Is m samengesteld, dan is $m = ab$ met $1 < a < m$, $1 < b < m$. Er geldt dan $ab \equiv 0 \pmod{m}$. Zijn A en B de restklassen met $a \in A$, $b \in B$, dan is AB = N, terwijl $A \neq N$, $B \neq N$, d.w.z. de ring heeft nuldelers. Is p priemgetal, dan heeft de ring van restklassen modulo p geen nuldelers.

Inverse.

We onderzoeken nu onder welke voorwaarden een restklasse A een inverse voor de vermeniguvldiging heeft, dat is een restklasse X met AX = E.

Zij $a \in A$, $x \in X$ dan geeft dit de vergelijking $ax \equiv 1 \pmod{m}$. Deze is aequivalent met $ax + my = 1$. Volgens hoofdstuk I stelling 7 is dit dan en slechts dan oplosbaar als $(a,m) \mid 1$, d.w.z. $(a,m) = 1$.
We merken op dat als $a \in A$, $a_1 \in A$, dat dan $a_1 = a + km$ zodat $(m,a) = (m,a+km) = (m,a_1)$ (zie pag. 9, laatste 2 regels). Alle elementen van een restklasse hebben dus dezelfde grootste gemene deler met m.
Is voor $a \in A$, $(a,m) \neq 1$ dan heeft $ax \equiv 1 \pmod{m}$ geen oplossing, zodat de restklasse A geen inverse heeft. Veronderstel nu dat voor $a \in A$ geldt $(a,m) = 1$. Dan zijn er x_0 en y_0 met $ax_0 + my_0 = 1$, zodat $ax_0 \equiv 1 \pmod{m}$. De vergelijking $ax \equiv 1 \pmod{m}$ heeft dus een oplossing $x = x_0$.
Veronderstel nu dat ook x_1 een oplossing is, zodat $ax_1 \equiv 1 \pmod{m}$. Dan volgt $ax_0 \equiv ax_1 \pmod{m}$ en daar $(a,m) = 1$ is volgens stelling 2b $x_0 \equiv x_1 \pmod{m}$. Is omgekeerd $x_1 \equiv x_0 \pmod{m}$ dan is volgens stelling 1c ook $ax_1 \equiv ax_0 \equiv 1 \pmod{m}$. De oplossing van $ax \equiv 1 \pmod{m}$ is dus een restklasse X_0 modulo m. Er geldt dan $AX_0 = E$.
We hebben hiermee gevonden dat de restklasse A met $(a,m) = 1$ voor $a \in A$ een eenduidig bepaalde restklasse als inverse voor de vermenigvuldiging heeft: notatie A^{-1}.
Daar iedere restklasse modulo m één representant in $0,1,2,\ldots,m-1$ heeft, en daar $a.0 \not\equiv 1 \pmod{m}$ volgt uit het bovenstaande in het bijzonder:

Gevolg 3. Is $a,m \in Z$, $m \geq 1$ en $(a,m) = 1$, dan is er precies één b met $1 \leq b \leq m-1$ zodat $ab \equiv 1 \pmod{m}$

Priemrestklassen.
Een restklasse A waarvoor geldt $(a,m) = 1$ als $a \in A$ heet priemrestklasse. De verzameling priemrestklassen modulo m noemt men een gereduceerd stelsel restklassen modulo m. Kiezen we uit iedere priemrestklasse één representant dan noemt men de gekozen elementen een gereduceerd stelsel representanten modulo m.
Zijn A en B priemrestklassen dan is eenvoudig in te zien dat ook AB en A^{-1} priemrestklassen zijn. Uiteraard is ook E een priemrestklasse, terwijl $E^{-1} = E$. Priemrestklassen kunnen we dus vermenigvuldigen en delen (met delen door A wordt vermenigvuldigen met A^{-1} bedoeld).

De verzameling van priemrestklassen modulo m is een multiplicatieve abelse groep.
Is in het bijzonder p een priemgetal, dan hebben alle restklassen modulo p - uitgezonderd N - een inverse. We kunnen de restklassen dan optellen, aftrekken, vermenigvuldigen en delen (uitgezonderd natuurlijk delen door N). De restklassen modulo een priemgetal p vormen dus een lichaam.
Is m geen priemgetal, dan zijn er restklassen modulo m, verschillend van N, die geen inverse hebben. De restklassen modulo een samengesteld getal m vomen geen lichaam.

We vatten het gevondene samen in de volgende stelling.

Stelling 3. Zij $m \in Z$, $m \geq 1$. De restklassen modulo m vormen een additieve groep en een ring. De priemrestklassen modulo m vormen een multiplicatieve groep. De restklassen modulo m vormen dan en slechts dan een lichaam als m priemgetal is.

Voorbeelden.
1) Zij m = 6. We geven de restklassen modulo 6 weer door de representanten 0,1,2,3,4,5. We krijgen dan voor optelling en vermenigvuldiging de volgende schema's:

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

optelling

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

vermenigvuldiging

We zien hieruit dat alleen de restklassen behorend bij de representanten 1 en 5 een inverse voor de vermenigvuldiging hebben.

2) Zij m = 5 en laten we 0,1,2,3,4 als volledig stelsel representanten nemen. We krijgen dan de volgende schema's:

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

optelling

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

vermenigvuldiging

Nu hebben alle restklassen -uitgezonderd die behorend bij 0- een inverse.

Definitie 2. Onder $\phi(n)$ voor $n \in Z$, $n \geq 1$ verstaan we het aantal positieve getallen $\leq n$, dat relatief priem is met n; $\phi(n)$ heet de functie van Euler.

Gevolgen.

4) $\phi(1) = 1$; is p priemgetal dan is $\phi(p) = p-1$.

5) Het aantal priemrestklassen modulo m is $\phi(m)$.

Stelling 4. (stelling van Euler)
Zij $a,m \in Z$, $m \geq 1$ en $(a,m) = 1$. Dan geldt

$$a^{\phi(m)} \equiv 1 \pmod{m} .$$

Anders geformuleerd: is A een priemrestklasse modulo m dan is $A^{\phi(m)} = E$.

Bewijs. Zij $r_1, r_2, \ldots, r_{\phi(m)}$ een gereduceerd stelsel representanten mod.m. We zullen aantonen dat $ar_1, ar_2, \ldots, ar_{\phi(m)}$ weer een gereduceerd stelsel representanten mod.m is. Daar $(a,m) = 1$ ligt ar_i $(i = 1,2,\ldots,\phi(m))$ in een priemrestklasse. Stel nu $ar_i \equiv ar_j \pmod{m}$ dan volgt uit stelling 2b dat $r_i \equiv r_j \pmod{m}$, zodat $i = j$. De elementen $ar_1, ar_2, \ldots, ar_{\phi(m)}$ liggen dus in verschillende priemrestklassen en vormen een gereduceerd stelsel representanten mod.m.

Hieruit volgt dat er bij iedere r_i ($i \in 1,2,\ldots,\phi(m)$) één ar_j bestaat met $r_i \equiv ar_j \pmod{m}$. Op grond van stelling 1c is dan

$$r_1 r_2 \ldots\ldots r_{\phi(m)} \equiv ar_1 ar_2 \ldots\ldots ar_{\phi(m)} \pmod{m}.$$

Daar $(r_1 r_2 \ldots r_{Q(m)}, m) = 1$ volgt uit stelling 2b het gestelde.
(Deze stelling is ook te bewijzen m.b.v. de stelling van Lagrange uit de groepentheorie; zie bijvoorbeeld Grosswald p.44, 277).

Is p een priemgetal dan volgt uit stelling 4:
Stelling 5. (stelling van Fermat)
Zij $a,p \in Z$, p priemgetal en $p \nmid a$, dan is

$$a^{p-1} \equiv 1 \pmod{p}.$$

Opmerkingen.
2) Is p priemgetal dan is $a^p \equiv a \pmod{p}$ voor alle $a \in Z$.
3) Is A priemrestklasse mod.m, dan volgt uit stelling 4, $A.A^{\phi(m)-1} = E$, zodat $A^{\phi(m)-1} = A^{-1}$. Anders geformuleerd: is $a \in A$ en $(a,m) = 1$ dan is $a^{\phi(m)-1} \in A^{-1}$.

Stelling 6. (stelling van Wilson)
Is p een priemgetal, dan is $(p-1)! \equiv -1 \pmod{p}$.

Bewijs.
Voor $p = 2$ en $p = 3$ volgt het gestelde direct door invullen. Zij nu $p \geq 5$. Zij $r \in Z$ met $1 \leq r \leq p-1$. Daar $(r,p) = 1$ bestaat er volgens gevolg 3 precies één s met $rs \equiv 1 \pmod{p}$ en $1 \leq s \leq p-1$. Is $r = 1$, dan is $s = 1$ en is $r = p-1$, dan is $s = p-1$, zoals direct door invullen volgt. Zij nu $2 \leq r \leq p-2$, dan is ook $2 \leq s \leq p-2$. We zullen nu aantonen dat dan $r \neq s$. Stel $r = s$ dan is $r^2 \equiv 1 \pmod{p}$ ofwel $p \mid r^2-1 = (r-1)(r+1)$, hetgeen onmogelijk is, daar $(r-1,p) = (r+1,p) = 1$. Het even aantal getallen $2,3,4,\ldots,p-2$ is dus te verdelen in paren van verschillende getallen r,s met $rs \equiv 1 \pmod{p}$. Hieruit volgt $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$.

Merk op dat als n geen priemgetal is, dat dan n = a.b voor zekere $a \in Z$, $1 < a < n$, zodat $a \mid (n-1)!$ en $a \nmid (n-1)! + 1$, ofwel $n \nmid (n-1)! + 1$ en $(n-1)! \not\equiv -1 \pmod{n}$.

Vergelijkingen met congruenties

Zij $m,n,a_i \in Z$ $(i = 1,2,\ldots,n)$, $m > 1$, $a_0 \not\equiv 0 \pmod{m}$. Zij $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$. We beschouwen de vergelijking $f(x) \equiv 0 \pmod{m}$. Een oplossing is een $u \in Z$ met $f(u) \equiv 0 \pmod{m}$. Is u een oplossing en $u_1 \equiv u \pmod{m}$ dan is volgens gevolg 1 ook u_1 een oplossing. De oplossing bestaat dus uit een aantal (eventueel 0) restklassen modulo m. We zullen in het onderstaande een restklasse van (onderling congruente) oplossingen steeds als één oplossing beschouwen, die we aan kunnen geven door 1 representant van de restklassen. Wanneer we dus zeggen, dat een congruentie k oplossingen $r_1,r_2,\ldots,r_k$ heeft, dan bedoelen we dat de congruentie k verschillende restklassen als oplossing heeft, bepaald door de representatnten $r_1,r_2,\ldots,r_k$. De vergelijking $f(x) \equiv 0 \pmod{m}$ heeft uiteraard maximaal m oplossingen. Deze kunnen in een concreet geval gevonden worden, door te onderzoeken door middel van substitutie welke van de getallen $0,1,2,\ldots,m-1$ voldoen.

Voorbeelden.

3) $x^2 + 1 \equiv 0 \pmod{7}$ heeft geen oplossingen.

4) $x^2 + 1 \equiv 0 \pmod{5}$ heeft 2 oplossingen: 2 en 3.

5) $x^2 - 1 \equiv 0 \pmod{8}$ heeft 4 oplossingen: 1,3,5 en 7.

6) Is p een priemgetal dan heeft volgens stelling 5 de vergelijking $x^{p-1} - 1 \equiv 0 \pmod{p}$ de p-1 oplossingen $1,2,3,\ldots,p-1$.

De oplossing van een congruentie heeft dus een geheel andere structuur dan de oplossing van een gewone vergelijking.

De vergelijking ax + by = c.

Ter inleiding van de lineaire congruentie-vergelijking bepalen we eerst de volledige oplossing van de vergelijking $ax + by = c$, $a,b,c \in Z$.

Volgens hoofdstuk I stelling 7 is deze dan en slechts dan oplosbaar als $(a,b)|c$. Stel nu $d = (a,b)|c$. Dan is $a = a_1 d$, $b = b_1 d$, $c = c_1 d$ en $(a_1,b_1) = 1$. De vergelijking gaat dan over in de (oplosbare) vergelijking

$$a_1 x + b_1 y = c_1. \tag{1}$$

Zij $x = x_0$, $y = y_0$ een oplossing en $x = x_1$, $y = y_1$ een andere oplossing dan volgt uit

$$a_1 x_0 + b_1 y_0 = c, \quad a_1 x_1 + b_1 y_1 = c$$

door aftrekken

$$a_1(x_1-x_0) + b_1(y_1-y_0) = 0 \tag{2}$$

zodat

$$a_1 | b_1(y_1-y_0) \quad , \quad b_1 | a_1(x_1-x_0).$$

Daar $(a_1,b_1) = 1$ volgt

$$a_1 | y_1-y_0 \quad , \quad b_1 | x_1-x_0$$

ofwel

$$y_1-y_0 = t_1 a_1 \quad , \quad x_1-x_0 = t_2 b_1 \quad , \quad t_1,t_2 \in Z.$$

Uit (2) volgt dan nog $t_1 = -t_2$, zodat

$$x_1 = x_0+tb_1 \quad , \quad y_1 = y_0-ta_1 \quad , \quad t \in Z. \tag{3}$$

Is dus (x_0,y_0) een oplossing van (1) dan is iedere andere oplossing van (1) van de gedaante (3). Is omgekeerd (x_0,y_0) een oplossing van (1) dan is voor iedere $t \in Z$ ook $x = x_0+tb_1$, $y = y_0-ta_1$ een oplossing van (1) zoals direct door invullen volgt.

Hiermee is de volgende stelling bewezen als uitbreiding van hoofdstuk I stelling 7.

Stelling 7. Zij $a,b,c \in Z$, a en b niet beide 0 en $d = (ab)$. Gegeven is de vergelijking

$$ax + by = c.$$

a) Als $d \nmid c$, dan is de vergelijking niet oplosbaar in $x,y \in Z$.
b) Als $d \mid c$, dan is de vergelijking wel oplosbaar in $x,y \in Z$; als $x = x_0$, $y = y_0$ een oplossing is, dan wordt de volledige oplossing gegeven door

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t, \quad t \in Z.$$

Lineaire vergelijking $ax \equiv b \pmod{m}$.
De vergelijking $ax \equiv b \pmod{m}$ is aequivalent met $ax + my = b$, zodat hij volgens stelling 7 alleen oplosbaar is als $d = (a,m) \mid b$, terwijl de oplossing voor x dan gegeven wordt door $x = x_0 + \frac{m}{d}t$, $t \in Z$.
We beschouwen nu deze oplossingen modulo m. Als $x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2 \pmod{m}$, dan volgt $\frac{m}{d}(t_1-t_2) = rm$ voor zekere $r \in Z$, zodat $t_1 - t_2$ een veelvoud van d is. Is omgekeerd $t_1 - t_2$ een veelvoud van d, dan is $x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2 \pmod{m}$. De d oplossingen $x_0 + \frac{m}{d}t$, $t = 0,1,2,\ldots,d-1$ zijn dus incongruent modulo m, terwijl iedere andere oplossing congruent is met één van deze d oplossingen.
We vonden dus de volgende stelling:

Stelling 8. Zij $a,b,m \in Z$, $m \geq 1$ en $d = (a,m)$.
Gegeven is de vergelijking

$$ax \equiv b \pmod{m}$$

a) Als $d \nmid b$, dan is de vergelijking niet oplosbaar in $x \in Z$.

b) Als $d \mid b$, dan heeft de vergelijking d oplossingen; deze zijn van de gedaante $x = x_0 + \frac{m}{d} t$, $t = 0,1,2,\ldots,d-1$.

c) Is in het bijzonder $d = 1$ dan heeft de vergelijking één oplossing.

Opmerkingen.

4) De vergelijking $ax \equiv 1$ (mod.m) is reeds onderzocht bij het bepalen van de inverse van een restklasse. Merk op dat de daar gevonden oplossing overeenkomt met stelling 8.

5) Is $(a,m) = 1$, dan is volgens stelling 8c de vergelijking $ax \equiv b$ (mod.m) eenduidig oplosbaar. Volgens stelling 4 is $a^{\phi(m)-1}b$ de oplossing. (vergelijk opmerking 3).

Stelsels lineaire vergelijkingen.

Stelling 9. Zij m_1, m_2, a_1, $a_2 \in Z$, $m_1 \geq 1$, $m_2 \geq 1$ en $d = (m_1,m_2)$. Zij gegeven het stelsel

$$\begin{cases} n \equiv a_1 & (\text{mod.}m_1) \\ n \equiv a_2 & (\text{mod.}m_2) \end{cases}.$$

a) Als $d \nmid a_2-a_1$ dan is het stelsel niet oplosbaar

b) Als $d \mid a_2-a_1$ dan heeft het stelsel één oplossing modulo $[m_1,m_2]$

Opmerking 6. Stelling 9 is ook als volgt te lezen: de doorsnede van een restklasse mod.m_1 en een restklasse mod.m_2 is óf leeg, óf een restklasse mod.$[m_1,m_2]$.

Bewijs stelling 9. Het stelsel is aequivalent met

$$(4) \qquad \begin{cases} n = a_1 + xm_1 \\ n = a_2 + ym_2 \end{cases} \qquad x,y \in Z$$

Hieruit volgt

$$(5) \qquad xm_1 - ym_2 = a_2 - a_1.$$

Volgens stelling 7 is vergelijking (5) slechts oplosbaar als $d|a_2-a_1$. Stel nu $d|a_2-a_1$, dan volgt uit stelling 7, dat de oplossing van (5) is

$$x = x_0 + \frac{m_2}{d}t, \quad y = y_0 - \frac{m_1}{d}t, \quad t \in Z.$$

Door invullen in (4) volgt dat het stelsel één oplossing modulo $\frac{m_1m_2}{d} = [m_1,m_2]$ (hoofdstuk I gevolg 4) heeft.

Een uitbreiding van stelling 9 is de volgende stelling:

Stelling 10. (Chinese reststelling)
Zij $m_i,a_i \in Z$, $m_i \geq 1$ $(i=1,2,\ldots,r.)$ Zij verder $(m_i,m_j) = 1$ voor ieder paar (i,j) met $i \neq j$. Dan heeft het stelsel congruenties

$$n \equiv a_i \pmod{m_i} \quad i = 1,2,\ldots,r$$

één oplossing mod. $m = m_1m_2\ldots m_r$.

Bewijs. Daar $(m_1,m_2) = 1$ is volgens stelling 9 de oplossing van $n \equiv a_1 \pmod{m_1}$ en $n \equiv a_2 \pmod{m_2}$ een restklasse mod. m_1m_2. Laat deze bepaald zijn door $n \equiv b_2 \pmod{m_1m_2}$. Daar $(m_1m_2,m_3) = 1$ is de oplossing van $n \equiv b_2 \pmod{m_1m_2}$ en $n \equiv a_3 \pmod{m_3}$ een restklasse mod. $m_1m_2m_3$ van de vorm $n \equiv b_3 \pmod{m_1m_2m_3}$ enz.
We kunnen de oplossing van het stelsel als volgt eenvoudig berekenen. Zij $t_i = \frac{m}{m_i}$ $(i = 1,2,\ldots,r)$ dan is

$$(t_i,m_i) = 1 \quad ,$$
$$t_i \equiv 0 \pmod{m_j} \text{ voor } i \neq j. \tag{6}$$

Volgens stelling 8 bestaat er een y_i met

$$t_iy_i \equiv 1 \pmod{m_i} \quad . \tag{7}$$

Zij nu

$$x_0 = a_1 t_1 y_1 + a_2 t_2 y_2 + \ldots + a_r t_r y_r \,. \tag{8}$$

Dan is volgens (6) en (7)

$$x_0 \equiv a_i t_i y_i \equiv a_i \pmod{m_i}$$

zodat x_0 de oplossing van het stelsel is.

De dertien rovers.

Dertien rovers moeten een buit bestaande uit een zak goudstukken verdelen. Als ze allen een gelijk aantal goudstukken gekregen hebben, blijven er nog 10 goudstukken over. Over deze laatste 10 goudstukken ontstaat een gevecht; hierbij sneuvelen 3 rovers. De overgebleven 10 rovers gaan de goudstukken opnieuw verdelen. Nu blijft er 1 goudstuk over. Hierover ontstaat weer een gevecht, waarin 3 rovers sneuvelen. Als de overgebleven 7 rovers de buit opnieuw verdelen, blijkt er voor ieder een gelijk aantal goudstukken te zijn. Als er nu gegeven is, dat de buit uit minder dan 1000 goudstukken bestond, hoe groot was de buit dan?

Oplossing. Zij n het aantal goudstukken, dan is blijkbaar

$$\begin{cases} n \equiv 10 \pmod{13} \\ n \equiv 1 \pmod{10} \\ n \equiv 0 \pmod{7} \end{cases}$$

Volgens stelling 10 is er één oplossing mod. 13.10.7 = 910.
Volgens (8) is de oplossing

$$x_0 = a_1 t_1 y_1 + a_2 t_2 y_2 + a_3 t_3 y_3 \,.$$

Hierin is $a_1 = 10$, $a_2 = 1$, $a_3 = 0$, zodat t_3 en y_3 niet bepaald hoeven te worden.

Nu is $t_1 = 70$, zodat y_1 moet voldoen aan $70y_1 \equiv 1$ (mod.13) ofwel daar $70 \equiv 5$ (mod.13) $\quad 5y_1 \equiv 1$ (mod.13) waarvan $y_1 = 8$ een oplossing is. Verder is $t_2 = 91$, zodat y_2 moet voldoen aan $91y_2 \equiv 1$ (mod.10), ofwel $y_2 \equiv 1$ (mod.10) met $y_2 = 1$ als oplossing. We krijgen dus

$$x_0 = 10.70.8 + 1.91.1 = 5691 \equiv 231 \text{ (mod.910)}$$

Daar $n < 1000$ is er één oplossing nl. 231.

Congruenties van hogere graad.

