PVS A·
RITH-
ME
TICAE·
BOETIVS
PY
TAGO
RAS

CWI Syllabi

Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

The CWI is a research institute of the Stichting Mathematisch Centrum, which was founded on February 11, 1946, as a nonprofit institution aiming at the promotion of mathematics, computer science, and their applications. It is sponsored by the Dutch Government through the Netherlands Organization for the Advancement of Research (N.W.O).

CWI Syllabus 27

Vacantiecursus 1990
Getallentheorie
en haar toepassingen

Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science

1980 Mathematics Subject Classification: 11-01.
ISBN 90 6196 392 3
NUGI-code: 811

Inhoud

Ten Geleide

Het onderwerp van de vakantiecursus 1990 is bepaald op grond van de uitslag van een equête onder de deelnemers aan de cursus in 1989. De getallentheorie kwam daarin op overtuigende wijze naar voren, hetzij ongenuanceerd, hetzij voorgesteld door een van haar vele deelgebieden. Aan de commissie van voorbereiding was de taak toebedeeld om uit de vele aspecten die de getallentheorie heeft- en dat zijn er inderdaad vele!- een keuze te maken. Het resultaat daarvan vindt U in de inhoudsopgave vermeld. Nu hoopt de commissie maar dat de keuze in de smaak valt. De getallentheorie is "une mer à boire", wij zeggen van harte "prosit".

De commissie hoopt echter dat de deelnemers niet alleen ter plekke iets wijzer zullen worden, maar vooral ook dat de voordrachten een stimulans zullen zijn tot zelfstandige studie op een of meer van de aangestipte gebieden en - mocht het mogelijk zijn - dat zij er ook iets van kunnen doorgeven aan hun leerlingen; het betreft immers een onderwerp dat helaas niet behoort tot het reguliere curriculum, maar dat- naar de ervaring leert- de leerlingen altijd boeit, ook, en vooral, in haar eenvoudigste vorm.

Tot slot, als altijd- en als altijd even oprecht gemeend- een woord van hartelijke dank aan de medewerksters en de medewerkers van het CWI, die zoveel aandacht en tijd besteed hebben aan het tot stand komen van deze als altijd zo mooi uitgevoerde syllabus.

A.W. Grootendorst

Inleiding

A.W. Grootendorst
Aardbeistraat 11, 2564 TM Den Haag

A.1. Hoewel het aanvankelijk de bedoeling was om deze inleiding geheel te wijden aan een aantal hoogtepunten uit de geschiedenis van de getallentheorie, moest daarvan worden afgezien omdat het bleek dat er enkele hulpstellingen - nodig voor een goed begrip van het gebodene - waren die wegens tijdgebrek geen plaats konden vinden in de betreffende voordrachten en toch behandeld moesten worden. Deze zijn nu in de inleiding opgenomen.

Omdat we echter niet "met de deur in huis willen vallen" is de inleiding in twee delen gesplitst. Het eerste deel bevat enkele algemene opmerkingen, het tweede deel behandelt de bedoelde hulpstellingen.

A2. Over de gehele getallen, het onderwerp waarop de getallentheorie zich richt, zijn in de loop van de eeuwen zeer markante uitspraken gedaan. Overbekend zijn de uitspraken van Leopold Kronecker (1823-1891), gedaan tijdens de Berliner Naturforscher Versammlung in 1886: "Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk" en de uitspraak van Gauss (1777-1855) waarin hij de wiskunde de koningin der wetenschappen noemt en de getallentheorie de koningin der wiskunde.

Er zijn echter meer en oudere uitspraken die het fundamentele belang onderstrepen dat men steeds gehecht heeft aan de gehele (aanvankelijk slechts de natuurlijke) getallen. Zo is er een fragment, toegeschreven aan de Pythagoreeër Philolaus ($\pm$ 450 v. Chr.), dat luidt: "Inderdaad heeft alles wat men kan kennen een getal, want het is niet mogelijk iets te begrijpen of te kennen zonder het getal". Ook een fragment van Chrysogonos ($\pm$ 500 v. Chr.) spreekt duidelijke taal: "Wij leven door getal en berekening, deze immers redden de stervelingen". Getal is daarbij steeds natuurlijk getal.

De schok was daarom groot toen men reeds ten tijde van Pythagoras (ca. 560- ca. 480 v. Chr.) ontdekte dat niet alles in de ons omringende realiteit

door (natuurlijke) getallen kan worden uitgedrukt, zoals bijv. de verhouding tussen de zijde en de diagonaal van een vierkant.

Tekenend voor de schok die de ontdekking van het irrationale teweegbracht is wel het verhaal dat Iamblichus brengt in zijn "Leven van Pythagoras" (caput 88) dat degene die deze ontdekking naar buiten bracht, Hippasos van Metapontum, als straf de dood op zee vond.

A3. Met de intrede van het irrationale ontstond een strenge scheiding tussen de leer van de getallen en de leer van de "grootheden", die meetkundig geïnterpreteerd werden. In de "Elementa" van Euclides (ca. 295 v. Chr.) vinden we in de boeken 7, 8, 9 en 11 de toenmaals bekende getallentheorie weergegeven. Later in de klassieke oudheid verscheen het beroemde werk van Diophantus van Alexandrië (250 na Chr.) waarin tal van speciale problemen werden opgelost o.a. de later als Diophantische vergelijkingen bekend staande onbepaalde vergelijkingen. Diophantus zocht daarvoor rationale getallen als oplossingen.

Leopold Kronecker
(1823 - 1891)

A4. Veel later, in de 17^e eeuw, heeft Pierre (de) Fermat (1601-1665), jurist in Toulouse, het werk van Diophantus weer opgepakt, maar in een essentieël andere richting voortgezet doordat hij - in tegenstelling tot Diophantus - alleen geheeltallige oplossingen toeliet. In die zin kan hij beschouwd worden als de grondlegger van de "zuivere" getallentheorie. Aan de beroemde Diophantische vergelijking $x^n+y^n=z^n$ $(n\geqslant 3)$ waarvan Fermat zegt bewezen te hebben dat deze onoplosbaar is, wordt aandacht gegeven in de voordracht van Dr. Beukers.

De aanpak van Fermat - beperking tot gehele getallen - leidde tot grote belangstelling voor priemgetallen en deelbaarheid, bij hem en anderen. Met betrekking tot Fermat zelf zij hier alleen genoemd zijn vermoeden dat alle getallen van de gedaante $2^{2^n}+1$ priem zouden zijn. Euler (1707-1783)

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

CVM COMMENTARIIS C. G. BACHETI V. C.
& obſeruationibus D. P. de FERMAT *Senatoris Toloſani.*

Acceſſit Doctrinæ Analyticæ inuentum nouum, collectum
ex varijs eiuſdem D. de FERMAT Epiſtolis.

TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Ieſu.
M. DC. LXX.

weerlegde dit vermoeden in 1753 door aan te tonen dat reeds $n=5$ een ontbindbaar getal oplevert. De gevallen $n=0, 1, 2, 3, 4$ zijn tot op heden de enige bekende "priemgetallen van Fermat".

Van de vele belangrijke bijdragen van Fermat zij nog slechts genoemd zijn methode van de "descente infinie". Deze kan worden gebruikt om de non-existentie van een getal met een bepaalde eigenschap te bewijzen, door aan te tonen dat, als er een natuurlijk getal met die eigenschap zou bestaan, er ook een kleiner natuurlijk getal met die eigenschap zou bestaan, etc. Aangezien echter elke niet lege verzameling natuurlijke getallen een kleinste bevat, leidt dit dan tot een tegenspraak. Door de slechte verspreiding en het ontbreken van bewijzen werd het werk van Fermat niet voldoende bekend. Euler besteedde in zijn werken veel aandacht aan Fermat en deed zo de belangstelling opleven.

Van Fermat's tijdgenoten noemen we slechts de Jezuiet Marin Mersenne (1588-1648) die op grond van zijn uitgebreide correspondentie met vele geleerden, over geheel Europa verspreid, wel genoemd werd de "secretaris-generaal" van geleerd Europa. Hij hield zich o.a. bezig met de naar hem genoemde getallen van de gedaante 2^s-1. Het onderzoek naar de primaliteit daarvan is het onderwerp van de lezing van Prof. Duparc.

A5. De eerste die in die tijd de tot dan toe verworven getallentheoretische resultaten samenvatte en daaraan tevens briljante eigen ideeën toevoegde was Carl Friedrich Gauss (1777-1855), de "princeps mathematicorum". In 1801 deed hij zijn magistrale werk de "Disquisitiones Arithmeticae" verschijnen en vestigde daarmee voorgoed zijn naam als wiskundige. Met dit werk stelde hij de "Essai sur la Théorie des Nombres" van Legendre (1752-1833) dat drie jaar te voren verschenen was in de schaduw. In de "Disquisitiones" werd de getallentheorie als één geheel behandeld en werd de grondslag gelegd voor latere ontwikkelingen o.a. de theorie van de congruenties, de algebraïsche getallentheorie en de tweede- en hogere- graads vormen. Het is een moeilijk boek en werd daarom wel "het boek met zeven zegelen" genoemd. Later zou Dirichlet (1805-1859), die dit boek altijd bij zich had, veel ervan verduidelijken in zijn in 1863 - posthuum - door Dedekind (1831-1916) uitgegeven "Vorlesungen über Zahlentheorie". Uiteraard zou aan dit werk een gehele vakantie cursus- en meer - gewijd kunnen worden. Helaas kunnen wij er slechts weinig van aan de orde stellen. In de inleiding komt wel de kwadratische reciprociteitsstelling aan de orde. Een onderwerp - niet uit de Disquisitiones, maar wel door Gauss als eerste aangepakt - wordt behandeld door Dr. van de Lune: de vraag naar het aantal roosterpunten (d.w.z. punten met geheeltallige coördinaten) binnen een cirkel met gegeven straal $\sqrt{t}$, met name de vraag naar het verschil tussen dit aantal $P(t)$ en de oppervlakte πt van de cirkel en het gedrag daarvan voor grote t. Het zal dan blijken hoe zeer de computer de getallentheorie kan steunen.

A6. Dit brengt ons bij de vraag naar de hulpmiddelen die van nut kunnen zijn bij de bestudering van de getallentheorie. Immers, een bewering over gehele getallen kan in vele gevallen niet bewezen worden met behulp van uitsluitend

gehele getallen. Over de rol van de analyse (reëel en complex) in de getallentheorie worden we ingelicht in de voordracht van Prof. van der Blij. Ook de voordracht van Prof. Tijdeman slaat een brug tussen de getallentheorie en zijn omgeving. In het begin van deze inleiding duidden we al op de schok die de ontdekking van het irrationale "getal" teweegbracht. In de voordracht van Prof. Tijdeman zal besproken worden hoe deze irrationale getallen benaderd kunnen worden. Naast klassieke methoden zullen ook zeer recente algoritmen worden besproken. Ook zal een aantal praktische toepassingen worden gegeven.

A7. Lange tijd was getallentheorie een luxe, zonder veel praktische toepassingen. Dit is tegenwoordig wel anders. Een voorbeeld: de cryptografie, de leer van het geheimschrift. Ook dit zou een onderwerp kunnen zijn voor een vakantiecursus. Misschien iets voor een volgende keer. Wel is voor een onderwerp uit het dagelijkse leven plaats ingeruimd. Prof. van de Craats behandelt met getallentheoretische methoden de problematiek van de fraude-bestendige identiteitsdocumenten en dan zijn wij midden in de realiteit van alledag en zien we hoe de koningin der wetenschappen haar boudoir in de ivoren toren heeft verlaten.

B1. In dit gedeelte van de inleiding zullen enkele hulpmiddelen worden aangereikt die voor het volgen van deze cursus nodig zullen blijken, met name waar het de voordracht betreft van Prof. Duparc over de priemtoets van Lucas. Daarbij is nl. kennis nodig van enkele eigenschappen van kwadraatresten en aangezien deze behoren tot de theorie van de congruenties zullen we allereerst daaraan enige aandacht besteden. Hoewel velen van de deelnemers aan deze cursus daarmee vermoedelijk wel bekend zullen zijn, zullen we toch "from scratch" beginnen. Wij zijn dan in goed gezelschap. Het eerder genoemde, magistrale werk van Gauss, de "Disquisitiones Arithmeticae" begint eveneens - heel gewoontjes - met de allereerste beginselen van congruenties. Om U tevens iets te laten proeven van de accurate stijl waarin Gauss schrijft, volgt hier de definitie van congruentie in een letterlijke vertaling van de eerste twee paragrafen van de "Disquisitiones Arithmeticae" [1][1]

1. *Indien het getal a deelbaar is op het verschil van de getallen b en c, dan worden de getallen b en c congruent genoemd met betrekking tot a; indien dit niet het geval is, dan worden zij incongruent genoemd; a zelf noemen wij de modulus. Elk van beide, b en c, wordt in het eerste geval een rest van de ander genoemd, in het tweede geval echter een niet-rest. Deze begrippen gelden voor alle gehele getallen, zowel positieve als negatieve* en kunnen echter niet uitgebreid worden tot breuken. Bijv.* -9 *en* $+16$ *zijn congruent m.b.t. 5;* -7 *is van 15 een rest m.b.t. de modulus 11, m.b.t. de modulus 3 echter een niet-rest. Voorts is - aangezien ieder getal deelbaar is door nul - ieder getal met zichzelf congruent te beschouwen m.b.t.*

1. De tussen [ ] geplaatste getallen verwijzen naar de aantekeningen aan het einde van het betreffende artikel.

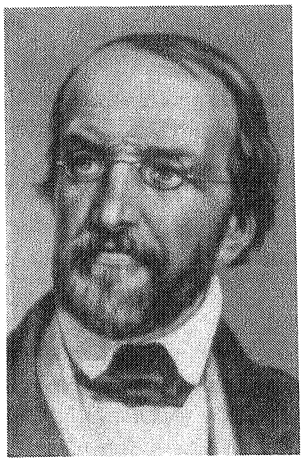
elke modulus.

2. *Alle resten van een gegeven getal a, volgens de modulus m, zijn bevat in de formule a + km, waarbij k een willekeurig geheel getal voorstelt. Van de stellingen die wij hierna zullen weergeven kunnen de meer eenvoudige zonder enige moeite hiermee bewezen worden, maar de waarheid ervan zal iedereen even gemakkelijk direct kunnen inzien. In het vervolg zullen wij congruentie van getallen aangeven met dit teken:* $\equiv$ *en de modulus - waar dat nodig is - daaraan tussen haakjes toevoegen,* $-16 \equiv 9 (\mathrm{mod}.5)$, $-7 \equiv 15 (\mathrm{mod}.11)$**

Gauss voegt hieraan twee aantekeningen toe:
* *De modulus moet kennelijk absoluut genomen worden, d.w.z. zonder teken.*
** *We hebben dit symbool genomen wegens de overeenkomst tussen gelijkheid en congruentie. Om dezelfde reden gebruikte Legendre in de verhandeling die ons vaak de gelegenheid zal geven deze aan te halen, éénzelfde teken voor gelijkheid en congruentie. Om dubbelzinnigheid te voorkomen hebben wij een onderscheid gemaakt.*

De verhandeling van Legendre (1752-1833) waarop Gauss zinspeelt, is diens "Essai sur la théorie des nombres" uit het jaar VI van de Franse revolutionaire jaartelling, dus uit 1798 volgens onze kalender.

Adrien-Marie Legendre
(1752 - 1833)



Peter Gustav Lejeune Dirichlet
(1805 - 1859)

B2. ENKELE FUNDAMENTELE EIGENSCHAPPEN

Na deze definitie noemen we zonder bewijs enkele fundamentele eigenschappen die - Gauss merkte het al op - zeer eenvoudig uit de definitie zijn af te leiden.

(i) Reflexiviteit: $a \equiv a\ (n)$

(ii) Symmetrie: $a \equiv b\ (n) \Leftrightarrow b \equiv a\ (n)$

(iii) Transitiviteit: $\left.\begin{matrix} a \equiv b\ (n) \\ b \equiv c\ (n) \end{matrix}\right\} \Rightarrow a \equiv c\ (n)$

en de rekenregels:

(iv) $\left.\begin{matrix} a \equiv b\ (n) \\ b \equiv c\ (n) \end{matrix}\right\} \Rightarrow a \pm b \equiv c \pm d\ (n)$ en $a.b \equiv c.d\ (n)$.

De reflexiviteit, symmetrie en transitiviteit induceren in de gehele getallen een indeling van alle gehele getallen in onderling disjuncte klassen van onderling congruente getallen (de " formule" $a + km$ bij Gauss).

Zo zijn er modulo 6 zes klassen, nl. die van alle zes-vouden, die van alle zes-vouden $+1$, etc. t/m die van alle zes-vouden $+5$. Vaak worden deze klassen aangegeven met [0], [1], . . . , [5] of $\bar{0}$, $\bar{1}$, . . . , $\bar{5}$ of ook simpelweg door een willekeurige representant bijv. 0, 1, . . . , 5.

Uit de genoemde rekenregels volgt dat men deze klassen kan optellen, aftrekken en vermenigvuldigen door deze bewerkingen toe te passen op willekeurig gekozen representanten van de betreffende klassen, d.w.z. men kan definiëren:

$$[a] \pm [b] := [a \pm b] \quad \text{en} \quad [a] \cdot [b] := [a \cdot b]$$

en men kan bewijzen dat deze definitie zinvol is omdat het resultaat van de bewerking onafhankelijk is van de keuze van a en b uit hun klassen.

Zo geldt bijv. modulo 6:

$$[5]+[3]=[8]=[2] \quad \text{en} \quad [5] \cdot [3]=[15]=[3].$$

N.B. Uit $[a] \cdot [b]=[0]$ volgt niet noodzakelijk dat $[a]=[0]$ of $[b]=[0]$, wel echter als de modulus priem is.

Zo geldt bijv. modulo 6: $[2] \cdot [3]=[0]$. Als echter voor een prieme modulus p geldt: $[a] \cdot [b]=[0]$, dan geldt of $[a]=[0]$ of $[b]=[0]$, immers

$$[a] \cdot [b]=[0] \Rightarrow [ab]=[0] \Rightarrow p \mid ab \quad (p \text{ deelbaar op } ab) \Rightarrow$$

$$p \mid a \quad \text{of} \quad p \mid b \Rightarrow [a]=[0] \quad \text{of} \quad [b]=[0]. \qquad [2]$$

Tot slot nog twee definities

(i) Onder een volledig restsysteem modulo n ($n \in \mathbb{N}$) verstaan we een n-tal getallen waarvan er niet twee congruent zijn modulo n. Een voorbeeld: als $n=6$, dan is een volledig restsysteem bijv. $\{0,7,14,-3,10,5\}$.

(ii) Onder een gereduceerd restsysteem modulo n ($n \in \mathbb{N}$) verstaan we een volledig restsysteem modulo n waaruit de getallen die met n onderling deelbaar zijn, weggelaten zijn. Een voorbeeld: als $n=12$, dan is een gereduceerd restsysteem bijv.: $\{1,5,7,11\}$. Voor een priemgetal p kan men als gereduceerd restsysteem nemen $\{1,2,3, \ldots, p-1\}$.

Het aantal elementen in een gereduceerd restsysteem modulo n geeft men aan

met $\phi(n)$. Voor een priemgetal p geldt dus $\phi(p)=p-1$.

B3. TWEE BELANGRIJKE STELLINGEN

Allereerst leiden we nu met behulp van de ingevoerde begrippen en de geformuleerde rekenregels twee stellingen af, nl. de - kleine - stelling van Fermat (1601-1665) [3] en de stelling van John Wilson (1741-1793) [4].

(i) De kleine stelling van Fermat luidt als volgt:

Voor p priem en $a\in\mathbb{Z}$ met $p\nmid a$ (p niet deelbaar op a) geldt $a^{p-1}\equiv 1 \pmod p$,

Men kan dit als volgt bewijzen (bewijs van Gauss). Beschouw de volgende rijen getallen

$$1,\ 2,\ 3,\ \ldots,\ p-1 \tag{3.1}$$

(een gereduceerd restsysteem modulo p dus) en

$$a,\ 2a,\ 3a,\ \ldots,\ (p-1)a. \tag{3.2}$$

Dit tweede stel getallen is eveneens een gereduceerd restsysteem modulo p. Geen ervan is immers deelbaar door p, vanwege de eis $p\nmid a$ en er staan juist $p-1$ modulo p verschillende getallen, immers

$$aj \equiv ak \pmod p$$

impliceert $p \mid a$ of $p \mid j-k$ en dit kan slechts indien $j=k$ daar $p\nmid a$ en $1\leqslant j,k\leqslant p-1$.

Elk getal van (3.2) is dus modulo p congruent met precies één getal van (3.1). Het product van alle getallen uit (3.1) is dus modulo p congruent met het product van alle getallen van (3.2), dus

$$(p-1)! \equiv (p-1)!a^{p-1} \pmod p$$

en dus, daar $p\nmid(p-1)!$, geldt

$$a^{p-1} \equiv 1 \pmod p \tag{3.3}$$

voor p priem en $(a,p)=1$*.

Aangezien voor alle $a\in\mathbb{Z}$ geldt dat $a\equiv a(p)$, geldt ook voor prieme p en alle $a\in\mathbb{Z}$

$$a^p \equiv a \pmod p \tag{3.4}$$

OPMERKING 1. Deze stelling laat zich gemakkelijk uitbreiden tot de stelling van Fermat-Euler:

$$a^{\phi(m)} \equiv 1 \pmod m. \tag{3.5}$$

voor alle a en $m\in\mathbb{Z}$ met $(a,m)=1$. Beschouw daartoe i.p.v. (3.1) een gereduceerd restsysteem modulo m.

* (a,p) is de g.g.d. van a en p.

OPMERKING 2. Uit $a^{p-1} \equiv 1 \pmod{p}$ volgt, als $p > 2$

$$p \mid (a^{\frac{p-1}{2}} + 1) \text{ of } p \mid (a^{\frac{p-1}{2}} - 1).$$

Men kan zich dan afvragen welke van beide mogelijkheden zich voordoet. Deze vraag zullen we beantwoorden op blz. 13 i.v.m. de theorie van de kwadraatresten.

OPMERKING 3. Men kan de stelling van Fermat-Euler (dus ook die van Fermat) ook zien als een resultaat uit de groepentheorie. De restklassen $[a]$ modulo m, waarbij $(a,m)=1$ vormen nl. een multiplicatieve groep met orde $\phi(m)$ en dus geldt volgens een stelling van Lagrange (1736-1813)

$$[a]^{\phi(m)} = [1]$$

en dus $a^{\phi(m)} \equiv 1 \pmod{m}$ als $(a,m)=1$.

OPMERKING 4. Het omgekeerde van de stelling van Fermat is niet waar, d.w.z. als $a^{m-1} \equiv 1 \pmod{m}$ voor zekere a met $(a,m)=1$ dan is m niet noodzakelijk priem. Men kan zelfs bewijzen dat voor iedere $a > 1$ er oneindig veel samengestelde m zijn met $(a,m)=1$ en $a^{m-1} \equiv 1 \pmod{m}$ [5].

(ii) De stelling van Wilson zegt dat voor prieme p geldt

$$(p-1)! \equiv -1 \pmod{p}. \tag{3.6}$$

Voor $p=2$ is de stelling triviaal. Voor $p > 2$ kan men o.a. het volgende bewijs geven.

Neem

$$a \in \{2, 3, 4, \ldots, p-2\} \tag{3.7}$$

en beschouw de rij getallen

$$a, 2a, 3a, \ldots, (p-1)a. \tag{3.8}$$

Het is dan eenvoudig in te zien dat dit een gereduceerd restsysteem modulo p is (de beperking $a \neq 1$, $a \neq p-1$ is daarbij niet essentieel). Dit betekent dat één element van (3.8) modulo p congruent is met 1, d.w.z. er is een $k \in \{1,2, \ldots, p-1\}$ zó dat

$$ka \equiv 1 \pmod{p}.$$

Is het mogelijk dat $k = a$? Dan zou gelden

$$a^2 \equiv 1 \pmod{p}$$

dus $p \mid a^2 - 1$, maar dan zou $p \mid a-1$ of $p \mid a+1$, hetgeen niet mogelijk is op grond van (3.7). Er is dus bij elke $a \in \{2,3, \ldots, p-2\}$ een van a verschillende partner a', zodanig dat

$$a'a \equiv 1 \pmod{p}.$$

Zo krijgt men $\frac{p-3}{2}$ congruenties die bij vermenigvuldiging opleveren

$$(p-2)! \equiv 1 \pmod{p}.$$

Aangezien

$$p-1 \equiv -1 \pmod{p}$$

geldt dus

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

B4. KWADRAATRESTEN

In de vorige paragraaf zagen we al dat als $a \in \{1,2,3,\ldots,p-1\}$ (p priem), de rij getallen $a, 2a, 3a, \ldots, (p-1)a$ een gereduceerd restsysteem modulo p is. In het vervolg nemen we aan dat $p > 2$. Bij gegeven $m (p \nmid m)$ is er dus bij elke $a \in \{1,2,3,\ldots,p-1\}$ een a' uit dezelfde verzameling zó dat

$$aa' \equiv m \pmod{p}.$$

We vragen ons nu af of het mogelijk is dat $a = a'$. Indien dit het geval is, dan bestaat er bij de gegeven m dus een $a \in \{1,2,3,\ldots,p-1\}$ met $a^2 \equiv m \pmod{p}$. In dit geval noemt men m een kwadraatrest modulo p, kortweg: een rest modulo p. Indien er bij gegeven m niet een a bestaat met $a^2 \equiv m \pmod{p}$, dan noemt men m een niet-kwadraatrest modulo p, kortweg: een niet-rest modulo p.

Het gaat hier dus om de oplosbaarheid van de congruentie

$$x^2 \equiv m \pmod{p}. \tag{4.1}$$

Allereerst is duidelijk dat, als a een oplossing is van (4.1), ook $p-a$ een oplossing is.

Modulo p zijn er geen andere oplossingen, immers als

$$x^2 \equiv m \text{ en } a^2 \equiv m \pmod{p}.$$

dan geldt

$$x^2 \equiv a^2 \pmod{p}.$$

dus

$$p \mid x-a \text{ of } p \mid x+a$$

dus

$$x \equiv a \ (p) \text{ of } x \equiv -a \equiv p-a \pmod{p}.$$

We onderzoeken nu de beide mogelijkheden voor m nader.

(i) *m is een kwadraatrest modulo p*

Er is dus een a in $\{1,2,3,\ldots,p-1\}$ met $a^2 \equiv m$ en $(p-a)^2 \equiv m \pmod{p}$. De overige elementen van deze verzameling zijn te verdelen in $\frac{p-3}{2}$ paren (x,x') van onderling verschillende elementen waarvoor geldt

$$xx' \equiv m \pmod{p}.$$

Vermenigvuldiging van alle elementen van deze verzameling levert

$$(p-1)! \equiv m^{\frac{p-3}{2}}.a(p-a) \equiv -m^{\frac{p-1}{2}} \pmod{p}. \tag{4.2}$$

(ii) *m is geen kwadraatrest modulo p*

In dit geval zijn de elementen van $\{1,2,3,\ldots,p-1\}$ te verdelen in $\frac{p-1}{2}$ paren onderling verschillende elementen x en x' waarvoor geldt

$$xx' \equiv m \pmod{p}.$$

Nu levert vermenigvuldiging op

$$(p-1)! \equiv m^{\frac{p-1}{2}} \pmod{p}. \tag{4.3}$$

Uit (4.2) en (4.3) volgt:

$$(p-1)! \equiv \mp m^{\frac{p-1}{2}} \pmod{p}.$$

al naar dat m wel of geen kwadraatrest modulo p is. Voor p priem ($p>2$) en $m \in \mathbb{Z}$ met $p \nmid m$ introduceren we nu het kwadratische-restsymbool oftewel het symbool van Legendre $(\frac{m}{p})$ en definiëren dit als volgt

$(\frac{m}{p}) = +1$ als m kwadraatrest modulo p is

$(\frac{m}{p}) = -1$ als m geen kwadraatrest modulo p is.

We hebben dan

$$(p-1)! \equiv -(\frac{m}{p})m^{\frac{p-1}{2}} \pmod{p}. \tag{4.4}$$

5. Enkele stellingen over $(\frac{m}{p})$

a. Met behulp van de eerder afgeleide stelling van Wilson (3.6) zien we onmiddellijk in dat

$$(\frac{m}{p}) \equiv m^{\frac{p-1}{2}} \pmod{p}. \tag{5.1}$$

rest dagegen aller Primzahlen von der Form $6n + 5$ oder, mit Ausschluss von 2, aller Primzahlen von der Form $3n + 2$, d. h. aller derer, die Nichtreste von 3 sind. Man erkennt leicht, dass hieraus alle übrigen Fälle von selbst folgen.

Die auf die Reste $+3$ und -3 bezüglichen Sätze sind schon Fermat bekannt gewesen, *Opera Wallisii, T. II. p. 857,* doch gab zuerst Euler die Beweise, *Comm. Nov. Petr. T. VIII p. 105 u. ff.* Um so mehr muss man sich wundern, dass die Beweise der auf die Reste $+2$ und -2 bezüglichen Sätze, die auf ganz ähnlichen Kunstgriffen beruhen, seinem Scharfsinn stets entgangen sind. Man vergleiche auch die Abhandlung von Lagrange, *Nouv. Mém. de l'Ac. de Berlin 1775 p. 352.*

Reste $+5$ und -5.

121.

Durch Induction findet man, dass $+5$ von keiner ungeraden Zahl von der Form $5n + 2$ oder $5n + 3$ Rest ist, d. h. von keiner ungeraden Zahl, welche Nichtrest von 5 ist. Dass aber diese Regel keine Ausnahme erleidet, wird so bewiesen: Es sei, wenn es eine giebt, die kleinste Zahl, welche von dieser Regel auszunehmen ist, gleich t, so dass dieselbe Nichtrest der Zahl 5 ist, während 5 Rest von t ist. Es sei ferner $a^2 = 5 + tu$, so dass a gerade und kleiner als t ist. Dann wird also u ungerade und kleiner als t, $+5$ aber Rest von u sein. Wenn nun a nicht durch 5 teilbar ist, so wird dasselbe von u gelten; offenbar aber ist tu Rest von 5, somit wird, da t Nichtrest von 5 ist, auch u Nichtrest von 5 sein. D. h. es giebt einen ungeraden Nichtrest der Zahl 5, dessen Rest $+5$ ist und der kleiner als t ist. Dies steht aber im Widerspruch mit unsrer Voraussetzung. Ist dagegen a durch 5 teilbar, so setze man $a = 5b$ und $u = 5v$, so wird $tv \equiv -1 \equiv 4 \pmod 5$, d. h. tv wird Rest der Zahl 5 sein. Im Übrigen schreitet der Beweis ebenso fort, wie im ersteren Falle.

122.

Von allen Primzahlen also, welche zu gleicher Zeit Nichtreste von 5 und von der Form $4n + 1$ sind, d. h. von allen Primzahlen von der Form $20n + 13$ oder $20n + 17$, sind $+5$ und -5 Nichtreste; von allen Primzahlen von der Form $20n + 3$ oder $20n + 7$ dagegen ist $+5$ Nichtrest, -5 aber Rest.

Auf ganz analoge Weise kann man zeigen, dass -5 Nichtrest ist von allen Primzahlen von einer der Formen $20n + 11$, $20n + 13$, $20n + 17$, $20n + 19$, und hieraus folgt, wie man leicht sieht, dass $+5$ Rest ist von allen Primzahlen von der Form $20n + 11$ oder $20n + 19$, dagegen Nichtrest aller derer von der Form $20n + 13$ oder $20n + 17$. Und da jede Primzahl ausser 2 und 5 (von denen ± 5 Rest ist) in irgend einer der Formen $20n + 1, 3, 7, 9, 11, 13, 17, 19$ enthalten ist, so kann man offenbar

Hiermee is tevens de vraag op blz. 9 beantwoord, nl.

$$p \mid m^{\frac{p-1}{2}} - 1 \text{ als } m \text{ een kwadraatrest modulo } p \text{ is}$$

en $$p \mid m^{\frac{p-1}{2}} + 1 \text{ als } m \text{ geen kwadraatrest modulo } p \text{ is.}$$

b. We kunnen de stelling van Wilson ook afleiden uit (4.4) en wel door daarin $m = 1$ te stellen. Daar ten duidelijkste geldt dat $(\frac{1}{p}) = 1$, levert (4.4)

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

c. Indien we in (5.1) stellen $m = -1$, dan vinden we

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

en, daar $(\frac{-1}{p}) = \pm 1$, geldt dus

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}.$$

In woorden: -1 is kwadraatrest modulo de priemgetallen van de vorm $4n+1$ en niet-rest modulo de priemgetallen van de vorm $4n-1$.

d. Voor het bepalen van het aantal kwadraatresten modulo p zouden we in principe moeten berekenen $1^2, 2^2, 3^2, \ldots, (p-1)^2$ en nagaan hoeveel modulo p verschillende uitkomsten dit oplevert. Aangezien echter $a^2 \equiv (p-a)^2$ kunnen we ons beperken tot de kwadraten

$$1^2, 2^2, 3^2, \ldots, (\frac{p-1}{2})^2.$$

Deze blijken inderdaad alle onderling verschillend mod p, immers uit $a^2 \equiv b^2$ zou volgen dat $p \mid a-b$ of $p \mid a+b$. Daar echter $1 \leqslant a,b \leqslant \frac{p-1}{2}$, impliceert dit dat $a = b$.

De genoemde $\frac{p-1}{2}$ kwadraten leveren dus modulo p alle kwadraatresten. De overige resten (in de "oude" betekenis) zijn dus geen kwadraatresten. Er zijn dus evenveel kwadraatresten als niet-kwadraatresten, nl. $\frac{p-1}{2}$.

Een simpel voorbeeld. Neem $p = 13$; dan zijn de kwadraatresten $1^2, 2^2, 3^2, 4^2, 5^2, 6^2$ dus 1,4,9,3,12,10 en de overige resten 2,5,6,7,8,11 zijn de niet-kwadraatresten. Met behulp van een lijst van kwadraatresten modulo p kan men van ieder getal vaststellen of het een kwadraatrest modulo p is of niet.

6. Het lemma van Gauss

Het lemma van Gauss geeft ook een mogelijkheid om een uitspraak te doen over het kwadratische karakter van een getal m modulo een priemgetal p en het luidt

$$(\frac{m}{p})=(-1)^{\mu}. \tag{6.1}$$

Hierin is μ het aantal kleinste positieve resten modulo p van de getallen

$$m, 2m, 3m, \ldots, \frac{p-1}{2}m \tag{6.2}$$

dat ligt tussen $\frac{p}{2}$ en p.

We lichten dit toe. Onder de kleinste positieve rest van een getal m modulo p verstaan we het kleinste positieve getal waarmee m modulo p congruent is, dus het getal r zodanig dat

$$m=[\frac{m}{p}]p+r \quad \text{met} \quad 1\leqslant r\leqslant p-1.$$

Hierin is $[\frac{m}{p}]$ zoals gebruikelijk het grootste gehele getal dat kleiner is dan, of gelijk is aan $\frac{m}{p}$ (entier van $\frac{m}{p}$). De kleinste positieve resten van de getallen $m, 2m, \ldots, \frac{p-1}{2}m$ liggen alle op het interval $<0,p>$ en μ is dan het aantal dat ligt op $<\frac{p}{2},p>$.

Eerst maar een voorbeeld. Stel $p=17$, $m=27$. Het gaat dan om de getallen 27, 54, 81, 108, 135, 162, 189, 216. Hun kleinste positieve resten zijn 10, 3, 13, 6,16, 9, 2, 12. Hiervan liggen 2,3,6 op $<0,8>$ en 9, 10, 12, 13, 16 op $<8,17>$ dus $\mu=5$. Volgens het lemma van Gauss geldt dan $(\frac{22}{17})=(-1)^5$, dus 27 is geen kwadraatrest modulo 17, hetgeen gemakkelijk te verifiëren is door 27 modulo 17 te vergelijken met de kwadraten $1^2,2^2,3^2,4^2,5^2,6^2,7^2,8^2$ die modulo 17 opleveren 1, 4, 9, 16, 8, 2, 15, 13.

Nu het bewijs. Zoals gezegd, bepalen we bij gegeven prieme p en gegeven m ($p>2$, $p\nmid m$) de getallen

$$m, 2m, 3m, \ldots, \frac{p-1}{2}m \tag{6.3}$$

en berekenen hiervan de kleinste positieve resten modulo p

$$r_1, r_2, \ldots, r_\lambda, s_1, s_2, \ldots, s_\mu \tag{6.4}$$

waarbij

$$0<r_i<\frac{p}{2} \quad \text{en} \quad \frac{p}{2}<s_j<p.$$

Allereerst merken we op dat de getallen r_i en s_j ($1\leqslant i\leqslant\lambda$; $1\leqslant j\leqslant\mu$) alle

onderling incongruent zijn modulo p, immers, als twee ervan congruent zouden zijn modulo p, dan zou voor zekere a en b behorende tot $\{1,2,\ldots,\frac{p-1}{2}\}$ gelden

$$am \equiv bm \quad (p)$$

dus $p \mid (a-b)m$ en dat kan slechts als $a=b$, want $0 \leqslant |a-b| \leqslant \frac{p-1}{2}$ en $p \nmid m$.

Dit houdt in dat ook de $\frac{p-1}{2}$ getallen

$$r_1, r_2, \ldots, r_\lambda, p-s_1, p-s_2, \ldots, p-s_\mu$$

alle onderling incongruent zijn. Zij liggen echter op het interval $<0,\frac{p}{2}>$ en zijn dus de getallen $1,2,\ldots,\frac{p-1}{2}$, wellicht in andere volgorde. Dan geldt echter modulo p

$$m.2m.3m \cdots \frac{p-1}{2}m \equiv r_1 r_2 \cdots r_\lambda . s_1 s_2 \cdots s_\mu$$

$$\equiv r_1 r_2 \cdots r_\lambda (p-s_1)(p-s_2)\cdots(p-s_\mu).(-1)^\mu$$

$$= 1.2.3.\cdots\frac{p-1}{2}.(-1)^\mu$$

en dus, omdat $p \nmid 1.2.3.\cdots\frac{p-1}{2}$

$$m^{\frac{p-1}{2}} \equiv (-1)^\mu \quad (\text{mod}.p).$$

We weten al uit (5.1) dat

$$(\frac{m}{p}) \equiv m^{\frac{p-1}{2}} \quad (\text{mod}.p)$$

dus

$$(\frac{m}{p}) \equiv (-1)^\mu \quad (\text{mod}.p)$$

en, omdat,

$$(\frac{m}{p}) = \pm 1$$

moet wel gelden dat

$$(\frac{m}{p}) = (-1)^\mu.$$

7. Enkele toepassingen van het lemma van Gauss
Het kwadratische karakter van 2 en van 3.

a. Stelling. 2 is een kwadraatrest van de priemgetallen p met $p=8v\pm1$ en een niet-rest van de priemgetallen p met $p=8v\pm3$.

Bewijs. Het gaat nu om de kleinste positieve resten modulo p van de getallen $2,4,6,\ldots,\frac{p-1}{2}.2$. Deze liggen al op $<0,p>$ en zijn dus zelf hun kleinste positive resten. Het getal μ is kennelijk het aantal even getallen op $<\frac{p}{2},p>$ en dat is

$$\frac{p-1}{2}-\left[\frac{p}{4}\right].$$

M.b.t. $[\frac{p}{4}]$ lijkt het verstandig te onderscheiden $p=4k+1$ en $p=4k+3$, maar we zullen zien dat we dan nog een verfijning moeten aanbrengen.

(i) $p=4k+1$. Dan geldt $[\frac{p-1}{2}]=2k$, $[\frac{p}{4}]=k$, en $\mu=k$, dus

$$(\frac{2}{p})=(-1)^k=+1 \text{ als } k\equiv 0\ (2),\ \text{bijv. } k=2v$$

en

$$(\frac{2}{p})=(-1)^k=-1 \text{ als } k\equiv 1\ (2),\ \text{bijv. } k=2v-1.$$

(ii) $p=4k+3$. Dan geldt $[\frac{p-1}{2}]=2k+1$, $[\frac{p}{4}]=k$, en $\mu=k+1$, dus

$$(\frac{2}{p})=(-1)^{k+1}=+1 \text{ als } k\equiv 1\ (2),\ \text{bijv. } k=2v-1$$

en

$$(\frac{2}{p})=(-1)^{k+1}=-1 \text{ als } k\equiv 0\ (2),\ \text{bijv. } k=2v.$$

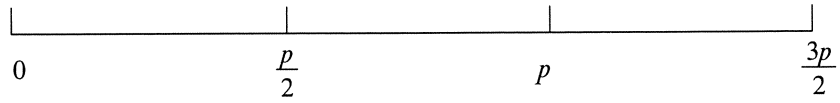
Samengevat

$$\boxed{(\frac{2}{p})=+1 \quad \text{als} \quad p=8v\pm1;\ (\frac{2}{p})=-1 \quad \text{als} \quad p=8v\pm3}$$

b. Stelling. 3 is een kwadraatrest van de priemgetallen $p=12v\pm1$ en een niet-rest van de priemgetallen $p=12v\pm5$.

Bewijs. Het gaat nu om de kleinste positieve resten modulo p van de getallen $3,6,9,\ldots,\frac{p-1}{2}.3$ (zie 6.2). Het is duidelijk dat deze getallen liggen op

$<0, \frac{3}{2}p>$.



De eventuele getallen op $<p, \frac{p}{3}>$ komen bij reductie modulo p op het interval $<0, \frac{p}{2}>$ en interesseren ons dus niet. Het getal μ is dus het aantal 3-vouden op het interval $<\frac{p}{2}, p>$ dus $\mu=[\frac{p}{3}]-[\frac{p}{6}]$.

De ervaring met het vorige geval doet ons nu maar meteen p bekijken modulo 12.

(i) $p=12v+1$. Dan geldt $[\frac{p}{3}]=4v$, $[\frac{p}{6}]=2v$ en $\mu=2v$, dus

$$(\frac{3}{p})=(-2)^{2v}=1$$

(ii) $p=12v-1$; Dan geldt $[\frac{p}{3}]=4v-1$, $[\frac{p}{6}]=2v-1$ en $\mu=2v$, dus

$$(\frac{3}{p})=(-2)^{2v}=1$$

(iii) $p=12v+5$. Dan geldt $[\frac{p}{3}]=4v+1$, $[\frac{p}{6}]=2v$ en $\mu=2v+1$, dus

$$(\frac{3}{p})=(-2)^{2v+1}=-1$$

(iv) $p=12v-5$. Dan geldt $[\frac{p}{3}]=4v-2$, $[\frac{p}{6}]=2v-1$ en $\mu=2v-1$, dus

$$(\frac{3}{p})=(-2)^{2v-1}=-1.$$

Samengevat

$$(\frac{3}{p})=+1 \quad \text{als} \quad p=12v\pm1; \quad (\frac{3}{p})=-1 \quad \text{als} \quad p=12v\pm5$$

8. De kwadratische reciprociteitsstelling

In een inleidende voordracht over kwadraatresten mag aandacht voor de kwadratische reciprociteitssteling - meestal kortweg de reciprociteitsstelling genoemd - niet ontbreken. Deze stelling werd al vermoed door Legendre, maar eerst door Gauss bewezen (Disquisitiones Arithmeticae, art. 130-152).
De stelling luidt als volgt.
Indien p en q oneven priemgetallen zijn, dan geldt voor de Legendre-symbolen

$(\frac{p}{q})$ en $(\frac{q}{p})$ de volgende

STELLING

$$(\frac{p}{q})(\frac{q}{p})=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{8.1}$$

Van deze stelling bestaan meerdere bewijzen. Gauss zelf gaf er drie van. Een fraai elementair bewijs is ook dat van Eisenstein (1823-1852), oorspronkelijk gepubliceerd in Journal de Crelle **29** (1845). Het berust op een elementair te bewijzen geometrische formule en is ook te vinden in "A Course in Arithmetic" door J.P. Serre.

Het volgende is een zeer gangbaar bewijs dat nauw aansluit bij wat we tot nu toe bespraken m.n. het lemma van Gauss.

Voor dit bewijs beschouwen we evenals in paragraaf B6, de rij getallen

$$q, 2q, 3q, \ldots, \frac{p-1}{2}q.$$

Voor elk van hen kunnen we schrijven.

$$kq = pq_k + r_k \quad (1 \leqslant k \leqslant \frac{p-1}{2}) \tag{8.2}$$

met

$$q_k = \left[\frac{kq}{p}\right] \quad \text{en} \quad 1 \leqslant r_k \leqslant p-1.$$

De getallen r_k zijn dus de kleinste positieve resten modulo p van de getallen kq en zijn, evenals in B6, te verdelen in de resten

$$a_1, a_2, \ldots, a_\lambda \text{ met } 1 \leqslant a_i < \frac{p}{2}$$

en

$$b_1, b_2, \ldots, b_\mu \text{ met } \frac{p}{2} < b_t \leqslant p-1.$$

We zagen al dat dan de getallen

$$a_1, a_2, \ldots, a_\lambda, p-b_1, p-b_2, \ldots, p-b_\mu$$

juist de getallen $1, 2, 3, \ldots, \frac{p-1}{2}$ zijn, eventueel in een andere volgorde. Hieruit volgt dan dat

$$\sum_{i=1}^{\lambda} a_i + \sum_{t=1}^{\mu} (p-b_t) = 1+2+\cdots\frac{p-1}{2}.$$

Stellen we $\sum_{i=1}^{\lambda} a_i = a$ en $\sum_{t=1}^{\mu} b_t = b$, dan vinden we

I. Si l'on a $\left(\frac{a}{b}\right)=-1$, il s'ensuit $\left(\frac{b}{a}\right)=-1$.

II. Si l'on a $\left(\frac{b}{a}\right)=+1$, il s'ensuit $\left(\frac{a}{b}\right)=+1$.

III. Si l'on a $\left(\frac{\mathrm{B}}{b}\right)=+1$, il s'ensuit $\left(\frac{b}{\mathrm{B}}\right)=-1$.

IV. Si l'on a $\left(\frac{\mathrm{B}}{b}\right)=-1$, il s'ensuit $\left(\frac{b}{\mathrm{B}}\right)=+1$.

V. Si l'on a $\left(\frac{a}{\mathrm{A}}\right)=+1$, il s'ensuit $\left(\frac{\mathrm{A}}{a}\right)=+1$.

VI. Si l'on a $\left(\frac{a}{\mathrm{A}}\right)=-1$, il s'ensuit $\left(\frac{\mathrm{A}}{a}\right)=-1$.

VII. Si l'on a $\left(\frac{a}{b}\right)=+1$, il s'ensuit $\left(\frac{b}{a}\right)=+1$.

VIII. Si l'on a $\left(\frac{b}{a}\right)=-1$, il s'ensuit $\left(\frac{a}{b}\right)=-1$.

Démonstration des cas I *et* II.

(167) J'observe d'abord que l'équation $x^2+ay^2=bz^2$, ou plus généralement l'équation $(4f+1)x^2+(4g+1)y^2=(4n+3)z^2$ est impossible; car x et y étant supposés premiers entre eux, le premier membre sera toujours compris dans les formes $4k+1$ et $4k+2$, tandis que le second ne peut l'être que dans les formes $4k$ et $4k+3$.

Mais suivant le n° 27, l'équation $x^2+ay^2=bz^2$ serait résoluble, si on pouvait trouver deux entiers λ et μ tels que $\frac{\lambda^2+a}{b}$ et $\frac{\mu^2-b}{a}$ fussent des entiers. D'un autre côté, la condition pour que b soit diviseur de λ^2+a est $\left(\frac{-a}{b}\right)=1$, ou $\left(\frac{a}{b}\right)=-1$, et la condition pour que a divise μ^2-b est $\left(\frac{b}{a}\right)=+1$. Donc on ne saurait avoir à-la-fois $\left(\frac{a}{b}\right)=-1$ et $\left(\frac{b}{a}\right)=+1$; d'ailleurs chacune de ces expressions ne peut être que $+1$ ou -1; donc

$$a+\mu p-b=\frac{p^2-1}{8}. \tag{8.3}$$

Ook geldt (zie 8.2):

$$\sum_{k=1}^{\frac{p-1}{2}} kq=\sum_{k=1}^{\frac{p-1}{2}} pq_k+\sum_{k=1}^{\frac{p-1}{2}} r_k=p\sum_{k=1}^{\frac{p-1}{2}} q_k+\sum_{i=1}^{\lambda} a_i+\sum_{t=1}^{\mu} b_t \tag{8.4}$$

dus

$$q\frac{p^2-1}{8}=p\sum_{k=1}^{\frac{p-1}{2}} q_k+a+b. \tag{8.5}$$

Vermindering van (8.5) met (8.3) geeft

$$\frac{p^2-1}{8}(q-1)=p\sum_{k=1}^{\frac{p-1}{2}} q_k-\mu p+2b.$$

Aangezien p en q beide oneven ondersteld zijn, volgt hieruit dat

$$\mu\equiv\sum_{k=1}^{\frac{p-1}{2}} q_k \pmod 2$$

en dus

$$(\frac{q}{p})=(-1)^{\mu}=(-1)^{Q}$$

met

$$Q=\sum_{k=1}^{\frac{p-1}{2}} q_k.$$

Analoog vinden we

$$(\frac{p}{q})=(-1)^{P}$$

met

$$P=\sum_{t=1}^{\frac{p-1}{2}} p_t$$

waarbij - overeenkomstig (8.2) - de getallen p_t zijn bepaald door

$$tp=qp_t+s_t \quad 1\leqslant t\leqslant\frac{1}{2}(q-1)$$

met

$$p_t=[\frac{tp}{q}] \text{ en } 1\leqslant s_t\leqslant q-1.$$

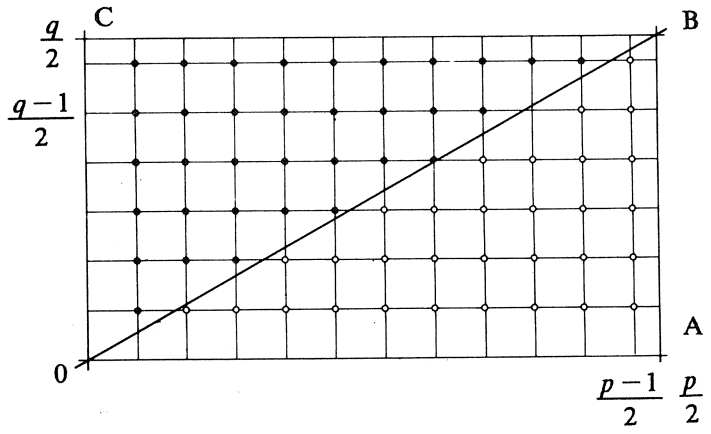
We vinden dus

$$(\frac{p}{q})(\frac{q}{p})=(-1)^{P+Q}.$$

Rest dus nog aan te tonen dat

$$P+Q=\sum_{t=1}^{\frac{p-1}{2}}\left[\frac{tp}{q}\right]+\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]=\frac{p-1}{2}.\frac{q-1}{2} \tag{8.6}$$

Dit is geen groot probleem als we letten op de meetkundige betekenis van één en ander. Daartoe beschouwen we de rechthoek OAB (zie afb.)



met $O(0,0)$; $A(\frac{p}{2},0)$; $B(\frac{p}{2},\frac{q}{2})$ en $C(0,\frac{q}{2})$ als hoekpunten. Het aantal roosterpunten daarbinnen is ten duidelijkste $\frac{p-1}{2}.\frac{q-1}{2}$.