We beperken ons tot congruenties van de vorm

$$(9) \qquad a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \text{ (mod.p)}, \quad a_0 \not\equiv 0 \text{ (mod.p)},$$

waarin p een priemgetal is. Voor een behandeling van congruenties van graad $n > 1$ modulo m met m een samengesteld getal zie bijvoorbeeld Le Veque p.36-39 of Niven-Zuckerman p.38-44.

Volgens opmerking 2 is $a^p \equiv a$ (mod.p) voor alle $a \in Z$, zodat $a^{p+1} \equiv a^2$ (mod.p), $a^{p+2} \equiv a^3$ (mod.p) enz. Hieruit volgt dat voor x^k met $k \geq p$ geldt $x^k \equiv x^j$ (mod.p) voor zekere j met $1 \leq j \leq p-1$.

We kunnen ons dus beperken tot congruenties van de vorm (9) met $n \leq p-1$.

Stelling 11. Zij p een priemgetal, $a_i \in Z$ $(i = 1,\ldots,n)$ en $a_0 \not\equiv 0$ (mod.p) dan heeft de congruentie

$$(9) \qquad a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \quad \text{(mod.p)}$$

ten hoogste n wortels modulo p.

Opmerking 7. Uit voorbeeld 5 blijkt dat de bewering van stelling 11 niet geldt als p samengesteld is.

Bewijs stelling 11.

We geven een bewijs met volledige inductie.

Is n = 1 dan is de stelling juist op grond van stelling 8.

Zij nu n > 1 en zij x_1 een wortel (mod.p) van (9) zodat

$$(10) \qquad a_0x_1^n + a_1x_1^{n-1} + \ldots + a_n \equiv 0 \pmod{p} .$$

Door aftrekken van (9) en (10) krijgen we

$$(11) \qquad a_0(x^n-x_1^n) + a_1(x^{n-1}-x_1^{n-1}) + \ldots + a_{n-1}(x-x_1) \equiv 0 \pmod{p} .$$

Nu is algemeen

$$a^k - b^k = (a-b)(a^{k-1}+a^{k-2}b + \ldots + ab^{k-2}+b^{k-1})$$

waaruit volgt dat (11) te schrijven is als

$$(x-x_1)(a_0x^{n-1}+b_1x^{n-2}+\ldots+b_{n-1}) \equiv 0 \pmod{p} .$$

Omdat p priemgetal is, kan aan deze congruentie alleen voldaan zijn als $x \equiv x_1 \pmod{p}$ of als

$$(12) \qquad a_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1} \equiv 0 \pmod{p} .$$

Veronderstel nu dat de stelling bewezen is voor polynomen van de graad $\leq$ n-1. Dan heeft (12) ten hoogste n-1 wortels. Hieruit volgt dat (9) ten hoogste n wortels heeft.

Literatuur bij hoofdstuk II.

E. Grosswald: Topics from the theory of numbers, Chapter 4.

I. Niven, H.S. Zuckerman: An introduction to the theory of numbers, Chapter 2.

W.J. Le Veque: Topics in number theory, volume I, Chapter 3.

Hoofdstuk III

Arithmetische functies

Definitie 1. Een functie die gedefinieerd is op de verzameling van de natuurlijke getallen heet een arithmetische functie.

Definitie 2. Een arithmetische functie f heet multiplicatief als $f(nm) = f(n)f(m)$ voor ieder paar natuurlijke getallen n, m met $(n,m) = 1$. Een arithmetische functie f heet totaal multiplicatief als $f(nm) = f(n)f(m)$ voor ieder willekeurig paar natuurlijke getallen n, m.

Voorbeeld 1. $f(n) = n^k$ is voor iedere k een totaal multiplicatieve functie en dus ook een multiplicatieve functie.

Gevolgen.

1) Is f multiplicatief, dan is $f(1) = f(1.1) = f(1)^2$, zodat $f(1) = 1$ of $f(1) = 0$. Is $f(1) = 0$ dan volgt $f(n) = f(1.n) = f(1).f(n) = 0$, zodat $f(n) = 0$ voor alle natuurlijke getallen n. Is f multiplicatief dan is óf f de nulfunctie óf $f(1) = 1$.
2) Is f multiplicatief en $n = p_1^{a_1} \ldots p_r^{a_r}$ de kanonieke ontbinding van het natuurlijke getal n, dan is

$$f(n) = \prod_{i=1}^{r} f(p_i^{a_i}) \quad (1)$$

Hieruit volgt dat een multiplicatieve functie geheel bepaald is door zijn waarden op de machten van de priemgetallen.

We zullen in het onderstaande een aantal belangrijke arithmetische functies onderzoeken.

De functie ϕ.

In hoofdstuk II definitie 2 definieerden we de ϕ-functie van Euler op de volgende wijze:

---

syll. Z C. 78, afl. 4.

Definitie 3. Onder $\phi(n)$ voor $n \in Z$, $n \geq 1$ verstaan we het aantal positieve getallen $\leq n$, dat relatief priem is met n.

Stelling 1. ϕ is multiplicatief.

Bewijs. Zij n en m natuurlijke getallen met (n,m) = 1. Beschouw de getallen z = xn+ym, waarin x een volledig stelsel representanten modulo m en y een volledig stelsel representanten modulo n doorloopt. We zullen aantonen dat dan z een volledig stelsel representanten modulo mn doorloopt. Daartoe is het voldoende aan te tonen dat alle mn getallen z niet congruent modulo mn zijn.
Stel

$$x_i n + y_j m \equiv x_k n + y_l m \pmod{mn}.$$

Dan is

$$n(x_i - x_k) + m(y_j - y_l) \equiv 0 \pmod{mn}.$$

Hieruit volgt

$$n(x_i - x_k) \equiv 0 \pmod{m}$$

en daar (m,n) = 1 is dan $x_i \equiv x_k \pmod{m}$ ofwel i = k. Analoog volgt j = l, zodat alle mn getallen xn + ym niet congruent modulo mn zijn. Nu is (xn+ym,mn) = 1 gelijk aan

$$(xn+ym,m) = 1 \quad \text{en} \quad (xn+ym,n) = 1$$

die aequivalent zijn met

$$(xn,m) = 1 \quad \text{en} \quad (ym,n) = 1$$

(vergelijk pag. 9 laatste 2 regels).
Daar (n,m) = 1 zijn deze laatste gelijk aan

$$(x,m) = 1 \quad \text{en} \quad (y,n) = 1.$$

We vinden dus

$$(xn+ym,mn) = 1 \longleftrightarrow \begin{cases} (x,m) = 1 \\ (y,n) = 1. \end{cases}$$

M.a.w. doorloopt x een gereduceerd stelsel representanten mod. m en y een gereduceerd stelsel representanten mod. n, dan doorloopt $z = xn+ym$ een gereduceerd stelsel representanten mod. mn. Daar $\phi(n)$ het aantal gereduceerde restklassen mod. n voorstelt volgt $\phi(mn) = \phi(m)\phi(n)$.

Stelling 2. Is n een natuurlijk getal, dan is

$$\phi(n) = n \prod_{p|n} (1-\frac{1}{p}),$$

waarin het product genomen wordt over alle priemgetallen p die delers zijn van n.

Bewijs. Zij p een priemgetal en a een natuurlijk getal dan is $\phi(p^a)$ het aantal natuurlijke getallen n met $1 \leq n \leq p^a$ en $(n,p^a) = 1$. Nu zijn alle getallen n met $1 \leq n \leq p^a$ relatief priem met p^a met uitzondering van de getallen kp, $k = 1, 2, \ldots, p^{a-1}$. Zodat

$$\phi(p^a) = p^a - p^{a-1} = p^a(1-\frac{1}{p}).$$

Is de kanonieke ontbinding van n gelijk aan $p_1^{a_1} \ldots p_r^{a_r}$ dan is volgens (1)

$$\phi(n) = \prod_{i=1}^{r} \phi(p_i^{a_i}) = \prod_{i=1}^{r} p_i^{a_i}(1-\frac{1}{p_i}) = n \prod_{p|n} (1-\frac{1}{p}).$$

Gevolg 3. Is $n \geq 3$ dan is $\phi(n)$ even omdat óf n deelbaar is door een priemgetal $p \geq 3$, zodat in het product voor $\phi(n)$ de even factor $p^{a-1}(p-1)$ voorkomt, óf $n = 2^k$, zodat $\phi(n) = 2^{k-1}$ even is.

De functies τ, σ, σ_k.

Definitie 4. Voor ieder natuurlijk getal n verstaan we onder

a) $\tau(n)$ het aantal positieve delers van n.

b) $\sigma(n)$ de som van de positieve delers van n.

c) $\sigma_k(n)$ de som van de k^e machten van de positieve delers van n.

In formule:

$$\tau(n) = \sum_{d|n} 1,\ \sigma(n) = \sum_{d|n} d,\ \sigma_k(n) = \sum_{d|n} d^k.$$

Stelling 3. τ, σ en σ_k zijn multiplicatief.

Bewijs. Zij n, m natuurlijke getallen met (n,m) = 1. Op grond van de eenduidige ontbinding van natuurlijke getallen is iedere deler d_0 van nm op precies één manier te schrijven als product van een deler d_1 van n en een deler d_2 van m. Omgekeerd is iedere product van een deler d_1 van n en een deler d_2 van m een deler d_0 van nm, zodat

$$\sum_{d_1|n} d_1^k \cdot \sum_{d_2|m} d_2^k = \sum_{d_0|nm} d_0^k ,$$

ofwel

$$\sigma_k(n)\sigma_k(m) = \sigma_k(nm).$$

Daar $\tau = \sigma_0$ en $\sigma = \sigma_1$ volgen hieruit de multiplicativiteit van τ en σ als bijzondere gevallen.

Stelling 4. Zij n een natuurlijk getal en $p_1^{a_1} \ldots p_r^{a_r}$ de kanonieke ontbinding van n, dan is

$$\tau(n) = \prod_{i=1}^{r} (a_i+1),\ \sigma(n) = \prod_{i=1}^{r} \frac{p_i^{a_i+1}-1}{p_i-1},\ \sigma_k(n) = \prod_{i=1}^{r} \frac{p_i^{(a_i+1)k}-1}{p_i-1}.$$

Bewijs. Zij p priemgetal en a een natuurlijk getal dan zijn de delers van p^a de getallen 1, p, p^2, ..., p^a, zodat $\tau(p^a) = a+1$ en

$$\sigma_k(p^a) = 1+p^k+p^{2k}+ \ldots + p^{ak} = \frac{p^{(a+1)k}-1}{p^k-1}.$$

Uit (1) en $\sigma = \sigma_1$ volgt dan het gestelde.

Zij n een natuurlijk getal en P(n) het product van de delers van n, dan geldt

$$P(n) = \prod_{d|n} d = \prod_{d|n} \frac{n}{d},$$

zodat

$$(2) \qquad P^2(n) = \prod_{d|n} d \cdot \prod_{d|n} \frac{n}{d} = \prod_{d|n} n = n^{\tau(n)}.$$

We maken nu gebruik van het volgende lemma (voor een bewijs zie bijvoorbeeld Pólya-Szegö I, p. 50-51).

Lemma. Zij $a_1, a_2, \ldots, a_k$ een aantal positive reële getallen, dan is het meetkundig gemiddelde kleiner of gelijk het rekenkundig gemiddelde. In formule:

$$\sqrt[k]{a_1 a_2 \cdots a_k} \leq \frac{a_1+a_2+\ldots+a_k}{k}.$$

Pas het lemma toe met voor $a_1, a_2, \ldots, a_k$ de delers van n, dan volgt

$$\sqrt[\tau(n)]{P(n)} \leq \frac{\sigma(n)}{\tau(n)}$$

en met (2)

$$\sqrt{n} \leq \frac{\sigma(n)}{\tau(n)},$$

zodat

$$\tau(n)\ \sqrt{n} \leq \sigma(n).$$

Daar voor $n \geq 2$ altijd 1 en n twee verschillende delers van n zijn, zodat $\tau(n) \geq 2$ is hiermee de volgende stelling bewezen:

Stelling 5. Is n een natuurlijk getal, dan is

$$2\sqrt{n} \leq \tau(n)\ \sqrt{n} \leq \sigma(n).$$

Perfecte getallen.

Definitie 5. Een natuurlijk getal n heet perfect of volkomen als $\sigma(n) = 2n$, m.a.w. als n gelijk is aan de som van zijn delers, uitgezonderd n zelf.

Voorbeeld 2. Perfecte getallen zijn bijvoorbeeld $6 = 1+2+3$ en $28 = 1+2+4+7+14$.

Het is niet bekend of er oneven perfecte getallen bestaan. De even perfecte getallen worden gekarakteriseerd door de volgende stelling:

Stelling 6.

a) (Euclides) Als p en $2^p - 1$ beide priemgetal zijn, dan is $n = 2^{p-1}(2^p-1)$ een perfect getal.

b) (Euler) Omgekeerd is ieder even perfect getal n van de vorm $n = 2^{p-1}(2^p-1)$ waarin zowel p als $2^p - 1$ priemgetal zijn.

Bewijs.

a) Stel dat p en $2^p - 1$ priemgetal zijn, dan is

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p-1) = (2^{p-1})2^p = 2n,$$

zodat n een perfect getal is.

b) Is omgekeerd n een even perfect getal, dan is n te schrijven als $n = 2^{k-1}m$ met m oneven en $k \geq 2$. Uit $\sigma(n) = 2n$ volgt

$$(2^k-1)\sigma(m) = 2^k m.$$

Daar

$$(2^k-1, 2^k) = 1$$

volgt

$$m = c(2^k-1) \text{ en } \sigma(m) = c2^k \text{ voor zekere } c \in Z.$$

We zullen nu bewijzen dat $c = 1$. Stel $c > 1$, dan heeft m minstens de delers 1, c en m, zodat

$$\sigma(m) \geq 1+c+m > c+m = c2^k = \sigma(m).$$

Tegenspraak; dus $c = 1$ zodat

(3) $\qquad m = 2^k-1 \quad \text{en} \quad \sigma(m) = 2^k.$

We vinden dus $n = 2^{k-1}m = 2^{k-1}(2^k-1)$.
We zullen nu aantonen dat $m = 2^k-1$ priem is. Stel dat m niet priem is, dan heeft m meer delers dan 1 en $m = 2^k-1$ zodat

$$\sigma(m) > 2^k$$

in tegepsraak met (3), dus $m = 2^k-1$ is priem. Tot slot tonen we aan dat $2^k - 1$ alleen maar priem kan zijn als k een priemgetal is. Stel $k = ab$ met $1 < a < k$, $1 < b < k$. Daar algemeen geldt

$$\frac{x^b-1}{x-1} = x^{b-1} + x^{b-2} + \ldots + x+1$$

volgt met $x = 2^a$ dat $2^a-1 \mid 2^{ab}-1 = 2^k-1$, zodat 2^k-1 geen priemgetal kan zijn als k geen priemgetal is.

Opmerking 1. We vonden in het bewijs van stelling 6 dat als $2^k - 1$ priemgetal is, dat dan k een priemgetal moet zijn. Het omgekeerde geldt niet: als p een priemgetal is, dan is niet noodzakelijk ook $2^p - 1$ een priemgetal. De getallen $2^p - 1$ die priemgetal zijn, heten de priemgetallen van Mersenne. De eerste tien zijn de getallen corresponderend met

$$p = 2,3,5,7,13,17,19,31,61,89. \text{ (vergelijk voorbeeld 2).}$$

Het is niet bekend of er oneindig veel priemgetallen van Mersenne bestaan.

Getallenmagie.
De perfecte of volkomen getallen spelen een belangrijke rol in de getallenmagie. De delers van n ongelijk n zelf heten de aliquote delen van n, zodat een getal perfect is als het gelijk is aan de som van zijn aliquote delen. Volmaakte zaken hangen volgens de getallenmystiek samen met perfecte getallen. God schiep hemel en aanrde in 6 dagen, terwijl de maanperiode 28 dagen is (beide perfecte getallen).

Is $\sigma(n) < 2n$, dan heet n deficient en is $\sigma(n) > 2n$, dan heet n abundant. Volgens Alcuin, de leermeester van Karel de Grote was het mensengeslacht onvolkomen omdat het afstamde van de 8 zielen in de ark van Noach, terwijl 8 deficient is.
Een ander bekend begrip uit de getallenmagie zijn de bevriende getallen; dit is een getallenpaar n, m zodanig dat de som van de aliquote delen van de een gelijk is aan de ander. In formule $\sigma(m) = \sigma(n) = n+m$. Bevriende getallen symboliseren absolute vriendschap en liefde. Het bekendste paar bevriende getallen is $220 = 2^2.5.11$ en $284 = 2^2.71$. Fermat, Descartes, Euler e.a. hebben zich bezig gehouden met het opsporen van bevriende getallen. Voor enkele resultaten zie bijvoorbeeld Ore pag. 96-100. We vermelden nog dat een 16 jaar oude Italiaanse jongen Nicolò Paganini in 1866 het paar bevriende getallen $1184 = 2^5.37$ en $1210 = 2.5.11^2$ vond.

De functie Λ.

Definitie 6. Onder de arithmetische functie Λ, de functie van Mangoldt verstaat men de functie bepaald door

$$\Lambda(n) = \begin{cases} \log p & \text{als } n = p^k \text{ met p priemgetal} \\ 0 & \text{anders.} \end{cases}$$

We merken op dat Λ geen multiplicatieve functie is. De functie van Mangoldt speelt een belangrijke rol bij het onderzoek van de verdeling van priemgetallen.

Stelling 7. Is n een natuurlijk getal, dan is

$$\sum_{d|n} \Lambda(n) = \log n,$$

waar de som genomen wordt over alle delers van n.

Bewijs. Zij $n = p_1^{a_1} \ldots p_k^{a_k}$ de kanonieke ontbinding van n. Dan is, daar $\Lambda(n) = 0$ als $n \neq p^k$ met p priemgetal,

$$\sum_{d|n} \Lambda(n) = \sum_{i=1}^{k} \sum_{a=1}^{a_i} \Lambda(p_i^a) = \sum_{i=1}^{k} a_i \log p_i = \sum_{i=1}^{k} \log p_i^{a_i} = \log n.$$

Convolutieproduct.

Het blijkt handig te zijn voor arithmetische functies naast het gewone product een ander product in te voeren.

Definitie 7. Zij f en g twee arithmetische functies dan verstaan we onder het convolutieproduct f*g de functie bepaald door

$$f*g(n) = \sum_{d|n} f(d)\, g(\tfrac{n}{d}),$$

waar de som genomen wordt over alle delers van n.

Definitie 8. Onder de arithmetische functies 0, e en E verstaan we de volgende functies:

a) $0(n) = 0$ voor alle n.

b) $e(n) = \begin{cases} 1 & \text{voor } n = 1 \\ 0 & \text{voor } n > 1. \end{cases}$

c) $E(n) = 1$ voor alle n.

Gevolg 4. Uit definities 7 en 8 volgt dat voor iedere arithmetische functie f geldt:

a) $0*f = 0$

b) $e*f = f$, zodat e het eenheidselement voor het convolutieproduct is.

c) $E*f(n) = \sum_{d|n} f(d)$.

In het bijzonder volgt dan met definitie 4

d) $\tau = E*E$, $\sigma = E*n$, $\sigma_k = E*n^k$.

Uit stelling 7 volgt

e) $E*\Lambda(n) = \log n$.

Stelling 8. Zijn f, g en h arithmetische functies dan geldt:

a) $f*g = g*f$,

b) $f*(g*h) = (f*g)*h$,

c) $f*(g+h) = f*g + f*h$.

Stelling 8 volgt direct door uitschrijven.

Gevolg 5. De arithmetische functies met als optelling de gewone optelling en als vermenigvuldiging het convolutieproduct vormen een commutatieve ring met eenheidselement. We kunnen eenvoudig aantonen dat de ring geen nuldelers heeft, d.w.z. is $f \neq 0$ en $g \neq 0$, dan is $f*g \neq 0$. Is nl. $f(n) = 0$ voor $n = 1, 2, \ldots, k-1$, $f(k) \neq 0$ en $g(n) = 0$ voor $n = 1, 2, \ldots, h-1$, $g(h) \neq 0$, dan is $f*g(kh) = f(k)g(h) \neq 0$.

Stelling 9. Zij f een arithmetische functie. Bij f bestaat een eenduidig bepaalde functie g zodat $f*g = e$, dan en slechts dan als $f(1) \neq 0$.

Bewijs. Stel $f*g = e$, dan volgt $n = 1$: $f(1)g(1) = 1$, zodat $f(1) \neq 0$.
Stel nu dat $f(1) \neq 0$. We zullen een arithmetische functie g bepalen zodat $f*g = e$. Met $n = 1$ volgt $f(1)g(1) = 1$, zodat $g(1) = f(1)^{-1}$. Stel nu dat $g(n)$ berekend is voor $n = 1, 2, \ldots, k-1$ $(k \geq 2)$. We zullen aangeven hoe $g(k)$ te berekenen is. Er moet gelden $f*g(k) = e(k) = 0$. Ofwel

$$(4) \qquad f(1)g(k) + \sum_{\substack{d \mid k \\ d \neq k}} g(d) f\left(\frac{k}{d}\right) = 0.$$

Daar $g(d)$ voor $d \mid k$, $d \neq k$ volgens de onderstelling reeds bekend is, is hieruit $g(k)$ te berekenen. De functie g blijkt bovendien eenduidig bepaald te zijn.
We zullen g de inverse van f t.o.v. het convolutieproduct noemen.

Gevolg 6. Is f een multiplicatieve functie en $f \neq 0$, dan is volgens gevolg 1 $f(1) = 1$, zodat f een inverse t.o.v. het convolutieproduct heeft.

Stelling 10. Zijn f en g multiplicatieve arithmetische functies, dan is ook $f*g$ multiplicatief.