Op de diagonaal OB liggen geen roosterpunten. Immers voor een roosterpunt (m,n) daarop zou gelden $pn-qm=0$, dus $p\mid m$ en $q\mid m$, hetgeen niet mogelijk is, daar $0\leqslant m\leqslant\frac{p-1}{2}$ en $0\leqslant m\leqslant\frac{1}{2}(q-1)$. Het genoemde aantal roosterpunten is dus ook gelijk aan de som van het aantal roosterpunten binnen driehoek OAB en het aantal roosterpunten binnen OBC. Deze aantallen zijn resp.

$$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{q}{p}k\right] \text{ en } \sum_{t=1}^{\frac{1}{2}(q-1)}\left[\frac{p}{q}t\right].$$

Hiermee is (8.6) bewezen en dus ook de reciprociteitssteling

$$(\frac{p}{q})(\frac{q}{p})=(-1)^{\frac{p-1}{2}.\frac{q-1}{2}}.$$

AANTEKENINGEN

[1] Voor de liefhebbers volgt hier de originele tekst.

Numeri congrui, moduli, residua et nonresidua.

1.

Si numerus a numerorum b,c differentiam metitur, b et c *secundum a congrui* dicuntur, sin minus, *incongrui*: ipsum *a modulum* appellamus. Uterque numerorum b,c priori in casu alterius *residuum*, in posteriori vero *nonresiduum* vocatur.

Hae notiones de omnibus numeris integris tam positivis quam negativis*) valent, neque vero ad fractos sunt extendendae. E.g. -9 et $+16$ secundum modulum 5 sunt congrui; -7 ipsius $+15$ secundum modulum 11 residuum, secundum modulum 3 vero nonresiduum. Ceterum quoniam cifram numerus quisque metitur, omnis numerus tamquam sibi ipsi congruus secundum modulum quemcunque est spectandus.

2.

Omnia numeri dati a residua secundum modulum m sub formula $a+km$ comprehenduntur, designante k numerum integrum indeterminatum. Propositionum quas post trademus faciliores nullo negotio hinc demonstrari possunt: sed istarum quidem veritatem aeque facile quivis intuendo poterit perspicere. Numerorum congruentiam hoc signo $\equiv$, in posterum denotabimus, modulum ubi opus erit in clausulis adiungentes, $-16\equiv 9 \pmod 5$, $-7\equiv 15 \pmod{11}$**

[2] Men kan eenvoudig bewijzen dat de restklassen modulo een samengesteld getal een commutatieve ring met eenheid en met nuldelers vormen en dat die modulo een priemgetal een lichaam vormen.

[3] Deze stelling heet de kleine stelling van Fermat in tegenstelling tot de zgn. grote stelling van Fermat die uitspreekt dat de vergelijking $x^n+y^n=z^n$ geen oplossingen in $\mathbb{Z}$ heeft (m.u.v. $x=y=z=0$) voor natuurlijke getallen $n\geqslant 3$ (zie hiervoor de voordracht van Dr. Beukers). De oorspronkelijke vorm die Fermat gaf aan de stelling (1640, zonder bewijs; wel schreef hij aan Frénicle (1605-1675) dat hij een bewijs bezat) luidde: Als p priem is en als t het kleinste getal is met de eigenschap dat $a^t=kp+1$, dan is t een deler van $p-1$. Het eerste bewijs van de kleine stelling van Fermat is gegeven door Euler in 1736. Dit berust op volledige inductie. Voor $a=1$ is de stelling triviaal. Verder geldt $(a+1)^p\equiv a^p+1$ omdat voor prieme p geldt: $\binom{p}{t}\equiv 0 \pmod p$ voor $2\leqslant t\leqslant p-1$. Dus als de stelling geldt voor a dan geldt hij ook voor $a+1$, immers dan geldt

$$(a+1)^p \equiv a^p+1 \equiv a+1 \pmod p.$$

[4] Deze stelling draagt de naam van Wilson, wellicht ten onrechte. Waring (1741-1793) noemt hem zonder bewijs in zijn "Meditationes Algebraicae" (1770) en schrijft hem daarbij toe aan Wilson. Het eerste bewijs is van Lagrange (1773). Gauss heeft hierover een zure opmerking in zijn "Disquisitiones Arithmeticae" (art. 76).

> Theorema hoc elegans ... primum a cel. Waring est prolatum armigeroque Wilson adscriptum, *Meditt. algebr. Ed. 3. p. 380.* Sed neuter demonstrare potuit, et cel. Waring fatetur demonstrationem eo difficiliorem videri, quod nulla *notatio* fingi possit, quae numerum primum exprimat. — At nostro quidem iudicio huiusmodi veritates ex notionibus potius quam ex notationibus hauriri debebant.

d.w.z. Deze fraaie stelling ... is voor het eerst geformuleerd door de beroemde Waring en door hem toegeschreven aan zijn schildknaap Wilson (Meditationes Algebr., 3e Ed., p. 380). Maar geen van beiden kon deze bewijzen en de beroemde Waring geeft toe dat het bewijs daarom zo moeilijk schijnt omdat er geen *notatie* bedacht kan worden om een priemgetal weer te geven. Maar naar mijn mening moeten waarheden van dit soort eerder uit *noties* (begrippen) dan uit *notaties* voortvloeien.

[5] Zie hiervoor Hardy & Wright, blz. 72.

LITERATUUR

ALLENBY, R.B.J.T. and REDFERN, E.J., Introduction to Number Theory with Computing, Edward Arnold, 1989.

BELLMAN, R., Analytic Number Theory, An Introduction, Reading Mass., 1980.

BURTON, D.M., Elementary Number Theory, Allyn and Bacon, Inc., 1980.

DICKSON, L.E., History of the Theory of Numbers, Carnegie Institution, 1934.

Dictionary of Scientific Biography, Charles Scribner's Sons, 1981.

GAUSS, C.F., Disquisitiones Arithmeticae, Lipsiae, 1801.

GAUSS, C.F., Disquisitiones Arithmeticae, translated by Arthur Clarke, revised by W.C. Waterhouse, C. Greither and A.W. Grootendorst, Springer-Verlag 1986.

HARDY, G.H. and WRIGHT, E.M., An Introduction to the Theory of Numbers, Clarendon Press, 1983.

HUA LOO KENG, Introduction to Number Theory, Springer-Verlag, 1982.

KLINE, M., Mathematical Thought from Ancient to Modern Times, Oxford University Press, 1972.

KOBLITZ, N., A Course in Number Theory and Cryptography, Springer-Verlag, 1987.

NIVEN, I. and ZUCKERMAN, H.S., An Introduction to the Theory of Numbers, Wiley & Sons, 1972.

RIBENBOIM, P., 13 Lectures on Fermat's Last Theorem, Springer-Verlag, 1979.
SCHARLAU, W. and OPOLKA, H., Von Fermat bis Minkowski, Springer-Verlag, 1980.
SCHROEDER, M.R., Number Theory in Science and Communication, Springer-Verlag, 1984.
SERRE, J.P., A Course in Arithmetic, Springer-Verlag, 1973.
STARK, H.M., An Introduction to Number Theory, M.I.T. Press, 1979.
WEIL, A., Number Theory, Birkhäuser, 1987 2nd. ed.

Systematic Computations on Gauss' Lattice Point Problem (In Commemoration of Johannes Gualtherus van der Corput, 1890-1975)

J. van de Lune
Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam

E. Wattel
Free University
Department of Mathematics and Information Theory
De Boelelaan 1081, 1081 HV Amsterdam

0. Introduction

A point $(x,y)\in\mathbb{R}^2$ is called a *lattice point* if both its coordinates x and y are (rational) integers.

For $t \geqslant 0$ we denote by $P(t)$ the number of lattice points in the closed circular disc in $\mathbb{R}^2$ about the origin (0,0) with radius $r = t^{1/2}$, i.e. $P(t)$ is the number of lattice points (x,y) satisfying

$$x^2 + y^2 \leqslant t. \tag{0.0}$$

(In the sequel n will always denote a positive integer.)

Since x and y are integral, so is $x^2 + y^2$, from which it is clear that $P(t)$ is a non-decreasing step-function which is constant on all intervals of the form $n-1 \leqslant t < n$ with upshot-discontinuities only at those $t = n$ which can, in the usual number theoretical sense, be written as the sum of two squares.

In the early 1800's Gauss [7, 8] studied the asymptotic behaviour of $P(t)$ and showed, by a simple geometrical argument, that

$$P(t) = \pi t + \mathcal{O}(t^{1/2}), \quad (t\to\infty) \tag{0.1}$$

which may be rephrased by saying that $P(t)$ equals the area of the disc save for an error of (at most) the order of its circumference.

It seems that, for quite a long time after Gauss, the study of the 'true size' of the error term in (0.1) has not attracted much attention. Not until 1906 did Sierpinski [34] sharpen (0.1) to

$$P(t) = \pi t + \mathcal{O}(t^{1/3}) \tag{0.2}$$

by applying an analytical method devised by Voronoï [37] for the analogous Dirichlet divisor problem.

In 1912 Landau [23, 24] also obtained (0.2) after having 'rigorized' a more or

less heuristic geometrical method of PFEIFFER [33] dating back to 1886. Since the proofs of (0.2) are still rather demanding, we mention here that VINOGRADOV [36; p. 169] has shown, in a rather elementary (though sophisticated) way, the slightly weaker result

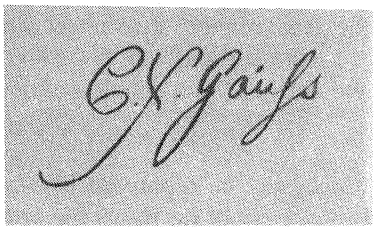
$$P(t) = \pi t + \mathcal{O}(t^{1/3}\log(t)). \tag{0.3}$$

(By the way, is there any 'really simple' proof of (0.1) with just $\mathcal{O}$ replaced by o ?)

For many years (0.2) was the best result on the asymptotic behaviour of $P(t)$ and it seems that around the 1920's there was a more or less general concensus that (0.2) is the best possible result for Gauss' lattice point problem. Compare LANDAU [27; pp. 183-184]. Also see VAN DER CORPUT & LANDAU [3] and LANDAU [28].

Therefore, it must have come as a great surprise to the number theoretical world that, in 1923, VAN DER CORPUT [2] proved that

$$P(t) = \pi t + \mathcal{O}(t^{33/100}). \tag{0.4}$$



Carl Friedrich Gauss
(1777 - 1855)

(Compare the result of JARNIK [18] that for more general curves the exponent in the equivalent of (0.4) is $\geqslant 1/3$.)

Let from now on

$$E(t) := P(t) - \pi t, \quad (t \geqslant 0) \tag{0.5}$$

be the error function in Gauss' lattice point problem, and let α denote any real number for which

$$E(t) = \mathcal{O}(t^{\alpha}), \quad (t \to \infty) \tag{0.6}$$

is true. Denoting the infimum of all these α's by θ, we have the following time table for the successive results on the order of $E(t)$, i.e. the value of θ. (We must admit that, when consulting various historical accounts, we became mildly confused by the discrepancies between some cross-references.)

$\theta \leqslant 1/2 = 0.5$	$\pm$1830, Gauss [7, 8]
$\theta \leqslant 1/3 = 0.333333...$	1906, Sierpinski [34]
$\theta \leqslant 33/100 = 0.33$	1923, van der Corput [2]
$\theta \leqslant 37/112 = 0.330357...$	1924, Landau [26]
	1924, Littlewood & Walfisz [29]
$\theta \leqslant 163/494 = 0.329959...$	1927, Walfisz [38, 39]
$\theta \leqslant 27/82 = 0.329268...$	1928, Nieland [31]
$\theta \leqslant 15/46 = 0.326086...$	1934, Titchmarsh [35]
$\theta \leqslant 13/40 = 0.325$	1942, Hua Loo Keng [12]
$\theta \leqslant 12/37 = 0.324324...$	1962, Yin Wen Lin [41]
$\theta \leqslant 12/37 = 0.324324...$	1963, Chen Jing Run [1]
$\theta \leqslant 35/108 = 0.324074...$	1984, Nowak [32]
$\theta \leqslant 139/429 = 0.324009...$	1985, Kolesnik [21]
$\theta \leqslant 7/22 = 0.318181...$	1988, Iwaniec & Mozzochi [17]

In the opposite direction we have that

$$\theta \geqslant 1/4. \tag{0.7}$$

This was shown in 1915 by LANDAU [25], and, independently, by HARDY [9]. It occurs to us that it is worth mentioning here that, in 1956, ERDÖS & FUCHS [4] proved (0.7) in a different manner by means of a 'very general' theorem.

In 1916 HARDY [10] showed that (0.6) is false for $\alpha = 1/4$. In fact he showed that there exists a positive constant K such that

$$\frac{E(t)}{t^{1/4}} < -K\,(\log(t))^{1/4} \tag{0.8}$$

for infinitely many arbitrarily large values of t. Hence, the left-hand side of (0.8) does not have a finite lower bound as $t \to \infty$. Also see LANDAU [27; pp. 240-249].

In the opposite direction there is a (somewhat less specific) result of INGHAM [15] saying that the left-hand side of (0.8) does not have a finite upper bound as $t \to \infty$.

For further refinements of these results see FRICKER [6] and KRÄTZEL [22]. In view of the best (theoretical) results available at present, we are tempted to

believe that, for large t, the 'extremal negative deviations of $E(t)$ are somewhat larger than those in the positive direction'. Our numerical results (see Sections 4 and 6) corroborate this belief. At present it is not known whether (0.6) is false for any $\alpha > 1/4$. Besides some (minor, though difficult) refinements, we thus only know that

$$1/4 \leqslant \theta \leqslant 7/22 \tag{0.9}$$

so that we are left with some uncertainty as to the true value of θ (note that $7/22 - 1/4 = 3/44 = 0.068181818...$).

For more detailed historical accounts of the subject we refer to FRICKER [6], HUA [13; par. 45], IVIC [16], KRÄTZEL [22] and WILTON [40]. Also see H.J.A. DUPARC & J. KOREVAAR, (*in Memoriam) Johannes Gualtherus van der Corput*, Nieuw Archief voor Wiskunde (3) XXX (1982) pp. 1-39.

The *opinions* on the true value of θ vary. In LANDAU [27; p. 189] we read *ob* $\theta > 1/4$ *ist, weiss ich nicht. Ich vermute - nichts.* FRICKER [6; p. 87] states that some believe that θ is quite close to $1/3$, that others believe that $\theta = 1/4$, and that there are authors which are explicitly prudent to express any conjecture with respect to θ. HUA [14; p. 134] just mentions that $\theta = 1/4$ is a famous conjecture in number theory. HARDY seems to have been the first to state the conjecture that $\theta = 1/4$.

In 1965 KATAI [19] showed that for some $\lambda > 0$ (compare WILTON [39; par. 5])

$$\int_0^t (E(u))^2 \, du = \lambda \, t^{3/2} + \mathcal{O}(t \log^2(t)) \tag{0.10}$$

from which one may derive that

$$\frac{1}{t} \int_0^t |E(u)| \, du = \mathcal{O}(t^{1/4}) \tag{0.11}$$

which might be seen as an indication that $\theta = 1/4$.

Since there seems to be a lack of further 'convincing' heuristical arguments supporting any of the opinions, the question about the true value of θ remains unsettled. To this we might add that HEJHAL [11; p. 451, Remark 4.3] states that it is conceivable that the circle problem could be more difficult than the Riemann Hypothesis.

1. NUMERICAL COMPUTATIONS IN THE 1960'S

In order to get an impression of the true value of θ one has computed $P(t)$ and hence $E(t)$ for several quite large values of t. The first recorded computations related to this subject may be found in GAUSS [7, 8], from which we infer that, for example, $P(100{,}000) = 314{,}197$.

To the best of our knowledge there have been only three more attempts of this kind (all in the 1960's, on IBM computers): FRASER & GOTLIEB [5], MITCHELL [30], and KELLER & SWENSON [20].

Fraser & Gotlieb evaluated $P(t)$ for $t = n^2$ where n runs as follows

$$n = 1\ (1)\ 50\ (5)\ 200\ (100)\ 1000\ (200)\ 1800 \tag{1.1}$$

and for some (unspecified) values of t in the range $1800^2 < t \leqslant 2000^2$. Their conclusion is that the conjecture that θ is 'arbitrarily close to 1/4 is not inconsistent with the observed results'.

Although we haven't had Mitchell's results in front of us, we mention here that Keller & Swenson found that his results are incorrect for all considered $t \geqslant 9{,}000{,}000$ (i.e. radii $\geqslant 3{,}000$).

Assuming that Mitchell's results for $t < 9{,}000{,}000$ are correct, it occurs to us that his results are just a minor extension of those of Fraser & Gotlieb. We do not know Mitchell's conclusion as to the true value of θ.

Keller & Swenson evaluated $P(t)$ for $t = n^2$ where n runs as follows

First n	Step	Last n
1	1	10,000
10,000	250	100,000
100,000	1	100,099
100,000	10,000	150,000
150,000	1	150,099
150,000	250	259,750
200,000	1	200,099
250,000	1	250,099

and for all $t = x^2$ where x runs as follows

First x	Step	Last x
100,000	1/64	100,002
150,000	1/64	150,002
200,000	1/64	200,002
250,000	1/64	250,002

The conclusions of Keller & Swenson may be summarized as follows (almost entirely in their own words): The results clearly suggest that (0.6) is valid for $\alpha = 0.35$ or even perhaps for $\alpha = 0.34$. But since (0.6) is known to be valid for all $\alpha \geqslant 0.325$ no useful quantitative estimates are obtained. However, an extrapolation of the data does suggest that a smaller order should suffice and that computations for larger values of t could indicate this. For example, to obtain a significant improvement, say $\alpha \leqslant 0.30$, a crude extrapolation implies a radius of about 10^8. Unfortunately, calculations by our method for such radii would require at least two hours per case on an IBM 7090. Thus Keller & Swenson.

From the t-listings above we infer that $P(t)$ (and hence $E(t)$) has almost exclusively been evaluated for square integral values of t. In Section 6 we will see that, sadly enough, these t's do not seem to be the most relevant ones for

the purpose they were meant to serve.

2. Preliminary systematic experiments on the order of $E(t)$

In this section we describe some *preliminary systematic* computations concerning the order of $E(t)$.

We begin by confessing that, prior to our numerical approach to Gauss' lattice point problem, we did not have any specific opinion about the true value of θ.

We recall that n denotes a positive integer and that

$$E(t) := P(t) - \pi t, \quad (t \geqslant 0). \tag{2.1}$$

It is clear that $E(t)$ is a sawtooth function with the following properties.

(E1) $E(t)$ is linear on all intervals of the form $n-1 \leqslant t < n$ with slope $-\pi$
(E2) $E(t)$ is continuous from the right for $t \geqslant 0$
(E3) all discontinuities of $E(t)$ are 'upshot-discontinuities' at points $t = n$, where n is representable, in the usual number theoretical sense, as the sum of two squares
(E4) all local maxima of $E(t)$ are assumed at $t = 0$ and certain points of the form $t = n$
(E5) $E(n-0) := \lim_{t \uparrow n} E(t) = E(n-1) - \pi$
(E6) (by convenient abuse of language) all local infima of $E(t)$ are 'assumed' at certain points of the form $t = n-0$.

(Note that $E(t)$ is completely determined by its values at the points $t = n-1$.)

From Section 1 we know that $E(t)$ is unbounded (in the positive as well as in the negative direction). Our aim is to find a 'non trivial, though simple' real function $B(t)$ such that, for $t \geqslant 1$, say,

(B1) $|E(t)| \leqslant B(t)$
(B2) $B(t)$ is smooth, positive, and monotonically increasing.

It is clear that in order to study the 'size' of $E(t)$ we will be interested only in those t-values for which $E(t)$ is **extremal,** i.e. t-values (which, by (E4) and (E6) above, are non-negative integers) for which

(M) E has a local maximum at t and $E(u) < E(t)$ for all $u < t$

or

(I) E has a local infimum at $t-0$ and $E(u) > E(t-0)$ for all $u < t$.

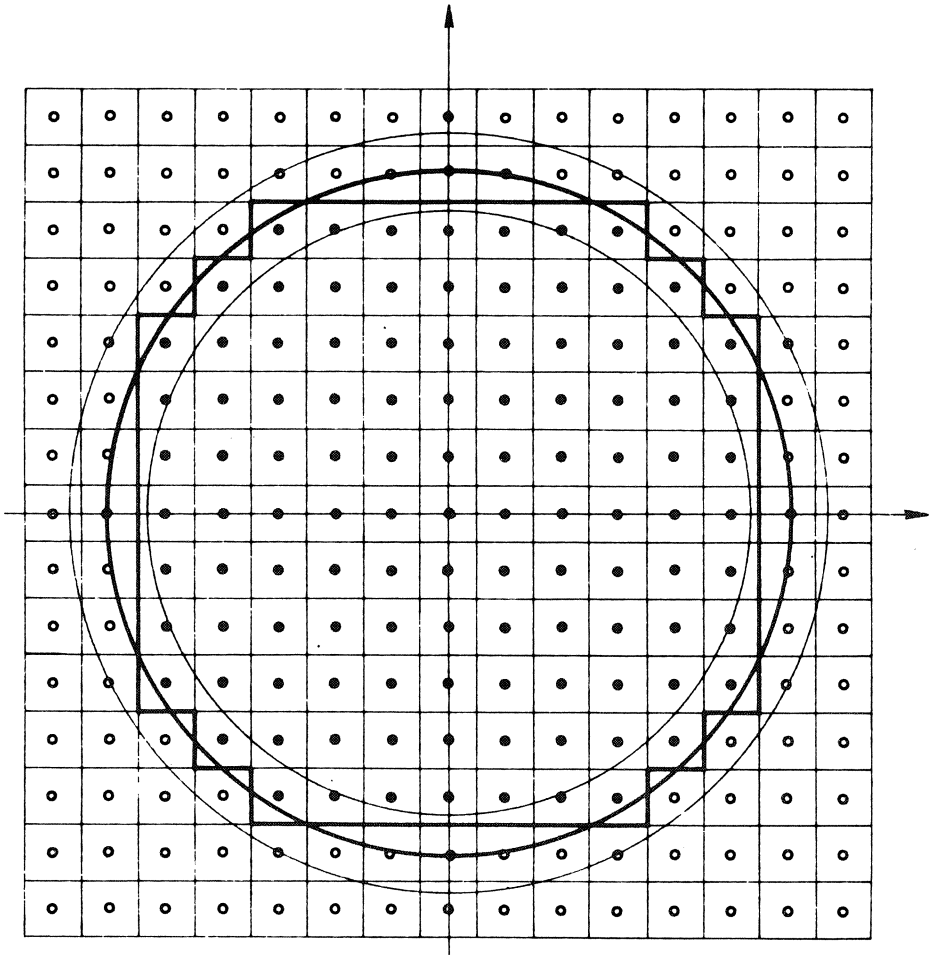
Instead, extremal values might as well be called *champion-extremes.*

Since $E(0) = 1$ and $E(1-0) = 1-\pi$, all local maxima (infima) of $E(t)$ which

are extremal are positive (negative).
In order to get a first impression as to which $B(t)$ to choose we computed $E(n)$ (and $E(n-0) = E(n-1)-\pi$) for all $n \leqslant 100{,}000$. This was carried out by means of the following intentionally unsophisticated FORTRAN 2 program GAUSSEXP on an IBM PS / 2 70 386. (As a not irrelevant byproduct, such a robust program yields valuable testvalues for more sophisticated programs.)