Bewijs. Zij n_1, n_2 natuurlijke getallen met $(n_1, n_2) = 1$. Zij $h = f*g$ dan is

$$h(n_1)h(n_2) = \sum_{d_1 \mid n_1} f(d_1) g\left(\frac{n_1}{d_1}\right) \sum_{d_2 \mid n_2} f(d_2) g\left(\frac{n_2}{d_2}\right).$$

$$(5) \qquad h(n_1)h(n_2) = \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1)f(d_2)g(\frac{n_1}{d_1})g(\frac{n_2}{d_2}).$$

Is d_1 een deler van n_1 en d_2 een deler van n_2, dan is daar $(n_1,n_2) = 1$ ook $(d_1,d_2) = 1$ en $(\frac{n_1}{d_1},\frac{n_2}{d_2}) = 1$, zodat daar f en g multiplicatief zijn (5) te schrijven is als

$$(6) \qquad \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1d_2)g(\frac{n_1n_2}{d_1d_2}).$$

Als $d_1|n_1$ en $d_2|n_2$ dan volgt uiteraard $d = d_1d_2|n_1n_2$. Omgekeerd is iedere deler d van n_1n_2 daar $(n_1,n_2) = 1$ op eenduidige wijze te schrijven als $d = d_1d_2$ met $d_1|n_1$, $d_2|n_2$. Hieruit volgt

$$\sum_{d_1|n_1} \sum_{d_2|n_2} \ldots = \sum_{d|n_1n_2} \ldots .$$

Dan is (6) gelijk aan

$$\sum_{d|n_1n_2} f(d)g(\frac{n_1n_2}{d}) = f*g(n_1n_2) = h(n_1n_2),$$

zodat h multiplicatief is.

Gevolg 7. Daar E multiplicatief is, is voor een multiplicatieve functie f ook $E*f(n) = \sum_{d|n} f(d)$ multiplicatief. In het bijzonder zijn $\tau = E*E$, $\sigma = E*n$ en $\sigma_k = E*n^k$ multiplicatief (vergelijk stelling 3).

Stelling 11. Is f multiplicatief en $f \neq 0$, dan is de inverse van f t.o.v. het convolutieproduct ook multiplicatief.

Bewijs. Daar $f \neq 0$ heeft f volgens gevolg 6 een inverse t.o.v. het convolutieproduct.
We construeren een arithmetische functie h op de volgende wijze:

$$h(1) = f(1)^{-1}.$$

Zij p een priemgetal en veronderstel dat $h(p^l)$ al gedefinieerd is voor $l = 0, 1, 2, \ldots, k-1$ $(k \geq 1)$. We bepalen $h(p^k)$ m.b.v. (4) zódat $f*h(p^k) = 0$. We eisen nu bovendien nog dat h multiplicatief is; volgens gevolg 2 is h dan geheel bepaald. Beschouw nu $u = f*h$. Daar f en h multiplicatief zijn, is u ook multiplicatief. Kennelijk is $u(1) = f(1)h(1) = 1$ en $u(p^k) = f*g(p^k) = 0$ (p priemgetal, $k \geq 1$), zodat $u(n) = 0$ voor $n > 1$. Dan volgt $u(n) = e(n)$, zodat h de inverse van f t.o.v. het convolutieproduct is. Daar volgens constructie h multiplicatief is, is dus de inverse van f multiplicatief.

Gevolg 8. Uit stelling 8b, 10 en 11 volgt: de multiplicatieve functies ongelijk 0 vormen een multiplicatieve groep t.o.v. het convolutieproduct als vermenigvuldiging.

Definitie 9. De functie van Möbius is de arithmetische functie μ bepaald door $\mu*E = e$.

Stelling 12. De functie μ is multiplicatief en

$$\mu(n) = \begin{cases} 1 & \text{als } n = 1 \\ (-1)^t & \text{als } n = p_1 \cdots p_t, \text{ waarin } p_1, \ldots, p_t \\ & \text{verschillende priemgetallen zijn} \\ 0 & \text{anders.} \end{cases}$$

Bewijs. Daar E multiplicatief is, volgt uit stelling 11 dat μ multiplicatief is.
Daar $\mu*E = e$ volgt $\mu(1)E(1) = 1$, zodat $\mu(1) = 1$.
Is p priemgetal, dan is $0 = \mu*E(p) = \mu(1)E(p) + \mu(p)E(1) = 1 + \mu(p)$, zodat $\mu(p) = -1$.
Verder is $0 = \mu*E(p^k) = \mu(1)+\mu(p)+\mu(p^2)+\ldots+\mu(p^k) = \mu(p^2)+\mu(p^3)+\ldots+\mu(p^k)$.
Met opvolgend $k = 2, 3, \ldots$ volgt hieruit $\mu(p^k) = 0$ voor $k \geq 2$. Daar μ multiplicatief is volgt $\mu(n)$ voor andere natuurlijke getallen n direct uit (1).

Opmerking 2. $\mu*E = e$ is uit te schrijven als

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{voor } n = 1 \\ 0 & \text{voor } n > 1. \end{cases}$$

Stelling 13. (Omkeerstelling van Möbius)
Is f een arithmetische functie en is

(7) $$F(n) = \sum_{d|n} f(d)$$

dan is

(8) $$f(n) = \sum_{d|n} F(d)\mu(\tfrac{n}{d}).$$

Bewijs. Relatie (7) is te lezen als $F = f*E$. Door beide kanten met μ te vermenigvuldigen volgt

$$F*\mu = f*E*\mu = f*e = f.$$

Dit is relatie (8).

Stelling 14. Zij f een arithmetische functie en F als in (7), dan is f multiplicatief dan en slechts dan als F multiplicatief is.

Bewijs. Er geldt $F = f*E$ en $f = F*\mu$, zodat stelling 14 een direct gevolg van stelling 10 is.

Toepassingen.
Uit gevolg 4 volgen de volgende toepassingen van stelling 13.

1) $\tau = E*E$ zodat $E = \mu*\tau$ ofwel

$$\sum_{d|n} \mu(d)\tau(\tfrac{n}{d}) = 1 \quad \text{voor alle natuurlijke getallen n.}$$

2) $\sigma_k = E*n^k$, zodat $n^k = \mu*\sigma_k$ ofwel

$$\sum_{d|n} \mu(d)\sigma_k(\tfrac{n}{d}) = n^k \quad \text{voor alle n.}$$

3) $E*\Lambda(n) = \log n$, zodat $\mu*\log n = \Lambda(n)$ ofwel

$$\sum_{d|n} \mu(d) \log \frac{n}{d} = \Lambda(n)$$

waaruit m.b.v. opmerking 2 volgt

$$\sum_{d|n} \mu(d) \log d = -\Lambda(n).$$

4) Zij $g = \mu*n$ dan is $g(1) = \mu(1) = 1$.
Is p priemgetal, k natuurlijk getal dan is
$g(p^k) = \mu(1)p^k+\mu(p)p^{k-1}+0 = p^k-p^{k-1}$, zodat $g(p^k) = \phi(p^k)$ voor ieder priemgetal p en natuurlijk getal k. Daar g en ϕ beide multiplicatief zijn is dan volgens gevolg 2 $g(n) = \phi(n)$ voor alle natuurlijke getallen n. We vinden dus $\mu*n = \phi$, zodat $\phi*E = n$ ofwel

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

Voor andere bewijzen van deze relatie zie bijvoorbeeld Hardy, Wright p. 54 of LeVeque p. 30.

5) $\tau*\phi = E*E*\phi = E*n = \sigma$.

Voortbrengende functie.

We zullen in het volgende gebruik maken van enkele stellingen uit de theorie van de Dirichletreeksen. (zie hiervoor bijvoorbeeld Titchmarsh, chapter IX).
Een Dirichletreeks is een reeks van de gedaante $\sum_{n=1}^{\infty} a_n n^{-s}$, waarin s een complexe variabele voorstelt. Een dergelijke reeks convergeert absoluut in een zeker halfvlak Re $s > \sigma_a$, waarbij $-\infty \leq \sigma_a \leq +\infty$. Bovendien geldt zeker voor Re $s > \sigma_a$

$$(9)\quad \frac{d}{ds}\left(\sum_{n=1}^{\infty} a_n n^{-s}\right) = \sum_{n=1}^{\infty} \frac{d}{ds}\left(a_n n^{-s}\right) = -\sum_{n=1}^{\infty} (a_n \log n) n^{-s}.$$

Is f een arithmetische functie dan heet de formele Dirichletreeks $\sum_{n=1}^{\infty} f(n)n^{-s}$ de voortbrengende functie van f.

Is in het bijzonder f = E, dan is de voortbrengende functie $\sum_{n=1}^{\infty} n^{-s} = \zeta(s)$ de ζ-functie van Riemann. Deze reeks convergeert absoluut voor Re s > 1. Volgens (9) geldt dan voor Re s > 1

$$(10) \qquad \zeta'(s) = -\sum_{n=1}^{\infty} \log n \, n^{-s}.$$

Stelling 15. Zijn f en g twee arithmetische functies met voortbrengende functies $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ en $G(s) = \sum_{n=1}^{\infty} g(n)n^{-s}$. Als de beide Dirichletreeksen absoluut convergeren voor Re s > σ_a, dan convergeert ook $\sum_{n=1}^{\infty} f*g(n)n^{-s}$ absoluut voor Re s > σ_a, terwijl deze reeks gelijk is aan F(s).G(s).

Het bewijs van stelling 15 berust op het feit dat de absoluut convergente dubbelreeks $\sum_n \sum_m f(n)n^{-s}g(m)m^{-s}$ in iedere volgorde gesommeerd mag worden; Zie Titchmarsh p. 27-33.

Toepassingen.

Uit gevolg 4 volgen de volgende twee toepassingen van stelling 15.

6) Daar $\tau = E*E$ volgt $\sum_{n=1}^{\infty} \tau(n)n^{-s} = \zeta^2(s)$ voor Re s > 1.

7) Uit $\sigma_k = E*n^k$ volgt $\sum_{n=1}^{\infty} \sigma_k(n)n^{-s} = \zeta(s) \sum_{n=1}^{\infty} n^k.n^{-s} = \zeta(s)\zeta(s-k)$ voor Re s > k+1.

In het bijzonder geldt:

$$\sum_{n=1}^{\infty} \sigma(n)n^{-s} = \zeta(s)\zeta(s-1) \text{ voor Re } s > 2.$$

8) Uit $\mu*E = 2$ (opmerking 2) volgt $\sum_{n=1}^{\infty} \mu(n)n^{-s}.\zeta(s) = 1$, zodat $\sum_{n=1}^{\infty} \mu(n)n^{-s} = \zeta^{-1}(s)$ voor Re s > 1.

Merk op dat hieruit volgt dat $\zeta(s)$ geen nulpunten heeft voor Re s > 1.

9) Uit $\phi = \mu*n$ (toepassing 4) volgt $\sum_{n=1}^{\infty} \phi(n)n^{-s} =$

$$\sum_{n=1}^{\infty} \mu(n)n^{-s} \sum_{n=1}^{\infty} n.n^{-s} = \zeta^{-1}(s)\zeta(s-1) \text{ voor Re } s > 2.$$

10) Uit $\Lambda = \mu * \log n$ (toepassing 3) en (10) volgt

$$\sum_{n=1}^{\infty} \Lambda(n)n^{-s} = \sum_{n=1}^{\infty} \mu(n)n^{-s} . \sum_{n=1}^{\infty} \log n \; n^{-s} = -\zeta^{-1}(s)\zeta'(s) \text{ voor Re } s > 1.$$

Literatuur bij hoofdstuk III

E. Grosswald: Topics from the theory of numbers, chapter 6.

G. Hardy, E.M. Wright: An introduction to the theory of numbers, pag. 54, chapter XVI, XVII.

W.J. LeVeque: Topics in number theory, pag. 30, chapter 6.

I. Niven, H.S. Zuckerman: An introduction to the theory of numbers, chapter 4.

O. Ore: Number theory and its history, chapter 5.

G. Pólya, G. Szegö: Aufgaben und Lehrsätze aus der Analysis I, p. 50-51.

E.C. Titchmarsh: The theory of functions, p. 27-33, chapter IX.

Hoofdstuk IV: Grootteorde van arithmetische functies.

Bij het afschatten van de orde van grootte van arithmetische functies maakt men vaak gebruik van de O- en o-symbolen van Landau - Bachmann.

Definitie 1. Zij $f(x)$ een willekeurige functie en $g(x)$ een positieve functie beide gedefinieerd op alle gehele getallen $x \geq$ een zeker getal A óf op alle reele getallen $x \geq A$.

1e) $f(x) = O(g(x))$ voor $x \to \infty$ betekent dat
$|f(x)| \leq C\, g(x)$ voor zekere constante C en $x \geq A$.

2e) $f(x) = o(g(x))$ voor $x \to \infty$ betekent

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$$

De O- en o-symbolen worden meestal gebruikt om de grootteorde van een gecompliceerde functie $f(x)$ te schatten m.b.v. een eenvoudiger functie $g(x)$.

Voorbeelden.

1) $3x^2 + 4x \sin x + \log x = O(x^2)$ voor $x \to \infty$.
2) $\log x = o(x)$ voor $x \to \infty$.

Gevolgen.

1) Is $f(x) = o(g(x))$ voor $x \to \infty$, dan is $f(x) = O(g(x))$ voor $x \to \infty$.
2) Is $f(x) = O(g_1(x))$ voor $x \to \infty$ en is $g_1(x) \leq g_2(x)$
dan is $f(x) = O(g_2(x))$ voor $x \to \infty$.
3) Is $f(x) = O(g(x))$ en is $h(x)$ positief, dan is
$h(x)f(x) = O(h(x)g(x))$, zodat $h(x)O(g(x)) = O(h(x)g(x))$.
4) Is $f_1(x) = O(g(x))$ en $f_2(x) = O(g(x))$, dan is $f_1(x) + f_2(x) = O(g(x))$,
zodat $O(g(x)) + O(g(x)) = O(g(x))$.

---

syll. Z C. 78, afl. 5.

Definitie 2. Zij x een reeel getal, dan is [x] (spreek uit: x-entier) het grootste gehele getal $\leq x$.

Voorbeeld 3.
$[1\frac{1}{2}] = 1$, $[5] = 5$, $[-7,3] = -8$, $[\pi] = 3$, $[4,753\ldots] = 4$.

We zullen het afleiden van formules voor de grootteorde van arithmetische functies demonstreren aan de functie τ. De functie τ zelf is zeer onregelmatig. Zo is $\tau(2^m) = m+1$, terwijl voor ieder priemgetal p geldt $\tau(p) = 2$. Men kan aantonen dat voor ieder positief getal δ geldt

$$\tau(n) = o(n^{\delta}) \quad \text{voor} \quad n \to \infty.$$

(zie bijvoorbeeld Hardy & Wright 260-261 of Chandrasekharan VI.6-8).

Interessanter is echter de functie

$$T(N) = \sum_{n=1}^{N} \tau(n)$$

die veel regelmatiger is. We zullen hiervoor een schatting afleiden. Hiertoe behandelen we eerst een stelling uit de analyse, die ook op zichzelf interessant is.

Harmonische reeks.
De oneindige reeks $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \ldots$ heet de harmonische reeks.
Daar

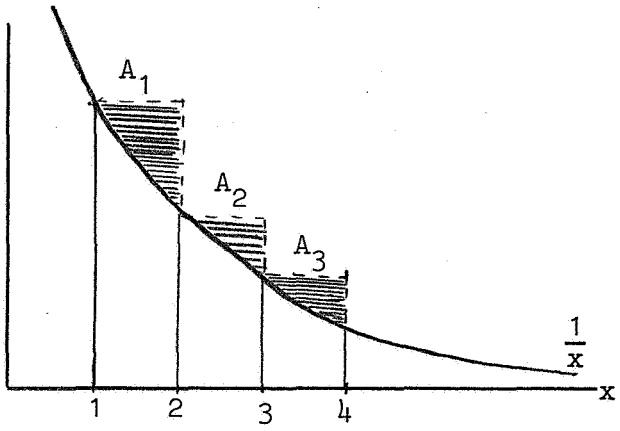
$$\frac{1}{3} + \frac{1}{4} > 2.\frac{1}{4} = \frac{1}{2}\ ,\ \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} > 4.\frac{1}{8} = \frac{1}{2}\ ,\ \frac{1}{9} + \frac{1}{10} + \ldots + \frac{1}{16} > 8.\frac{1}{16} = \frac{1}{2},\ \text{enz.}$$

volgt direct dat de som van de reeks onbegrensd toeneemt (de som is"oneindig"). We zullen nu aantonen

Stelling 1. $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} = \log n + \gamma + O(\frac{1}{n})$ voor $n \to \infty$,

waarin γ een constante is, de zogenaamde constante van Euler - Mascheroni; $\gamma = 0,57721\ldots$ (Het grondtal van de log is e).

Bewijs: Beschouw de functie $\frac{1}{x}$ voor $x \geq 1$.



Voor $k \leq x \leq k+1$ $(k \in 1,2,3,\ldots)$ geldt $\frac{1}{k+1} \leq \frac{1}{x} \leq \frac{1}{k}$, zodat

(1) $\quad \frac{1}{k+1} < \int_k^{k+1} \frac{1}{x}\,dx < \frac{1}{k}$.

Zij

(2) $\quad A_k = \frac{1}{k} \int_k^{k+1} \frac{1}{x}\,dx$ voor $k = 1,2,3,\ldots$ (zie figuur)

dan volgt uit (1)

(3) $\quad 0 < A_k < \frac{1}{k} - \frac{1}{k+1}$ $\qquad (k = 1,2,3,\ldots)$

Voor ieder natuurlijk getal n geldt dan

$$\sum_{k=1}^{n} A_k < \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1}\right) = \left(1-\frac{1}{2}\right) + \left(\frac{1}{2}-\frac{1}{3}\right) + \ldots \left(\frac{1}{n}-\frac{1}{n+1}\right) = 1-\frac{1}{n+1} < 1.$$

Daar alle A_k positief zijn en $\sum_{k=1}^{n} A_k < 1$ voor alle n volgt dat $\sum_{k=1}^{\infty} A_k$ bestaat. Nu definieren we

(4) $\quad \gamma \overset{\text{def}}{=\!=} \sum_{k=1}^{\infty} A_k$.

Uit (3) volgt verder

$$\sum_{k=n+1}^{\infty} A_k < \sum_{k=n+1}^{\infty} \left(\frac{1}{k} - \frac{1}{k+1}\right) = \frac{1}{n+1} < \frac{1}{n}.$$

Zodat

$$(5) \quad \sum_{k=n+1}^{\infty} A_k = O\left(\frac{1}{n}\right) \quad \text{voor} \quad n \to \infty .$$

Uit (4), (5) en (2) volgt

$$\gamma = \sum_{k=1}^{\infty} A_k = \sum_{k=1}^{n} A_k + O\left(\frac{1}{n}\right) = \sum_{k=1}^{n} \frac{1}{k} - \int_1^{n+1} \frac{1}{x}\,dx + O\left(\frac{1}{n}\right) =$$

$$\sum_{k=1}^{n} \frac{1}{k} - \int_1^{n} \frac{1}{x}\,dx - \int_n^{n+1} \frac{1}{x}\,dx + O\left(\frac{1}{n}\right) .$$

Verder is

$$\int_1^{n} \frac{1}{x}\,dx = \log n \quad \text{(het grondtal van de logarithme is e)}$$

terwijl uit (1) volgt

$$\int_n^{n+1} \frac{1}{x}\,dx = O\left(\frac{1}{n}\right) \quad \text{voor } n \to \infty .$$

We krijgen dan

$$\gamma = \sum_{k=1}^{n} \frac{1}{k} - \log n + O\left(\frac{1}{n}\right)$$

Ofwel

$$\sum_{k=1}^{n} \frac{1}{k} = \log n + \gamma + O\left(\frac{1}{n}\right) \quad \text{voor } n \to \infty .$$

<u>Opmerking 1.</u> Het is niet bekend of γ een rationaal of een irrationaal getal is. (Een rationaal getal is een getal van de vorm $\frac{p}{q}$ met $p, q \in Z$)

Opmerking 2. Het bovenstaande bewijs is direct te generaliseren tot een bewijs van de volgende stelling (zie Chandrasekharan VI 9-10).

Stelling 2. Is $g(x)$ een monotoon afnemende, positieve functie gedefinieerd voor $x \geq 1$, dan geldt

$$\sum_{k=1}^{n} g(k) = \int_{1}^{n} g(x)dx + A + O(g(n)) \qquad \text{voor } n \to \infty ,$$

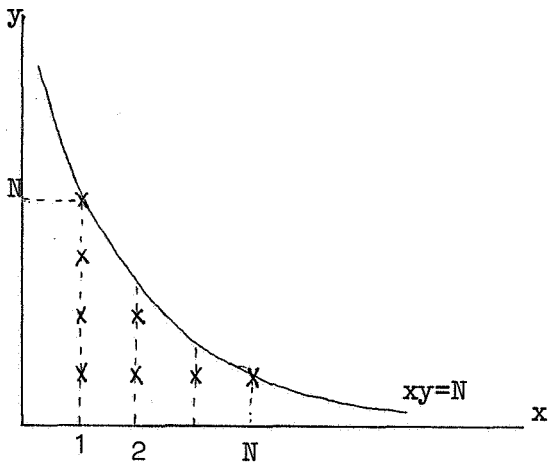
waarin A een constante is.

Afschatting T(N).

Volgens definitie is $\tau(n) = \sum_{d \mid n} 1 = \sum_{d_1 d_2 = n} 1$, waarbij in het laatste lid de sommatie genomen moet worden over de paren gehele getallen (d_1, d_2) met product n. Dan is

$$T(N) = \sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \sum_{d_1 d_2 = n} 1 = \sum_{d_1 d_2 \leq N} 1 .$$

In woorden: T(N) is het aantal paren (d_1, d_2) met $d_1 d_2 \leq N$. Beschouw in het x, y-vlak de punten (x,y) met $x \in Z$, $y \in Z$, de zogenaamde roosterpunten. Dan volgt dat T(N) gelijk is aan het aantal roosterpunten gelegen in het stuk tussen de x-as, de y-as en de hyperbool $xy = N$.



We geven eerst een grove schatting voor T(N).

De te tellen roosterpunten liggen op de lijnen $x = 1,2,3,\ldots, N$.

Voor vaste x hebben we $[\frac{N}{x}]$ roosterpunten op de corresponderende lijn.

Stellen we $[\frac{N}{x}] = \frac{N}{x} - \theta_x$ dan volgt

$$T(N) = \sum_{x=1}^{N} [\frac{N}{x}] = \sum_{x=1}^{N} \frac{N}{x} - \sum_{x=1}^{N} \theta_x .$$

Daar $0 \leq \theta_x < 1$ volgt $\left| \sum_{x=1}^{N} \theta_x \right| < N$ zodat $\sum_{x=1}^{N} \theta_x = O(N)$ voor $N \to \infty$.

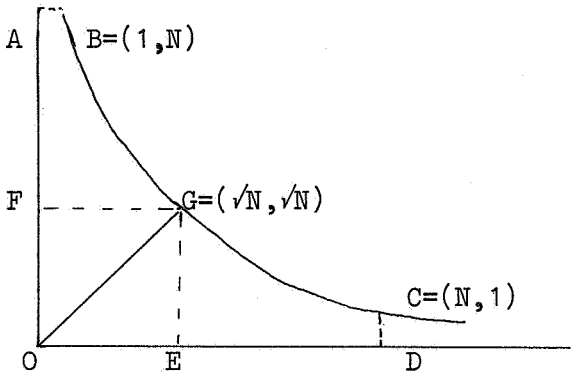
Met behulp van stelling 1 volgt dan

$$T(N) = N \sum_{x=1}^{N} \frac{1}{x} + O(N) = N\{(\log N + \gamma + O(\frac{1}{N})\} + O(N).$$

Daar volgens gevolgen 2, 3 en 4 geldt $N\gamma + NO(\frac{1}{N}) + O(N) = O(N)$ voor $N \to \infty$ volgt

$$T(N) = N \log N + O(N) \qquad \text{voor } N \to \infty .$$

We kunnen echter op eenvoudige wijze de schatting aanzienlijk verbeteren.



De hyperbool is symmetrisch t.o.v. de lijn y = x. Het aantal te tellen roosterpunten is dus 2× het aantal in het stuk ABGEO minus het aantal in het vierkant OEGF (zie figuur). De roosterpunten in ABGEO liggen op de lijnen x = 1,2,..., $[\sqrt{N}]$. Het aantal roosterpunten in OEGF is $[\sqrt{N}]^2$.

Zijn $[\frac{N}{x}] = \frac{N}{x} - \theta_x$ en $[\sqrt{N}] = \sqrt{N} - \theta$, dan volgt

$$T(N) = 2 \sum_{x=1}^{[\sqrt{N}]} [\frac{N}{x}] - [\sqrt{N}]^2 = 2 \sum_{x=1}^{[\sqrt{N}]} \frac{N}{x} - 2 \sum_{x=1}^{[\sqrt{N}]} \theta_x - (\sqrt{N}-\theta)^2 .$$

Daar

$$\left| -2 \sum_{x=1}^{[\sqrt{N}]} \theta_x + 2\theta\sqrt{N} - \theta^2 \right| \leq 2\sqrt{N} + 2\sqrt{N} + 1$$

volgt

$$T(N) = 2N \sum_{x=1}^{N} \frac{1}{x} - N + O(\sqrt{N}).$$

Met stelling 1 volgt dan

$$(6) \quad T(N) = 2N\{ \log [\sqrt{N}] + \gamma + O(\frac{1}{[\sqrt{N}]})\} - N + O(\sqrt{N}).$$

Nu is

$$0 \leq \log \sqrt{N} - \log [\sqrt{N}] = \int_{[\sqrt{N}]}^{\sqrt{N}} \frac{1}{x}\, dx < \frac{1}{[\sqrt{N}]} \leq \frac{2}{\sqrt{N}},$$

zodat

$$(7) \quad \log [\sqrt{N}] = \log \sqrt{N} + O(\frac{1}{\sqrt{N}}) \quad \text{voor } N \to \infty .$$

Verder is daar $\frac{1}{[\sqrt{N}]} \leq \frac{2}{\sqrt{N}}$.

$$(8) \quad O(\frac{1}{[\sqrt{N}]}) = O(\frac{1}{\sqrt{N}}) \quad \text{voor } N \to \infty .$$

Uit (6), (7) en (8) volgt

$$T(N) = 2N \{ \log \sqrt{N} + O(\frac{1}{\sqrt{N}} + \gamma \} - N + O(\sqrt{N}) .$$

Daar volgens gevolgen 3 en 4

$$\tfrac{1}{2}NO(\frac{1}{\sqrt{N}}) + O(\sqrt{N}) = O(\sqrt{N}) \quad \text{voor } N \to \infty$$

is hiermee bewezen

<u>Stelling 3.</u> $T(N) = N \log N + N(2\gamma-1) + O(\sqrt{N})$ voor $N \to \infty$.

<u>Opmerking 3.</u> Stelling 3 is afkomstig van Dirichlet (1849). De vraag of de restterm $O(\sqrt{N})$ in deze stelling nog verscherpt kan worden, staat bekend als het deler-probleem van Dirichlet. Voronoï (1903) bewees

dat $O(\sqrt{N})$ in stelling 3 vervangen kan worden door $O(N^{1/3})$ en van der Corput (1922) verscherpte de $\frac{1}{3}$ nog tot $\frac{33}{100}$. Hardy en Landau (1915) bewezen dat in stelling 3 de $O(\sqrt{N})$ niet vervangen kan worden door $O(N^{\frac{1}{4}})$. De juiste macht van N is nog onbekend.

Voor σ en ϕ kan men de volgende formules afleiden (zie Hardy & Wright 266-268 of Le Veque 120-121).

Stelling 4.

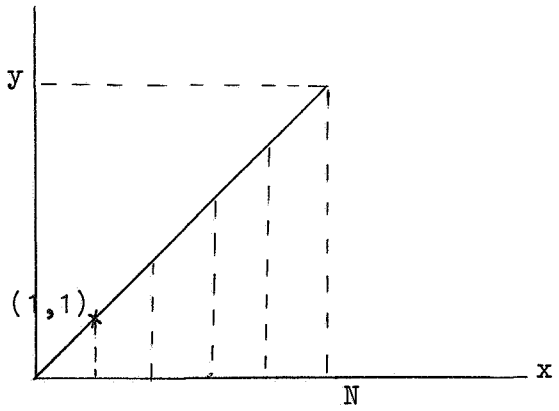
a) $S(N) = \sum_{n=1}^{N} \sigma(n) = \frac{1}{12}\pi^2 N^2 + O(N\log N)$ voor $N \to \infty$.

b) $\Phi(N) = \sum_{n=1}^{N} \Phi(n) = \frac{3N^2}{\pi^2} + O(N\log N)$ voor $N \to \infty$.

Opmerking 4. Zij $W(N)$ het aantal breuken $\frac{x}{y}$ met $1 \le x \le N$, $1 \le y \le N$, die niet te vereenvoudigen zijn, d.w.z. $(x,y) = 1$.
Het totaal aantal breuken $\frac{x}{y}$ met $1 \le x \le N$, $1 \le y \le N$ is uiteraard N^2.
We definieren nu de kans dat een (positieve) breuk $\frac{x}{y}$ niet te vereenvoudigen is als

$$P = \lim_{N\to\infty} \frac{W(N)}{N^2} .$$

We zullen m.b.v. stelling 4b aantonen dat de limiet bestaat en dat P eenvoudig te berekenen is. Volgens de definitie is $\phi(n)$ het aantal getallen m met $1 \le m \le n$ en $(m,n) = 1$, zodat $\Phi(n)$ gelijk is aan het aantal roosterpunten (x,y) op de lijn $x = n$ met $1 \le y \le n$ en $(x,y) = 1$. Dan is $\Phi(N)$ gelijk aan het aantal roosterpunten (x,y) in de driehoek $1 \le x \le N$, $1 \le y \le x$ met $(x,y) = 1$.



$W(N)$ is gelijk aan het aantal roosterpunten (x,y) in het vierkant $1 \leq x \leq N$, $1 \leq y \leq N$. Dit vierkant is symmetrisch t.o.v. de diagonaal $y = x$. Op de diagonaal ligt slechts 1 roosterpunt met $(x,y) = 1$ namelijk $x = y = 1$. Hieruit volgt

$$W(N) = 2\,\Phi(N) - 1.$$

Dan is volgens stelling 4b:

$$P = \lim_{N\to\infty} \frac{W(N)}{N^2} = \lim_{N\to\infty} \frac{2\,\Phi(N)-1}{N^2} = \frac{6}{\pi^2} \quad .$$

<u>Literatuur bij hoofdstuk IV:</u>

K. Chandrasekharan : Einführung in die Analytische Zahlentheorie, Kapitel VI.

G.H. Hardy, E.M. Wright: An introduction to the theory of numbers, Chapter XVIII.

W.J. LeVeque : Topics in number theory, volume I, Chapter 6.

Hoofdstuk V: Priemgetallen.

We zullen een bewijs geven van de volgende stelling van Tchebycheff (vergelijk Inleiding).

Stelling 1. Zij $\pi(x)$ het aantal priemgetallen $\leq x$, dan bestaan er positieve constanten c_1 en c_2 zodat

$$c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x} \quad \text{voor } x \geq 2.$$

In het bewijs maken we gebruik van de θ- en van de ψ-functie, die eenvoudiger te hanteren zijn dan $\pi(x)$.

Definitie 1.

(1) $\theta(x) = \sum_{p \leq x} \log p$, waarbij de sommatie genomen wordt over alle priemgetallen $p \leq x$.

(2) $\psi(x) = \sum_{n \leq x} \Lambda(n)$, waarbij de sommatie genomen wordt over alle natuurlijke getallen $n \leq x$.

We onderzoeken eerst het verband tussen $\theta(x)$, $\psi(x)$ en $\pi(x)$.
Volgens hoofdstuk III definitie 6 is $\Lambda(p^k) = \log p$ als p priemgetal en $\Lambda(n) = 0$ voor alle andere waarden van n. Zij p een vast priemgetal met $p \leq x$, dan is $p^k \leq x$ voor $k = 1,2,\ldots, [\frac{\log x}{\log p}]$, zodat uit (2) volgt

(3) $\psi(x) = \sum_{p \leq x} [\frac{\log x}{\log p}] \log p.$

Uit (1) en (3) volgt

(4) $\theta(x) \leq \psi(x)$.

---

sylï. ZC 78, afl.6

Daar $[a] \leq a$ volgt uit (3) voor $x \geq 2$

$$(5) \quad \psi(x) \leq \sum_{p \leq x} \log x = \pi(x)\log x.$$

Zij $0 < \alpha < 1$, dan volgt daar $\pi(x^\alpha) \leq x^\alpha$

$$\theta(x) \geq \sum_{x^\alpha < p \leq x} \log p \geq \alpha \log x(\pi(x)-\pi(x^\alpha)) \geq$$

$$\alpha \log x(\pi(x)-x^\alpha),$$

zodat

$$(6) \quad \pi(x)\log x \leq \frac{\theta(x)}{\alpha} + x^\alpha \log x.$$

We hebben dus gevonden in (4), (5) en (6)

Lemma 1.

$$\theta(x) \leq \psi(x) \leq \pi(x)\log x \leq \frac{\theta(x)}{\alpha} + x^\alpha \log x$$

voor $0 < \alpha < 1$ en $x \geq 2$.

Opmerking 1. Daar $\lim_{x\to\infty} \frac{\log x}{x^{1-\alpha}} = 0$ voor $0 < \alpha < 1$ en daar lemma 1 geldt voor alle α in $(0,1)$ is uit dit lemma af te leiden dat als één van de limieten $\lim_{x\to\infty} \frac{\theta(x)}{x}$, $\lim_{x\to\infty} \frac{\psi(x)}{x}$ of $\lim_{x\to\infty} \frac{\pi(x)\log x}{x}$ bestaat, dat dan ook de beide andere bestaan en dat ze alle drie gelijk zijn. (zie bijvoorbeeld Chandrasekharan VII.6).

Stelling 1 volgt nu uit lemma 1 en de beide volgende stellingen.

Stelling 2. Er is een constante A zodat

$$\theta(x) < Ax.$$

Stelling 3. Er is een positieve constante B zodat

$$\psi(x) > Bx \quad \text{voor } x \geq 2.$$

Bewijs stelling 1.

Uit lemma 1 en stelling 3 volgt

$$\pi(x) \geq \frac{\psi(x)}{\log x} > \frac{Bx}{\log x} \quad \text{voor } x \geq 2.$$

Uit lemma 1 en stelling 2 volgt voor $x \geq 2$

$$\pi(x) \leq \frac{\theta(x)}{\alpha \log x} + x^{\alpha} < \frac{Ax}{\alpha \log x} + x^{\alpha} = \frac{x}{\log x}\left(\frac{A}{\alpha} + \frac{\log x}{x^{1-\alpha}}\right).$$

Uit $\lim_{x \to \infty} \frac{\log x}{x^{1-\alpha}} = 0$ volgt dat er een constante D bestaat zodat

$$\frac{\log x}{x^{1-\alpha}} < D \text{ voor } x \geq 2.$$

Dan is

$$\pi(x) < \frac{x}{\log x}\left(\frac{A}{\alpha} + D\right) \quad \text{voor } x \geq 2.$$

Bewijs stelling 2.

Zij n een positief geheel getal en

$$N = \binom{2n}{n} = \frac{(n+1)(n+2)\ldots 2n}{1.2.3\ldots n},$$

dan treedt N op als binomiaalcoefficient in de ontwikkeling van $(1+1)^{2n}$ zodat N een geheel getal is en

$$N < 2^{2n}. \tag{7}$$

Is p een priemgetal met $n < p \leq 2n$, dan volgt $p \mid N$ zodat

$$\prod_{n<p\leq 2n} p \leq N,$$

waaruit volgt

$$\log N \geq \sum_{n<p\leq 2n} \log p = \theta(2n) - \theta(n).$$

Met (7) krijgen we dan

$$\theta(2n) - \theta(n) < 2n\log 2. \tag{8}$$

Daar $\theta(1) = 0$ volgt uit (8) met $n = 2^r$

$$\theta(2^m) = \sum_{r=0}^{m-1} \{\theta(2^{r+1}) - \theta(2^r)\} < 2\log 2 \sum_{r=0}^{m-1} 2^r < 2^{m+1}\log 2.$$

Zij nu $x \geq 2$ en m geheel zodat $2^{m-1} \leq x < 2^m$ dan volgt

$$\theta(x) \leq \theta(2^m) < 2^{m+1}\log 2 \leq 4x\log 2.$$

Hiermee is stelling 2 bewezen met $A = 4\log 2$.

Opmerking 2.
In bovenstaande is bewezen $\theta(x) < 4x\log 2$. Door i.p.v. $N = \binom{2n}{n}$ gebruik te maken van $\binom{2n+1}{n}$ kan men op analoge wijze de scherpere schatting

$$\theta(x) < 2x\log 2 \tag{9}$$

afleiden (zie bijvoorbeeld Hardy & Wright p. 341-342). Merk op dat (9) aequivalent is met

$$\prod_{p\leq x} < 4^x \qquad \text{voor } x \geq 2.$$

Het bewijs van stelling 3 berust op het volgende lemma.

Lemma 2. Zij m een positief geheel getal, dan is

$$\sum_{d=1}^{m} \Lambda(d)\left[\frac{m}{d}\right] = \log m!$$

Bewijs.
Volgens hoofdstuk III stelling 7 geldt

$$\sum_{d|n} \Lambda(d) = \log n$$

zodat

$$(10) \qquad \sum_{n=1}^{m} \sum_{d|n} \Lambda(d) = \sum_{n=1}^{m} \log n = \log m!$$

Zij nu d een vast geheel getal met $1 \leq d \leq m$, dan komt d in het linkerlid van (10) even vaak voor als er d-vouden zijn in de verzameling $1,2,3,\ldots,m$, d.w.z. $[\frac{m}{d}]$ maal. Hieruit volgt het lemma.

Opmerking 3.
Daar $\Lambda(n) = \log p$ voor $n = p^r$ en $\Lambda(n) = 0$ voor alle andere waarden van n is lemma 2 gelijk aan

$$\sum_{p \leq m} ([\frac{m}{p}] + [\frac{m}{p^2}] + \ldots) \log p = \log m!$$

Lemma 2 is dus gelijk aan de volgende stelling:
zij p een priemgetal met $p \leq m$, dan is het aantal factoren p in m! gelijk aan

$$[\frac{m}{p}] + [\frac{m}{p^2}] + [\frac{m}{p^3}] + \ldots .$$

Bewijs stelling 3.
Zij als in het bewijs van stelling 2 n een natuurlijk getal en $N = \binom{2n}{n} = \frac{(2n)!}{(n!)^2}$, dan volgt uit lemma 2

$$\log N = \log(2n)! - 2\log n! = \sum_{d=1}^{2n} \Lambda(d)[\frac{2n}{d}] - 2\sum_{d=1}^{n} \Lambda(d)\,[\frac{n}{d}].$$

Daar $[\frac{n}{d}] = 0$ voor $d > n$ kunnen we de laatste sommatie zonder bezwaar tot 2n laten lopen, zodat

$$(11) \qquad \log N = \sum_{d=1}^{2n} \Lambda(d) \{[\tfrac{2n}{d}] - 2[\tfrac{n}{d}]\} .$$

Nu is $[2a] - 2[a] < 2a - 2(a-1) = 2$

$> 2a-1-2a = -1,$

zodat $[2a] - 2[a] = 0$ of 1.

Uit (11) volgt dan

$$(12) \qquad \log N \leq \sum_{d=1}^{2n} \Lambda(d) = \psi(2n).$$

Nu is

$$N = \binom{2n}{n} = \frac{n+1}{1} \cdot \frac{n+2}{2} \cdots \frac{2n}{n} \geq 2^n,$$

zodat uit (12) volgt

$$\psi(2n) \geq n\log 2 .$$

Zij x nu een willekeurig getal met $x \geq 4$ en $2n \leq x < 2n+2$ dan volgt

$$\psi(x) \geq \psi(2n) \geq n\log 2 > (\tfrac{x}{2} - 1)\log 2 \geq \tfrac{1}{4}x\log 2.$$

Het is duidelijk dat deze ongelijkheid ook geldt voor $2 \leq x < 4$, zodat stelling 2 bewezen is met $B = \frac{1}{4}\log 2$.

Stelling 4. Er bestaan positieve constanten a_1 en a_2 zodat voor het r^e priemgetal p_r geldt

$$a_1 r\log r < p_r < a_2 r\log r \qquad \text{voor } r \geq 2.$$

Bewijs. Uit stelling 1 met $x = p_r$ volgt

$$(13) \qquad c_1 \frac{p_r}{\log p_r} < r < c_2 \frac{p_r}{\log p_r} .$$

Uit de 2^e ongelijkheid van (13) volgt daar $p_r \geq r$

$$p_r > \frac{1}{c_2} r\log p_r \geq \frac{1}{c_2} r\log r,$$

waaruit de 1^e ongelijkheid van stelling 4 volgt.

Uit de 1^e ongelijkheid van (13) volgt

(14) $$p_r < \frac{1}{c_1} r\log p_r.$$

We hebben nu nog een bovengrens voor $\log p_r$ nodig. Deze vinden we als volgt. De 1^e ongelijkheid van (13) is ook te schrijven als

$$\frac{c_1 \sqrt{p_r}\sqrt{p_r}}{\log p_r} < r$$

zodat

$$\sqrt{p_r} < \frac{r}{c_1} \frac{\log p_r}{\sqrt{p_r}}$$

Daar $\lim_{x\to\infty} \frac{\log x}{\sqrt{x}} = 0$ is dan

$$\sqrt{p_r} < r$$

als r voldoende groot is, ofwel

(15) $$p_r < r^2 \quad \text{als } r > r_0.$$

Dan volgt uit (14) en (15)

(16) $$p_r < \frac{2}{c_1} r\log r \quad \text{als } r > r_0.$$

We kunnen nu de factor $\frac{2}{c_1}$ vergroten zodat (16) ook geldt voor $r = 1,2,3,\ldots,r_0$, zodat

$$p_r < a_2 r\log r$$

voor geschikte constante a_2.

Stelling 5. Er bestaan positieve constanten b_1 en b_2 zodat

$$b_1 \text{ loglogx} < \sum_{p \leq x} \frac{1}{p} < b_2 \text{ loglogx} \qquad \text{voor } x \geq 3 .$$

Bewijs.
Uit stelling 4 volgt

$$(17) \qquad \frac{1}{a_2} \sum_{r=2}^{\pi(x)} \frac{1}{r\log r} < \sum_{3 \leq p \leq x} \frac{1}{p} < \frac{1}{a_1} \sum_{r=2}^{\pi(x)} \frac{1}{r\log r} .$$

Daar

$$\int_2^n \frac{1}{x\log x}\, dx = \text{loglogn} - \text{loglog2}$$

volgt uit hoofdstuk IV stelling 2

$$(18) \qquad \sum_{r=2}^{n} \frac{1}{r\log r} = \text{loglogn} + R(n)$$

met

$$(19) \qquad |R(n)| < A + \frac{c}{n\log n} < B \qquad \text{voor } n \geq 3$$

waarin A, C en B positieve constanten zijn.
Uit (17), (18), (19) en $\pi(x) \leq x$ volgt

$$\sum_{p \leq x} \frac{1}{p} < \tfrac{1}{2} + \frac{1}{a_1} \sum_{r=2}^{x} \frac{1}{r\log r} < \frac{1}{a_1} \text{loglogx} + \tfrac{1}{2} + B.$$

Voor $x \geq 3$ is $\text{loglogx} > 0$, zodat er een constante b_2 bestaat met

$$\frac{1}{a_1} \text{loglogx} + \tfrac{1}{2} + B < b_2 \text{ loglogx} \qquad \text{voor } x \geq 3.$$

Hiermee is de 2^e ongelijkheid van stelling 5 bewezen. Zij c_1 de positieve constante uit stelling 1
dan is

$$\frac{c_1 x}{\log x} > \sqrt{x}$$

als x voldoende groot is, zeg $x > x_1 \geq 3$.
Dan is $\pi(x) > \sqrt{x} > 1$ voor $x > x_1$.
Voor $x > x_1$ volgt dan uit (17), (18) en (19)

$$\sum_{p \leq x} \frac{1}{p} > \frac{1}{a_2} \sum_{r=2}^{\pi(n)} \frac{1}{r \log r} > \frac{1}{a_2} \log\log\sqrt{x} - B =$$

$$\frac{1}{a_2} \log\log x - \frac{1}{a_2} \log 2 - B.$$

Nu is het laatste lid groter dan $\frac{1}{2a_2} \log\log x$ als x voldoende groot is, zeg $x > x_2 \geq x_1$.
Dan geldt voor $x > x_2$ de 1^e ongelijkheid van stelling 5 met $b_1 = \frac{1}{2a_2}$
Daar $\log\log x > 0$ voor $x \geq 3$ kunnen we de factor $\frac{1}{2a_2}$ verkleinen tot een positieve factor b_1 zodat de ongelijkheid geldt voor alle $x \geq 3$.