Program GAUSSEXP

```
      PROGRAM GAUSSEXP
C   LANGUAGE: IBM FORTRAN / 2
C   COMPUTER: IBM PS / 2 70 386 ( + i 387 math coprocessor )
C   SUBJECT: EXPERIMENT on GAUSS' LATTICE POINT PROBLEM.
C   IMPRESSION of ALL EXTREMALS of E( t ) := P( t ) - pi * t, for t >= 0.
C   TABULATION of t = N , P( N ) , E( N ) , H( N ) := E( N ) / N ** (1 / 4).
      IMPLICIT DOUBLE PRECISION ( D )
      OPEN ( UNIT = 1 , FILE = 'CON' )
      OPEN ( UNIT = 6 , FILE = 'PRN' )
      WRITE ( 6 , 10 )
 10   FORMAT ( / , '              PROGRAM GAUSSEXP ' , / ,
     $         '              ***************** ' , / )
      ROOTHALF = DSQRT( .5D0 )
      DPI = 4.D0 * DATAN( 1.D0 )
      EMAX = - 1.
      EINF = + 1.
      WRITE( 1 , 20 )
 20   FORMAT( ' INPUT LASTN in I7 Format ' )
      READ( 1 , 30 ) LASTN
 30   FORMAT( I7 )
C
C                        .....  MAIN LOOP  .....
C
      DO 70 N = 0 , LASTN
      RN = FLOAT( N )
C  Note that  P( N ) = P( RN ) = P( RN + .5 )              SAFETY FIRST !
      RNPLUSH = RN + .5
      CALL GAUSS( ROOTHALF , RNPLUSH , NROFPTS )
      E = NROFPTS - DPI * RN
      IF( E .LE. EMAX ) GOTO 50
      EMAX = E
      HATMAX = EMAX / SQRT( SQRT( RN ) )
      WRITE( 6 , 40 ) N , NROFPTS , EMAX , HATMAX
 40   FORMAT( ' N = ' , I7 , '          P = ' , I7 ,
     $ '     E = ' , F8.3 , '     H = ' , F6.3 )
 50   E = E - DPI
      IF( E .GE. EINF ) GOTO 70
      EINF = E
      HATINF = EINF / SQRT( SQRT( RN + 1.) )
      WRITE( 6 , 60 ) N + 1 , NROFPTS , EINF , HATINF
 60   FORMAT( ' N = ' , I7 , '(-0)     P = ' , I7 ,
     $ '     E = ' , F8.3 , '     H = ' , F6.3 )
 70   CONTINUE
      END
C
C
      SUBROUTINE GAUSS( ROOTHALF , RNPLUSH , NROFPTS )
      R = SQRT( RNPLUSH )
      K = R * ROOTHALF
      L = R
      NROFPTS = 1 + 4 * ( L + K ** 2 )
      KPLUS1 = K + 1
      IF( KPLUS1 .GT. L ) GOTO 90
      NPTS = 0
      DO 80 I = KPLUS1 , L
      NPTS = NPTS + SQRT( RNPLUSH - I ** 2 )
 80   CONTINUE
      NROFPTS = NROFPTS + 8 * NPTS
 90   RETURN
      END
```



More or less out of curiosity, and to have a 'point of orientation', we also computed $H(t) := E(t)/t^{\frac{1}{4}}$ for all $t = n \leqslant 100{,}000$ for which $E(t)$ is extremal. The reader may find it interesting to know that, for $t > 0$, the local maxima and infima of $H(t)$ which are most relevant for our purpose coincide with the extremal values of $E(t)$. This may be shown by observing that $t^{1/4}$ is strictly increasing, and that, for $n-1 < t < n$, the function $H(t)$ is differentiable, the sign of $H'(t)$ being the same as that of

$$-\pi\, t^{1/4} - \frac{1}{4} t^{-3/4} E(t) \tag{2.2}$$

which is trivially negative (for all $t > 0$), so that our claim follows. From the definition of $E(t)$ it is clear that the long and the short of the evaluation of $E(t)$ is the computation of $P(t)$. There are various techniques for computing $P(t)$ (also see Sections 5 and 7) of which we have chosen here (mainly for reasons of running speed when programmed in FORTRAN 2 and implemented on an IBM PS / 2 70 386) the following method due to Gauss (also see KELLER & SWENSON [20])

$$P(n) = 1+4(L+K^2)+8S \tag{2.3}$$

where, writing $r = n^{1/2}$,

$$L = [r] \tag{2.4}$$

$$K = [r/\sqrt{2}] \tag{2.5}$$

and

$$S = \sum_{i=K+1}^{L} [(n-i^2)^{1/2}] \tag{2.6}$$

the last sum being defined as 0 if $K+1 > L$ (which is the case only if $n < 5$).

TABEL 1

Main results of program GAUSSEXP (for $n \leqslant 100{,}000$)

n	$E(n)$	$H(n)$
0	1.000	****
1(− 0)	−2.142	−2.142
1	1.858	1.858
2	2.717	2.285
4(− 0)	−3.566	−2.522
5	5.292	3.593
8(− 0)	−4.133	−2.457
10	5.584	3.140
16(− 0)	−5.265	−2.633
20	6.168	2.917

24(− 0)	−6.398	−2.891
25(− 0)	−9.540	−4.266
26	7.319	3.241
41	8.195	3.238
53	10.496	3.890
80(− 0)	−10.327	−3.453
97(− 0)	−11.734	−3.739
130	12.593	3.729
143(− 0)	−12.248	−3.542
144(− 0)	−15.389	−4.443
149	12.903	3.693
205	12.974	3.429
234	13.867	3.546
287(− 0)	−16.637	−4.042
288(− 0)	−19.779	−4.801
340	16.858	3.926
410	16.947	3.766
425	17.823	3.925
481(− 0)	−22.106	−4.720
586	20.027	4.070
625(− 0)	−22.495	−4.499
841(− 0)	−25.079	−4.657
850	22.646	4.194
986	27.390	4.888
1152(− 0)	−26.115	−4.483
1444(− 0)	−27.460	−4.455
1508(− 0)	−28.522	−4.577
1680(− 0)	−28.876	−4.510
1681(− 0)	−32.017	−5.000
1700	28.292	4.406
1844(− 0)	−32.097	−4.898
2260	29.001	4.206
2592(− 0)	−34.008	−4.766
3024(− 0)	−35.176	−4.744
3025(− 0)	−38.318	−5.167
3146	33.550	4.480
3400	35.585	4.660
3960(− 0)	−39.707	−5.005
3961(− 0)	−42.849	−5.401
5183(− 0)	−45.875	−5.407
5184(− 0)	−49.016	−5.777
5525	43.701	5.069
7921(− 0)	−51.555	−5.465
9701	48.410	4.878
9797(− 0)	−53.183	−5.346
11234(− 0)	−55.652	−5.406

14884(− 0)	−58.465	−5.293
15120(− 0)	−59.881	−5.400
15121(− 0)	−63.023	−5.683
17225	59.067	5.156
19594(− 0)	−63.366	−5.356
21601(− 0)	−64.543	−5.324
21604(− 0)	−65.968	−5.441
21605(− 0)	−69.109	−5.700
22178(− 0)	−69.242	−5.674
28560(− 0)	−70.886	−5.453
28561(− 0)	−74.028	−5.694
31680(− 0)	−76.655	−5.746
31681(− 0)	−79.797	−5.981
32850	67.681	5.027
38016(− 0)	−81.786	−5.857
38017(− 0)	−84.928	−6.082
38018(− 0)	−88.070	−6.307
40321(− 0)	−91.157	−6.433
45994	70.587	4.820
46330	71.012	4.840
52417(− 0)	−91.862	−6.071
52418(− 0)	−95.004	−6.279
58081(− 0)	−97.843	−6.303
61685	71.857	4.560
64181	74.442	4.677
69290	76.045	4.687
80642(− 0)	−99.315	−5.894
83753	79.190	4.655
85264(− 0)	−99.756	−5.838
95459(− 0)	−100.293	−5.706
95460(− 0)	−103.435	−5.885
95461(− 0)	−106.576	−6.063
95464(− 0)	−108.001	−6.144

From this table we get the impression that the relevant values of $|H(t)|$ behave more or less proportional to $\log(t)$. This suggests that we should try, for example,

$$B(t) := 1+t^{1/4}\log(t), \quad (t \geqslant 1). \tag{2.7}$$

We define

$$Q(t) := \frac{E(t)}{B(t)} = \frac{P(t)-\pi\, t}{1+t^{1/4}\log(t)}, \quad (t \geqslant 1) \tag{2.8}$$

and hope that we will obtain a clear indication for boundedness of $Q(t)$.

3. SYSTEMATIC COMPUTATION OF THE EXTREMAL VALUES OF $E(t)$

First observe that the local maxima and infima of $Q(t)$ coincide with those of $E(t)$. This may be shown by considering the derivative of $Q(t)$ for $n < t < n+1$, the sign of which is the same as that of

$$-\pi\,(1+t^{1/4}\log(t))-(\frac{1}{4}t^{-3/4}\log(t)+t^{-3/4})(P(t)-\pi\,t). \tag{3.1}$$

Since (3.1) is negative if and only if

$$P(t) > \pi\,t\,\frac{4-3\log(t)-4t^{-1/4}}{4+\log(t)} \tag{3.2}$$

our claim follows since it is a matter of routine to show that

$$4-3\log(t)-4t^{-1/4} < 0, \quad (t>1) \tag{3.3}$$

whereas $P(t) > 0$.

Hence, since $B(t)$ is monotonically increasing, we need only determine those t's for which $E(t)$ is extremal. From Table 1 we infer that it is to be expected that these values of $E(t)$ occur only very rarely, so that we should try and find a procedure for finding the extremal values of $E(t)$ which avoids 'as many evaluations of $E(t)$ as possible' (note the large 'gaps' in Table 1).

We now give an outline of how this can be achieved. For further details we refer to the full program listing in Section 5.

Suppose that we already know all extremal values of $E(t)$ for $t < n$ and that we have just evaluated $E(n)$. Since $E(t)$ is a rather trivial function for small t, we might, for example, take $n = 1$. Let *Einf* and *Emax* be the most extreme values of $E(t)$ for $t < n+1$. Also assume that the next extremal infimum of $E(t)$ is assumed at $t = n+m(-0)$. (For the moment we do not worry about possible new positive extremal values of $E(t)$.)

Then m is a positive integer satisfying

$$E(n+m-0) < Einf. \tag{3.4}$$

Since $E(n+1-0) = E(n)-\pi$, we avoid trivialities by assuming $m > 1$.

Since $P(t)$ is non-decreasing we have

$$P(n+v) \geqslant P(v), \quad (v \geqslant 0) \tag{3.5}$$

whereas

$$P(n+m-0) = P(n+m-1). \tag{3.6}$$

Hence, m must satisfy

$$\begin{aligned} Einf > E(n+m-0) &= P(n+m-0)-\pi\,(n+m) = \\ &= P(n+m-1)-\pi\,(n+m) \geqslant P(n)-\pi\,(n+m) \end{aligned} \tag{3.7}$$

or, equivalently,

$$m > \frac{P(n)-\pi\,n-Einf}{\pi} = \frac{E(n)-Einf}{\pi}. \tag{3.8}$$

We set

$$Exces := E(n) - Einf \tag{3.9}$$

and, in order to avoid trivialities, we assume that $Exces > 0$.
Then, m being an integer, condition (3.8) may also be written as

$$m \geqslant [\frac{Exces}{\pi}] + 1. \tag{3.10}$$

This may also be seen immediately from the graph of $E(t)$ by observing that, when jumping from $t = n$ to $t = n + m$, $E(t)$ cannot decrease more than $m\,\pi$. More formally this reads

$$E(n+v) \geqslant E(n) - \pi\, v, \quad (v > 0). \tag{3.11}$$

Hence, if the next evaluation of $E(t)$ actually takes place at $t = n + j$ with

$$j := [\frac{Exces}{\pi}] + 1 \tag{3.12}$$

then we have not rushed past the next low extremal value of $E(t)$. In other words, we can afford a jump of size j. This (rather trivial) fact is, in essence, the central point of our story!

Immediately after the evaluation of $E(t)$ at $t = n + j$ we check whether we have to adjust *Einf* and record the result accordingly. Note that, even if $E(n+j) > Emax$, we do not know (yet) whether $E(n+j)$ is the first new positive extremal value of $E(t)$.
In practice, (3.12) turns out to be very efficient. Experiments show that a 'random evaluation' of $E(n)$ usually yields a value quite close to 0 so that, based upon (3.12), we can make a reasonably accurate prediction as to the (average) size of the jump j.

For $n = 10^9$, for example, we find $Einf < -1{,}630$ so that from here on j is, on average, (at least) about 518. For $n = 10^{10}$ we found that $Einf < -2{,}597$ so that from here on j is, on average, (at least) about 826, a figure which is comparable to a total speed-up factor corresponding to three noteworthy hardware innovations (measured by present day standards). Clearly, the more the computations proceed, the larger the jump j will be (on average).

At first sight it may seem disappointing that the procedure sketched above has the drawback (the more so when j is large) of not yielding any new information about *Emax*. However, things are not as bad as they seem to be. For convenience let us write $k = n + j$ and assume that there is an extremal maximum of $E(t)$ at $k - i$ (strictly) between n and k. Then we must have

$$E(k-i) > Emax. \tag{3.13}$$

Since, by (3.11),

$$E(k) = E((k-i)+i) \geqslant E(k-i) - \pi\, i \tag{3.14}$$

it follows from (3.13) that

$$E(k)+\pi\, i > Emax \tag{3.15}$$

or, equivalently,

$$i > \frac{Emax-E(k)}{\pi}. \tag{3.16}$$

Writing

$$Defect := Emax-E(k) \tag{3.17}$$

it follows that i, being an integer, must satisfy

$$i \geqslant [\frac{Defect}{\pi}]+1. \tag{3.18}$$

It should be clear that we apply this analysis only if $Defect > 0$ (the case $Defect \leqslant 0$ being a rather trivial situation).
Hence, if possible at all, when making a backstep i of the size of the right-hand side of (3.18), we are sure (this time argueing from the right to the left) that we do not rush past the sought most extremal maximum of $E(t)$ between n and k.
If necessary, we save the relevant data concerning $E(k-i)$, and repeat this backstep-procedure a number of times in order to find all extremal maxima of $E(t)$ for $n < t \leqslant k$. For more details we refer to subroutine CHECKMAX in the full listing of program GAUSSXTR in Section 5. In practice it turns out that, usually, we need only perform one such backstep (before passing the 'barrier' $t = n$). Similarly as before, dropping $E(k)$ from (3.16) one can make a fairly accurate prediction as to the average size of one backstep.

4. Numerical tables for (some of) the most relevant extremal values of $E(t)$

In this section we present tables of (some of) the most significant t-values for which $E(t)$ is extremal, together with the corresponding values of $Q(t)$.

Tabel 2

Listing of *almost all* extremal values of $E(t)$ for $t \leqslant 25{,}000{,}000$.

t	$E(t)$	$Q(t)$
0	1.000	****
1(− 0)	−2.142	−2.142
1	1.858	1.858
2	2.717	1.489
4(− 0)	−3.566	−1.205
5	5.292	1.553
8(− 0)	−4.133	−0.919
10	5.584	1.096
16(− 0)	−5.265	−0.804
20	6.168	0.841

25(− 0)	−9.540	−1.164
26	7.319	0.876
41	8.195	0.788
53	10.496	0.896
80(− 0)	−10.327	−0.732
97(− 0)	−11.734	−0.764
130	12.593	0.722
144(− 0)	−15.389	−0.845
149	12.903	0.698
205	12.974	0.614
234	13.867	0.621
288(− 0)	−19.779	−0.813
340	16.859	0.648
410	16.947	0.604
425	17.823	0.626
481(− 0)	−22.106	−0.739
586	20.027	0.619
625(− 0)	−22.495	−0.678
841(− 0)	−25.079	−0.673
850	22.646	0.605
986	27.390	0.691
1,152(− 0)	−26.115	−0.621
1,444(− 0)	−27.460	−0.599
1,508(− 0)	−28.522	−0.612
1,681(− 0)	−32.017	−0.659
1,700	28.292	0.580
1,844(− 0)	−32.097	−0.638
2,260	29.001	0.535
2,592(− 0)	−34.008	−0.596
3.025(− 0)	−38.318	−0.634
3,146	33.550	0.547
3,400	35.585	0.564
3,961(− 0)	−42.849	−0.642
5,184(− 0)	−49.016	−0.666
5,525	43.701	0.580
7,921(− 0)	−51.555	−0.602
9,701	48.410	0.526
9,797(− 0)	−53.183	−0.575
11,234(− 0)	−55.652	−0.574
14,884(− 0)	−58.465	−0.546
15,121(− 0)	−63.023	−0.585
17,225	59.067	0.524
19,594(− 0)	−63.366	−0.537
21,605(− 0)	−69.109	−0.566
22,178(− 0)	−69.242	−0.562
28,561(− 0)	−74.028	−0.551

31,681(− 0)	−79.797	−0.573
32,850	67.681	0.480
38,018(− 0)	−88.070	−0.594
40,321(− 0)	−91.157	−0.603
45,994	70.587	0.446
46,330	71.012	0.448
52,418(− 0)	−95.004	−0.574
58,081(− 0)	−97.843	−0.571
61,685	71.857	0.411
64,181	74.442	0.420
69,290	76.045	0.418
80,642(− 0)	−99.315	−0.519
83,753	79.190	0.409
85,264(− 0)	−99.756	−0.512
95,464(− 0)	−108.001	−0.533
100,053	79.230	0.385
100,058	79.522	0.386
103,241	83.833	0.403
106,250(− 0)	−117.219	−0.558
114,244(− 0)	−123.111	−0.572
121,252	84.608	0.386
136,490	85.019	0.372
138,581	95.948	0.418
147,652	102.562	0.438
178,345	105.658	0.424
186,624(− 0)	−135.587	−0.535
201,601(− 0)	−151.221	−0.582
233,546	110.602	0.406
316,205	113.695	0.377
330,986	117.814	0.385
361,201(− 0)	−161.408	−0.513
382,330	119.881	0.374
393,121(− 0)	−165.046	−0.510
418,609(− 0)	−165.959	−0.503
449,530	120.854	0.358
457,317	137.272	0.404
459,649(− 0)	−172.922	−0.508
574,544(− 0)	−182.210	−0.498
574,561(− 0)	−203.617	−0.556
574,925	140.844	0.385
574,930	149.136	0.407
776,161(− 0)	−212.696	−0.527
776,529	159.198	0.394
776,533	162.632	0.403
905,130	167.242	0.394
1,067,625	170.143	0.380

1,121,473(− 0)	−218.338	−0.481
1,149,122(− 0)	−256.233	−0.560
1,444,801(− 0)	−263.208	−0.534
1,515,940	171.033	0.342
1,528,250	182.027	0.363
1,764,425	188.382	0.359
1,860,490(− 0)	−280.716	−0.526
2,298,244(− 0)	−297.467	−0.521
2,372,905	208.084	0.361
2,694,250	208.993	0.348
3,104,644(− 0)	−325.782	−0.518
3,520,525	217.523	0.333
3,565,393	224.544	0.342
3,710,538	242.078	0.364
3,823,306	254.958	0.380
4,112,656(− 0)	−336.876	−0.490
4,523,905(− 0)	−341.714	−0.483
4,700,194(− 0)	−341.941	−0.477
5,945,122	257.400	0.334
6,350,400(− 0)	−376.987	−0.479
7,050,325	271.775	0.334
7,441,954(− 0)	−423.015	−0.511
7,602,208	280.196	0.336
7,646,609	318.341	0.381
14,310,920(− 0)	−424.138	−0.418
15,124,082(− 0)	−443.904	−0.430
15,657,472(− 0)	−474.009	−0.454
15,675,545	367.987	0.353
19,368,610(− 0)	−477.886	−0.429
19,368,720(− 0)	−511.461	−0.459
19,547,730	368.038	0.329
24,091,652	372.064	0.312

TABEL 3

A *selection* of extremal values of $E(t)$ for
$25{,}000{,}000 \leqslant t \leqslant 60{,}000{,}000{,}000$.

t	$E(t)$	$Q(t)$
26,666,613(− 0)	−514.497	−0.418
27,320,785(− 0)	−532.446	−0.430
29,953,729(− 0)	−561.974	−0.441
30,727,658	432.365	0.337

34,307,381	480.886	0.362
35,069,800(− 0)	−617.043	−0.461
40,589,641(− 0)	−660.977	−0.472
50,822,641(− 0)	−674.602	−0.450
62,204,769(− 0)	−692.309	−0.434
67,737,269	490.335	0.300
70,543,201(− 0)	−737.022	−0.445
74,192,186	506.509	0.301
85,090,865	516.628	0.294
87,522,761	522.021	0.295
88,328,308	529.483	0.298
91,814,696(− 0)	−765.445	−0.426
98,748,329	532.059	0.290
99,605,300	543.261	0.290
101,351,189	550.205	0.297
104,386,801(− 0)	−814.153	−0.436
113,005,576	585.624	0.306
121,396,324(− 0)	−826.651	−0.423
122,522,401(− 0)	−841.882	−0.429
133,055,770(− 0)	−1,004.550	−0.500
144,198,053	597.033	0.290
153,494,125	597.531	0.285
158,566,570	661.583	0.312
218,300,480(− 0)	−1,035.243	−0.444
233,523,725	662.101	0.278
235,606,625	662.763	0.277
243,062,921	674.026	0.280
253,955,521(− 0)	−1,058.112	−0.433
256,616,225	681.748	0.278
257,133,029	682.098	0.278
260,467,205(− 0)	−1,108.729	−0.450
269,336,500	715.256	0.288
278,933,890	733.339	0.292
302,074,037	757.521	0.294
311,875,200(− 0)	−1,228.157	−0.473
390,664,970	789.233	0.284
446,537,725	792.589	0.274
491,388,368	798.032	0.268
496,731,610	848.218	0.284
541,632,249(− 0)	−1,341.406	−0.437
585,410,810	864.972	0.275
606,981,145(− 0)	−1,385.000	−0.436
650,785,330	893.208	0.275
666,283,418	893.803	0.274
678,784,770	910.199	0.277
702,687,466	932.045	0.281

766,791,440(− 0)	−1,425.740	−0.419
767,469,385	947.229	0.278
815,575,834	972.460	0.280
844,192,753(− 0)	−1,518.039	−0.433
933,851,529(− 0)	−1,630.050	−0.451
968,670,820	997.141	0.273
1,092,520,490	1,043.720	0.276
1,283,376,866	1,046.987	0.264
1,288,411,133	1,054.764	0.265
1,329,859,250	1,074.892	0.268
1,354,041,098	1,186.865	0.294
1,402,274,381(− 0)	−1,660.667	−0.407
1,761,564,481(− 0)	−1,691.334	−0.388
1,879,394,212(− 0)	−1,708.618	−0.384
1,931,450,706	1,188.260	0.265
2,008,153,888	1,215.181	0.268
2,041,411,684(− 0)	−1,848.407	−0.406
2,149,665,572	1,244.330	0.265
2,406,612,881	1,266.016	0.265
2,644,046,005	1,267.939	0.258
2,736,440,713(− 0)	−1,875.945	−0.377
2,772,443,605(− 0)	−2,076.960	−0.416
2,959,608,836	1,320.323	0.260
2,968,668,450	1,335.536	0.262
3,118,999,104(− 0)	−2,114.680	−0.409
3,397,875,892	1,368.883	0.258
3,437,151,605	1,369.458	0.258
3,693,897,829	1,378.302	0.254
3,741,923,026	1,380.220	0.253
3,760,264,705(− 0)	−2,147.781	−0.393
3,844,899,194	1,387.336	0.252
3,849,617,125	1,437.967	0.262
3,900,164,266	1,499.141	0.272
4,082,823,361(− 0)	−2,351.822	−0.420
4,474,983,258	1,508.730	0.263
4,723,459,364	1,515.528	0.260
5,725,069,549	1,549.571	0.249
5,792,465,045	1,737.452	0.280
6,237,998,005(− 0)	−2,372.616	−0.374
6,334,876,800(− 0)	−2,471.276	−0.388
7,595,644,004(− 0)	−2,489.249	−0.370
7,760,245,844	1,795.439	0.266
7,893,075,529(− 0)	−2,563.135	−0.377
8,385,247,125(− 0)	−2,597.435	−0.376
8,790,245,320	1,852.436	0.264
9,318,871,985	1,881.180	0.264

9,787,590,649	1,933.757	0.267
10,190,557,141	1,954.847	0.267
10,672,749,305(− 0)	−2,625.194	−0.354
10,736,689,625(− 0)	−2,884.774	−0.388
12,569,997,245(− 0)	−2,911.536	−0.374
13,401,828,392	2,016.022	0.254
15,191,288,109(− 0)	−2,952.800	−0.359
15,606,496,945(− 0)	−2,981.684	−0.359
15,743,054,441	2,024.090	0.243
15,803,589,556	2,079.522	0.250
16,015,227,425	2,081.050	0.249
17,287,834,888	2,116.386	0.248
17,713,744,117(− 0)	−3,008.537	−0.349
18,461,195,545(− 0)	−3,291.657	−0.378
19,644,066,922	2,124.219	0.239
20,519,211,530	2,176.897	0.242
22,965,971,474	2,211.729	0.238
23,705,632,197	2,282.203	0.243
24,226,688,548	2,449.795	0.260
24,436,957,514	2,478.932	0.262
25,139,994,610(− 0)	−3,329.063	−0.349
27,658,343,752(− 0)	−3,428.744	−0.350
28,061,275,133(− 0)	−3,519.195	−0.357
29,818,037,041(− 0)	−3,607.474	−0.360
29,853,030,425	2,562.427	0.256
31,580,944,265	2,584.647	0.254
31,650,524,809(− 0)	−3,681.216	−0.361
34,788,692,045	2,740.430	0.261
35,756,257,745	2,813.445	0.266
36,922,391,089(− 0)	−3,965.172	−0.372
40,029,315,730	2,831.406	0.259
44,860,907,521(− 0)	−4,068.345	−0.360
47,463,413,689(− 0)	−4,350.656	−0.379
52,360,419,101(− 0)	−4,389.584	−0.372
55,939,956,749	2,836.211	0.236
56,651,262,026	2,863.528	0.237
58,956,361,256	3,136.765	0.257

In view of these tables the conjecture

$$E(t) = \Theta(t^{1/4}\log(t)) \tag{4.1}$$

seems to be very plausible. They also indicate that the Θ-constant in (4.1) is at most 1.

Moreover, the data do not exclude the possibility that even

$$E(t) = o(t^{1/4}\log(t)). \tag{4.2}$$

More extensive, though less systematic, computations in Section 6 support (4.1) (and (4.2)).
Therefore, it is tempting to replace the original conjecture (4.1) by (4.2).

5. Listing of the main program

In this section we present the full listing of a Quick Basic version of the *various programs* that we have actually implemented.

Program GAUSSXTR

```
10   ' Program GAUSSXTR ( in Micro Soft Quick Basic ( QB or QB87 ) )
20   ' Designed for IBM PS / 2 70 386 ( + i 387 math coprocessor )
30   ' FORTRAN versions run CONSIDERABLY FASTER
40   ' EXHAUSTIVE search for ALL EXTREMAL VALUES of E(n) := P(n) - pi * n
50   '                        ********************
60   ' METHOD : " Maximal Slope Principle "
70   ' TABULATION of : n , E , Q = E( n ) / ( 1 + n ^ (1 / 4) * LOG( n ) )
80   ' We also print the maxima of D( n ) if E( n - 0 ) is EXTREMAL
90   LPRINT
100  LPRINT " PROGRAM GAUSSXTR ( GAUSS - ROOT - METHOD ) IN DOUBLE PRECISION "
110  LPRINT " ************************************************************** "
120  LPRINT
130  '
140  '                       ........................
150  '                            INITIALIZATIONS
160  '                       ........................
170  '
180  DIM PRIME1( 200 ) , PRIME3( 200 ) , TEMPMAX#( 200 ) , TEMPN#( 200 )
190  ' TEMPMAX#( . ) and TEMPN#( . ) are used in SUBROUTINE CHECKMAX
200  NPR1% =  100                      ' Number of PRIMES of the form 4k + 1
210  NPR3% =  100                      ' Number of PRIMES of the form 4k + 3
220  ' !      NPR1% and NPR3% may also be REGULATED DYNAMICALLY      !
230  INPUT " INPUT OLDN# >= 1" ; OLDN#           ' From previous output
240  IF OLDN# < 1# THEN GOTO 230 ELSE OLDN# = INT( OLDN# )
250  INPUT " INFIMUM# = " ; INFIMUM#             ' From previous output
260  INPUT " MAXIMUM# = " ; MAXIMUM#             ' From previous output
270  INPUT " PRINTCYCLE " ; PRCY%                ' PRCY% = 10,000 is OK
280  NATINF# = OLDN#
290  NATMAX# = OLDN#
300  INPUT " INPUT previous MAXIMUM of D( n ) "; DMAXIMUM
310  '
320  '                       ......................
330  '                       END of INITIALIZATIONS
340  '                       ......................
```

```
350  '
360  CALL MAKEPR1( NPR1% )
370  CALL MAKEPR3( NPR3% )
380  PI# = 4# * ATN( 1# )
390  EPS# = .5# ^ 16
400  PIEPS# = PI# + EPS#
410  PIEPSINV# = 1# / PIEPS#
420  LPRINT: LPRINT " We START with OLDN = "; OLDN#
430  LPRINT: LPRINT " We TRY to DEFEAT the INFIMUM = "; INFIMUM#
440  LPRINT: LPRINT " We TRY to DEFEAT the MAXIMUM = "; MAXIMUM#
450  LPRINT
460  CALL GAUSS( OLDN# , P# )
470  E# = P# - PI# * OLDN#
480  IF E# - PI# > INFIMUM# AND E# < MAXIMUM# GOTO 540
490  LPRINT
500  LPRINT "                    !  .....  WARNING  .....  !"
510  LPRINT
520  LPRINT " OLDN = "; OLDN#; " E - PI = "; E# - PI#; " E = "; E#
530  LPRINT
540  T0= TIMER
550  FIRSTN# = OLDN#
560  '                          START of the PRINT - LOOP
570  FOR I% = 1 TO PRCY%
580  JUMP# = 1# + INT( ( E# - INFIMUM# ) / PIEPS# )
590  IF JUMP# < 1# THEN JUMP# = 1#
600  NEWN# = OLDN# + JUMP#
610  ' We first determine  NPOINTS#  for NEWN#
620  CALL GAUSS( NEWN# , NPOINTS# )
630  E# = NPOINTS# - PI# * NEWN#
640  EXCES# = E# - INFIMUM#
650  IF EXCES# < 0 GOTO 700          ' ! .....  NEW INFIMUM IN THE MAKE
660  ' We now CHECK for new MAXIMA in [ OLDN# , NEWN# ]
670  CALL CHECKMAX( OLDN# , NEWN# , MAXIMUM# , E# )
680  OLDN# = NEWN#                  ' Note that now E# = E#( OLDN# )
690  GOTO 970
700  ' We ARE GOING TO FIND a NEW INFIMUM  !   ..............
710       INFIMUM# = E#
720       NATINF# = NEWN#
730       NEXTN# = NEWN# + 1#
740       CALL SALTUS( NEXTN# , UPSHOT )
750  ' UPSHOT is either 0 or 1
760       IF UPSHOT > 0 GOTO 830                ' EXTREMAL INFIMUM FOUND
770  ' If UPSHOT < 1 we need NOT EVALUATE at NEWN#
780       NEWN# = NEXTN#
790       NATINF# = NATINF# + 1#
800       INFIMUM# = INFIMUM# - PI#
810       E# = INFIMUM#
820       GOTO 730
830  NAUX# = NATINF# + 1#
840  L# = LOG( NAUX# )
850  QATINF = ( ( INFIMUM# - PI# ) / ( 1# + SQR( SQR( NAUX# ) ) * L# ) )
860  LPRINT " (-) N = "; NAUX#;
870  LPRINT "   E = "; CSNG( INFIMUM# - PI# ); "   Q = "; QATINF;
880  D = ( (1 + INT( SQR(NAUX# - .5#) )) ^ 2 - NAUX# ) / SQR( SQR( NAUX# ) )
890  LPRINT "   D = "; D
900  IF D <= DMAXIMUM THEN GOTO 950 ELSE DMAXIMUM = D
910  LPRINT: LPRINT " N = "; NAUX#, " DMAXIMUM = "; DMAXIMUM
920  ROOT = SQR( NAUX# ): FRACROOT = ROOT - INT( ROOT )
930  LPRINT " Fractional part of SQR("; NAUX#; ") = "; FRACROOT
```

```
940  LPRINT
950  CALL CHECKMAX ( OLDN# , NAUX# , MAXIMUM# , E# )
960  OLDN# = NATINF#
970  NEXT I%
980  '                          END of PRINT - LOOP
990  PROGRESS# = OLDN# - FIRSTN#
1000 REPORT% = REPORT% + 1
1010 LPRINT: LPRINT " ( REPORT "; REPORT%; ", PRCY = "; PRCY%; ")";
1020 LPRINT " CONTINUE with OLDN = "; OLDN#
1030 LPRINT " Extremes : "; CSNG( INFIMUM# - PI# ); " and "; CSNG( MAXIMUM# ),
1040 LPRINT " PROGRESS PER SEC. ="; INT( .5# + PROGRESS# / ( TIMER - T0 ) )
1050 LPRINT
1060 GOTO 540              ' BACK TO PRINT - LOOP
1070 '
1080 '
1090 SUB GAUSS( N# , NPOINTS# ) STATIC
1100 ' THE SQUARES MAY ALSO BE PRECOMPUTED AND STORED IN SQUARE( . ), SAY
1110 ' THE NEXT PRINT SLOWS THE PROCESS DOWN !     ONE MAY JUST DELETE IT
1120 ' PRINT N#,        ' THIS SHOWS THE ZIG - ZAGGING (ON THE SCREEN !)
1130 NPLUSH# = N# + .5#
1140 K# = INT( SQR( NPLUSH# / 2# ) )
1150 L# = INT( SQR( NPLUSH# ) )
1160 NPOINTS# = 1 + 4# * ( L# + K# ^ 2 )
1170 KPLUS1# = K# + 1#
1180 IF KPLUS1# > L# GOTO 1260          ' Only necessary for SMALL N#
1190 P# = 0#
1200 ' We apply NO TRICKS here ! They are, in general, too machine dependent.
1210 ' If FAST memory permits, PRECOMPUTE the SQUARES I#^2 for the next loop
1220 FOR I# = KPLUS1# TO L#
1230 P# = P# + INT( SQR( NPLUSH# - I# ^ 2 ) )
1240 NEXT I#
1250 NPOINTS# = NPOINTS# + 8# * P#
1260 END SUB
1270 '
1280 '
1290 SUB SALTUS( NUMBER# , UPSHOT ) STATIC
1300 SHARED NPR1% , NPR3% , PRIME1( ) , PRIME3( )
1310 INTEGER# = NUMBER#
1320 ' We first REMOVE ALL PRIMES 4K+1 from INTEGER#
1330 CALL CLEAN( INTEGER# , NPR1% )
1340 IF INTEGER# < 2# GOTO 1580
1350 IP1# = INTEGER# + 1#
1360 Q# = INT( IP1# / 4# )
1370 IF Q# * 4# <> IP1# GOTO 1400
1380 UPSHOT = 0                          ' NO UPSHOT; INTEGER = 4k - 1
1390 GOTO 1590
1400 FOR I% = 1 TO NPR3%
1410 POWER% = 0
1420 P# = PRIME3( I% )
1430 Q# = INT( INTEGER# / P# )
1440 IF P# * Q# <> INTEGER# GOTO 1480
1450 POWER% = POWER% + 1
1460 INTEGER# = Q#
1470 GOTO 1430                       ' TRY to find a HIGHER POWER of P#
1480 IF 2 * INT( POWER% / 2 ) = POWER% GOTO 1510
1490 UPSHOT = 0
1500 GOTO 1590
1510 IF INTEGER# < P# GOTO 1580
1520 NEXT I%
```

```
1530 IP1# = INTEGER# + 1#
1540 Q# = INT( IP1# / 4# )
1550 IF Q# * 4# <> IP1# GOTO 1580   ' INTEGER# is NOT of the FORM 4k - 1
1560 UPSHOT = 0
1570 GOTO 1590
1580 UPSHOT = 1                     ' This "GUESS" is SAFE !
1590 END SUB
1600 '
1610 '
1620 SUB MAKEPR3( NPR3% ) STATIC
1630 SHARED PRIME3( )
1640 PRIME3( 1 ) = 3
1650 N = 3
1660 FOR K% = 2 TO NPR3%
1670 N = N + 4
1680 MAXD = INT( SQR( N + .5 ) )
1690 D = 1
1700 D = D + 2
1710 IF D <= MAXD GOTO 1740
1720 PRIME3( K% ) = N
1730 GOTO 1770
1740 Q = INT( N / D )
1750 IF D * Q <> N GOTO 1700
1760 GOTO 1670
1770 NEXT K%
1780 ' LPRINT
1790 ' LPRINT " PRIME3("; NPR3%; ") = "; PRIME3( NPR3% )
1800 END SUB
1810 '
1820 '
1830 SUB MAKEPR1( NPR1% ) STATIC
1840 SHARED PRIME1( )
1850 PRIME1( 1 ) = 2
1860 N = 1
1870 FOR K% = 2 TO NPR1%
1880 N = N + 4
1890 MAXD = INT( SQR( N + .5 ) )
1900 D = 1
1910 D = D + 2
1920 IF D <= MAXD GOTO 1950
1930 PRIME1( K% ) = N
1940 GOTO 1980
1950 Q = INT( N / D )
1960 IF D * Q <> N GOTO 1910
1970 GOTO 1880
1980 NEXT K%
1990 ' LPRINT
2000 ' LPRINT " PRIME1("; NPR1%; ") = "; PRIME1( NPR1% )
2010 END SUB
2020 '
2030 '
2040 SUB CLEAN( I# , NPR1% ) STATIC
2050 ' We REMOVE "ALL" PRIMES of the form 4k + 1 FROM I#
2060 SHARED PRIME1( )
2070 FOR K% = 1 TO NPR1%
2080 PK# = PRIME1( K% )
2090 Q# = INT( I# / PK# )
2100 IF Q# * PK# <> I# GOTO 2130
2110 I# = Q#
2120 GOTO 2090
2130 IF I# < 2# GOTO 2150
2140 NEXT K%
2150 END SUB
2160 '
2170 '
```

```
2180 SUB CHECKMAX( OLDN# , NEWN# , MAXIMUM# , E# ) STATIC
2190 ' E# HAS ALREADY BEEN EVALUATED AT NEWN#.     E# = E#( NEWN# )
2200 SHARED INFIMUM# , PI# , PIEPS# , NPOINTS# , TEMPMAX#( ) , TEMPN#( )
2210 AUXNEWN# = NEWN#
2220 KOUNT = 0
2230 AUXE# = E#                          ' INPUT E# MUST BE SAVED
2240 IF AUXE# < MAXIMUM#  GOTO 2300      ' ( <  for "SAFETY FIRST" )
2250 KOUNT = KOUNT + 1                   ' THE MAXIMUM IS DEFEATED
2260 ' We STORE the DATA corresponding to this (TEMPORARY) MAXIMUM
2270 TEMPN#( KOUNT ) = AUXNEWN#
2280 TEMPMAX#( KOUNT ) = AUXE#
2290 ' We MIGHT CALL SALTUS( , ) HERE.  However, the GAIN will be MINUTE.
2300 I# = 1# + INT( ( MAXIMUM# - AUXE# ) / PIEPS# )
2310 IF I# > 1# GOTO 2330
2320 I# = 1#
2330 AUXNEWN# = AUXNEWN# - I#
2340 IF AUXNEWN# <= OLDN# GOTO 2500
2350 CALL SALTUS( AUXNEWN# , UPSHOT )
2360 IF UPSHOT > 0 GOTO 2430
2370 '       Some SREEN INFORMATION !
2380 '       PRINT
2390 '       PRINT "*....."; AUXNEWN#; ".....*     NO EVALUATION NECESSARY "
2400 AUXNEWN# = AUXNEWN# - 1#
2410 AUXE# = AUXE# + PI#
2420 GOTO 2340
2430 CALL GAUSS( AUXNEWN# , NPOINTS# )
2440 AUXE# = NPOINTS# - PI# * AUXNEWN#
2450 IF AUXE# < MAXIMUM# GOTO 2300     'The INFIMA have already been checked
2460 KOUNT = KOUNT + 1
2470 TEMPN#( KOUNT ) = AUXNEWN#
2480 TEMPMAX#( KOUNT ) = AUXE#
2490 GOTO 2300
2500 IF KOUNT < 1 GOTO 2680
2510 MAXIMUM# = TEMPMAX#( KOUNT )
2520 IK# = TEMPN#( KOUNT )
2530 QATMAX = MAXIMUM# / (1# + SQR( SQR( IK# ) ) * LOG( IK# ) )
2540 LPRINT " (+) N = "; IK#;
2550 LPRINT "   E = "; CSNG( MAXIMUM# ); "   Q = "; QATMAX
2560 ' LPRINT " SQR("; IK#; ") ="; SQR( IK# )
2570 IF KOUNT < 2 GOTO 2680
2580 ' Now we UNSCRAMBLE the MAXIMA
2590 FOR K = KOUNT - 1 TO 1 STEP -1
2600 IF TEMPMAX#( K ) < MAXIMUM# GOTO 2670
2610 MAXIMUM# = TEMPMAX#( K )
2620 IK# = TEMPN#( K )
2630 QATMAX = MAXIMUM# / ( 1# + SQR( SQR( IK# ) ) * LOG( IK# ) )
2640 LPRINT " (+) N = "; IK#;
2650 LPRINT "   E = "; CSNG( MAXIMUM# ); "   Q = "; QATMAX
2660 ' LPRINT " SQR("; IK#; ") = "; SQR( IK# )
2670 NEXT K
2680 END SUB
```

There are various methods for the computation of $P(t)$. Without going into details (which are quite machine dependent) we make a few brief comments on some possible approaches (also see Keller & Swenson [20]).

- We call the method (see subroutine GAUSS) in program GAUSSXTR the 'root-method'. If (fast) memory permits, it may be advantageous to precompute the necessary squares. One may also experiment with building these squares by means of a linear recurrence: $(i+1)^2 = i^2+j$, where $j = 2i+1$.
  The root-method appears to be fast when implemented on computers equipped with a math coprocessor.
- Keller & Swenson [20] used the 'step-method'. In case this method is faster than the root-method one may speed up this method slightly by subdividing the basis of the half-moon-shaped sector of the circle in intervals I_n such that the slope of the circle is $<-n$ in I_n. Inside such an interval one may apply upward steps of size n instead of 1. The endpoints of these intervals are easily computed by elementary calculus. This method seems to be preferable on computers without a math coprocessor (in our case the Sun 4 SPARC Station 1).

Since, for large t, the negative extremal values of $E(t)$ appear to be definitely more pronounced than the positive ones, one might decide to concentrate entirely on the negative ones by deleting the subroutine CHECKMAX (with all fittings) from the main program.

This yields a speedup factor of about 2 at the cost of 'some' completeness of the results.

6. Further observations and experiments

At first sight it seemed to us that the extremal values of $E(t)$ occur rather 'randomly'. However, a closer look revealed that there seems to be a fascinating 'quasi regularity', especially with respect to the negative extremal values. The reader may check for himself that if $E(t)$ is extremal and negative then t 'always lies just below' a perfect square. As a typical simple example we mention $t = 97(-0)$. Since we have not found any exception to the 'rule' just stated, we have ventured to promote this observation to a doctrine and wrote a special program that searches for 'low values' of $E(t)$, only for t's just below perfect squares.

We present a *selection* of the results of this program.

Tabel 4. *Some* low values of $E(t)$ for $t = n^2 - \mathcal{O}(\sqrt{n})$

t	$E(t)$	$Q(t)$
64,407,835,130(− 0)	−4,661.0	−0.372
66,501,577,825(− 0)	−4,766.2	−0.377
85,429,935,378(− 0)	−4,779.2	−0.351

88,815,918,244(− 0)	−4,804.2	−0.349
91,021,079,444(− 0)	−5,026.1	−0.363
101,405,304,001(− 0)	−5,327.6	−0.373
104,720,838,337(− 0)	−5,468.3	−0.379
152,521,478,773(− 0)	−5,746.9	−0.357
179,934,604,660(− 0)	−6,153.4	−0.365
200,220,451,202(− 0)	−6,393.6	−0.367
242,696,137,050(− 0)	−7,357.9	−0.400
485,392,279,681(− 0)	−7,614.0	−0.339
523,604,188,801(− 0)	−7,841.1	−0.342
591,033,446,305(− 0)	−8,312.6	−0.350
638,954,027,714(− 0)	−8,522.9	−0.351
886,358,229,149(− 0)	−8,634.4	−0.323
962,429,671,165(− 0)	−8,799.8	−0.322
985,195,196,576(− 0)	−9,070.1	−0.330
1,097,591,472,016(− 0)	−9,191.3	−0.324
1,141,061,921,864(− 0)	−9,490.0	−0.331
1,325,441,033,284(− 0)	−9,790.5	−0.327
1,465,932,511,466(− 0)	−10,647.0	−0.345
2,051,723,921,626(− 0)	−10,833.7	−0.319
3,256,974,567,522(− 0)	−10,978.9	−0.284
3,435,399,231,265(− 0)	−11,849.1	−0.302
3,453,241,721,716(− 0)	−12,563.8	−0.319
5,076,464,116,145(− 0)	−12,948.3	−0.295
6,271,578,593,284(− 0)	−13,863.0	−0.297
7,027,504,080,416(− 0)	−14,614.2	−0.303
8,930,695,934,245(− 0)	−15,763.3	−0.306
10,155,789,844,210(− 0)	−16,371.0	−0.306
18,105,195,196,546(− 0)	−17,741.1	−0.282
27,739,182,240,000(− 0)	−18,315.5	−0.258
29,218,349,160,000(− 0)	−18,320.5	−0.254
36,001,176,008,449(− 0)	−21,391.5	−0.280
46,500,397,574,400(− 0)	−21,602.7	−0.263
74,798,973,849,553(− 0)	−23,961.7	−0.255
100,081,536,563,088(− 0)	−24,822.5	−0.243
100,118,735,162,177(− 0)	−24,932.4	−0.244
100,209,729,800,645(− 0)	−26,787.5	−0.263
100,620,800,502,202(− 0)	−30,749.0	−0.301
228,719,465,828,473(− 0)	−31,863.5	−0.248
339,804,982,440,000(− 0)	−34,179.7	−0.238
825,183,363,254,825(− 0)	−35,378.8	−0.192
920,095,256,946,308(− 0)	−38,393.3	−0.202
969,150,181,400,018(− 0)	−39,358.9	−0.204
998,610,560,638,085(− 0)	−39,751.5	−0.205
1,015,043,733,773,154(− 0)	−40,505.4	−0.208
1,050,871,873,459,634(− 0)	−40,623.9	−0.206

1,095,502,295,247,104(− 0)	−44,045.4	−0.221
1,374,644,087,373,226(− 0)	−45,487.5	−0.214
1,684,294,158,258,064(− 0)	−51,193.2	−0.228
1,777,808,461,651,993(− 0)	−54,819.6	−0.240
2,025,014,490,021,601(− 0)	−57,142.1	−0.242
2,280,284,160,887,041(− 0)	−59,432.9	−0.243

We suggest that in future systematic computations one might gather some statistics concerning the distances of the true low extremal t-values to the corresponding nearest squares.
For t's for which $E(t)$ is negatively extremal we define

$$d(t) := \frac{([(t-1/2)^{1/2}]+1)^2 - t}{t^{1/4}}. \tag{6.1}$$

Although $d(t)$ is usually quite small (< 2), we nevertheless get the impression that $d(t)$ is unbounded and that significant extremes of $E(t)$ may occur indeed for quite large values of $d(t)$ (>10, for example) so that Table 4 will most probably *not* be complete (nor optimal).

With respect to the positive extremal values of $E(t)$ we did not find such a simple 'rule', although it seems likely that they are usually located close to t's of the form $t=(n+1/4)^2$. Since the negative extremal values seem to be the most significant ones for our purpose, and in order to save computation time we have not pursued this subject any further.

7. Machines, programs, and future computations

The first versions of all our programs (in Micro Soft Quick Basic) were developed on an Olivetti M24 and an IBM AT (equipped with a math coprocessor). Soon afterwards the programs were translated into FORTRAN 2 for implementation on an IBM PS / 2 70 386 (equipped with an i387 math coprocessor), and into the language C for a Sun 3/50, a Sun 4/80 SPARC and a Sun 4 SPARC Station 1. Various checks were carried out, by means of a FORTRAN 5 program, on a CDC CYBER 990 system.

Remark. During the preparation of this lecture, J.T. Tromp (at CWI) notified us that he has already developed a considerably faster procedure for (systematically) finding the extremal values of $E(t)$. See Tromp [42].

Suggestion (by J.T. Tromp). Any reader who wishes to perform a check on our tables (or to find better extremes of $E(t)$) is recommended to compute $P(n)$ by means of a subroutine such as

```
      SUB GAUSS( N , P )  STATIC
REM   TROMP's IMPROVED STEP - METHOD
      ROOT = SQR( N + 0.5 )
      K = INT( ROOT / SQR( 2 ) )
      L = INT( ROOT )
      I = 2 * L - 1
      IK = 2 * K + 1
      SUM = 0
      IF I < IK GOTO 246
      J = - 1
      IJ = L * L - N
245   J = J + 2
      IJ = IJ + J
      IF IJ <= 0 GOTO 245
      SUM = SUM + J
      IJ = IJ - I
      I = I - 2
      IF I >= IK GOTO 245
246   P = IK * IK + 4 * SUM
      END SUB
```

The adjustment of the necessary type-declarations of the various variables is left to the reader.

References

[1] Chen Jing Run, *The lattice points in a circle*, Sci. Sinica 12 (1963) pp. 633-649.

[2] J.G. van der Corput, *Neue zahlentheoretische Abschätzungen*, Math. Ann. 89 (1923) pp. 215-254.

[3] J.G. van der Corput & E. Landau, *Über Gitterpunkte in ebenen Bereichen*, Nachr. Ges. Wiss. Göttingen, Math. Phys. Klasse (1920) pp. 135-171.

[4] P. Erdös & W.H.J. Fuchs, *On a problem of additive number theory*, J. London Math. Soc. 31 (1956) pp. 67-73.

[5] W. Fraser & C.C. Gotlieb, *A calculation of the number of lattice points in the circle and sphere*, Math. Comp. (1962) pp. 282-290.

[6] F. Fricker, *Einführung in die Gitterpunktlehre*, Birkhäuser, 1982.

[7] C.F. Gauss, *De nexu inter multitudinem classium, in quas formae binariae*

secundi gradus distribuuntur, earumque determinantem, Werke (1863), Vol. 2, pp. 269-291 (in particular p. 280).

[8] C.F. GAUSS, *Disquisitiones arithmeticae*, (German edition by H. Maser), 1886, p. 657.

[9] G.H. HARDY, *On the expression of a number as the sum of two squares*, Quart. J. Math., Oxford Ser. 46 (1915) pp. 263-283. Collected Papers, Vol. 2 (1967) pp. 243-283.

[10] G.H. HARDY, *On Dirichlet's divisor problem*, Proc. London Math. Soc. 15 (1916) pp. 1-25.

[11] D.A. HEJHAL, *The Selberg trace formula and the Riemann zeta function*, Duke Math. J. 43 (1976) pp. 441-482.

[12] HUA LOO KENG, *The lattice points in a circle*, Quart. J. Math., Oxford Ser. 13 (1942) pp. 18-29.

[13] HUA LOO KENG, *Die Abschätzung von Exponentialsummen und ihre Anwendung in der Zahlentheorie*, Enzycl. Math. Wiss. Anw., Vol. 1, Part 2, *Analytische Zahlentheorie*, Leipzig, 1959.

[14] HUA LOO KENG, *Introduction to Number Theory*, Springer, 1982.

[15] A.E. INGHAM, *On two classical lattice point problems*, Proc. Cambr. Phil. Soc. 36 (1940) pp. 131-138.

[16] A. IVIC, *The Riemann zeta - function*, Wiley & Sons, New York, 1985, p. 383.

[17] H. IWANIEC & C.J. MOZZOCHI, *On the divisor and circle problems*, J. of Number Th. 29 (1988) pp. 60-93.

[18] V. JARNIK, *Über die Gitterpunkte auf konvexen Kurven*, Math. Z. 24 (1925) pp. 500-518.