Opmerking 4. Stelling 5 is te verscherpen tot

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + c + O\left(\frac{1}{\log x}\right) \quad \text{voor } x \to \infty,$$

waarin c een constante is. (zie bijvoorbeeld LeVeque pag. 101-108).

Stelling 6. Voor ieder natuurlijk getal n, bestaat er minstens één priemgetal p met $n < p \leq 2n$.

Opmerking 5. In 1845 toonde Bertrand aan dat stelling 6 waar is voor $1 \leq n \leq 6.10^6$ en hij sprak het vermoeden uit dat de stelling voor alle n geldt. Dit werd bewezen door Tchebycheff in 1850.

Bewijs stelling 6.
Veronderstel dat de stelling niet waar is voor zekere $n \geq 8$. Beschouw als boven $N = \binom{2n}{n} = \frac{(2n)!}{(n!)^2}$.

De priemgetallen p met $p \leq 2n$ delen we in 4 klassen in:

1) $n < p \leq 2n$,

2) $\frac{2}{3}n < p \leq n$,

3) $\sqrt{2n} < p \leq \frac{2}{3}n$,

4) $p \leq \sqrt{2n}$.

ad1. Volgens de veronderstelling zijn er geen priemgetallen in deze klasse.

ad2. Voor een priemgetal p in deze klasse geldt dat $p \leq 2n$ en $2p \leq 2n$, terwijl alle andere p-vouden groter dan 2n zijn. Daar $n \geq 8$ is $p \neq 2$ zodat (2n)! precies 2 factoren p bevat. Verder is $p \leq n$ terwijl alle andere p-vouden groter dan n zijn, zodat n! precies 1 factor p bevat. N bevat dus geen factoren p uit deze klasse.

ad 3 en 4. Uit (12) en (3) volgt

$$\log N \leq \psi(2n) = \sum_{p \leq 2n} \left[\frac{\log 2n}{\log p}\right] \log p.$$

Een priemfactor p komt dus hoogstens tot de macht $\left[\frac{\log 2n}{\log p}\right]$ in N voor.

ad3. Uit $p > \sqrt{2n}$ volgt

$$\left[\frac{\log 2n}{\log p}\right] < 2$$

zodat een priemgetal uit klasse 3 hoogstens tot de macht 1 in N voorkomt. We krijgen dus

$$\log N \leq \sum_{\sqrt{2n} < p \leq \frac{2}{3}n} \log p + \sum_{p \leq \sqrt{2n}} \left[\frac{\log 2n}{\log p}\right] \log p \leq$$

(20)

$$\theta\left(\frac{2n}{3}\right) + \pi(\sqrt{2n}) \log 2n.$$

Uit $n \geq 8$ volgt $\sqrt{2n} \geq 4$ en daar 1 en 4 geen priemgetallen zijn is dan

(21) $$\pi(\sqrt{2n}) \leq \sqrt{2n} - 2.$$

Uit (20), (9) en (21) volgt

(22) $$\log N \leq \frac{4n}{3}\log 2 + (\sqrt{2n} - 2)\log 2n.$$

Anderzijds is N de grootste binomiaalcoefficient in de ontwikkeling van $(1+1)^{2n}$ zodat

(23) $$N > \frac{2^{2n}}{2n+1} > \frac{2^{2n}}{4n^2}.$$

Uit (22) en (23) volgt dan

$$\frac{1}{3}\sqrt{2n\log 2} < \log 2n.$$

Dit is onjuist voor $n \geq 450$. De stelling is dus juist voor $n \geq 450$. Verder is in de rij priemgetallen 2,3,4,7,13,23,43,83,163,317,557 ieder priemgetal kleiner dan tweemaal zijn voorganger. Hieruit volgt dat de stelling ook geldt voor $n < 450$.

Literatuur bij hoofdstuk V:

K. Chandrasekharan: Einführung in die Analytische Zahlentheorie, Kapitel VII.

G.H. Hardy, E.M. Wright: An introduction to the theory of numbers, Chapter XXII.

W.J. LeVeque: Topics in number theory, volume I, Chapter 6.

I. Niven, H.S. Zuckerman: An introduction to the theory of numbers, Chapter 8.

Hoofdstuk VI: Voorstelling van een natuurlijk getal als som van kwadraten.

Stelling 1. (Lagrange) Ieder natuurlijk getal n is te schrijven als som van vier kwadraten van gehele getallen: $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$, $x \in Z (i = 1,2,3,4)$.

Bewijs. Het bewijs verloopt in 3 stappen.

a) Allereerst merken we op dat de stelling waar is voor n = 1 en n = 2. Verder volgt uit de identiteit van Euler

$$(x_1^2+x_2^2+x_3^2+x_4^2)\,(y_1^2+y_2^2+y_3^2+y_4^2) =$$

$$(1)\quad (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 + (x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 +$$

$$(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2 + (x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2$$

dat als de stelling waar is voor n en m dat hij dan ook waar is voor nm. We hoeven dus alleen te bewijzen dat de stelling waar is voor alle priemgetallen p > 2.

b) Zij p priemgetal met p > 2. We bewijzen eerst dat er een veelvoud mp van p bestaat dat te schrijven is als som van 3 (dus van 4) kwadraten op de volgende wijze

$$mp = x^2+y^2+1 \quad \text{met} \quad 1 \leq m < p.$$

Laat x de getallen $0,1,2,\ldots,\frac{p-1}{2}$ doorlopen en beschouw de bijbehorende getallen x^2. Uit $x_i^2 \equiv x_j^2$ (mod.p) volgt $p|(x_i-x_j)(x_i+x_j)$ zodat $p|x_i-x_j$ of $p|x_i+x_j$ hetgeen beide onmogelijk is. De getallen x^2 liggen dus in $\frac{p+1}{2}$ verschillende restklassen mod.p. Laat evenzo y de getallen $0,1,2,\ldots,\frac{p-1}{2}$ doorlopen, dan liggen de getallen $-1-y^2$ eveneens in $\frac{p+1}{2}$ verschillende restklassen mod.p.
Daar er p restklassen mod.p zijn, bestaan er een zekere $x \in 0,1,\ldots\frac{p-1}{2}$ en een $y \in 0,1,\ldots,\frac{p-1}{2}$ zodat x^2 en $-1-y^2$ in dezelfde restklasse liggen,

---

syll. ZC 78, afl. 7.

d.w.z.

$$x^2+y^2+1 = mp \qquad \text{voor zekere } m.$$

Verder is

$$0 < x^2+y^2+1 \leq 2(\frac{p-1}{2})^2+1 < p^2 ,$$

zodat $1 \leq m < p$.

c) Zij nu m_0p het <u>kleinste</u> positieve veelvoud van p dat als som van 4 kwadraten te schrijven is

$$(2) \qquad m_0p = x_1^2+x_2^2+x_3^2+x_4^2 , \quad \text{zodat } 1 \leq m_0 < p .$$

We zullen bewijzen $m_0 = 1$; daarmee is dan het bewijs van stelling 1 voltooid.

Stel dat m_0 even is. Dan zijn er 3 mogelijkheden:

1e) x_1, x_2, x_3, x_4 alle even.

2e) x_1, x_2, x_3, x_4 alle oneven.

3e) Van de x_1, x_2, x_3, x_4 zijn 2 getallen even en 2 oneven; laten in dit geval x_1 en x_2 even zijn.

In alle 3 gevallen zijn $\frac{1}{2}(x_1+x_2)$, $\frac{1}{2}(x_1-x_2)$, $\frac{1}{2}(x_3+x_4)$ en $\frac{1}{2}(x_3-x_4)$ gehele getallen, terwijl uit (2) volgt

$$\tfrac{1}{2}m_0p = (\frac{x_1+x_2}{2})^2 + (\frac{x_1-x_2}{2})^2 + (\frac{x_3+x_4}{2})^2 + (\frac{x_3-x_4}{2})^2 ,$$

d.w.z. ook $\frac{1}{2}m_0p$ is te schrijven als som van 4 kwadraten. Dit is in tegenspraak met de onderstelling dat m_0 de kleinste was; dus m_0 is oneven.

Stel $m_0 \geq 3$; we leiden een tegenspraak af, waaruit dan volgt $m_0 = 1$.

Schrijf

$$(3) \qquad x_i = b_im_0+y_i \qquad (i = 1,2,3,4).$$

Daar m_0 oneven is, kunnen we gehele getallen b_i zo kiezen dat

$$(4) \qquad |y_i| < \tfrac{1}{2} m_0.$$

Uit (2) volgt dat de x_i niet alle deelbaar door m_0 zijn, zodat de y_i niet alle 0 zijn, ofwel

$$y_1^2+y_2^2+y_3^2+y_4^2 > 0 \quad .$$

Verder is volgens (4)

$$y_1^2+y_2^2+y_3^2+y_4^2 < 4(\tfrac{1}{2}m_0)^2 = m_0^2 \quad . \tag{5}$$

Uit (2) en (3) volgt verder

$$y_1^2+y_2^2+y_3^2+y_4^2 \equiv 0 \pmod{m_0}, \tag{6}$$

zodat uit (5) en (6) volgt

$$y_1^2+y_2^2+y_3^2+y_4^2 = m_1m_0 \text{ met } 1 \leq m_1 < m_0. \tag{7}$$

Uit (2), (7) en (1) volgt dat ook $m_0pm_1m_0$ te schrijven is als som van 4 kwadraten:

$$m_0^2m_1p = z_1^2+z_2^2+z_3^2+z_4^2 \quad . \tag{8}$$

Uit (1), (3) en (7) volgt verder

$$z_1 = \Sigma x_iy_i = \Sigma(b_im_0+y_i)y_i \equiv 0 \pmod{m_0}.$$

Analoog volgt $z_2 \equiv z_3 \equiv z_4 \equiv 0 \pmod{m_0}$.
Schrijf $z_i = m_0t_i$ dan volgt uit (8)

$$m_1p = t_1^2+t_2^2+t_3^2+t_4^2 \quad ,$$

waarin $m_1 < m_0$. Dit is in tegenspraak met het feit dat m_0p het kleinste veelvoud van p is dat als som van 4 kwadraten te schrijven is.

<u>Som van drie kwadraten</u>.

Het is niet mogelijk ieder natuurlijk getal als som van 3 kwadraten te schrijven. Dit is als volgt eenvoudig in te zien. Een kwadraat is modulo 8 steeds congruent één van de getallen 0,1 of 4. Een som

van 3 kwadraten is dan modulo 8 congruent met één van de getallen 0,1,2,3,4,5 of 6. Een natuurlijk getal n met $n \equiv 7 \pmod{8}$ is dus niet te schrijven als som van 3 kwadraten.

Opmerking 1.

Van Waring (1770) is de veronderstelling afkomstig dat er voor iedere k een kleinste getal g(k) bestaat zodat ieder natuurlijk getal als som van g(k) k^e machten te schrijven is. Zoals boven is aangetoond is $g(2) = 4$. Verder is $g(3) = 9$. Hilbert bewees in 1909 het bestaan van g(k) voor willekeurige k. De waarden van g(4) en g(5) zijn onbekend, terwijl g(k) voor $k \geq 6$ bekend is op een kleine onzekerheid na. (zie hiervoor bijvoorbeeld Hardy & Wright p..337).
Van belang is ook G(k): het kleinste getal met de eigenschap dat ieder natuurlijk getal op eindig vele na te schrijven is als de som van G(k) k^e machten. Uiteraard is $G(k) \leq g(k)$. Uit bovenstaande berekeningen volgt $G(2) = 4$. Verder is $G(3) \leq 7$, daar ieder natuurlijk getal groter dan 454 als som van 7 derde machten te schrijven is. De waarde van G(k) is alleen voor $k = 2$ en $k = 4$ bekend.

Som van twee kwadraten.

We onderzoeken welke natuurlijke getallen als som van 2 kwadraten te schrijven zijn. Daarbij gebruiken we twee stellingen die ook op zichzelf interessant zijn.

Stelling 2. Zij p een priemgetal, $p \neq 2$.

a) Is $p \equiv 1 \pmod{4}$, dan is de vergelijking $x^2 \equiv -1 \pmod{p}$ oplosbaar.

b) Is $p \equiv 3 \pmod{4}$, dan is de vergelijking $x^2 \equiv -1 \pmod{p}$ niet oplosbaar.

Bewijs.

a) Volgens de stelling van Wilson (zie pag.19) geldt

$$(1.2\ldots\frac{p-1}{2})(\frac{p+1}{2} \ldots p-1) \equiv -1 \pmod{p}$$

ofwel

$$\prod_{j=1}^{\frac{p-1}{2}} j(p-j) \equiv -1 \pmod{p}$$

zodat

$$(-1)^{\frac{p-1}{2}} \prod_{j=1}^{\frac{p-1}{2}} j^2 \equiv -1 \pmod{p}.$$

Daar $\frac{p-1}{2}$ even is voor $p \equiv 1 \pmod{4}$ heeft de vergelijking $x^2 \equiv -1 \pmod{p}$ de oplossing $x = \prod_{j=1}^{\frac{p-1}{2}} j$.

b) Stel dat voor zekere a geldt $a^2 \equiv -1 \pmod{p}$, dan volgt daar $\frac{p-1}{2}$ oneven is
$a^{p-1} = (a^2)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ wat in strijd is met de stelling van Fermat (zie pag. 19).

Stelling 3. Zij α een reëel getal en n een natuurlijk getal, dan bestaan er gehele getallen x en y zodat

$$|\alpha - \frac{x}{y}| \leq \frac{1}{(n+1)y} \quad , \qquad 1 \leq y \leq n.$$

Bewijs. We beschouwen de n getallen

$$k\alpha - [k\alpha] \quad , \; k = 1,2,\ldots,n.$$

Deze liggen alle in het interval $[0,1)$.
We nummeren ze opvolgend naar grootte $0 \leq c_1 \leq c_2 \leq \ldots \leq c_n < 1$. Beschouw de n + 1 afstanden c_1-0, $c_2-c_1,\ldots,c_n-c_{n-1}$, $1-c_n$. Minstens één van deze is $\leq \frac{1}{n+1}$.
Nu is c_i-c_{i-1} $(i=2,\ldots,n)$ van de vorm $k_1\alpha - [k_1\alpha] - (k_2\alpha-[k_2\alpha]) = s\alpha-t$ voor zekere gehele getallen s en t, waarin $1 \leq |s| \leq n$. Dit geldt ook voor c_1-0 en $1-c_n$. Er bestaan dus gehele getallen s en t met

$$|s\alpha-t| \leq \frac{1}{n+1} \quad , \quad 1 \leq |s| \leq n \; .$$

Met $y = |s|$ en $x = t$ voor $s > 0$, $x = -t$ voor $s \leq 0$ volgt de stelling.

Gevolg 1. Uit stelling 3 volgt:
Zij α een reëel getal, dan bestaan er gehele getallen x en y zodat

$$|\alpha - \frac{x}{y}| < \frac{1}{y^2} \quad .$$

Stelling 4. Zij p een priemgetal met $p \equiv 1 \pmod{4}$ dan bestaan er gehele getallen a en b zodat $p = a^2+b^2$.

Bewijs. Volgens stelling 2a bestaat er een u zodat

$$u^2 \equiv -1 \pmod{p} \tag{9}$$

We gebruiken nu stelling 3 met $\alpha = \frac{u}{p}$, $n = [\sqrt{p}]$.
Er bestaan dan getallen x en y met

$$|\frac{u}{p} - \frac{x}{y}| \leq \frac{1}{([\sqrt{p}]+1)y} < \frac{1}{\sqrt{p}y} , \quad 1 \leq y \leq \sqrt{p}.$$

Zodat

$$|uy-xp| < \sqrt{p} \quad .$$

Stel $a = uy-xp$, $b = y$ dan is $|a| < \sqrt{p}$, $1 \leq b \leq \sqrt{p}$.

Hieruit volgt $1 \leq a^2+b^2 < p+p = 2p$.
Verder is volgens (9)

$$a^2+b^2 \equiv u^2y^2+y^2 \equiv 0 \pmod{p}$$

zodat

$$a^2+b^2 = p.$$

Opmerking 2. Is p een priemgetal met $p \equiv 3 \pmod{4}$ dan is als volgt eenvoudig in te zien dat p niet te schrijven is als som van twee kwadraten. Een kwadraat is mod.4 altijd congruent met een van de getallen 0 of 1, zodat de som van 2 kwadraten mod.4 congruent is met 0,1 of 2.

Stelling 5. Zij n een natuurlijk getal. Komen in de kanonieke ontbinding van n alle priemgetallen van de vorm $p \equiv 3 \pmod 4$ tot een even macht voor, dan is n te schrijven als som van twee kwadraten.

Bewijs. Volgens het gegeven is n te schrijven als $n = n_1^2 n_2$, waarbij in n_2 alleen priemgetallen van de vorm 2 of $p \equiv 1 \pmod 4$ voorkomen. Deze priemgetallen zijn alle als som van 2 kwadraten te schrijven (zie stelling 4).
Verder volgt uit

$$(a_1^2+b_1^2)(a_2^2+b_2^2) = (a_1a_2+b_1b_2)^2 + (a_1b_2-a_2b_1)^2$$

dat als p en q als som van 2 kwadraten te schrijven zijn, dat dan ook pq de som is van 2 kwadraten. Door herhaald toepassen hiervan volgt dat ook n_2 te schrijven is als som van 2 kwadraten: $n_2 = a^2+b^2$, waaruit volgt $n = (n_1a)^2 + (n_1b)^2$.

Stelling 6. Zij n een natuurlijk getal. Komt in de kanonieke ontbinding van n een priemgetal p met $p \equiv 3 \pmod 4$ tot een oneven macht voor dan is n niet te schrijven als som van twee kwadraten.

Bewijs. Stel $n = a^2+b^2$.
Zij $(a,b) = d$, $a = da_1$, $b = db_1$, dan volgt $(a_1,b_1) = 1$ en $n = d^2(a_1^2+b_1^2)$. Dan is n deelbaar door d^2: zij $n = d^2n_1$. Daar n een oneven aantal factoren p bevat, heeft ook n_1 factoren p.
We hebben nu

$$n_1 = a_1^2+b_1^2 \ , \quad (a_1,b_1) = 1, \ p \mid n_1.$$

Uit $p \mid a_1$ volgt, daar $p \mid n_1$, dat $p \mid b_1$, wat in tegenspraak is met $(a_1,b_1) = 1$. Dus $p \nmid a_1$ en analoog $p \nmid b_1$. Uit pag. 22-23 stelling 8 volgt dan dat er een geheel getal u bestaat met $a_1u \equiv b_1 \pmod p$. Dan is

$$a_1^2+a_1^2u^2 \equiv a_1^2+b_1^2 \equiv 0 \pmod p.$$

Hieruit volgt daar $(a_1,p) = 1$ dat $1+u^2 \equiv 0 \pmod p$ in tegenspraak met stelling 2b.

Grootte-orde van R(N).

Zij n een natuurlijk getal, dan is n te schrijven als $n = a^2+b^2$, $a \in Z$, $b \in Z$, dan en slechts dan als het roosterpunt (a,b) ligt op de cirkel om (0,0) met straal $\sqrt{n}$. Zij r(n) het aantal roosterpunten op deze cirkel, dan is r(n) gelijk aan het aantal mogelijkheden om n als som van 2 kwadraten te schrijven. Merk op dat hierbij voorstellingen die uit $n = a^2+b^2$ ontstaan door a of b van teken te wisselen (als $a \neq 0$ of $b \neq 0$) of a en b te verwisselen (als $a \neq b$) als verschillende voorstellingen geteld worden.

We hebben $r(1) = 4$, $r(2) = 4$, $r(3) = 0$, $r(4) = 4$, $r(5) = 8$ enz.

Men kan bewijzen: zij $n = 2^k n_1 n_2$ waarin n_1 alle priemfactoren $p \equiv 1 \pmod 4$ en n_2 alle priemfactoren $p \equiv 3 \pmod 4$ bevat, dan is

$$r(n) = \begin{cases} 4\tau(n_1) & \text{als } n_2 \text{ een kwadraat is} \\ 0 & \text{als } n_2 \text{ geen kwadraat is.} \end{cases}$$

(vergelijk stelling 6)

(zie bijvoorbeeld LeVeque p.132).

We zullen een schatting geven voor $R(N) = \sum_{n=1}^{N} r(n)$. R(N) is gelijk aan het aantal roosterpunten binnen en op de cirkel om (0,0) met straal $\sqrt{N}$. Om dit aantal roosterpunten te tellen voegen we aan ieder roosterpunt A binnen of op de cirkel het eenheidsvierkant toe waarvan A het rechterboven hoekpunt is. Dezevierkanten vormen een samenhangend stuk H, waarbij R(N) = oppervlakte H. Daar H bevat is in de cirkel om (0,0) met straal $\sqrt{N} + \sqrt{2}$ en de cirkel om (0,0) met straal $\sqrt{N} - \sqrt{2}$ omvat (als $N \geq 2$), volgt

$$\pi(\sqrt{N}-\sqrt{2})^2 < R(N) < \pi(\sqrt{N}+\sqrt{2})^2$$

zodat

$$R(N) = \pi N + O(\sqrt{N}) \qquad \text{voor } N \to \infty .$$

Gehele getallen van Gauss.