[19] I. KATAI, *The number of lattice points in a circle*, (in Russian), Ann. Univ. Sci. Budapest Rolando Eötvös, Sect. Math. 8 (1965) pp. 39-60.

[20] H.B. KELLER & J.R. SWENSON, *Experiments on the lattice problem of Gauss*, Math. Comp. 17 (1963) pp. 223-230.

[21] G. KOLESNIK, *On the method of exponent pairs*, Acta Arithm. 45 (1985) pp. 115-143.

[22] E. KRÄTZEL, *Lattice points*, Kluwer Acad. Publ., Dordrecht, 1988.

[23] E. LANDAU, *Die Bedeutung der Pfeiffer'schen Methode für die analytische Zahlentheorie*, Sitzber. K. Akad. Wiss. Wien, Math. Natw. Klasse 121 (1912) pp. 2298-2328.

[24] E. LANDAU, *Über die Zerlegung der Zahlen in zwei Quadrate*, Annali di Matematica, Ser. 3, Vol. 20 (1913) pp. 1-28.

[25] E. LANDAU, *Über die Gitterpunkte in einem Kreise (II)*, Göttinger Nachr. (1915) pp. 161-171.

[26] E. LANDAU, *Note on the preceding paper*, see [28; pp. 110-111] or [29; pp. 487-488].

[27] E. LANDAU, *Vorlesungen über Zahlentheorie*, Vol. 2, Part 8, 1927.

[28] E. LANDAU, (edited by A. Walfisz), *Ausgewählte Abhandlungen zur Gitterpunktlehre*, Deutscher Verl. Wiss., 1962.

[29] J.E. LITTLEWOOD & A. WALFISZ, *The lattice points of a circle*, Proc. Roy. Soc. London, Ser. A 106 (1924) pp. 478-487. Followed by a note by Landau, pp. 487-488.

[30] H.L. MITCHELL, *Numerical experiments on the number of lattice points in the circle*, Techn. Report No. 17, Appl. Math. Stat. Labs., Stanford Univ., Stanford, California.

[31] L.W. NIELAND, *Zum Kreisproblem*, Math. Ann. 98 (1928) pp. 717-736.

[32] W.-G. NOWAK, *Lattice points in a circle and divisors in arithmetic progressions*, Manuscr. Math. 49 (1984) pp. 195-205.

[33] E. PFEIFFER, *Über die Periodicität in der Teilbarkeit der Zahlen und über die Verteilung der Klassen positiver quadratischer Formen auf ihre Determinanten*, Jahresber. der Pfeiffer'schen Lehr- und Erziehungsanstalt zu Jena (1886) pp. 1-21.

[34] W. SIERPINSKI, *O pewnem zagadnieniu z rachunku funkcyj asymptotycznych*, Prace mat. fyz. 17 (1906) pp. 77-118.
Summary in French: *Sur un probleme du calcul des fonctions asymptotiques*, pp. 115-118.

[35] E.C. TITCHMARSH, *The lattice points in a circle*, Proc. London Math. Soc. (2) 38 (1934) pp. 96-115. Corrigendum p. 555.

[36] I.M. VINOGRADOV, *Elements of Number Theory*, Dover Publ., 1954.

[37] G. VORONOÏ, *Sur un problème du calcul des fonctions asymptotiques*, J. r. a. M. 126 (1903) pp. 241-282.

[38] A. WALFISZ, *Über zwei Gitterpunktprobleme*, Math. Ann. 95 (1927) pp. 69-83.

[39] A. WALFISZ, *Teilerprobleme*, Math. Z. 26 (1927) pp. 66-88.

[40] J.R. WILTON, *The lattice points of a circle: an historical account of the problem*, Mess. Math. 48 (1928) pp. 67-80.

[41] YIN WEN LIN, *The lattice points in a circle*, Sci. Sinica 11 (1962) pp. 10-15.

[42] J.T. TROMP, *More computations on Gauss' lattice point problem*, Mathematical Centre Report CS-R9017 (1990) 10 p.

Analyse Helpt Getaltheorie

F. van der Blij
Ruysdaellaan 6
3723 CC Bilthoven

0. Verantwoording

> Je kunt sommige formules in de wiskunde bestuderen als schilderijen. Met een beetje uitleg zie je er veel meer in dan je eerst dacht te zien. Toch weet je dat je zo'n schilderij nooit zelf zult maken. Maar daarom is het niet minder mooi.

Getaltheorie is een onderdeel van de wiskunde waarbij vele andere gebieden van de wiskunde te hulp geroepen worden. Natuurlijk gezond verstand, verder combinatoriek, algebra, maar ook groepentheorie, analyse, speciaal ook complexe funktietheorie. Het vak is al oud en de toepassing van complexe funktietheorie is ook al tientallen jaren oud; de formules die we vandaag bestuderen zijn al voor de tweede wereldoorlog gevonden.

Een recent artikel van Marvin J. Knopp (Notices Amer. Math. Soc., april 1990) [1] laat zien dat de oude theorie relaties heeft met recent onderzoek. Een artikel uit 1980 vestigt de aandacht op een aantal raadsels, waarbij de funkties die we in de analytische getaltheorie tegenkomen in verband gebracht worden met zeer algemene stellingen uit de groepentheorie [2].

Uit de getaltheorie noemen we even enkele kernwoorden die van belang zijn voor het onderdeel waar we ons mee bezig zullen houden: sommen van machten van delers, representatie door sommen van kwadraten, met op de achtergrond rekenkundige eigenschappen van Lie groepen, elliptische funkties, kubische krommen, enz.

1. INLEIDING

In deze voordracht gaat het om getaltheorie zonder meer. De toepassingen komen in andere voordrachten wel aan de orde. Het doel van deze voordracht is om aan een enkel voorbeeld te schetsen hoe interessante eigenschappen met betrekking tot natuurlijke getallen soms verkregen kunnen worden met vrij gecompliceerde methoden uit de complexe funktietheorie.

Wij zullen als regel niets bewijzen, ten hoogste aanduiden op welke manier de bewijzen gestructureerd zijn. Voor uitvoerige bewijzen verwijzen we naar de literatuur.

Laat voor ieder natuurlijk getal n een getal $a(n)$ (meestal een aantal) gedefiniëerd zijn. Bijvoorbeeld: het aantal manieren waarop een getal n te schrijven is als de som twee kwadraten plus twee derde machten, het aantal oplossingen van een congruentie modulo n, het aantal delers van n.

Om nadere informatie over zulke getallen $a(n)$ te krijgen kan men met deze getallen een machtreeks definiëren

$$f(z) = \sum_{n=0}^{\infty} a(n)z^n.$$

Zo'n machtreeks kan men op twee manieren opvatten. Allereerst als een "formele machtreeks", d.w.z. de machtreeks is niets anders als een (handige) notatie voor de funktie die aan n het getal $a(n)$ toevoegt. Maar de machtreeks-notatie maakt sommige manipulaties meer doorzichtig [3].

VOORBEELD. Laat $p_e(n)$ het aantal manieren zijn waarop n te schrijven is als de som van een even aantal verschillende positieve gehele getallen.

$p_e(7)=3$ want $7=1+6=2+5=3+4$

$p_e(8)=3$ want $8=1+7=2+6=3+5$

$p_e(9)=4$ want $9=1+8=2+7=3+6=4+5$

$p_e(10)=5$ want $10=1+9=2+8=3+7=4+6=1+2+3+4$

$p_e(11)=6$ want $11=1+10=2+9=3+8=4+7=5+6=1+2+3+5$

$p_e(12)=7$ want $12=1+11=2+10=3+9=4+8=5+7=$
$=1+2+4+5=1+2+3+6.$

Laat $p_o(n)$ het aantal manieren zijn waarop n te schrijven is als de som van een oneven aantal verschillende positieve gehele getallen.

$p_o(7)=2$ want $7=7=1+2+4$

$p_o(8)=3$ want $8=8=1+3+4=1+2+5$

$p_o(9)=4$ want $9=9=1+2+6=1+3+5=2+3+4$

$p_o(10)=5$ want $10=10=1+2+7=1+3+6=1+4+5=2+3+5$

$$p_o(11)=6 \quad \text{want} \quad 11=11=1+2+8=1+3+7=1+4+6=$$
$$=2+4+5=2+3+6$$
$$p_o(12)=8 \quad \text{want} \quad 12=12=1+2+9=1+3+8=1+4+7=$$
$$=1+5+6=2+3+7=2+4+6=3+4+5.$$

We merken op dat

$$p_e(7)-p_o(7)=1 \quad \text{en} \quad 24\times 7+1=13^2$$
$$p_e(8)-p_o(8)=0 \quad \text{en} \quad 24\times 8+1=193$$
$$p_e(9)-p_o(9)=0 \quad \text{en} \quad 24\times 9+1=217$$
$$p_e(10)-p_o(10)=0 \quad \text{en} \quad 24\times 10+1=241$$
$$p_e(11)-p_o(11)=0 \quad \text{en} \quad 24\times 11+1=265$$
$$p_e(12)-p_o(12)=-1 \quad \text{en} \quad 24\times 12+1=17^2.$$

Vermoeden: $p_e(n)=p_o(n)$ tenzij $24n+1$ een kwadraat is.

Nu geldt (formeel)

$$\sum_{n=0}^{\infty}[p_e(n)-p_o(n)]z^n=\prod_{m=1}^{\infty}(1-z^m).$$

Schrijven we $z=x^{24}$, dan is ons vermoeden te formuleren als

$$x\prod_{m=1}^{\infty}(1-x^{24m})=\sum_{k=-\infty}^{+\infty}(-1)^k x^{(6k-1)^2}$$

en deze identiteit tussen formele machtreeksen kan met combinatorische middelen bewezen worden [4]. Maar ook met methoden uit de complexe funktietheorie. Alleen moet dan de *convergentie* van de oneindige reeks en het oneindige produkt (voor bepaalde waarden van x) wel vastgesteld worden.

Om de coëfficienten $a(n)$ van een analytische funktie

$$f(z)=\sum_{n=0}^{\infty}a(n)z^n$$

te bepalen kan men integraalrekening gebruiken. De complexe funktietheorie leert dat er een getal R (niet negatief, eventueel oneindig) bestaat zo dat de reeks voor $|z|<R$ convergeert en voor $|z|>R$ divergeert. Het gedrag op de convergentie cirkel $|z|=R$ kan van punt tot punt verschillen.

Men kan nu de getallen $a(n)$ bepalen door gebruik te maken van eigenschappen van de complexe funktie. Wanneer de machtreeks een positieve convergentiestraal R heeft dan geldt

$$a(n)=\frac{1}{2\pi i}\oint\frac{f(z)}{z^{n+1}}dz$$

waarin de integraal over een (nette) gesloten contour, die de oorsprong één

maal positief omvat, genomen moet worden. De contour moet natuurlijk binnen het convergentie gebied liggen [5].

2. PARTITIES

Onder het aantal partities $p(n)$ verstaan we het aantal manieren waarop n te schrijven is als de som van een aantal, niet noodzakelijk verschillende, positieve gehele getallen. Eenvoudig tellen (!) leert

n	$p(n)$
1	1
2	2
3	3
4	5
5	7
6	11
7	15
8	22
9	30
10	42.

En met andere methoden vindt men

n	$p(n)$
10	42
20	627
30	5604
40	37338
50	204226
60	966467
70	4087968
80	15796476
90	56634173
100	190569292.

Voor grotere waarden van n neemt $p(n)$ snel toe; zo is $p(14031) \approx 9 \times 10^{126}$.

We construeren nu de funktie

$$f(z) = \sum_{n=0}^{\infty} p(n) z^n = 1 + z + 2z^2 + 3z^3 + 5z^4 + 7z^5 + \cdots .$$

Formeel rekenen laat ons zien dat

$$\frac{1}{1-z}=1+z^{1}+z^{1+1}+z^{1+1+1}+z^{1+1+1+1}+\cdots$$

$$\frac{1}{1-z^{2}}=1+z^{2}+z^{2+2}+z^{2+2+2}+z^{2+2+2+2}+\cdots$$

$$\frac{1}{1-z^{3}}=1+z^{3}+z^{3+3}+z^{3+3+3}+z^{3+3+3+3}+\cdots$$

Vermenigvuldigen we al deze formules dan vinden we

$$\prod_{n=1}^{\infty}(1-z^{n})^{-1}=\sum_{n=0}^{\infty}p(n)z^{n}.$$

We zien duidelijk dat er voor $|z|=1$ moeilijkheden optreden. Klassieke methoden uit de analyse laten zien dat er voor $|z|<1$ convergentie optreedt.

De procedure uit § 1 leert ons dat

$$p(n)=\frac{1}{2\pi i}\oint\prod_{n=1}^{\infty}(1-z^{n})^{-1}\frac{dz}{z^{n+1}}.$$

Maar hoe een goede contour te kiezen ? De funktie

$$\prod_{n=1}^{\infty}(1-z^{n})$$

heeft (formeel) nulpunten in alle complexe eenheidswortels, dus voor

$$z=e^{\frac{2\pi ih}{k}}.$$

We mogen ons beperken tot positieve gehele k, h, met k en h onderling ondeelbaar en $0\leqslant h<k$.

De listigheid is nu een contour te kiezen die aan de binnenkant van de eenheidscirkel loopt en rekening houdt met al deze bijzondere punten op deze cirkel. In de buurt van zo'n bijzonder punt wordt de integrand benaderd en sommatie van al deze benaderingen blijkt wonder boven wonder een *exacte* formule voor $p(n)$ op te leveren [6].

We schrijven de bedoelde formule even op

$$p(n)=\frac{2\pi}{\sqrt{(24n-1)^{3}}}\sum_{k=1}^{\infty}\frac{A_{k}(n)}{k}I_{3/2}(t) \qquad \text{(A)}$$

waarin

$$t=\frac{\pi}{6k}\sqrt{24n-1}$$

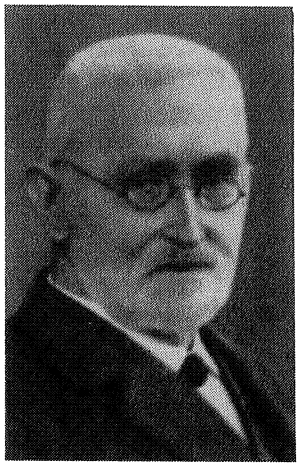
$I_{\nu}(z)$ een Besselfunktie [7]:

$$I_{\nu}(z)=(\frac{z}{2})^{\nu}\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}t^{-\nu-1}e^{t+z^{2}/4t}dt$$

$$A_{k}(n)=\sum_{\substack{0\leqslant h<k\\ \text{ggd}(h,k)=1}}\phi(h,k)e^{-\frac{2\pi inh}{k}}$$

Friedrich Wilhelm Bessel
(1784 - 1846)

S. Ramanujan
(1887 - 1920)



R. Dedekind
(1831 - 1916)

met $\phi(h,k)=e^{\pi i S(h,k)}$ en $S(h,k)$ een Dedekind som [8].

De formule voor $p(n)$ is niet alleen erg gecompliceerd, maar ook heel raadselachtig. Waar komen de Besselfunkties vandaan? Hoe kom je aan $24n-1$, of is het beter te spreken van $n-\frac{1}{24}$? We gaan wat heuristiek bedrijven:

$$\sum_{n=0}^{\infty} p(n) z^{n-\frac{1}{24}} = z^{-\frac{1}{24}} \prod_{n=1}^{\infty} (1-z^n)^{-1}.$$

Dus

$$\left\{ \sum_{n=0}^{\infty} p(n) z^{n-\frac{1}{24}} \right\}^{-24} = z \prod_{n=1}^{\infty} (1-z^n)^{24}$$

maar ook

$$\left\{ \sum_{n=0}^{\infty} p(n) z^{n-\frac{1}{24}} \right\}^{-1} = \sum_{m=-\infty}^{+\infty} (-1)^m z^{\frac{1}{24}(6m-1)^2}.$$

De funktie

$$\Delta^*(z) = z \prod_{n=1}^{\infty} (1-z^n)^{24}$$

is als een machtreeks te schrijven

$$\Delta^*(z) = \sum_{n=1}^{\infty} \tau(n) z^n = z - 24z^2 + 252z^3 - 1472z^4 + 4830z^5 - \cdots$$

waarin de getallen $\tau(n)$ de getallen van Ramanujan zijn. Deze getallen spelen in sommige delen van de getaltheorie een grote rol [9]. In de volgende paragraaf zullen we de funktie $\Delta^*(z)$ nader bestuderen. We voeren daartoe een nieuwe variabele in door te schrijven

$$z = e^{2\pi i \tau}$$

met een nieuwe complexe variabele τ (niet te verwarren met de getallen $\tau(n)$ van Ramanujan; zo is nu eenmaal het gebruik!)

De voorwaarde $|z|<1$ laat zich nu schrijven als

$$\mathrm{Im}(\tau)>0.$$

We beschouwen de funktie

$$\Delta(\tau) = e^{2\pi i \tau} \prod_{n=1}^{\infty} (1-e^{2\pi i n \tau})^{24}$$

in het boven-halfvlak $\mathrm{Im}(\tau)>0$.

Het is direct duidelijk dat

$$\Delta(\tau+1) = \Delta(\tau)$$

en we zullen in de volgende paragraaf zien dat

$$\Delta(\frac{-1}{\tau})=\tau^{12}\Delta(\tau).$$

Herhaald samenstellen van deze transformaties leert ons dat

$$\Delta\left[\frac{a\tau+b}{c\tau+d}\right]=(c\tau+d)^{12}\Delta(\tau)$$

met $a,b,c,d\in\mathbb{Z}$, $ad-bc=1$ [10].

3. Modulaire vormen en modulaire funkties

We kennen allen de (complexe) periodieke funkties. Bijvoorbeeld $\sin 2\pi z$, immers $\sin 2\pi(z+k)=\sin 2\pi z$ voor alle $k\in\mathbb{Z}$. Of $\operatorname{cotg}\pi z$, immers $\operatorname{cotg}\pi(z+k)=\operatorname{cotg}\pi z$ voor alle $k\in\mathbb{Z}$.

Nu bestaan er ook *dubbel periodieke* funkties, een generalisatie van periodieke funkties. Voor zo'n dubbel periodieke funktie bestaat een complexgetal τ, waarbij we steeds $\operatorname{Im}(\tau)>0$ mogen (en zullen) veronderstellen, zodat voor alle $k\in\mathbb{Z}$ en alle $l\in\mathbb{Z}$ geldt

$$f(z+k+l\tau)=f(z).$$

Dit noemen we dubbel periodieke funkties. We zullen ons alleen bezig houden met nette (analytische) dubbel periodieke funkties.

Er is een aardige manier om ze te maken. We bezien eerst

$$\phi_m(z)=\sum_{k\in\mathbb{Z}}\frac{1}{(z+k)^m},\quad m\in\mathbb{N}.$$

Voor $m\geqslant 2$ convergeert de reeks absoluut en het is duidelijk dat $\phi_m(z+1)=\phi_m(z)$.

Met goede afspraken over sommatie [11] is ook voor $m=1$ een betekenis aan de reeks toe te kennen

$$\phi_1(z)=\frac{\pi\cos(\pi z)}{\sin(\pi z)}=\pi\operatorname{cotg}\pi z.$$

De formule geeft een soort partiële breukontwikkeling voor de cotangens. Voor $z=0$ is de funktie niet gedefiniëerd. Maar

$$[\phi_{2m}(z)-\frac{1}{z^{2m}}]_{z=0}=2\zeta(2m)$$

waarin ζ de zeta funktie van Riemann is:

$$\zeta(s)=\sum_{k=1}^{\infty}\frac{1}{k^s}$$

een funktie die een grote rol in de theorie van de priemgetallen speelt.

Dit brengt ons er toe om analoog te bestuderen

$$F_m(z,\tau)=\sum_{k,l\in\mathbb{Z}}\frac{1}{(z+k+l\tau)^{2m}},\quad m\in\mathbb{N}.$$

Voor m voldoende groot convergeert de reeks absoluut. De som is dan een dubbel periodieke funktie van z. We bestuderen weer

$$[F_m(z,\tau)-\frac{1}{z^{2m}}]_{z=0}=\sum_{\substack{k,l\in\mathbb{Z}\\(k,l)\neq(0,0)}}\frac{1}{(k+l\tau)^{2m}}.$$

We definiëren nu

$$E_m(\tau)=\frac{1}{2\zeta(2m)}\sum_{\substack{k,l\in\mathbb{Z}\\(k,l)\neq(0,0)}}\frac{1}{(k+l\tau)^{2m}},\quad m\in\mathbb{N}.$$

Duidelijk is dat

$$E_m(\tau+1)=E_m(\tau)$$

$$E_m(\frac{-1}{\tau})=\tau^{2m}E_m(\tau)$$

en dus

$$E_m\left(\frac{a\tau+b}{c\tau+d}\right)=(c\tau+d)^{2m}E_m(\tau);\ a,b,c,d\in\mathbb{Z},\ ad-bc=1.$$

De funktie E_m is te schrijven als een machtreeks in $e^{2\pi i\tau}$. Dit vraagt alleen klassieke manipulaties. We vinden

$$E_m(\tau)=1+(-1)^m\frac{4m}{B_m}\sum_{n=1}^{\infty}\sigma_{2m-1}(n)e^{2\pi in\tau}.$$

Hierin is B_m het m-de getal van Bernoulli [12] en $\sigma_{2m-1}(n)$ is de som van de $(2m-1)$-de machten van alle positieve delers van n.

We zijn nu weer terug in de getaltheorie: sommen van delers, Bernoulli getallen, enzovoorts.

Nu komt weer een wonder

$$\Delta(\tau)=\frac{64}{27}\pi^{12}\{E_2^3(\tau)-E_3^2(\tau)\}$$

en dus

$$\Delta(\frac{-1}{\tau})=\tau^{12}\Delta(\tau).$$

Door deze transformaties is het mogelijk de funktie Δ in de omgeving van een punt $\tau=\frac{h}{k}$ goed te schatten. Door het verband tussen

$$f(z)=\sum_{n=0}^{\infty}p(n)z^n=\sum_{n=0}^{\infty}p(n)e^{2\pi in\tau}=\prod_{m=1}^{\infty}(1-e^{2\pi in\tau})^{-1}$$

en

$$\Delta(\tau)=e^{2\pi i\tau}\prod_{m=1}^{\infty}(1-e^{2\pi im\tau})^{24}$$

is ook het gedrag van $f(z)$ in een omgeving van

$$z = e^{2\pi i \frac{h}{k}}$$

goed te schatten [13].

Sommatie over alle k en alle h met ggd$(h,k)=1$ en $0 \leqslant h < k$ voert dan tot formule (A) voor $p(n)$ uit § 2.

4. DE MODULAIRE INVARIANT

We zoeken (nette) funkties die invariant zijn onder de transformaties

$$\tau \to \frac{a\tau + b}{c\tau + d}, \quad a,b,c,d \in \mathbb{Z}, \quad ad - bc = 1.$$

Al deze funkties zijn te schrijven als rationale uitdrukkingen van één enkele invariante functie. Voor deze ene kan men kiezen

$$J(\tau) = \frac{E_2^3(\tau)}{E_2^3(\tau) - E_3^2(\tau)}.$$

Deze funktie is als Laurent reeks in $e^{2\pi i \tau}$ te schrijven:

$$J(\tau) = \frac{1}{e^{2\pi i \tau}} + 744 + \sum_{n=1}^{\infty} c(n) e^{2\pi i n \tau}$$

$$c(1) = 2^2 \cdot 3^3 \cdot 1823 = 196884$$

$$c(2) = 2^{11} \cdot 5 \cdot 2099 = 21493760.$$

Voor de coëfficienten $c(n)$ kan een formule geheel analoog aan formule (A) voor $p(n)$ gevonden worden

$$c(n) = \frac{2\pi}{\sqrt{n}} \sum_{k=1}^{\infty} \frac{A_k(n)}{k} I_1\left[\frac{4\pi\sqrt{n}}{k}\right], \quad n \geqslant 1. \tag{B}$$

Hierin is

$I_1(z)$ een Besselfunktie,

$$A_k(n) = \sum_{\substack{h \bmod k \\ (h,k)=1}} \psi(h,k) e^{-\frac{2\pi i h n}{k}}, \quad \text{(een Kloostermansom)}$$

$$\psi(h,k) = e^{-\frac{2\pi i h'}{k}} \quad \text{met} \quad hh' \equiv -1 (\bmod k).$$

Recentelijk is het vermoeden gerezen dat de coëfficienten $c(n)$ een arithmetische betekenis hebben en wel in het kader van een wonderlijk fenomeen, de sporadische groepen. Simpele groepen zijn eindige groepen die geen ander homomorf beeld bezitten dan het triviale. In zekere zin zijn het de bouwstenen van alle eindige groepen. Deze simpele groepen omvatten een aantal grote families en dan nog 26 uitzonderlijke exemplaren, die niet in deze families passen.

Van deze sporadische groepen is *het monster* de grootste met

$$2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 7^{6}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71 =$$

$$808017424794512875886435990496171075700575436800000000$$

elementen.

De coëfficienten $c(n)$ hangen samen met de representaties van deze groep als groep van matrices. En verdere overeenkomsten tussen de coëfficienten van modulaire invarianten en representaties van het monster lijken er op te wijzen dat dit geen toeval is.

Natuurlijk doen zich nu veel vragen voor. De formules voor $p(n)$ en $c(n)$ zullen wel niet op zichzelf staan. Hoe moeten generalisaties van $\phi(h,k)$ en $\psi(h,k)$ gekozen worden en welke Besselfunkties moet men kiezen om coëfficienten $b(n)$ te vinden, die een arithmetische betekenis hebben en zo dat

$$\sum_{n=1}^{\infty} b(n)e^{2\pi i\tau n}$$

speciale eigenschappen heeft bij de transformaties

$$\tau \to \frac{a\tau+b}{c\tau+d}, \quad a,b,c,d\in\mathbb{Z}, \quad ad-bc=1.$$

Heeft de produktontwikkeling

$$\sum_{n=0}^{\infty} p(n)e^{2\pi in\tau} = \prod_{m=1}^{\infty}(1-e^{2\pi im\tau})^{-1}$$

nog een speciale betekenis?

§ 5. Multiplicatieve eigenschappen

Door een eenvoudige complexe transformatie kan een machtreeks

$$f(\tau)=\sum_{n=0}^{\infty} a(n)z^{n}=\sum_{n=0}^{\infty} a(n)e^{2\pi i\tau n}$$

omgezet worden in een Dirichlet reeks

$$g(s)=\sum_{n=1}^{\infty}\frac{a(n)}{n^{s}}.$$

Invariantie, op een macht van τ na, onder de transformatie

$$\tau \to \frac{-1}{\tau}$$

hangt samen met transformaties $s\to A-s$ en funktionaal vergelijkingen van Dirichlet reeksen. Bij de omgekeerde transformatie van $g(s)$ naar $f(\tau)$ doet zich het merkwaardige feit voor dat voor arithmetisch belangwekkende funkties (met zekere invarianties) de coëfficient $a(0)$ bepaald is door alle $a(n)$ met $n\geqslant 1$.

Van bijzonder belang zijn die arithmetische funkties $a(n)$ die multiplicatief zijn, d.w.z. waarvoor

$$a(nm)=a(n)\cdot a(m) \text{ voor alle } n \text{ en } m \text{ met } \gcd(n,m)=1.$$

Nog mooier is het als er een recursieve betrekking bestaat om de coëfficienten $a(p^\lambda)$ voor $\lambda\geqslant 2$ uit $a(p^{\lambda-1})$ en $a(p^{\lambda-2})$ af te leiden.

Dan is $g(s)$ te schrijven als een Euler produkt:

$$g(s)=\prod_p \left(1-\frac{a(p)}{p^s}+\frac{p^f}{p^{2s}}\right)^{-1}.$$

En nu kunnen zwaardere hulpmiddelen uit algebra en analyse (eigenfunkties van bepaalde lineaire operatoren) gebruikt worden om nog meer over die "eenvoudige" getaltheoretische funkties af te leiden.

In nog verder gaande onderzoekingen spelen nog een ander soort reeksen (Poincaré reeksen) een rol en komen de uit de theorie van de speciale funkties bekende Whittaker-funkties naar voren [14].

VERWIJZINGEN

We verwijzen als regel naar leerboeken en overzichtsartikelen. Daar kan men dan weer verwijzingen naar de oorspronkelijke literatuur vinden.

LITERATUUR

[1] MARVIN I. KNOPP, Rademacher on $J(\tau)$, Poincaré Series of Nonpositive Weights and the Eichler Cohomology, Notices of the American Mathematical Society 37, pp. 385-393, April 1990.

[2] J.H. CONWAY, Monsters and Moonshine, The Mathematical Intelligencer 2, pp. 165-171, 1980.

[3] In vrijwel alle leerboeken over combinatoriek worden zulke formele machtreeksen uitgelegd en gebruikt.

[4] Zie bijvoorbeeld: HARDY & WRIGHT, An introduction to the theory of numbers, Chapter XIX, partitions.

[5] De nauwkeurige formulering en het bewijs van deze stelling van Cauchy vindt men in ieder inleidend leerboek over complexe funktietheorie. De eigenschap hangt samen met het feit dat

$$\int_0^{2\pi} e^{int}dt=0 \quad \text{voor} \quad n\neq 0, \quad n\in\mathbb{Z},$$

$$=2\pi \quad \text{voor} \quad n=0.$$

[6] De afleiding van deze formule is onder andere vrij uitvoerig te vinden in Tom M. Apostol, Modular Functions and Dirichlet Series in Number Theory (Graduate Texts in Mathematics), Springer Verlag, 1976, Chapter 5, Rademacher's series for the partition function.

Een aardig element is het in de normale volgorde schrijven van alle breuken $\frac{h}{k}$ met ggd$(h,k)=1$, $0 \leqslant h < k$ en $k \leqslant N$. Deze rij van breuken (Farey series) heeft zeer fraaie elementair te bewijzen eignschappen, zie b.v. HARDY & WRIGHT [4], Chapter III.

[7] Besselfunkties kunnen ook met behulp van machtreeksen gedefiniëerd worden:

$$I_\nu(z)=(\frac{z}{2})^\nu \sum_{k=0}^{\infty} \frac{(\frac{z}{2})^{2k}}{k!(k+\nu)!}.$$

[8] De Dedekindsom is een eenvoudig te definiëren rekenkundige som met bijzondere eigenschappen.
Laat

$$\begin{aligned} ((x)) &= x-[x]-\tfrac{1}{2} && \text{voor } x \notin \mathbb{Z} \\ &= 0 && \text{voor } x \in \mathbb{Z}. \end{aligned}$$

Dan geldt

$$S(h,k)=\sum_{0 \leqslant r < k} ((\frac{r}{k}))\cdot((\frac{hr}{k})).$$

[9] Zie bijvoorbeeld:
G.H. HARDY, Ramanujan, twelve lectures on subjects suggested by his life and work, Cambridge, 1940.

[10] De transformaties $\tau \to \frac{a\tau+b}{c\tau+d}$ met een gehele matrix $\binom{ab}{cd}$ met determinant 1 vormen een groep van transformaties die het boven-halfvlak $\mathrm{Im}(\tau)>0$ invariant laten. Deze groep van transformaties en het bijbehorende fundamentaalgebied is object van onderzoek over modulaire funkties en modulaire vormen. Een zeer beknopte en duidelijke inleiding is te vinden in:
J.P. SERRE, Cours d'Arithmétique, Presses Universitaires de France, 1970, Chaptre VII. (Bij Springer Verlag verscheen een Engelse vertaling.)

[11] We gebruiken daartoe de z.g. Eisenstein-sommatie

$$\sum_{k \in \mathbb{Z}} \alpha(k) = \lim_{N \to \infty} \sum_{k=-N}^{N} \alpha(k).$$

Een goede behandeling van deze zaken is te vinden in:
A. WEIL, Elliptic Functions according to Eisenstein and Kronecker, Springer Verlag, 1976.

[12] $B_1=\frac{1}{6}$, $B_2=\frac{1}{30}$, $B_3=\frac{1}{42}$, $B_4=\frac{1}{30}$, $B_5=\frac{5}{66}$, $B_6=\frac{691}{2730}$, $B_7=\frac{7}{6}$, $B_8=\frac{3617}{510}$, . . . De getallen B_n kunnen recursief gedefiniëerd worden, maar ook door

$$\frac{x}{e^x-1}=1-\frac{1}{2}x+\sum_{k=1}^{\infty}(-1)^{k+1}B_k\frac{x^{2k}}{(2k)!}.$$

[13] Zie bijvoorbeeld:
MARVIN I. KNOPP, Modular Functions in Analytic Number Theory, Markham (Chicago), 1970, Chapters 3, 4.
[14] Zie bijvoorbeeld:
R.W. BRUGGEMAN, Fourier Coefficients of Automorphic Forms, Springer, 1981.

Benaderingsbreuken

R. Tijdeman
Rijksuniversiteit Leiden
Afdeling Wiskunde en Informatica
Postbus 9512, 2300 RA Leiden

1. Kettingbreuken

Als we een handrekenmachine gebruiken, vinden we

$$\begin{aligned}\sqrt{2} &= 1{,}414213562,\\ e &= 2{,}718281828,\\ \log 3/\log 2 &= 1{,}584962501,\\ \pi &= 3{,}141592654.\end{aligned}$$

Dit zijn geen gelijkheden in wiskundige zin, maar afrondingen, want de getallen links zijn irrationaal, d.w.z. geen quotiënt van twee gehele getallen. De laatste gelijkheid moet gelezen worden als

$$\pi \approx 3{,}141592654 = \frac{3141592654}{10^9} \quad (\approx \text{is "is afgerond"}). \tag{1}$$

De afwijking ligt tussen 4×10^{-10} en 5×10^{-10}, want

$$\pi \approx 3{,}14159265358979323846264338327 95.$$

Er zijn echter breuken met teller en noemer kleiner dan 10^9 die minder van π afwijken dan (1). Sommige rationale benaderingen van π zijn al heel oud. Archimedes (278-212 v. Chr.) gebruikte al de bekende benadering $22/7 \approx 3{,}14285714$ en Tsu Chung Chih (430-501 n. Chr.) vond de verrassend goede benadering $355/113 \approx 3{,}14159292$. De breuk $208341/66317 \approx 3{,}14159265347$ benadert π al beter dan (1).

De volgende procedure maakt het ons mogelijk om de kwaliteit van benaderingen te vergelijken en "beste benaderingen" te definiëren. Hierbij wordt met

"best" niet bedoeld dat er geen betere benadering zou bestaan, maar dat de benadering "beter" is dan alle benaderingen met kleinere noemer. Zij α een reëel getal. Bereken de afstand $\|q\alpha\|$ van $q\alpha$ tot het dichtstbijzijnde gehele getal voor $q = 1,2, \cdots$ en noteer die q waarvoor die afstand kleiner is dan alle afstanden tot dan toe. Schrijven we voor $\alpha = \pi$ achtereenvolgens op: de gevonden q, het gehele getal p dat het dichtst bij $q\pi$ ligt en $q\pi - p$, dan krijgen we

q	p	$q\pi - p \approx$
1	3	0,1415927
7	22	-0,0088514
106	333	0,0088213
113	355	-0,0000301
33102	103993	0,0000191
33215	104348	-0,0000110
66317	208341	0,0000081.

De breuken p/q noemen we de *beste benaderingsbreuken* van π. Het eerste wat opvalt is dat in dit korte rijtje alle genoemde benaderingsbreuken p/q van π terug te vinden zijn. Ook merken we een lineair verband tussen opeenvolgende regels op: de laatste regel is de som van de twee voorgaande en zo is ook de vierde regel de som van de tweede en de derde. Bij nadere beschouwing blijkt elke volgende regel de som te zijn van de voorlaatste en een aantal a maal de laatste.

q	p	$d := q\pi - p \approx$	a	n
1	0	3,1415927		-1
0	1	-1	3	0
1	3	0,1415927	7	1
7	22	-0,0088514	15	2
106	333	0,0088213	1	3
113	355	-0,0000301	292	4
33102	103993	0,0000191	1	5
33215	104348	-0,0000110	1	6
66317	208341	0,0000081	1	7
99532	312689	-0,0000019	1	8
165849	521030	0,0000005	4	9.

Het is nu niet moeilijk meer de volgende regels te gissen en het ligt voor de hand bovenaan twee startregels toe te voegen. Tenslotte voegen we een regelteller n toe, duiden we de q, p en a op de n-de regel aan door resp. q_n, p_n en a_n, en schrijven we d_n voor $q_n\pi - p_n$. De a's heten *wijzergetallen.*

OPDRACHT 1. Schrijf een computerprogramma dat voor een willekeurig positief reëel getal α de beste benaderingen van α met noemer q kleiner dan 10000 bepaalt en produceer de tabellen voor $\alpha = \sqrt{2}$, e en $\log 3/\log 2$. Ga in elke

tabel na dat er een lineair verband tussen drie opeenvolgende regels bestaat en bepaal de wijzergetallen.

Achteraf gezien hadden we de tabel voor π veel sneller kunnen maken, nl. door als startwaarden te nemen

$$\begin{cases} q_{-1}=1 & p_{-1}=0 & d_{-1}=\alpha \\ q_0=0 & p_0=1 & d_0=-1 \quad a_0=\lfloor\alpha\rfloor \end{cases} \tag{1}$$

waarbij we voor α in dit geval π nemen en door verder q_n, p_n, d_n en a_n voor $n=1, 2, \cdots$ te berekenen volgens

$$\begin{cases} q_n = a_{n-1}q_{n-1}+q_{n-2} \\ p_n = a_{n-1}p_{n-1}+p_{n-2} \\ d_n = a_{n-1}d_{n-1}+d_{n-2} \\ a_n = \lfloor -d_{n-1}/d_n \rfloor . \end{cases} \tag{2}$$

Dit is een eenvoudig algoritme dat voor een willekeurig reëel getal α uit te voeren is.

We maken de tabel die hoort bij $\alpha=\log 3/\log 2\approx 1{,}58496250$

q	p	$d\approx$	a	n
1	0	1,5849625		-1
0	1	-1	1	0
1	1	0,5849625	1	1
1	2	-0,4150375	1	2
2	3	0,1699250	2	3
5	8	-0,0751875	2	4
12	19	0,0195500	3	5
41	65	-0,0165374	1	6
53	84	0,0030126	5	7
306	485	-0,0014741	2	8
665	1054	0,0000645	22	9.

We hebben geen zekerheid dat dit de beste benaderingen zijn, maar in ieder geval vinden we wel erg goede benaderingen, bijv. $1054/665 \approx 1{,}58496241$.

OPDRACHT 2. Schrijf een computerprogramma dat voor een willekeurig reëel getal α tabellen m.b.v. (1) en (2) maakt en produceer de tabellen voor $\alpha=\sqrt{2}$ en e. Ga na of de tabellen overeenkomen met de tabellen gevonden bij de eerste opdracht.

Tot nog toe hebben we alleen irrationale α's beschouwd. Waarom nemen we

niet rationale α's, bijv. $\alpha = 1054/665$.

De kolom voor d wordt nu exact.

q	p	d	a	n
1	0	1054/665		-1
0	1	-1	1	0
1	1	389/665	1	1
1	2	-276/665	1	2
2	3	113/665	2	3
5	8	-50/665	2	4
12	19	13/665	3	5
41	65	-11/665	1	6
53	84	2/665	5	7
306	485	-1/665	2	8
665	1054	0		9.

De tabel lijkt opvallend veel op die van $\log 3/\log 2$, maar de kolom voor d eindigt nu op 0 en het algoritme stopt. De gevonden benaderingsbreuk 1054/665 is ook ideaal.

De kolom voor d onthult nog een derde algoritme. Immers, we passen toe:

$$\begin{aligned}
\frac{1054}{665} &= 1+\frac{389}{665} \\
\frac{665}{389} &= 1+\frac{276}{389} \\
\frac{389}{276} &= 1+\frac{113}{276} \\
\frac{276}{113} &= 2+\frac{50}{113} \\
&\cdots
\end{aligned}$$

vergelijk Algoritme van Euclides

$$\begin{aligned}
1054 &= 1\times 665+389 \\
665 &= 1\times 389+276 \\
389 &= 1\times 276+113 \\
276 &= 2\times 113+50 \\
&\cdots
\end{aligned}$$

Op deze manier vinden we de zogenaamde *kettingbreuk* van 1054/665 waarbij de wijzergetallen 1,1,1,2,2,3,1,5,2 op een heel natuurlijk wijze verschijnen:

$$\frac{1054}{655} = 1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{5+\frac{1}{2}}}}}}}}$$

We kunnen hetzelfde procedé op irrationale getallen toepassen, maar krijgen dan een oneindig lange kettingbreuk. Stellen we $x_n = -d_{n-1}/d_n$ voor $n = 0,1,2, \cdots$, dan volgt uit (2) immers

$$x_{n-1} = -\frac{d_{n-2}}{d_{n-1}} = a_{n-1} - \frac{d_n}{d_{n-1}} = a_{n-1} + \frac{1}{x_n} = \lfloor x_{n-1} \rfloor + \frac{1}{x_n}. \qquad (3)$$

We kunnen x_n dus interpreteren als de noemer van de n-de breuk. Uit (3) volgt ook dat $x_n > 1$ voor $n = 1,2, \cdots$. De termen van de rij $\{d_n\}_{n=-1}^{\infty}$ wisselen dus van teken. (Dit alles tot eventueel $x_{n-1} \in \mathbb{Z}$ en de breuk afbreekt.) Ook geldt $|d_0| > |d_1| > \cdots$.

We maken de tabel die dit algoritme voor $\alpha = \sqrt{2}$ oplevert:

q	p	x	a	n
1	0			-1
0	1	$\sqrt{2}$	1	0
1	1	$\sqrt{2}+1$	2	1
2	3	$\sqrt{2}+1$	2	2
5	7	$\sqrt{2}+1$	2	3
12	17	$\sqrt{2}+1$	2	4
29	41	$\sqrt{2}+1$	2	5
70	99	$\sqrt{2}+1$	2	6.

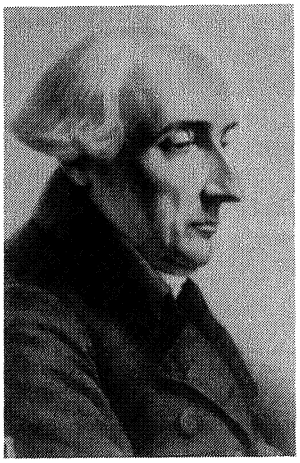
Omdat $((\sqrt{2}+1)-2)^{-1} = \sqrt{2}+1$ is de kolom voor x na het begin constant. Merk op dat $99/70 \approx 1{,}4142857$ terwijl $\sqrt{2} \approx 1{,}4142136$.

OPRACHT 3. Bewijs dat er oneindig veel paren natuurlijke getallen (x,y) zijn zó dat $x^2 - 2y^2 = 1$ en oneindig veel zó dat $x^2 - 2y^2 = -1$.

Voor we doorgaan met onze ontdekkingsreis enige filosofische woorden. Er zijn veel klachten van studenten en scholieren dat wiskunde saai is. Ik meen dat dit komt omdat wij, leraren, de stof presenteren in hapklare brokken die zo snel mogelijk verteerd moeten zijn. Ik probeer vandaag mijn verhaal zo te presenteren dat door het stellen van natuurlijke vragen en attent waarnemen zich een onverwachte samenhang openbaart die ook middelbare-schoolleerlingen het genoegen van het bedrijven van wiskunde kan doen beleven.

2. BEWIJZEN

Het is schrikbarend te merken hoe weinig gevoel en waardering er op het ogenblik bij middelbare schoolverlaters is voor bewijzen. Dit komt voor mijn gevoel door een wijdverbreid misverstand, nl. dat een bewijs de vertaling is in formules van wat je al gezien hebt. Het bewijs is echter de stap van vermoeden naar weten. Formulemanupulatie is geen doel, maar een middel om een bewijs te geven, een compacte taal die over de hele wereld geschreven en begrepen wordt. Een bewijs kan ook gegeven worden met veel omschrijvende tekst, zoals



Joseph-Louis Lagrange
(1736-1813)

de Grieken in de Oudheid deden. Het zoeken naar een bewijs dwingt tot logisch denken en nauwkeurig formuleren van voorwaarden; het leidt ook tot nieuw inzicht en schenkt een genoegen waarvoor ook geldt dat onbekend onbemind maakt.

Dat het algoritme gegeven door (1) en (2) equivalent is met het kettingbreukalgoritme volgt direct uit (3) en vereist geen dieper inzicht. Maar de equivalentie van het "zoek de beste benaderingsbreuken-algoritme" en het kettingbreukalgoritme kunnen we nu alleen maar vermoeden. Om een ander daarvan te overtuigen moeten we het zelf eerst beter doorgronden. Wel hebben we al gezien dat $x_n > 1$ voor $n = 1,2, \cdots$ en dat de rij $\{d_n\}_{n=0}^{\infty}$ alterneert. Uit (3) zien we verder dat de rij afbreekt dan en alleen dan als $x_{n-1} \in \mathbb{Z}$, en dat dan $x_{n-1} = a_{n-1}$ en $d_n = 0$. Zolang dit niet gebeurt, daalt de rij $\{|d_n|\}_{n=0}^{\infty}$ monotoon. De analogie tussen beide algoritmen suggereert dat $d_n = q_n\alpha - p_n$ en dus $d_n = 0 \Leftrightarrow \alpha = p_n/q_n$. Dat dit zo is, is gemakkelijk met volledige inductie uit (1) en (2) te bewijzen. Het algoritme breekt dus niet af als α irrationaal is. Breekt het algoritme altijd af als α rationaal is? Enig nadenken leert ons dat dit inderdaad het geval is. Alle getallen $d_{-1}, d_0, d_1, \cdots$ kunnen geschreven worden als een breuk met dezelfde noemer als α. De tellers worden in absolute waarde steeds kleiner en dat kan niet oneindig lang doorgaan.

Het wisselen van teken van $d_n = q_n\alpha - p_n$ leidt er toe dat $p_n/q_n \leqslant \alpha$ als n even is en $p_n/q_n \geqslant \alpha$ als n oneven is. Hoe kleiner de afstand tussen p_{n-1}/q_{n-1} en p_n/q_n, des te beter wordt α benaderd, omdat α er blijkbaar tussen in ligt. Het verschil tussen beide breuken is eenvoudig uit te drukken:

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^n, \quad (n = 1,2, \cdots). \tag{4}$$

Het bewijs is gemakkelijk met volledig inductie te geven. Maar we kunnen het

ook inzien. Elk paar gehele getallen (k,l) is te schrijven als

$$(k,l) = k(1,0)+l(0,1)=k(q_{-1},p_{-1})+l(q_0,p_0)$$

m.a.w. (q_{-1},p_{-1}) en (q_0,p_0) vormen een basis van $\mathbb{Z}^2$. Omdat (q_{-1},p_{-1}) volgens (3) gelijk is aan $(q_1,p_1)-a_0(q_0,p_0)$, is elk paar (k,l) ook te schrijven als lineaire combinatie van (q_0,p_0) en (q_1,p_1). Zo doorgaande vinden we dat (k,l) voor elke n te schrijven is als lineaire combinatie van (q_{n-1},p_{n-1}) en (q_n,p_n). Dus is de determinant in absolute waarde $|p_nq_{n-1}-p_{n-1}q_n|$, dat is tweemaal de oppervlakte van de driehoek met hoekpunten (0,0), (q_{n-1},p_{n-1}) en (q_n,p_n), gelijk aan 1.

OPDRACHT 4.a) Bewijs met volledige inductie dat $d_n=q_n\alpha-p_n$.
b) Bewijs (4) met volledige inductie.

OPDRACHT 5. Trek in het q,p-vlak de lijn $p=q\alpha$ met $\alpha=\log 3/\log 2$ en markeer de punten (q_n,p_n) uit de kettingbreuktabel van α. Geef meetkundige interpretaties voor d_n, a_n en (4).

Het is nu niet moeilijk meer aan te tonen dat het kettingbreukalgoritme inderdaad precies alle beste benaderingsbreuken levert. Uit (2) en (3) volgt dat $a_n\geqslant 1$ voor alle $n>0$ en dat

$$1 = q_1\leqslant q_2<q_3<q_4<\cdots.$$

Stel p/q is een beste benadering. We mogen $q>0$ veronderstellen. Kies n zó dat $q_{n-1}\leqslant q<q_n$. We hebben al opgemerkt dat elk paar gehele getallen, dus ook (q,p), te schrijven is als lineaire combinatie van (q_{n-1},p_{n-1}) en (q_n,p_n),

$$(q,p) = k(q_{n-1},p_{n-1})+l(q_n,p_n) \quad \text{met} \quad k,l\in\mathbb{Z}$$

ofwel $q=kq_{n-1}+lq_n$, $p=kp_{n-1}+lp_n$.

We onderscheiden nu drie gevallen:

$l>0$. Dan is $k<0$ omdat $q<q_n$. Nu volgt

$$|q\alpha-p| = |kd_{n-1}+ld_n|>|kd_{n-1}|\geqslant|d_{n-1}|=|q_{n-1}\alpha-p_{n-1}| \qquad (5)$$

en blijkt p_{n-1}/q_{n-1} een betere benadering te zijn.

$l=0$. Dan is $p/q=p_{n-1}/q_{n-1}$.

$l<0$. Dan is $k>0$ omdat $q>0$. Nu volgt (5) weer en blijkt p_{n-1}/q_{n-1} een betere benadering te zijn.

Het kettingbreukalgoritme levert dus alle beste benaderingen.

OPDRACHT 6. Interpreteer bovenstaande redenering in het plaatje dat u bij Opdracht 5 gemaakt heeft.

Merk op dat elke convergent p_n/q_n ook een beste benadering is, omdat $|q_n\alpha-p_n|=|d_n|<|d_{n-1}|<|d_{n-2}|<\cdots$ en we net gezien hebben dat de beste benaderingsbreuken door het kettingbreukalgoritme gevonden worden.

OPDRACHT 7. Bewijs met behulp van (4) dat een oplossing van $665x - 1054y = 1$ in gehele getallen gegeven wordt door $x = 485$, $y = 306$. Generaliseer dit.

OPDRACHT 8. Bewijs met volledige inductie:

a) $q_n x_n + q_{n-1} = x_n(q_{n-1}x_{n-1} + q_{n-2})$,

b) $|d_n| = 1/(q_n x_n + q_{n-1})$,

c) $$\frac{1}{q_n(q_{n+1}+q_n)} < |\alpha - \frac{p_n}{q_n}| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$

3. TOEPASSINGEN

A. *Toetsenverdeling op een klavier*

Een verhoging met een octaaf betekent een verdubbeling van de frequentie, terwijl bij een verhoging met een (reine) kwint de frequentie met 3/2 vermenigvuldigd wordt. Om per octaaf maar eindig veel toetsen te hebben en toch willekeurig te kunnen moduleren, is het nodig (kleine) natuurlijke getallen m en n te zoeken zó dat

$$A \times 2^m \quad \text{en} \quad A \times (\tfrac{3}{2})^n \quad \text{bijna gelijk zijn}$$

en dus

$$m \log 2 \quad \text{en} \quad n \log(3/2) \quad \text{weinig verschillen.}$$

Dan is

$$\left| \frac{\log(3/2)}{\log 2} - \frac{m}{n} \right|$$

klein en m/n dus een goede rationale benadering van $\beta = \log(3/2)/\log 2 = \log 3/\log 2 - 1 \approx 0{,}58496250$.