De verzameling complexe getallen $a + bi$ met $a \in Z$, $b \in Z$ heet de gehele getallen van Gauss. We noteren deze verzameling met R[i].

Zoals bekend is

$$(a_1+b_1i) \pm (a_2+b_2i) = a_1 \pm a_2 + (b_1 \pm b_2)i ,$$

$$(a_1+b_1i)(a_2+b_2i) = a_1a_2 - b_1b_2 + (a_1b_2+a_2b_1)i.$$

Is $\alpha = a+bi$ dan is de <u>norm</u> van α: $N\alpha = a^2+b^2$;
zodat $N\alpha \in Z$.
Er is eenvoudig af te leiden

(10) $$N\alpha\beta = N\alpha.N\beta.$$

Een element $\varepsilon \in R[i]$ heet een <u>eenheid</u> als ook $\frac{1}{\varepsilon} \in R[i]$.
We bepalen de eenheden van $R[i]$. Zij $\varepsilon = a+bi$ een eenheid dan is

$$\frac{1}{\varepsilon} = \frac{1}{a+bi} = \frac{a-bi}{a^2+b^2}$$

zodat $a^2+b^2 \mid a$ en $a^2+b^2 \mid b$. Hieruit volgt dat a of b gelijk 0 is. De eenheden zijn dus 1, -1, i en -i.

<u>Opmerking 3.</u> Een getal $\alpha \in R[i]$ is een eenheid dan en slechts dan als $N(\alpha) = 1$.

Is $\alpha \in R[i]$ dan heten $-\alpha$, $i\alpha$ en $-i\alpha$ de <u>geassocieerden</u> van α; een geassocieerde van α is dus van de vorm $\varepsilon\alpha$ met ε eenheid.
Het getal $\alpha \in R[i]$ heet een <u>deler</u> van $\beta \in R[i]$ als er een $\gamma \in R[i]$ bestaat zodat $\alpha\gamma = \beta$, notatie $\alpha \mid \beta$. Een getal $\alpha \in R[i]$ heeft altijd de eenheden en de geassocieerden van α als delers. Heeft $\pi \in R[i]$ geen delers behalve de eenheden en de geassocieerden van π dan heet π <u>priemelement</u> van $R[i]$. Is π priemelement van $R[i]$ en ε eenheid dan is ook $\varepsilon\pi$ priemelement.

Met redeneringen analoog aan die in hoofdstuk I voor de ontbinding in Z is aan te tonen dat ieder getal uit $R[i]$ in priemelementen te ontbinden is, waarbij de volgende stelling geldt. (zie bijvoorbeeld Hardy & Wright p. 185-187).

Stelling 7. Iedere $\alpha \in R[i]$ is te schrijven als product van priemelementen. Deze voorstelling is eenduidig afgezien van de volgorde, eenheden en de mogelijkheid priemelementen door geassocieerden te vervangen.

Lemma 1. Is $\alpha \in R[i]$ en is $N\alpha$ priemgetal uit Z, dan is α een priemelement van R[i].

Bewijs. Stel $\alpha = \beta\gamma$, dan volgt uit (10) dat $N\alpha = N\beta.N\gamma$. Daar $N\alpha$ priem is, volgt $N\beta = 1$ of $N\gamma = 1$. Stel $N\beta = 1$, dan is volgens opmerking 3 β een eenheid en dus $\gamma = \beta^{-1}\alpha$ een geassocieerde van α. Hieruit volgt dat α priemelement is.

We onderzoeken nu welke priemgetallen uit Z ook priemelementen van R[i] zijn.

a) Het getal 2 is te ontbinden als $2 = (1+i)(1-i)$, zodat 2 in R[i] geen priemgetal is. Daar $N(1\pm i) = 2$ een priemgetal uit Z is, zijn volgens lemma 1 $1+i$ en $1-i$ priemelementen van R[i]. Daar $1-i = -i(1+i)$ zijn $1+i$ en $1-i$ geassocieerd.

b) Is $p \in Z$, p priemgetal met $p \equiv 1 \pmod 4$ dan is volgens stelling 4 p in R[i] te ontbinden volgens $p = (a+bi)(a-bi)$. Hierin is $N(a\pm bi) = a^2+b^2 = p$ een priemgetal, zodat $a+bi$ en $a-bi$ volgens lemma 1 priemelementen van R[i] zijn. Men gaat eenvoudig na dat deze priemelementen niet geassocieerd zijn.

c) Zij $p \in Z$, p priemgetal met $p \equiv 3 \pmod 4$. Stel dat p in R[i] te ontbinden is volgens $p = (a+bi)(c+di)$. Dan volgt $p^2 = Np = N(a+bi)\,N(c+di) = (a^2+b^2)(c^2+d^2)$. De enige ontbindingen van p^2 zijn $p.p$ en $1.p^2$. Daar $a^2+b^2 = c^2+d^2 = p$ in strijd is met opmerking 2 volgt dat $a+bi$ of $c+di$ norm 1 heeft en dus een eenheid is, terwijl het andere element dan een geassocieerde van p is. Het getal p is dus priemelement van R[i].

We zullen nu bewijzen dat we hiermee alle priemelementen van R[i] gevonden hebben.

Stelling 8. De priemelementen van R[i] zijn:

a) 1+i

b) de factoren a+bi van de priemgetallen uit Z congruent 1 (mod.4)

c) de priemgetallen uit Z congruent 3 (mod.4) en hun geassocieerden.

Bewijs. Zij $\pi = a+bi$ een priemelement van R[i], dan is $(a+bi)(a-bi) = a^2+b^2$ een natuurlijk getal. Er bestaan dus natuurlijke getallen die π als deler hebben. Zij n het kleinste natuurlijke getal, dat π als deler heeft. We bewijzen dat n een priemgetal uit Z is. Stel dat n geen priemgetal is, dan is $n = n_1 n_2$ met $1 < n_1 < n$, $1 < n_2 < n$. Uit $\pi | n$ volgt met stelling 7 dat $\pi | n_1$ of $\pi | n_2$, in tegenspraak met het feit dat n het kleinste natuurlijke getal met π als deler is.
Alle priemelementen van R[i] zijn dus delers van priemgetallen uit Z. Uit de boven gevonden resultaten volgt dan de stelling.

Literatuur bij Hoofdstuk VI.

G.H. Hardy, E.M. Wright: An introduction to the theory of numbers, 12.6, 7, 8; 15.1; 16.9,10; 18.7; Chapter 20,21.

I. Niven, H.S. Zuckerman: An introduction to the theory of numbers, Chapter 5.

W.J. LeVeque: Topics in number theory, volume I, Chapter 7.

Hoofdstuk VII: Approximatie van reële getallen met rationale getallen.

In hoofdstuk VI stelling 3 en gevolg 1 vonden we: zij α een reëel getal en n een natuurlijk getal dan bestaat er een rationaal getal $\frac{x}{y}$ zodat

$$|\alpha - \frac{x}{y}| \leq \frac{1}{(n+1)y} \quad , \quad 1 \leq y \leq n$$

zodat

(1) $$|\alpha - \frac{x}{y}| < \frac{1}{y^2} \quad .$$

We bewijzen nu:

Stelling 1.

a) Is α een rationaal getal, dan heeft (1) slechts eindig veel oplossingen $\frac{x}{y}$ met $\frac{x}{y} \neq \alpha$.

b) Is α irrationaal, dan heeft (1) oneindig veel verschillende oplossingen.

Bewijs.

a) Zij $\alpha = \frac{a}{b}$ en $\frac{x}{y} \neq \frac{a}{b}$, dan volgt

$$|\frac{a}{b} - \frac{x}{y}| = \frac{|ay - bx|}{|by|} \geq \frac{1}{|by|} \quad .$$

Als $\frac{x}{y}$ voldoet aan (1), dan volgt $\frac{1}{|by|} < \frac{1}{y^2}$ zodat $|y| < |b|$. De noemer y kan dus slechts eindig veel verschillende waarden aannemen, zodat (1) slechts een eindig aantal oplossingen heeft.

b) Voor ieder natuurlijk getal n bestaat er een breuk $\frac{x_n}{y_n}$ zodat

$$|\alpha - \frac{x_n}{y_n}| \leq \frac{1}{(n+1)y_n} \quad , \quad 1 \leq y_n \leq n.$$

Deze voldoen dus aan (1). Onder de $\frac{x_n}{y_n}$ kunnen een aantal gelijk zijn.

Syll. ZC78, afl. 8.

Stel dat er slechts eindig veel verschillende zijn, dan zijn er slechts eindig veel verschillende getallen $|\alpha - \frac{x_n}{y_n}|$. Zij $|\alpha - \frac{x_k}{y_k}|$ de kleinste, dan volgt

$$|\alpha - \frac{x_k}{y_k}| \leq |\alpha - \frac{x_n}{y_n}| \leq \frac{1}{(n+1)y_n} \leq \frac{1}{n+1}$$

voor alle n. Dan is echter $\alpha = \frac{x_k}{y_k}$ in tegenspraak met het gegeven dat α irrationaal is.

We zullen in onderstaande een methode behandelen om de $\frac{x}{y}$ uit (1) te berekenen en bovendien deze ongelijkheid verscherpen.

Kettingbreukontwikkeling.

Zij α een reëel getal. We ontwikkelen α als volgt in een kettingbreuk. Zij $a_0 = [\alpha]$, dan stellen we $\alpha = a_0 + \rho_1$ met $0 \leq \rho_1 < 1$. Is $\rho_1 \neq 0$, stel dan $\rho_1 = \frac{1}{\alpha_1}$, zodat $\alpha = a_0 + \frac{1}{\alpha_1}$. Zij nu $a_1 = [\alpha_1]$, dan is $\alpha_1 = a_1 + \rho_2$ met $0 \leq \rho_2 < 1$. Is $\rho_2 \neq 0$, dan stellen we $\rho_2 = \frac{1}{\alpha_2}$, zodat $\alpha_1 = a_1 + \frac{1}{\alpha_2}$ en

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}} \quad .$$

We zetten dit proces voort. Is α_{n-1} gedefinieerd dan wordt α_n als volgt gevonden: $a_{n-1} = [\alpha_{n-1}]$ zodat $\alpha_{n-1} = a_{n-1} + \rho_n$ met $0 \leq \rho_n < 1$; is $\rho_n \neq 0$ dan stellen we $\rho_n = \frac{1}{\alpha_n}$, zodat $\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}$.

Is $\rho_i \neq 0$, $i = 1,2,\ldots,n$ dan is dus

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \frac{1}{\alpha_n}}}} \quad .$$

Een dergelijke breuk heet een kettingbreuk.
We noteren deze kettingbreuk met

$$(2) \qquad \alpha = \langle a_0, a_1, \ldots, a_{n-1}, \alpha_n \rangle$$

Merk op dat $a_1, a_2, \ldots$ positieve gehele getallen worden, dat a_0 een willekeurig geheel getal is en dat $\alpha_n > 1$ is.
Er zijn nu twee mogelijkheden.

a) Het proces breekt af omdat $\rho_{N+1} = 0$ voor zekere $N \geq 0$. In dat geval is $\alpha = \langle a_0, a_1, \ldots, a_N \rangle$ kennelijk een rationaal getal.
We tonen nu aan, dat als omgekeerd α een rationaal getal is het proces afbreekt omdat $\rho_{N+1} = 0$ voor zekere N.
Zij $\alpha = \frac{a}{b}$ dan is met $a_0, a_1, a_2, \ldots$ en $\rho_1, \rho_2, \ldots$ als boven

$$\frac{a}{b} = a_0 + \frac{r_1}{b} \text{ met } 0 \leq r_1 < b \text{ en } \rho_1 = \frac{r_1}{b}.$$

Is $r_1 \neq 0$ dan is $\frac{b}{r_1} = a_1 + \frac{r_2}{r_1}$ met $0 \leq r_2 < r_1$ en $\rho_2 = \frac{r_2}{r_1}$.

Is $r_2 \neq 0$ dan is $\frac{r_1}{r_2} = a_2 + \frac{r_3}{r_2}$ met $0 \leq r_3 < r_2$ en $\rho_3 = \frac{r_3}{r_2}$.

Algemeen: is $r_n \neq 0$, dan is $\frac{r_{n-1}}{r_n} = a_n + \frac{r_{n+1}}{r_n}$ met $0 \leq r_{n+1} < r_n$ en $\rho_{n+1} = \frac{r_{n+1}}{r_n}$.

De gevonden vergelijkingen zijn equivalent met

$$\begin{aligned}
a &= a_0 b + r_1 && 0 \leq r_1 < b \\
b &= a_1 r_1 + r_2 && 0 \leq r_2 < r_1 \\
r_1 &= a_2 r_2 + r_3 && 0 \leq r_3 < r_2 \\
&\ldots\ldots\ldots\ldots \\
r_{n-1} &= a_n r_n + r_{n+1} && 0 \leq r_{n+1} < r_n.
\end{aligned}$$

Dit schema is gelijk aan het algorithme van Euclides voor het berekenen van de G.G.D. van a en b (zie pag. 9,10). Het schema breekt dus af doordat $r_{N+1} = 0$ voor zekere N, zodat

$$\rho_{N+1} = \frac{r_{N+1}}{r_N} = 0.$$

b) Het proces breekt niet af, d.w.z. $\rho_{N+1} \neq 0$ voor alle N. Uit a) volgt dat α dan irrationaal is. Voor iedere n geldt (2):

$$\alpha = \langle a_0, a_1, \ldots, a_{n-1}, \alpha_n \rangle .$$

Zij $r_n = \langle a_0, a_1, \ldots, a_n \rangle$ voor $n = 0,1,2,\ldots$, dan is r_n een rationaal getal. In onderstaande (gevolg 5) tonen we aan $\lim_{n\to\infty} r_n = \alpha$. Op grond hiervan definiëren we de oneindige kettingbreuk $\langle a_0, a_1, \ldots \rangle$ als

$$\langle a_0, a_1, a_2, \ldots \rangle = \lim_{n\to\infty} \langle a_0, a_1, \ldots, a_n \rangle = \alpha.$$

De getallen $a_0, a_1, a_2, \ldots$ heten de wijzergetallen uit de kettingbreukontwikkeling van α. De rationale getallen r_n heten benaderende breuken.

Voorbeeld

Zij $\alpha = \frac{\sqrt{5}+1}{2}$, dan is $a_0 = 1$, zodat $\alpha = 1 + \frac{1}{\alpha_1}$, waaruit volgt $\alpha_1 = \alpha$. Dan is echter $a_1 = a_0 = 1$, $\alpha_2 = \alpha_1 = \alpha$. We vinden zo $a_n = 1$, $\alpha_{n+1} = \alpha$, $n = 0,1,2,\ldots$ zodat $\alpha = \langle 1,1,1,\ldots \rangle$.

Stelling 2.

Zij $a_0, a_1, a_2, \ldots$ de wijzergetallen uit de kettingbreukontwikkeling van zeker getal α. De getallen p_n en q_n worden gedefinieerd door:
$p_0 = a_0$, $q_0 = 1$, $p_1 = a_1 a_0 + 1$, $q_1 = a_1$, $p_n = a_n p_{n-1} + p_{n-2}$,
$q_n = a_n q_{n-1} + q_{n-2}$ $(n \geq 2)$. (Is de rij wijzergetallen eindig $a_0, a_1, \ldots, a_N$, d.w.z. α rationaal, dan worden p_n en q_n alleen gedefinieerd voor $0 \leq n \leq N$).
Dan geldt voor $x \neq 0$ dat

$$\langle a_0, \ldots, a_{n-1}, x \rangle = \frac{x p_{n-1} + p_{n-2}}{x q_{n-1} + q_{n-2}} \quad \text{voor } n \geq 2.$$

In het bijzonder is

$$r_n = \langle a_0, \ldots, a_{n-1}, a_n \rangle = \frac{p_n}{q_n} \quad \text{voor} \quad n = 0,1,2,\ldots .$$

Bewijs.

We bewijzen de stelling met volledige inductie. Men controleert eenvoudig dat de stelling juist is voor n = 0,1,2. Stel nu dat de stelling waar is voor $n = k \geq 2$. Dan is

$$(3) \qquad \langle a_0,\ldots,a_{k-1},y\rangle = \frac{yp_{k-1} + p_{k-2}}{yq_{k-1} + q_{k-2}} \quad .$$

Nu is voor $x \neq 0$

$$\langle a_0,\ldots,a_{k-1},a_k,x\rangle = \langle a_0,\ldots,a_{k-1},a_k + \frac{1}{x}\rangle,$$

zodat uit (3) met $y = a_k + \frac{1}{x}$ volgt

$$\langle a_0,\ldots,a_k,x\rangle = \frac{(a_k + \frac{1}{x})p_{k-1} + p_{k-2}}{(a_k + \frac{1}{x})q_{k-1} + q_{k-2}} =$$

$$\frac{x(a_kp_{k-1} + p_{k-2}) + p_{k-1}}{x(a_kq_{k-1} + q_{k-2}) + q_{k-1}} = \frac{xp_k + p_{k-1}}{xq_k + q_{k-1}} \quad ,$$

zodat de stelling ook geldt voor n = k+1.

Stelling 3.

Zij p_n, q_n als in stelling 2. Dan geldt:

a) $p_nq_{n-1} - p_{n-1}q_n = (-1)^{n-1}$ voor $n \geq 1$.

b) $p_nq_{n-2} - p_{n-2}q_n = (-1)^n a_n$ voor $n \geq 2$.

Bewijs.

a) Voor n = 1 is de stelling juist. Zij $n \geq 2$, dan is

$$p_nq_{n-1} - p_{n-1}q_n = (a_np_{n-1}+p_{n-2})q_{n-1} - p_{n-1}(a_nq_{n-1}+q_{n-2}) =$$

$$-(p_{n-1}q_{n-2}-p_{n-2}q_{n-1}).$$

Hiermee is de gevraagde vorm voor n, teruggebracht tot dezelfde vorm voor n-1. Door herhaald toepassen vinden we

$$p_nq_{n-1} - p_{n-1}q_n = (-1)^{n-1}(p_1q_0-p_0q_1) = (-1)^{n-1}.$$

b) $p_n q_{n-2} - p_{n-2} q_n = (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2}(a_n q_{n-1} + q_{n-2}) =$

$a_n(p_{n-1} q_{n-2} - p_{n-2} q_{n-1})$

en volgens a) is het laatste lid gelijk $(-1)^n a_n$.

Uit de definitie van q_n volgt direct dat $q_n > 0$ $(n = 0,1,2,\ldots)$ zodat uit stelling 3 volgt:

Gevolgen.

1) $$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}} \qquad n \geq 1.$$

2) $$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_n q_{n-2}} \qquad n \geq 2.$$

3) De breuken $\frac{p_n}{q_n}$ zijn irreducibel.

Stelling 4.

Zij r_n als in stelling 2, dan geldt:

a) De r_n met even n vormen een monotoon stijgende rij.

b) De r_n met oneven n vormen een monotoon dalende rij.

Bewijs.

Daar $q_n > 0$ voor $n = 0,1,2,\ldots$ en $a_n > 0$ voor $n = 2,3,\ldots$ is dit een direct gevolg van gevolg 2.

Stelling 5.

Zij α een reëel getal, p_n, q_n, α_{n+1} als boven, dan geldt:

$$\alpha - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(\alpha_{n+1} q_n + q_{n-1})} \qquad n \geq 1.$$

(Is α rationaal, $\alpha = \langle a_0,\ldots,a_N \rangle$, dan moet n beperkt worden tot $1 \leq n \leq N-1$).

Bewijs.
Er geldt volgens (2) en stelling 2

$$\alpha = \langle a_0,\ldots,a_n,\alpha_{n+1}\rangle = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} \quad \text{voor } n \geq 1,$$

zodat met stelling 3a

$$\alpha - \frac{p_n}{q_n} = \frac{p_{n-1}q_n - q_n p_{n-1}}{q_n(\alpha_{n+1}q_n+q_{n-1})} = \frac{(-1)^n}{q_n(\alpha_{n+1}q_n+q_{n-1}} .$$

Gevolg 4. Daar $q_n > 0$ en $\alpha_{n+1} > 1$ voor alle n zijn de $r_n = \frac{p_n}{q_n}$ met even n kleiner dan α en de r_n met oneven n groter dan α.

Stelling 6.
Zij α een reëel getal, p_n en q_n als boven dan geldt

$$\frac{1}{q_n q_{n+2}} < |\alpha - \frac{p_n}{q_n}| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2} \qquad n \geq 1.$$

Bewijs.
Daar $\alpha_{n+1}q_n + q_{n-1} < (a_{n+1}+1)q_n + q_{n-1} = q_{n+1} + q_n \leq q_{n+2}$ en

$\alpha_{n+1}q_n + q_{n-1} \geq a_{n+1}q_n + q_{n-1} = q_{n+1}$ volgen de eerste ongelijkheden uit stelling 5.
Verder volgt uit de definitie van q_n dat $q_{n+1} > q_n$ voor $n \geq 1$. Dit geeft de laatste ongelijkheid.

Gevolg 5. Is α irrationaal dan breekt de kettingbreukontwikkeling van α niet af, zodat p_n en q_n voor alle n gedefinieerd zijn.
Daar q_n een monotoon stijgende rij gehele getallen is, volgt uit stelling 6

$$\lim_{n\to\infty} \langle a_0,\ldots,a_n\rangle = \lim_{n\to\infty} \frac{p_n}{q_n} = \alpha.$$

Samenvatting.
De benaderende breuken $r_n = \langle a_0,\ldots,a_n\rangle = \frac{p_n}{q_n}$ uit de kettingbreukontwikkeling van α voldoen volgens stelling 6 aan de ongelijkheid (1).

Volgens gevolg 3 zijn de breuken $\frac{p_n}{q_n}$ irreducibel.

Is α rationaal dan breekt de kettingbreukontwikkeling af, zodat we hier slechts eindig veel oplossingen van (1) vinden. Is α irrationaal dan breekt de kettingbreukontwikkeling niet af en vinden we oneindig veel oplossingen van (1) met $\lim r_n = \alpha$.

Volgens stelling 4 en gevolg 4 vormen de r_n met even n een monotoon stijgende rij van getallen kleiner dan α en de r_n met oneven n een monotoon dalende rij van getallen groter dan α.

Gevolg 1 stelt ons in staat ongelijkheid (1) te verscherpen.

Stelling 7.

Van iedere twee opvolgende benaderende breuken $\frac{p_n}{q_n}$ met $n \geq 1$ uit een kettingbreukontwikkeling van een reëel getal α voldoet er minstens één aan

$$(4) \qquad |\alpha - \frac{p}{q}| < \frac{1}{2q^2} \quad .$$

Bewijs.

Van twee opvolgende breuken is er steeds één groter en één kleiner dan α zodat met gevolg 1

$$\frac{1}{q_n q_{n+1}} = |\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}| = |\frac{p_{n+1}}{q_{n+1}}| - \alpha| + |\alpha - \frac{p_n}{q_n}| .$$

Als nu $|\alpha - \frac{p_n}{q_n}| \geq \frac{1}{2q_n^2}$ en $|\alpha - \frac{p_{n+1}}{q_{n+1}}| \geq \frac{1}{2q_{n+1}^2}$,

dan zou volgen

$$\frac{1}{q_n q_{n+1}} \geq \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2} \quad ,$$

zodat $(q_{n+1}-q_n)^2 \leq 0$. Dit is onjuist.

Gevolg 6. Is α irrationaal dan bestaan er oneindig veel breuken $\frac{p}{q}$ waarvoor (4) geldt.

We tonen nu aan dat de benaderende breuken $\frac{p_n}{q_n}$ uit de kettingbreukontwikkeling van α in zekere zin de beste benadering van α door rationale getallen zijn.

Stelling 8.

Zij α een reëel getal, p_n, q_n als boven en $\frac{a}{b}$ een rationaal getal met $1 \leq b \leq q_n$, $\frac{a}{b} \neq \frac{p_n}{q_n}$. Dan geldt

$$|b\alpha - a| \geq |q_{n-1}\alpha - p_{n-1}| > |q_n\alpha - p_n| .$$

Bewijs.

We beschouwen de lineaire vergelijkingen

$$(5) \qquad \begin{cases} xp_{n+1} + yp_n = a \\ xq_{n-1} + yq_n = b \end{cases}$$

Daar volgens stelling 3 de determinant van het stelsel $(-1)^n$ is, heeft dit stelsel een paar gehele getallen x, y als oplossing.

Uit $x = 0$ volgt $\frac{a}{b} = \frac{p_n}{q_n}$ in tegenspraak met het gegeven, zodat $x \neq 0$.

We tonen nu aan dat als $y \neq 0$ is, dat dan x en y verschillend teken hebben. Stel $y < 0$, dan volgt daar $b > 0$, $q_n > 0$, $q_{n-1} > 0$ uit $xq_{n-1} = b - yq_n$ dat $x > 0$ is.

Is $y > 0$, dan volgt daar $b \leq q_n$ en $x \neq 0$ uit $xq_{n-1} = b - yq_n$ dat $x < 0$ is.

Uit stelling 5 volgt dat $q_{n-1}\alpha - p_{n-1}$ en $q_n\alpha - p_n$ ook tegengesteld teken hebben. Dan hebben $x(q_{n-1}\alpha - p_{n-1})$ en $y(q_n\alpha - p_n)$ hetzelfde teken als $y \neq 0$ is. Dus is

$$|x(q_{n-1}\alpha - p_{n-1}) + y(q_n\alpha - p_n)| \geq |x| \; |q_{n-1}\alpha - p_{n-1}| \geq |q_{n-1}\alpha - p_{n-1}| .$$

Anderzijds volgt met (5) dat

$$|x(q_{n-1}\alpha - p_{n-1}) + y(q_n\alpha - p_n)| = |b\alpha - a| .$$

Hieruit volgt de eerste ongelijkheid.

Uit stelling 6 volgt verder

$$\frac{1}{q_{n+2}} < |q_n\alpha - p_n| \leq \frac{1}{q_{n+1}} ,$$

zodat

$$|q_{n-1}\alpha - p_{n-1}| > \frac{1}{q_{n+1}} \geq |q_n\alpha - p_n| .$$

Hiermee is ook de tweede ongelijkheid bewezen.

Gevolg 7. Zij α een reëel getal, p_n, q_n als boven en $\frac{a}{b}$ een rationaal getal met $1 \leq b \leq q_n$, $\frac{a}{b} \neq \frac{p_n}{q_n}$ dan is

$$|\alpha - \frac{p_n}{q_n}| < |\alpha - \frac{a}{b}|.$$

Stelling 9.
Zij α een reëel getal en $\frac{p}{q}$ een breuk met de eigenschap dat voor ieder rationaal getal $\frac{a}{b}$ met $1 \leq b \leq q$, $\frac{a}{b} \neq \frac{p}{q}$ geldt

$$|q\alpha-p| < |b\alpha-a|$$

dan is $\frac{p}{q}$ een benaderende breuk uit de kettingbreukontwikkeling van α.

Bewijs.
Stel dat $\frac{p}{q}$ geen benaderende breuk is, dan is $q_{n-1} \leq q < q_n$ voor zekere n, terwijl $\frac{p}{q} \neq \frac{p_{n-1}}{q_{n-1}}$. Uit stelling 8 met $b = q$, $a = p$ volgt dan

$$|q\alpha-p| \geq |q_{n-1}\alpha-p_{n-1}| \quad .$$

Uit het gegeven met $a = p_{n-1}$, $b = q_{n-1}$ volgt echter

$$|q\alpha-p| < |q_{n-1}\alpha-p_{n-1}|.$$

Tegenspraak.

Als tegenhanger van stelling 7 bewijzen we nu

Stelling 10
Zij α een reëel getal en $\frac{p}{q}$ een rationaal getal met

$$|\alpha - \frac{p}{q}| < \frac{1}{2q^2} \quad ,$$

dan is $\frac{p}{q}$ een benaderende breuk uit de kettingbreukontwikkeling van α.

Bewijs.

Op grond van stelling 9 moeten we slechts bewijzen $|q\alpha-p| < |b\alpha-a|$ als $1 \leq b \leq q$ en $\frac{a}{b} \neq \frac{p}{q}$. Zij dus $1 \leq b \leq q$ en $\frac{a}{b} \neq \frac{p}{q}$.

Stel $|b\alpha-a| \leq |q\alpha-p| < \frac{1}{2q}$,

dan volgt

$$|\alpha - \frac{a}{b}| < \frac{1}{2bq}$$

zodat

$$|\frac{a}{b} - \frac{p}{q}| \leq |\frac{a}{b} - \alpha| + |\alpha - \frac{p}{q}| < \frac{1}{2bq} + \frac{1}{2q^2} = \frac{q+b}{2bq^2} .$$

Anderzijds

$$|\frac{a}{b} - \frac{p}{q}| \geq \frac{1}{bq} .$$

Hieruit volgt

$$\frac{1}{bq} < \frac{q+b}{2bq^2}$$

ofwel $q < b$, tegenspraak .

Relatie (1) en Stelling 7 kunnen nog iets verscherpt worden (voor een bewijs zie bijvoorbeeld Hardy & Wright p. 164-165).

Stelling 11.

Van iedere drie opvolgende benaderende breuken uit de kettingbreukontwikkeling van een reëel getal α voldoet er minstens één aan

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2\sqrt{5}} .$$

Hieruit volgt

Stelling 12. (Hurwitz).

Is α een irrationaal getal dan bestaan er oneindig veel rationale getallen $\frac{p}{q}$ waarvoor geldt

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2\sqrt{5}} .$$

We tonen nu aan dat de constante $\sqrt{5}$ in stelling 12 niet verder te verscherpen is. Zij $\alpha = \frac{\sqrt{5}+1}{2}$, dan is zoals boven werd aangetoond $\alpha_{n+1} = \alpha$ en $a_n = 1$ $(n = 0,1,2,\ldots)$. Dan is $q_0 = 1$, $q_1 = 1$ en $q_n = q_{n-1} + q_{n-2}$ zodat we voor q_n de rij getallen

$$1,1,2,3,5,8,13,21,\ldots$$

vinden; dit zijn de getallen van Fibonacci.
Voor p_n vinden we de rij

$$1,2,3,5,8,13,21,34,\ldots$$

zodat $p_{n-1} = q_n$. Dan is $\frac{q_{n-1}}{q_n} = \frac{q_{n-1}}{p_{n-1}}$ en dit convergeert naar $\frac{1}{\alpha}$. We stellen $\frac{q_{n-1}}{q_n} = \frac{1}{\alpha} + \varepsilon_n$, zodat $\lim_{n\to\infty} \varepsilon_n = 0$.

Met stelling 5 vinden we

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2} \frac{1}{\alpha_{n+1} + \frac{q_{n-1}}{q_n}} = \frac{1}{q_n^2} \frac{1}{\alpha + \frac{1}{\alpha} + \varepsilon_n} =$$

$$\frac{1}{q_n^2(\sqrt{5}+\varepsilon_n)} .$$

Stel nu dat $\frac{p}{q}$ voldoet aan

$$(6) \qquad \left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2} \quad \text{met} \quad c < \frac{1}{\sqrt{5}} .$$

Volgens stelling 10 is $\frac{p}{q}$ een benaderende breuk $\frac{p_n}{q_n}$, zodat

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2(\sqrt{5}+\varepsilon_n)} < \frac{c}{q_n^2} .$$

Daar $\lim \varepsilon_n = 0$ kan dit voor hoogstens eindige vele n gelden zodat (6) ten hoogste eindig veel oplossingen heeft.
Er bestaat dus een irrationaal getal $\alpha = \frac{\sqrt{5}+1}{2}$ waarvoor (6) slechts eindig vele oplossingen heeft; hieruit volgt dat de constante $\sqrt{5}$ in stelling 12 niet verder te verscherpen is.

Algebraïsche en transcendente getallen

We zullen nu voor een klasse van getallen een ondergrens voor $|\alpha - \frac{x}{y}|$ afleiden.

Definitie. Een algebraïsch getal van de graad n is een (reëel of complex) getal dat voldoet aan een n^e graads vergelijking met gehele coefficienten

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n = 0, \quad a_0 \neq 0 .$$

Is een getal niet algebraïsch, dan heet het transcendent.

Opmerking. Een algebraïsch getal van de graad 1 is een rationaal getal.

Stelling 13 (Liouville).
Is α een reëel algebräïsch getal van graad $n \geq 2$, dan bestaat er een constante $c > 0$, alleen afhankelijk van α, zodat voor alle rationale getallen $\frac{x}{y}$ geldt

$$|\alpha - \frac{x}{y}| > \frac{c}{|y|^n} .$$

Bewijs.
Het algebraïsch getal α voldoet aan een vergelijking

$$f(\alpha) = a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0.$$

Kies een interval $[\alpha-r,\alpha+r]$ om α zo dat $f(x) = 0$ op dit interval α als enige wortel heeft.
Zij $|f'(x)| < M$ voor $x \in [\alpha-r,\alpha+r]$.
Ligt $\frac{x}{y} \notin [\alpha-r,\alpha+r]$ dan geldt

$$|\alpha - \frac{x}{y}| > r \geq \frac{r}{|y|^n} .$$

Veronderstel nu $\frac{x}{y} \in [\alpha-r,\alpha+r]$.
Daar $f(\frac{x}{y}) \neq 0$ volgt

$$|f(\frac{x}{y})| = \frac{|a_0x^n+a_1x^{n-1}y + \ldots + a_ny^n|}{|y|^n} \geq \frac{1}{|y|^n} .$$

Nu is

$$f(\tfrac{x}{y}) = f(\tfrac{x}{y}) - f(\alpha) = (\tfrac{x}{y}-\alpha)\, f'(a)$$

voor zekere a tussen α en $\frac{x}{y}$ in. Dan is $|f'(a)| < M$, zodat

$$|\alpha - \tfrac{x}{y}| = \frac{|f(\frac{x}{y})|}{|f'(a)|} > \frac{1}{M|y|^n} .$$

Hieruit volgt de stelling met $c = \min(r, \frac{1}{M})$.

Gevolg 8. Zij $\xi = \sum_{n=1}^{\infty} 10^{-n!}$. We zullen aantonen dat ξ transcendent is.

Stel $\sum_{n=1}^{N} 10^{-n!} = \frac{p}{q}$, dan is $q = 10^{-N!}$ en

$$\xi - \frac{p}{q} = \sum_{n=N+1}^{\infty} 10^{-n!} < 2.10^{-(N+1)!} = 2q^{-(N+1)},$$

zodat

$$|\xi - \frac{p}{q}| < \frac{2}{q^{N+1}} .$$

Daar N willekeurig groot genomen kan worden, kan volgens stelling 13 ξ niet algebraïsch zijn. Uit dit voorbeeld blijkt tevens dat er irrationale getallen bestaan die een veel scherpere benadering met rationale getallen $\frac{x}{y}$ toelaten dan in stelling 12.

De ondergrens uit stelling 13 is later aanzienlijk verscherpt. Er geldt zelfs de volgende stelling. (zie bijvoorbeeld LeVeque II Chapter 4).

Stelling 13 (Thue-Siegel-Roth).
Is α een reëel algebraïsch getal van graad $n \geq 2$ en $\varepsilon > 0$, dan bestaat er een constante $c > 0$, alleen afhankelijk van α en ε zodat voor alle rationale getallen $\frac{x}{y}$ geldt

$$|\alpha - \tfrac{x}{y}| > \frac{c}{|y|^{2+\varepsilon}} .$$

Literatuur bij hoofdstuk VII.

G.H. Hardy, E.M. Wright:	An introduction to the theory of numbers, Chapter 10,11.
A.Ya. Khinchin:	Continued Fractions.
W.J. LeVeque:	Topics in number theory, volume I, Chapter 9; volume II, Chapter 4.
I. Niven, H.S. Zuckerman:	An introduction to the theory of numbers, Chapter 7.
O. Perron:	Die Lehre von den Kettenbrüchen, Band I.

Hoofdstuk VIII: Gelijkverdeling

Gelijkverdeling mod. 1

Zij $(x_n)_{n=1}^{\infty}$ een rij reële getallen. We beschouwen de corresponderende rij $(\{x_n\})_{n=1}^{\infty}$ in $[0,1)$. Zij $[\alpha,\beta)$ een deelinterval van $[0,1)$ dan noteren we het aantal van $x_1, x_2, \ldots, x_N$ met $\{x_n\} \in [\alpha,\beta)$ als $A([\alpha,\beta),N)$. Ligt de rij $(\{x_n\})$ regelmatig over $[0,1)$ verdeeld dan zal $\frac{A([\alpha,\beta),N)}{N}$ ongeveer gelijk aan $\beta-\alpha$ zijn. Uitgaande van deze gedachte definieren we

Definitie 1. Zij $(x_n)_{n=1}^{\infty}$ een rij reële getallen. De rij heet gelijkverdeeld mod. 1 als voor ieder deelinterval $[\alpha,\beta) \subset [0,1)$ geldt

$$(1) \qquad \lim_{N\to\infty} \frac{A([\alpha,\beta),N)}{N} = \beta-\alpha.$$

Opmerking 1. Het begrip gelijkverdeling (Gleichverteilung) is afkomstig van Hermann Weyl uit twee artikelen uit 1914 en 1916. In deze artikelen gaf hij de definitie en een aantal eigenschappen die van fundamentele betekenis voor de ontwikkeling van de gelijkverdeling gebleken zijn. Weyl definieerde gelijkverdeling als volgt: Zij $\alpha_1, \alpha_2, \ldots$ een rij punten op de reële as. Wikkel de as om een cirkel met omtrek 1. Zij a een boog van de cirkel met lengte $|a|$ en n_a het aantal van de $\alpha_1, \ldots, \alpha_n$ die bij oprollen in a terecht komen. De rij heet gelijkverdeeld als $\lim_{n\to\infty} \frac{n_a}{n} = |a|$ voor iedere cirkelboog.
Deze definitie is gelijkwaardig aan definitie 1.

We schrijven nu relatie (1) in een andere vorm. Zij $\chi_{[\alpha,\beta)}$ de karakteristieke functie van $[\alpha,\beta)$, d.w.z.

$$\chi_{[\alpha,\beta)}(x) = \begin{cases} 1 & \text{als } x \in [\alpha,\beta) \\ 0 & \text{als } x \notin [\alpha,\beta) \end{cases}$$

dan is (1) equivalent met

---

syll. ZC 78, afl. 9.

$$(2) \qquad \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \chi_{[\alpha,\beta)}(\{x_n\}) = \int_0^1 \chi_{[\alpha,\beta)}(x)dx.$$

Stelling 1. Is de rij reële getallen (x_n) gelijk verdeeld mod. 1 en is f een reëelwaardige, Riemann-integreerbare functie op $[0,1]$, dan geldt

$$(3) \qquad \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{x_n\}) = \int_0^1 f(x)dx.$$

Bewijs. Zij t een trapfunctie op $[0,1]$, d.w.z. t is een eindige lineaire combinatie van karakteristieke functies. Uit (2) volgt onmiddellijk

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} t(\{x_n\}) = \int_0^1 t(x)dx.$$

Volgens de definitie van Riemann-integraal bestaan er bij iedere $\varepsilon > 0$ trapfuncties t_1 en t_2 zodat

$$t_1(x) \leq f(x) \leq t_2(x) \qquad \text{voor } x \in [0,1]$$

en

$$\int_0^1 t_2(x)dx - \int_0^1 t_1(x)dx \leq \varepsilon.$$

Hieruit volgt

$$\frac{1}{N} \sum_{n=1}^{N} f(\{x_n\}) \leq \frac{1}{N} \sum_{n=1}^{N} t_2(\{x_n\}) \leq \int_0^1 t_2(x)dx + \varepsilon \leq \int_0^1 f(x)dx + 2\varepsilon$$

als N voldoende groot is.
Anderzijds

$$\frac{1}{N} \sum_{n=1}^{N} f(\{x_n\}) \geq \frac{1}{N} \sum_{n=1}^{N} t_1(\{x_n\}) \geq \int_0^1 t_1(x)dx - \varepsilon \geq \int_0^1 f(x)dx - 2\varepsilon$$

als N voldoende groot is.
Hiermee volgt (3).

Gevolg 1. Is f een complex-waardige Riemann-integreerbare functie op $[0,1]$, dan is f te schrijven als $f = f_1+if_2$ waarin f_1 en f_2 reëelwaardig zijn. Uit stelling 1 volgt dan dat (3) ook geldt voor complexwaardige Riemann-integreerbare functies.

Gevolg 2. Is $(x_n)_{n=1}^{\infty}$ gelijkverdeeld mod. 1 dan is

$$\lim_{N\to\infty} \frac{\{x_1\}+\{x_2\}+\ldots+\{x_N\}}{N} = \int_0^1 x\,dx = \frac{1}{2}$$

$$\lim_{N\to\infty} \frac{\{x_1\}^k+\{x_2\}^k+\ldots+\{x_N\}^k}{N} = \int_0^1 x^k\,dx = \frac{1}{k+1} \quad \text{voor } k \neq -1$$

$$(4) \qquad \lim_{N\to\infty} \frac{\cos 2\pi hx_1+\cos 2\pi hx_2+\ldots+\cos 2\pi hx_N}{N} = \int_0^1 \cos 2\pi hx\,dx = 0$$

als h geheel, $h \neq 0$.

$$(5) \qquad \lim_{N\to\infty} \frac{\sin 2\pi hx_1+\sin 2\pi hx_2+\ldots+\sin 2\pi hx_N}{N} = \int_0^1 \sin 2\pi hx\,dx = 0$$

als h geheel.

Daar $e^{i\phi} = \cos\phi + i\sin\phi$ volgt uit (4) en (5) de belangrijke relatie (vergelijk stelling 4):

$$(6) \qquad \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i hx_n} = 0 \quad \text{als h geheel, } h \neq 0.$$

Opmerking 2. Er bestaan formules die een schatting geven voor

$$\sum_{n=1}^{N} f(\{x_n\}) - N\int_0^1 f(x)\,dx$$

(zie bijv. syllabus Colloquium gelijkverdeling p. 37).
Als omgekeerde van stelling 1 bewijzen we

Stelling 2. Zij $(x_n)_{n=1}^{\infty}$ een rij reële getallen. Als (3) geldt voor iedere continue reëelwaardige functie f op [0,1] dan is (x_n) gelijkverdeeld mod. 1.

Bewijs. Zij χ de karakteristieke functie van een willekeurig deelinterval $[\alpha,\beta) \subset [0,1)$. We zullen bewijzen dat (2) geldt. Dit is equivalent met de bewering dat (x_n) gelijkverdeeld mod. 1 is.
Bij iedere $\varepsilon > 0$ bestaan twee continue functies f_1 en f_2 zodat

$$f_1 \leq \chi \leq f_2$$

en

$$\int_0^1 (f_2(x)-f_1(x))dx < \varepsilon.$$

Dan volgt

$$\frac{1}{N}\sum_{n=1}^{N} \chi(\{x_n\}) \leq \frac{1}{N}\sum_{n=1}^{N} f_2(\{x_n\}) \leq \int_0^1 f_2(x)dx + \varepsilon \leq \int_0^1 \chi(x)dx + 2\varepsilon$$

als N voldoende groot is.
Anderzijds

$$\frac{1}{N}\sum_{n=1}^{N} \chi(\{x_n\}) \geq \frac{1}{N}\sum_{n=1}^{N} f_1(\{x_n\}) \geq \int_0^1 f_1(x)dx - \varepsilon \geq \int_0^1 \chi(x)dx - 2\varepsilon$$

als N voldoende groot is.
Hieruit volgt (2).

Uit stelling 1 en 2 volgt

Stelling 3. De rij reële getallen (x_n) is dan en slechts dan gelijkverdeeld mod. 1 als voor iedere op [0,1] continue functie f geldt

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(\{x_n\}) = \int_0^1 f(x)dx.$$

Opmerking 3. Stelling 3 is zo fundamenteel dat bij sommige generalisaties van gelijkverdeling het gelden van relatie (3) voor alle continue functies als definitie gebruikt wordt.

Om de gelijkverdeling van een rij te onderzoeken is het niet nodig na te gaan of (3) geldt voor alle continue functies op [0,1]. Stelling 2 is namelijk te verscherpen tot (vergelijk (6)):

Stelling 4. (criterium van Weyl). Zij $(x_n)_{n=1}^{\infty}$ een rij reële getallen. Geldt voor ieder geheel getal $h \neq 0$ dat

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} e^{2\pi i h x_n} = 0, \tag{7}$$

dan is de rij gelijkverdeeld mod. 1.

In het bewijs van stelling 4 maken we gebruik van:

Hulpstelling (stelling van Weierstrass). Zij f een reëel- of complexwaardige continue functie op $[0,1]$. Voor iedere $\varepsilon > 0$ bestaat er een trigonometrisch polynoom $\phi(x) = \sum_{k=-K}^{K} a_k e^{2\pi ikx}$ zodat

$$|f(x) - \phi(x)| < \varepsilon \qquad \text{voor alle } x \in [0,1]. \tag{8}$$

Voor een bewijs zie bijv. Titchmarsh The theory of functions p. 414.

Bewijs van stelling 4. Uit (7) volgt dat (3) geldt voor ieder trigonometrisch polynoom. Zij nu f een continue functie op $[0,1]$. We zullen bewijzen dat (3) geldt voor f. Volgens stelling 2 is (x_n) dan gelijkverdeeld mod. 1. Zij $\varepsilon > 0$ en ϕ het trigonometrisch polynoom waarvoor (8) geldt. Dan is dus

$$\left|\int_0^1 (f(x)-\phi(x))dx\right| < \varepsilon \text{ en } \left|\frac{1}{N}\sum_{n=1}^{N} (f(\{x_n\})-\phi(\{x_n\}))\right| < \varepsilon. \tag{9}$$

Zodat

$$\left|\int_0^1 f(x)dx - \frac{1}{N}\sum_{n=1}^{N} f(\{x_n\})\right| \leq \left|\int_0^1 (f(x)-\phi(x))dx\right| +$$

$$\left|\int_0^1 \phi(x)dx - \frac{1}{N}\sum_{n=1}^{N} \phi(\{x_n\})\right| + \left|\frac{1}{N}\sum_{n=1}^{N} (\phi(\{x_n\})-f(\{x_n\}))\right|.$$

De eerste en derde term van het laatste lid zijn volgens (9) altijd $< \varepsilon$. Daar voor ϕ relatie (3) geldt, is de tweede term $< \varepsilon$ als N voldoende groot is. Hieruit volgt

$$\left|\int_0^1 f(x)dx - \frac{1}{N}\sum_{n=1}^{N} f(\{x_n\})\right| < 3\varepsilon \quad \text{als N voldoende groot is.}$$

Daar $\varepsilon > 0$ willekeurig te kiezen is, geldt (3) voor f.

Voorbeeld 1. Zij α een irrationaal getal en β een willekeurig reëel getal, dan is de rij $(\alpha n+\beta)_{n=1}^{\infty}$ gelijkverdeeld mod. 1.

Bewijs. Zij h een geheel getal, $h \neq 0$, dan geldt

$$\left| \sum_{n=1}^{N} e^{2\pi i h(\alpha n+\beta)} \right| = \left|e^{2\pi i h\beta}\right| \left| \frac{e^{2\pi i h\alpha N}-1}{e^{2\pi i h\alpha}-1} \right| =$$

$$1. \left| \frac{e^{2\pi i h\alpha(N-1)}-e^{-\pi i h\alpha}}{e^{\pi i h\alpha}-e^{-\pi i h\alpha}} \right| \leq \frac{2}{2|\sin \pi h\alpha|} .$$

Daar α irrationaal is, is $|\sin \pi h\alpha| \neq 0$. Uit stelling 4 volgt dan dat $(\alpha n+\beta)$ gelijkverdeeld mod. 1 is.

Opmerking 4. Is α rationaal, $\alpha = \frac{a}{b}$, $(a,b) = 1$, dan vormen de punten $\{n\alpha\}$, $n = 1, 2, \ldots$ de verzameling $0, \frac{1}{b}, \frac{2}{b}, \ldots, \frac{b-1}{b}$. In een interval $(\frac{k}{b},\frac{k-1}{b})$ liggen dus geen punten van de rij. Uit definitie 1 is dan eenvoudig af te leiden dat de rij $(\alpha n)_{n=1}^{\infty}$ niet gelijkverdeeld mod. 1 is. Een zelfde redenering toont aan dat de rij $(\alpha n+\beta)_{n=1}^{\infty}$ met α rationaal, β willekeurig reëel niet gelijkverdeeld mod. 1 is.

Voorbeelden. Men kan o.a. bewijzen dat de rij $(f(n))_{n=1}^{\infty}$ gelijkverdeeld mod. 1 is in de volgende gevallen (voor nadere informatie zie o.a. Cigler-Helmberg p. 8-9)

2) $f(n)$ is een polynoom met reële coëfficiënten:
   $f(n) = a_k n^k + \ldots + a_1 n + a_0$, waarin tenminste één van de coëfficiënten $a_k, \ldots, a_1$ irrationaal is.
3) $f(n) = an^t$ met a, t reëel $a \neq 0$, $t > 0$ en t niet geheel.
4) $f(n) = a(\log n)^t$ met a, t reëel, $a \neq 0$, $t > 1$.

Discrepantie. We beschouwen nu rijen (x_n) in $[0,1)$, zodat $\{x_n\} = x_n$; we zullen dan van gelijkverdeling spreken in plaats van gelijkverdeling mod. 1.

Definitie 2. Zij $(x_n)_{n=1}^{\infty}$ een rij getallen in $[0,1)$, dan verstaan we onder de discrepantie $d(N)$ van de rij

$$d(N) = \sup|A([\alpha,\beta),N) - (\beta-\alpha)N| \qquad (N = 1, 2, \ldots)$$

waarin het supremum genomen wordt over alle deelintervallen $[\alpha,\beta) \subset [0,1)$.

De discrepantie geeft een maat voor de onregelmatigheid van de verdeling. Is $\lim_{N\to\infty} \frac{d(N)}{N} = 0$ dan volgt uit definitie 1 dat de rij gelijkverdeeld is. Is omgekeerd de rij gelijkverdeeld, dan kan men bewijzen $\lim_{N\to\infty} \frac{d(N)}{N} = 0$.

Van der Corput stelde in 1935 de vraag of een rij zo regelmatig kan liggen in $[0,1)$ dat de discrepantie begrensd blijft, d.w.z. $d(N) < M$ voor zekere constante M en alle N.
Mevr. van Aardenne-Ehrenfest bewees in 1945 als eerste dat dit niet mogelijk is, d.w.z. $\limsup_{N\to\infty} d(N) = \infty$. In 1949 bewees ze bovendien dat voor iedere rij in $[0,1)$ geldt

$$d(N) > c_1 \frac{\log\log N}{\log\log\log N}$$

voor oneindig vele N, waarin c_1 een constante is.
In 1954 verbeterde Roth dit aanzienlijk door te bewijzen dat voor iedere rij geldt

$$d(N) > c_2 \sqrt{\log N}$$

voor zekere positieve constanten c_2 en oneindig vele N.
Onlangs bewees W. Schmidt dat dit nog te verbeteren valt tot

$$d(N) > 10^{-2} \log N.$$

Verdere verbeteringen zijn - afgezien misschien van de constante 10^{-2} - niet mogelijk. Er zijn namelijk rijen bekend met

$$d(N) < c \log N$$

voor alle N, waarin c een constante is.

Generalisaties. Het begrip gelijkverdeling is overgedragen op rijen in andere verzamelingen. Weyl zelf beschouwde al gelijkverdeling in de n-dimensionale eenheidskubus. Van andere vormen van gelijkverdeling ver-

melden we hier: gelijkverdeling in compacte groepen (Eckmann, Hlawka); de continue gelijkverdeling (Kuipers); gelijkverdeling van gehele getallen (Niven); gelijkverdeling van p-adische getallen (Cugiani, Chauvineau) en g-adische getallen (Meijer); gelijkverdeling in de verzamelingen GF[q,x] en GF{q,x} dat zijn resp. de polynomen en de Laurentreeksen over een eindig lichaam GF(q) (Hodges, Carlitz, Dijksma). Daarnaast zijn er allerlei varianten van het begrip gelijkverdeling ontwikkeld, waarin de verdeling meer of minder "gelijk" moet zijn.

Gelijkverdeling van gehele getallen. We zullen hier nog één situatie van gelijkverdeling nader beschouwen, namelijk de gelijkverdeling van gehele getallen.
In 1961 gaf Niven de volgende definitie:

Definitie 3. Zij $(a_n)_{n=1}^{\infty}$ een rij gehele getallen. Zij m een geheel getal, $m \geq 2$. Beschouw de getallen $a_n \pmod m$. Zij $A(j,m,N)$ het aantal onder $a_1, a_2, \ldots, a_N$ met $a_n \equiv j \pmod m$. Als geldt

$$\lim_{N\to\infty} \frac{A(j,m,N)}{N} = \frac{1}{m} \qquad \text{voor } j = 0, 1, 2, \ldots, m-1$$

dan heet de rij (a_n) gelijkverdeeld mod. m. Is de rij (a_n) gelijkverdeeld mod. m voor ieder geheel getal $m \geq 2$, dan heet de rij een gelijkverdeelde rij gehele getallen.

Voorbeelden.

5) De rij van natuurlijke getallen 1, 2, 3, 4, ... is een gelijkverdeelde rij gehele getallen.
6) Zijn a en b gehele getallen, dan is de rij $(an+b)_{n=1}^{\infty}$ uiteraard niet gelijkverdeeld mod. a en dus geen gelijkverdeelde rij gehele getallen.

Veel voorbeelden van gelijkverdeelde rijen gehele getallen volgen m.b.v. de volgende stelling.

Stelling 5. (Van der Eynden). Zij $(x_n)_{n=1}^{\infty}$ een rij reële getallen, zodanig dat de rij $(m^{-1}x_n)_{n=1}^{\infty}$ gelijkverdeeld mod. 1 is voor ieder geheel getal $m \geq 2$. Dan is de rij $([x_n])_{n=1}^{\infty}$ een gelijkverdeelde rij gehele getallen.

Bewijs. Zij m een geheel getal, $m \geq 2$ en zij $j \in 0, 1, 2, \ldots, m-1$. Is $[x_n] \equiv j \pmod{m}$, dan is $x_n \in [km+j, km+j+1)$ voor zeker geheel getal k. Dan is echter $m^{-1}x_n \in [k + \frac{j}{m}, k + \frac{j+1}{m})$ en $\{m^{-1}x_n\} \in [\frac{j}{m}, \frac{j+1}{m})$. Is omgekeerd $\{m^{-1}x_n\} \in [\frac{j}{m}, \frac{j+1}{m})$ dan leidt men analoog af dat $[x_n] \equiv j \pmod{m}$.
Hieruit volgt dat $A(j,m,N)$ voor de rij $([x_n])$ gelijk is aan $A([\frac{j}{m}, \frac{j+1}{m}),N)$ voor de rij $(\{m^{-1}x_n\})$. Daar $(m^{-1}x_n)$ gelijkverdeeld mod. 1 is, geldt

$$\lim_{N\to\infty} \frac{1}{N} A([\tfrac{j}{m}, \tfrac{j+1}{m}),N) = \frac{1}{m},$$

zodat

$$\lim_{N\to\infty} \frac{1}{N} A(j,m,N) = \frac{1}{m}.$$

Hieruit volgt dat $([x_n])$ een gelijkverdeelde rij gehele getallen is.

Voorbeelden. Uit stelling 5 en voorbeelden 1 t/m 4 volgt dat de rij $([f(n)])_{n=1}^{\infty}$ een gelijkverdeelde rij gehele getallen is, in o.a. de volgende gevallen:

7) $f(n) = \alpha n+\beta$, α irrationaal, β reëel.
8) $f(n)$ een polynoom met reële coëfficiënten:
   $f(n) = a_k n^k + \ldots + a_1 n + a_0$, waarin minstens één van de coëfficiënten $a_k, \ldots, a_1$ irrationaal is.
9) $f(n) = an^t$ met a, t reëel, $a \neq 0$, $t > 0$ en t niet geheel.
10) $f(n) = a(\log n)^t$ met a, t reëel, $a \neq 0$, $t > 1$.

Men kan bewijzen dat analoog aan stelling 4 het volgende criterium voor gelijkverdeling van gehele getallen geldt.

Stelling 6. (Uchiyama). Zij $(a_n)_{n=1}^{\infty}$ een rij gehele getallen.

a) Zij m een geheel getal, $m \geq 2$, dan is (a_n) gelijkverdeeld mod. m dan en slechts dan als

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i h m^{-1} a_n} = 0 \text{ voor } h = 1, 2, \ldots, m-1.$$

b) De rij (a_n) is een gelijkverdeelde rij gehele getallen dan en slechts dan als

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i t a_n} = 0$$

voor ieder rationaal, niet geheel getal t.

Metrische stellingen. H. Weyl beweees in zijn bovengenoemde artikel van 1916 de volgende stelling:

Stelling 7. Zij $(l_n)_{n=1}^{\infty}$ een rij gehele getallen, die onderling verschillend zijn, dan is de rij $(l_n x)_{n=1}^{\infty}$ voor bijna alle x gelijkverdeeld mod. 1.

"Bijna alle" betekent hier: "voor alle x met uitzondering van een verzameling met Lebesgue-maat 0".Een dergelijke stelling waarin een uitspraak gedaan wordt over de maat van een verzameling met een bepaalde eigenschap heet een metrische stelling. Uit stelling 7 en definitie 1 volgt dat de rij $(l_n x)_{n=1}^{\infty}$ ook voor bijna alle x gelijkverdeeld mod. 1 is, als niet alle l_n verschillend zijn, zolang er maar niet "al te veel" gelijke voorkomen.
Van Uchiyama stamt nu het volgende probleem. Stel dat $(a_n)_{n=1}^{\infty}$ een rij gehele getallen is, die gelijkverdeeld is, dan kunnen er in die rij "niet al te veel" gelijke elementen optreden. Is het nu waar dat ook nu $(a_n x)_{n=1}^{\infty}$ gelijkverdeeld mod. 1 is voor bijna alle x?
Als gedeeltelijk antwoord op deze vraag bewezen Kuipers en Uchiyama dat voor bijna alle x de rij $(a_n x)$ de volgende eigenschap heeft: er bestaat een oneindige deelrij n_k van de natuurlijke getallen zodat

$$\lim_{n_k\to\infty} \frac{1}{n_k} A([\alpha,\beta),n_k) = \beta-\alpha,$$

voor ieder deelinterval $[\alpha,\beta) \subset [0,1)$.
Ze noemen dit "bijna gelijkverdeeld".
Hoewel dit doet vermoeden dat het antwoord op de vraag van Uchiyama bevestigend moet luiden, toonde Meijer in 1970 aan dat het antwoord ontkennend is. Hij construeerde namelijk een gelijkverdeelde rij gehele getallen $(b_n)_{n=1}^{\infty}$ waarvoor $(b_n x)_{n=1}^{\infty}$ niet gelijkverdeeld mod. 1 is voor alle x in een verzameling V met $V \subset (0,1)$ en Lebesgue-maat $V \geq \frac{1}{2}$.

Literatuur bij hoofdstuk VIII

Overzichten.

1) J. Cigler - G. Helmberg: Neuere Entwicklungen der Theorie der Gleichverteilung, Jber. Deutsch. Math. Verein 64 (1962), 1-50.

2) H.G. Meijer: Verdeel beheerst, Openbare les, Delft 1969.

3) Syllabus colloquium "Gelijkverdeling" o.l.v. Prof.dr. G. Helmberg, Mathematisch Centrum 1963-64, Amsterdam.

Gelijkverdeling mod. 1.

4) H. Weyl: Über ein Problem aus dem Gebiet der Diophantischen Approximationen, Nachr. Ges. Wiss. Göttingen (1914), 234-244.

5) H. Weyl: Über die Gleichverteilung von Zahlen mod. Eins, Math. Ann. 77 (1916), 313-352.

Discrepantie.

6) T. van Aardenne-Ehrenfest: Proof of the impossibility of a just distribution, Indag. Math. 7 (1945), 71-76.

7) T. van Aardenne-Ehrenfest: On the impossibility of a just distribution, Indag. Math. 11 (1949), 264-269.

8) K.F. Roth: On irregularities of distribution, Mathematika 1 (1954), 73-79.

9) W.M. Schmidt: Irregularities of distribution VI (Verschijnt binnenkort.)

Gelijkverdeling van gehele getallen.

10) I. Niven: Uniform distribution of integers, Trans. Amer. Math. Soc. 98 (1961), 52-61.

11) S. Uchiyama: On the uniform distribution of sequences of integers, Proc. Japan Acad. 37 (1961), 605-609.

12) L. Kuipers - S. Uchiyama: Notes on the uniform distribution of sequences of integers, Proc. Japan Acad, 44 (1968), 608-613.

13) H.G. Meijer: On uniform distribution of integers and uniform distribution mod. 1.

Bibliographie

Bij het samenstellen van deze cursus is gebruik gemaakt van de volgende boeken:

1) K. Chandrasekharan: Einfürung in die Analytischen Zahlentheorie, Springer-Verlag (Lecture Notes in Mathematics), Berlin, 1966.

2) E. Grosswald: Topics from the theory of numbers, Collier-MacMillan, New York, 1966.

3) G.H. Hardy - E.M. Wright: An introduction to the theory of numbers, 4th ed., Clarendon Press, Oxford, 1960.

4) A.Ya. Khinchin: Continued Fractions, Phoenix Books, The University of Chicago Press, Chicago, 1964 (vertaald uit het Russisch).

5) W.J. LeVeque: Topics in number theory, volume I, Addison-Wesley Publ. Cy., 1956.

6) I. Niven - H.S. Zuckerman: An introduction to the theory of numbers, John Wiley & Sons Inc., New York, 1960.

7) O. Ore: Number theory and its history, McGraw-Hill, New York, 1948.

8) O. Perron: Die lehre von den Kettenbrüchen, I, Teubner, Stuttgart, 1954.

9) G. Pólya - G. Szegö: Aufgaben und Lehrsätze aus der Analysis I., 2e druk, Springer-Verlag (die Grundlehren der Math. Wiss.), Berlin, 1954.

10) E.C. Titchmarsch: The theory of functions, 2e druk, Clarendon Press, Oxford, 1939.

Correcties en aanvullingen.

pag. 2 toevoegen! In 1949 gaven Erdös en Selberg een elementair bewijs van de priemgetal-stelling. Elementair betekent hier: zonder gebruik te maken van complexe functie-theorie.

pag. 8 toevoegen: Stelling 8b: Zijn n, a, b $\in$ Z en (n,a) = 1, dan volgt uit $n \mid ab$ dat $n \mid b$.

Bewijs. Analoog bewijs stelling 8.

pag. 19 regel 4. Er staat $r_{Q(m)}$, dit moet zijn $r_{\phi(m)}$.

pag. 24 regel 4. Er staat $x = x_0 + \frac{m_2}{d} t$, dit moet zijn $x = x_0 - \frac{m_2}{d} t$.

pag. 31 Stelling 4, formule voor $\sigma_k(n)$. In de noemer staat $p_i - 1$, dit moet zijn $p_i^k - 1$.

pag. 33 Bewijs a) regel 2. Er staat $\sigma(n) = \ldots = (2^{p-1})2^p = 2n$, dit moet zijn $\sigma(n) = \ldots = (2^p - 1)2^p = 2n$.

pag. 35 regel 4 van onder. Er staat $\Lambda(n)$, dit moet zijn $\Lambda(d)$.

pag. 36 regel 1. Idem.

pag. 39 regel 6. Er staat $f * g(p^k)$, dit moet zijn $f * h(p^k)$.

pag. 42 regel 5 van onder. Er staat $\mu * E = 2$, dit moet zijn $\mu * E = e$.

pag. 42 toevoegen: $J(2) = \frac{\pi^2}{6}$, $J(4) = \frac{\pi^4}{90}$. Uit toepassing 6 volgt dan $\sum_{n=1}^{\infty} \frac{\tau(n)}{n^2} = \frac{\pi^4}{36}$ en $\sum_{n=1}^{\infty} \frac{\tau(n)}{n^4} = (\frac{\pi^4}{90})^2$.

pag. 60 regel 5 en regel 7 van onder. Er staat B, moet zijn Ba_1^{-1}.

pag. 61 regel 4. 1e) Er staat $\pi(n)$, moet zijn $\pi(x)$. 2e) laatste lid moet zijn $\frac{1}{a_2}$ (log log $\sqrt{x}$ - B).

pag. 61 regel 5. Er staat B moet zijn Ba_2^{-1}.

pag. 63 midden. In de rij priemgetallen 2, 3, 4, 7, ... moet 4 vervangen worden door 5.

pag. 74 Stelling 8. De woorden "en hun geassocieerden" moeten op een nieuwe regel staan. Bedoeld zijn de geassocieerden van de priemelementen genoemd onder a), b) en c).

pag. 84 Gevolg 7. toevoegen: In het bijzonder is

$$|\alpha - \frac{p_n}{q_n}| < |\alpha - \frac{p_{n-1}}{q_{n-1}}|.$$

pag. 87 De definitie moet als volgt luiden: Een algebraïsch getal van de graad n is een (reëel of complex) getal dat voldoet aan een n^e graads vergelijking met gehele coëfficiënten

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n = 0,\ a_0 \neq 0$$

en dat niet voldoet aan een vergelijking met gehele coëfficiënten van lagere graad. Is een getal niet algebraïsch, dan heet het transcendent.