Uit de in § 1 gemaakte tabel lezen we af dat

$$0/1,\ 1/1,\ 1/2,\ 3/5,\ 7/12,\ 24/41,\ 31/53,\ 179/306,\ 389/665,\ \cdots \qquad (6)$$

de beste benaderingsbreuken van β zijn. (Trek 1 af van de beste benaderingsbreuken van $\log 3/\log 2$.) Goede verdelingen per octaaf zijn dus mogelijk bij

5 toetsen,
12 toetsen,
41 toetsen,
53 toetsen, enz.

B. *Schrikkeldagen*

Een tropisch jaar is gelijk aan 365,242264 . . . dagen. Hoe vaak is er een

schrikkeldag ? De kettingbreukontwikkeling levert voor $\alpha = 0{,}242264$ dat

n	0	1	2	3	4	5	6
a_n	0	4	7	1	4	1	5
$\frac{p_n}{q_n}$	0	$\frac{1}{4}$	$\frac{7}{29}$	$\frac{8}{33}$	$\frac{39}{161}$	$\frac{47}{194}$	

De convergent 1/4 geeft aan dat in beginsel elk vierde jaar een schrikkeljaar is. De convergent 8/33 is terug te vinden in het voorstel van Omar Khayyam (1079 n. Chr.) om elke 33-ste schrikkeldag te laten vervallen. Volgens de Gregoriaanse kalender vervallen 3 op de 100 schrikkeldagen, nl. in 1700,1800,1900,2100,2200,2300,2500,... . De resterende 97 schrikkeldagen in 400 jaar leiden tot een benaderingsbreuk $97/400 = 0{,}2425$. Over enkele duizenden jaren zal een correctie nodig zijn in de zin dat "we" een extra schrikkeldag overslaan.

C. *Datum van Pasen*

Een tropisch jaar telt 365,242264 dagen, terwijl een synodische maand 29,53059 dagen telt. Praktisch valt Pasen op de eerste zondag na de eerste volle maan na 20 maart. De kettingbreukontwikkeling van $\alpha = \frac{365{,}242264}{29{,}53059} \approx 12{,}367589$ is

n	0	1	2	3	4	5	6
a_n	12	2	1	2	1	1	17
$\frac{p_n}{q_n}$	12	$\frac{25}{2}$	$\frac{37}{3}$	$\frac{99}{8}$	$\frac{136}{11}$	$\frac{235}{19}$	$\frac{4131}{334}$

De goede benadering $235/19 \approx 12{,}368421$ is terug te vinden in het voorstel van Meton van Athene (432 v. Chr.) om een cykel van 19 jaar aan te houden. Dit principe was vele eeuwen lang de basis voor de berekening van de Paasdatum, maar leidde door de gecumuleerde afwijking mede tot de vervanging van de Juliaanse door de Gregoriaanse kalender.

D. *Tandraderen*

Een omloopfrequentie van a omwentelingen per seconde moet omgezet worden in een omloopfrequentie van b omwentelingen per seconde. In de klassieke techniek werden dan tandraderen gebruikt met p en q tanden waarbij p/q een beste benadering is van b/a.

4. Simultane benaderingen

Een veel moeilijker probleem is om goede benaderingsbreuken te vinden voor reële getallen $\alpha_1, \ldots, \alpha_n$ $(n > 1)$ waarbij die breuken dezelfde noemer q hebben; anders gezegd, voor gegeven reële getallen $\alpha_1, \ldots, \alpha_n$ een natuurlijk getal q te vinden zó dat $q\alpha_1, \ldots, q\alpha_n$ allemaal dicht bij een geheel getal liggen.

Dit probleem treedt bijvoorbeeld op als we willen weten na hoeveel jaar een aantal planeten, elk draaiend met constante hoeksnelheid, weer op dezelfde plaats staan als waar ze nu staan. Een andere toepassing is de toetsenverdeling van het klavier als we niet alleen rekening houden met modulaties over een kwint, maar ook over een grote terts. Bij verhoging met een grote terts wordt de frequentie met 5/4 vermenigvuldigd. Het probleem komt er op neer natuurlijke getallen q te vinden zó dat

$$\|q\frac{\log(3/2)}{\log 2}\| \quad \text{en} \quad \|q\frac{\log(5/4)}{\log 2}\|$$

beide klein zijn, waarbij $\|x\|$ de afstand aangeeft van x tot het dichtstbijzijnde gehele getal.

Reeds in 1842 bewees Dirichlet een stelling die aangeeft welke kwaliteit van benadering we kunnen verwachten.

STELLING 1. *Bij elk stel reële getallen* $\alpha_1, \ldots, \alpha_n$ *en* $Q>1$ *bestaat een geheel getal* q *met* $1 \leqslant q \leqslant Q$ *zó dat*

$$\|q\alpha_j\| < \frac{1}{Q^{1/n}} \ (\leqslant \frac{1}{q^{1/n}}) \quad \textit{voor} \quad j=1,2,\ldots,n.$$

Voor $n=1$ (dat is het reeds behandelde geval van benadering van één getal) vinden we dat $\|q\alpha\|<q^{-1}$. Uit Opdracht 8 volgt dat elke convergent p/q van α voldoet aan $|\alpha-p/q|<q^{-2}$ en dat we dus zo q met $\|q\alpha\|<q^{-1}$ vinden. Bij simultane benadering van n getallen wordt het aantal cijfers van Q (zeg: het aantal variabelen) over de α_j's gelijkelijk verdeeld (elk $1/n$-de deel).

Het bewijs van de Stelling van Dirichlet is een eenvoudige toepassing van het ladenprincipe: als er $m+1$ ballen in m laden zitten, is er tenminste één la met tenminste twee ballen. Schrijf $\{x\}$ voor het fractionele deel van x, meer precies $\{x\}:=x-\lfloor x\rfloor$. Dan ligt voor elke q het punt $(\{q\alpha_1\},\{q\alpha_2\},\ldots,\{q\alpha_n\})$ in de eenheidskubus $[0,1)^n$. Neem voor het gemak even aan dat $Q^{1/n}$ een geheel getal k is. Verdeel elke ribbe van de eenheidskubus in k gelijke stukken. Dit induceert een opsplitsing van de eenheidskubus in k^n deelkubussen met ribbelengte $1/k$. Als we q laten lopen van 0 tot en met k^n, hebben we k^n+1 punten. Volgens het ladenprincipe is er dus een deelkubusje dat twee punten bevat, zeg de punten

$$(\{r\alpha_1\},\{r\alpha_2\},\ldots,\{r\alpha_n\}) \quad \text{en} \quad (\{s\alpha_1\},\{s\alpha_2\},\ldots,\{s\alpha_n\}).$$

Nu volgt dat $q:=|r-s|$ voldoet aan $1\leqslant q\leqslant k^n=Q$ en aan

$$\|q\alpha_j\| \leqslant |\{r\alpha_j\}-\{s\alpha_j\}| \leqslant \frac{1}{k}=\frac{1}{Q^{1/n}} \quad \text{voor} \quad j=1,2,\ldots,n.$$

Zo hebben we een iets zwakkere vorm van de stelling van Dirichlet bewezen. Het bewijs van de geformuleerde stelling vereist nog enkele technische verfijningen.

Hoewel het gegeven bewijs wel effectief is, is het allesbehalve efficiënt. Het aantal benodigde berekeningen is zeker zo groot als Q, terwijl we een constante macht van $\log Q$ zouden wensen, dat wil zeggen een constante macht van het aantal cijfers van de precisie die we willen hebben. Zo'n algoritme noemen we polynomiaal. Het kettingbreukalgoritme is polynomiaal. In de afgelopen honderd en vijftig jaar zijn verschillende generalisaties van het kettingbreukalgoritme voorgesteld en soms ook herontdekt, maar al deze algoritmen leveren onbevredigende resultaten vanuit het standpunt van benaderingen. Bij elk algoritme zijn getallen te vinden zó dat goede benaderingen overgeslagen worden en er zijn geen garanties te geven. Dit betekent nog niet dat er geen goed gegeneraliseerd kettingbreukalgoritme bestaat, maar wel dat de regels om alle goede benaderingen gegarandeerd te vinden zo ingewikkeld zijn dat het veel te veel tijd zou kosten om zo'n goed generaliseerd kettingbreukalgoritme uit te voeren. Er moet dus water bij de wijn gedaan worden. In 1982 vond er op dit gebied een doorbraak plaats toen A.K. Lenstra, H.W. Lenstra jr en L. Lovász hun roosterbasisreductiealgoritme introduceerden. Dit algoritme vindt in polynomiale tijd uit een gegeven basis voor een rooster een nieuw rooster waarvan de vectoren relatief kort zijn. Het is dus geen gegeneraliseerd kettingbreukalgoritme, dat een rij goede benaderingen vindt, maar het bepaalt één benadering (of enkele) met een van te voren op te geven precisie. Ten opzichte van de stelling van Dirichlet wordt alleen een factor afhangend van de dimensie n opgeofferd.

STELLING 2 (Lenstra, Lenstra, Lovász). *Het roosterbasisreductiealgoritme bepaalt bij elk stel rationale getallen* $\alpha_1,\alpha_2,\ldots,\alpha_n$ *en* $Q>1$ *in polynomiale tijd een geheel getal* q *met* $1\leqslant q\leqslant Q$ *zó dat*

$$\|q\alpha_j\|\leqslant\frac{2^{(n+1)/4}}{Q^{1/n}}\ \left(\leqslant\frac{2^{(n+1)/4}}{q^{1/n}}\right)\ \textit{voor}\quad j=1,2,\ldots,n.$$

Wat is het verband tussen goede rationale benaderingen en roosterbases? Een n-dimensionaal rooster is een verzameling van de vorm

$$L = \mathbb{Z}b_1+\mathbb{Z}b_2+\cdots+\mathbb{Z}b_n$$

waarbij $b_1,b_2,\ldots,b_n$ een stel lineair onafhankelijke vectoren in $\mathbb{R}^n$ is. Maken we een matrix door $b_1,b_2,\ldots,b_n$ als achtereenvolgende vectoren op te schrijven, dan is de absolute waarde $d(L)$ van de determinant van die matrix dus positief. Er zijn andere keuzen $b_1,b_2,\ldots,b_n$, d.w.z. andere bases, mogelijk die hetzelfde rooster L opleveren, maar de waarde $d(L)$ is voor elke basis van L dezelfde. Het roosterbasisreductiealgoritme vindt nu in polynomiale tijd een (zogenaamde gereduceerde) basis waarvan de eerste basisvector lengte $\leqslant 2^{(n-1)/4}(d(L))^{1/n}$ heeft.

Voor het vinden van een goede benaderingsbreuk van één rationaal getal α passen we het algoritme met $n=2$ toe. We kiezen dan $b_1=(-1,0)^T$ en $b_2=(\alpha,\delta)^T$ waarbij δ een klein positief getal is dat zo gekozen wordt dat we de gewenste precisie verkrijgen. Het algoritme levert een vector

$$p\begin{bmatrix}-1\\0\end{bmatrix}+q\begin{bmatrix}\alpha\\\delta\end{bmatrix}=\begin{bmatrix}q\alpha-p\\q\delta\end{bmatrix},\qquad (p,q\in\mathbb{Z})$$

op met lengte $\leqslant 2^{1/4}\delta^{1/2}$. Hieruit volgt

$$|q\alpha-p|\leqslant 2^{1/4}\delta^{1/2},\quad |q\delta|\leqslant 2^{1/4}\delta^{1/2}$$

en dus

$$|\alpha-p/q|\leqslant\frac{2^{1/4}\delta^{1/2}}{|q|},\quad |q|\leqslant\frac{2^{1/4}}{\delta^{1/2}}.$$

In het geval $n=2$ doet het basisreductiealgoritme hetzelfde als een kettingbreukalgoritme. Het trekt zo vaak mogelijk de ene vector van de andere af en verwisselt daarna beide vectoren. Passen we het algoritme toe op $\alpha=\pi$ met $\delta=10^{-8}$, dan moeten we dus een benadering p/q van π vinden met

$$|\pi-\frac{p}{q}|\leqslant\frac{0{,}00012}{|q|},\qquad |q|\leqslant 11892.$$

$b_i^*:=b_i$;
$\mu_{ij}:=(b_i,b_j^*)/B_j$; $b_i^*:=b_i^*-\mu_{ij}b_j^*$ } for $j=1,2,\ldots,i-1$;
$B_i:=(b_i^*,b_i^*)$
} for $i=1,2,\ldots,n$;

$k:=2$;

(1) perform (*) for $l=k-1$;
if $B_k<(\frac{3}{4}-\mu_{k\,k-1}^2)B_{k-1}$, go to (2);
perform (*) for $l=k-2,\ k-3,\ldots,1$;
if $k=n$, terminate;
$k:=k+1$;
go to (1);

(2) $\mu:=\mu_{k\,k-1}$; $B:=B_k+\mu^2B_{k-1}$; $\mu_{k\,k-1}:=\mu B_{k-1}/B$;
$B_k:=B_{k-1}B_k/B$; $B_{k-1}:=B$;
$\begin{pmatrix}b_{k-1}\\b_k\end{pmatrix}:=\begin{pmatrix}b_k\\b_{k-1}\end{pmatrix}$;
$\begin{pmatrix}\mu_{k-1\,j}\\\mu_{kj}\end{pmatrix}:=\begin{pmatrix}\mu_{kj}\\\mu_{k-1\,j}\end{pmatrix}$ for $j=1,2,\ldots,k-2$;
$\begin{pmatrix}\mu_{i\,k-1}\\\mu_{ik}\end{pmatrix}:=\begin{pmatrix}1&\mu_{k\,k-1}\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&-\mu\end{pmatrix}\begin{pmatrix}\mu_{i\,k-1}\\\mu_{ik}\end{pmatrix}$ for $i=k+1,\ k+2,\ldots,n$;
if $k>2$, then $k:=k-1$;
go to (1).

(*) If $|\mu_{kl}|>\frac{1}{2}$, then:
$r:=$integer nearest to μ_{kl}; $b_k:=b_k-rb_l$;
$\mu_{kj}:=\mu_{kj}-r\mu_{lj}$ for $j=1,2,\ldots,l-1$;
$\mu_{kl}:=\mu_{kl}-r$.

We vinden $q=113$ met $|\pi-355/113|\leqslant 0{,}000031/|q|$.

Voor het vinden van een goede simultane benaderingsnoemer q van n rationale getallen $\alpha_1,\ldots,\alpha_n$ passen we het algoritme op de volgende $n+1$ vectoren toe:

$b_1=(-1,0,\ldots,0)^T$, $b_2=(0,-1,0,\ldots,0)^T$, $\ldots$, $b_n=(0,0,\ldots,0,-1,0)^T$

en $b_{n+1}=(\alpha_1,\alpha_2,\ldots,\alpha_n,\delta)^T$ waarbij δ een klein positief getal is dat zo gekozen wordt dat we de gewenste precisie verkrijgen. Het algoritme levert een vector

$$p_1b_1+p_2b_2+\cdots+p_nb_n+qb_{n+1},\qquad (p_1,\ldots,p_n,q\in\mathbb{Z})$$

op met lengte $\leqslant 2^{n/4}\delta^{1/(n+1)}$. Hieruit volgt

$$|q\alpha_j-p_j|\leqslant 2^{n/4}\delta^{1/(n+1)},\ (j=1,2,\ldots,n),\ |q\delta|\leqslant 2^{n/4}\delta^{1/(n+1)}$$

en dus

$$|\alpha_j-\frac{p_j}{q}|\leqslant\frac{2^{n/4}\delta^{1/(n+1)}}{|q|},\quad |q|\leqslant\frac{2^{n/4}}{\delta^{n/(n+1)}}.$$

Het algoritme bestaat uit een uitgekiend stel regels waarbij telkens een vector een aantal malen van de daaropvolgende vector wordt afgetrokken tot ze bijna loodrecht op elkaar staan en daarna de vectoren zo geordend worden dat ze ongeveer in lengte toenemen. Het algoritme, dat hier afgedrukt wordt, is gemakkelijk voor een computer te programmeren; voor $n=3$ kan het zelfs op een programmeerbare handrekenmachine.

Passen we het algoritme toe op $\alpha_1=e$, $\alpha_2=\pi$ met $\delta=10^{-8}$, dan moeten we dus p_1, p_2 en q vinden zó dat

$$|e-\frac{p_1}{q}|\leqslant\frac{0{,}0031}{|q|},\ |\pi-\frac{p_2}{q}|\leqslant\frac{0{,}0031}{q},\ |q|\leqslant 304684.$$

We vinden $q=61345$ met

$$|e-\frac{166753}{61345}|\leqslant\frac{0{,}0013}{61345},\ |\pi-\frac{192721}{61345}|\leqslant\frac{0{,}0014}{61345}.$$

OPDRACHT 9. Schrijf een computerprogramma dat voor gegeven getallen α_1 en α_2 gehele getallen p_1, p_2, q met $q>0$ bepaalt zó dat

$$|q\alpha_1-p_1|<0{,}001,\ |q\alpha_2-p_2|<0{,}001,\ |q|\leqslant 3\times 10^6$$

en pas het algoritme toe op

a) $\alpha_1=e$, $\alpha_2=\pi$
b) $\alpha_1=\log 2$, $\alpha_2=\log 3$
c) $\alpha_1=\sqrt{2}$, $\alpha_2=\sqrt{3}$
d) $\alpha_1=\log(3/2)/\log 2$, $\alpha_2=\log(5/4)/\log 2$.

5. Toepassingen

A. *Toetsenverdeling op een klavier*
Een verhoging met een grote terts correspondeert met een frequentieverhoging met een factor 5/4. Om per octaaf maar eindig veel toetsen te hebben en toch willekeurig te kunnen moduleren, is het nodig (kleine) natuurlijke getallen m_1, m_2 en q te zoeken zó dat

$$A\times 2^{m_1} \text{ en } A\times(\tfrac{3}{2})^q \text{ evenals } A\times 2^{m_2} \text{ en } A\times(\tfrac{5}{4})^q \text{ bijna gelijk zijn}$$

en dus

$$m_1\log 2 \text{ en } q\log\tfrac{3}{2} \text{ evenals } m_2\log 2 \text{ en } q\log\tfrac{5}{4} \text{ weinig verschillen.}$$

Dan zijn

$$\|q\,\frac{\log(3/2)}{\log 2}\| \text{ en } \|q\,\frac{\log(5/4)}{\log 2}\| \text{ beide klein.}$$

Passen we het reductiealgoritme toe met $\alpha_1=\log(3/2)/\log 2$ en $\alpha_2=\log(5/4)/\log 2$, dan vinden we voor

$\delta=0{,}01$	de waarde	$q=12$
$\delta=0{,}001$	de waarde	$q=53$
$\delta=0{,}000001$	de waarde	$q=4296$.

De kwaliteit van de gevonden benaderingen blijkt uit:

$12\alpha_1$	= 7,01955,	$12\alpha_2$	= 3,86314,
$53\alpha_1$	= 31,00301,	$53\alpha_2$	= 17,06219,
$4296\alpha_1$	= 2152,9989,	$4296\alpha_2$	= 1383,0031.

Ik kan mensen die het gewone toonsysteem te onzuiver vinden, het 53-toonstelsel en in het bijzonder ook het 4296-toonstelsel aanbevelen.

B. Het reductiealgoritme van Lenstra, Lenstra en Lovász is met succes toegepast in verschillende gebieden die buiten het gebied van deze voordracht vallen. Ik volsta met een korte opsomming.

- Het factoriseren van polynomen in irreducibele factoren (A.K. Lenstra, 1982)
- Geheeltallige programmering (H.W. Lenstra, 1983)
- Het kraken van cryptosystemen (o.a. Shamir, 1984)
- Het weerleggen van het vermoeden van Mertens (Odlyzko en te Riele, 1985)
- Het oplossen van diophantische vergelijkingen (o.a. De Weger, 1988)

6. INHOMOGENE SIMULTANE APPROXIMATIE

Dit probleem treedt bijvoorbeeld op als we willen weten na hoeveel jaar een aantal planeten, waarvan we de positie en constante hoeksnelheid kennen, ongeveer in één lijn met de zon zullen staan. Wiskundig komt het er op neer dat bij gegeven reële getallen $\alpha_1,\alpha_2,\ldots,\alpha_n$ en $\theta_1,\theta_2,\ldots,\theta_n$ een natuurlijk getal q gezocht wordt zó dat $\|q\alpha_j-\theta_j\|$ klein is voor $j=1,2,\ldots,n$.

OPDRACHT 10. a) Bewijs dat er voor $\alpha_1=\frac{1}{2}$, $\alpha_2=\frac{5}{8}$, $\theta_1=\frac{1}{2}$, $\theta_2=\frac{1}{2}$ geen natuurlijk getal q bestaat met

$$\|q\alpha_1-\theta_1\|<\frac{1}{10},\quad \|q\alpha_2-\theta_2\|<\frac{1}{10}.$$

b) Bewijs dat als de getallen $\alpha_1,\alpha_2,\ldots,\alpha_n$ lineair afhankelijk zijn over $\mathbb{Q}$ (d.w.z. dat er gehele getallen $m_1,m_2,\ldots,m_n$ bestaan, niet alle nul, zó dat $m_1\alpha_1+m_2\alpha_2+\cdots+m_n\alpha_n=0$), er getallen $\theta_1,\theta_2,\ldots,\theta_n$ en ϵ zijn zó dat

$$\max_{j=1,\ldots,n}\|q\alpha_j-\theta_j\|\geqslant\epsilon \quad \text{voor alle} \quad q\in\mathbb{N}.$$

Kronecker bewees dat inhomogene simultane benadering wel mogelijk is als $\alpha_1,\alpha_2,\ldots,\alpha_n$ lineair onafhankelijk zijn over $\mathbb{Q}$.

STELLING VAN KRONECKER. *Als voor alle gehele getallen $m_1,m_2,\ldots,m_n$, niet alle nul, geldt*

$$\|m_1\alpha_1+m_2\alpha_2+\cdots+m_n\alpha_n\|\neq 0$$

dan bestaat er een natuurlijk getal q zó dat

$$\|q\alpha_j-\theta_j\|<\epsilon \quad \textit{voor} \quad j=1,2,\ldots,n.$$

Een bovengrens voor q, alleen afhangend van ϵ en n, zoals bij de Stelling van Dirichlet, is echter niet te geven.

OPDRACHT 11. Bepaal bij gegeven getallen $\epsilon>0$ en $Q>0$ reële getallen α en θ zó dat $\|q\alpha-\theta\|<\epsilon$ wel een oplossing heeft met een natuurlijk getal q, maar geen oplossing q met $1\leqslant q\leqslant Q$.

In 1988 bewezen Kannan en Lovász de volgende kwantitatieve vorm van de Stelling van Kronecker:

Als voor alle gehele getallen $m_1,m_2,\ldots,m_n$, niet alle nul, geldt

$$Q\|m_1\alpha_1+m_2\alpha_2+\cdots+m_n\alpha_n\|+\epsilon\sum_{i=1}^{n}|m_i|\geqslant c_0n^2$$

dan bestaat er een natuurlijk getal $q\leqslant Q$ zó dat

$$\|q\alpha_j-\theta_j\|<\epsilon \quad \textit{voor} \quad j=1,2,\ldots,n.$$

Ze bewezen ook dat de bewering niet meer waar is als in het rechterlid c_0n^2

vervangen wordt door $\frac{1}{2}$. (De c_0 in de stelling is een constante waarvoor ik geen afschatting in de literatuur heb gevonden.)

Reeds in 1986 had Babai het roosterreductiealgoritme gebruikt om aan te tonen dat zo'n q dan ook echt te vinden is.

Als de conditie uit de stelling van Kannan en Lovász geldt, dan is in polynomiale tijd een natuurlijk getal $q \leqslant 4\sqrt{n}\,2^{n/2}Q$ *te vinden zó dat*

$$\|q\alpha_j - \theta_j\| < \epsilon \quad \textit{voor} \quad j = 1,2,\ldots,n.$$

In de praktijk blijkt dit praktisch even snel te gaan als homogene simultane benadering en ook hier toont het roosterreductiealgoritme zijn grote nut.

REFERENTIES

Achtergrondinformatie, oudere leerboeken:

J.W.S. CASSELS, An introduction to diophantine approximation, Cambridge Univ. Press, 1957.

G.H. HARDY & E.M. WRIGHT, An introduction to the theory of numbers, Oxford Press, 4 th. ed., 1960.

O. PERRON, Die Lehre von den Kettenbrüchen, Teubner, Leipzig, 1929.

H.M. STARK, An introduction to number theory, Markham, Chicago, 1970.

Meerdimensionale Kettingbreuken:

A.J. BRENTJES, Multi-dimensional continued fraction algorithms, Math. Centre Tract 145, Amsterdam, 1981.

Homogene simultane benaderingen:

A.K. LENSTRA, H.W. LENSTRA & L. LOVÁSZ, Math. Ann. 261 (1982) pp. 513-534.

Toepassingen:

M. GRÖTSCHEL, L. LOVÁSZ & A. SCHRIJVER, Geometric algorithms and combinatorial optimization, Springer Verlag, 1988.

R. KANNAN, Algorithmic geometry of numbers, Ann. Rev. Comput. Sci. 2 (1987) pp. 231-267.

Inhomogene simultane benaderingen:

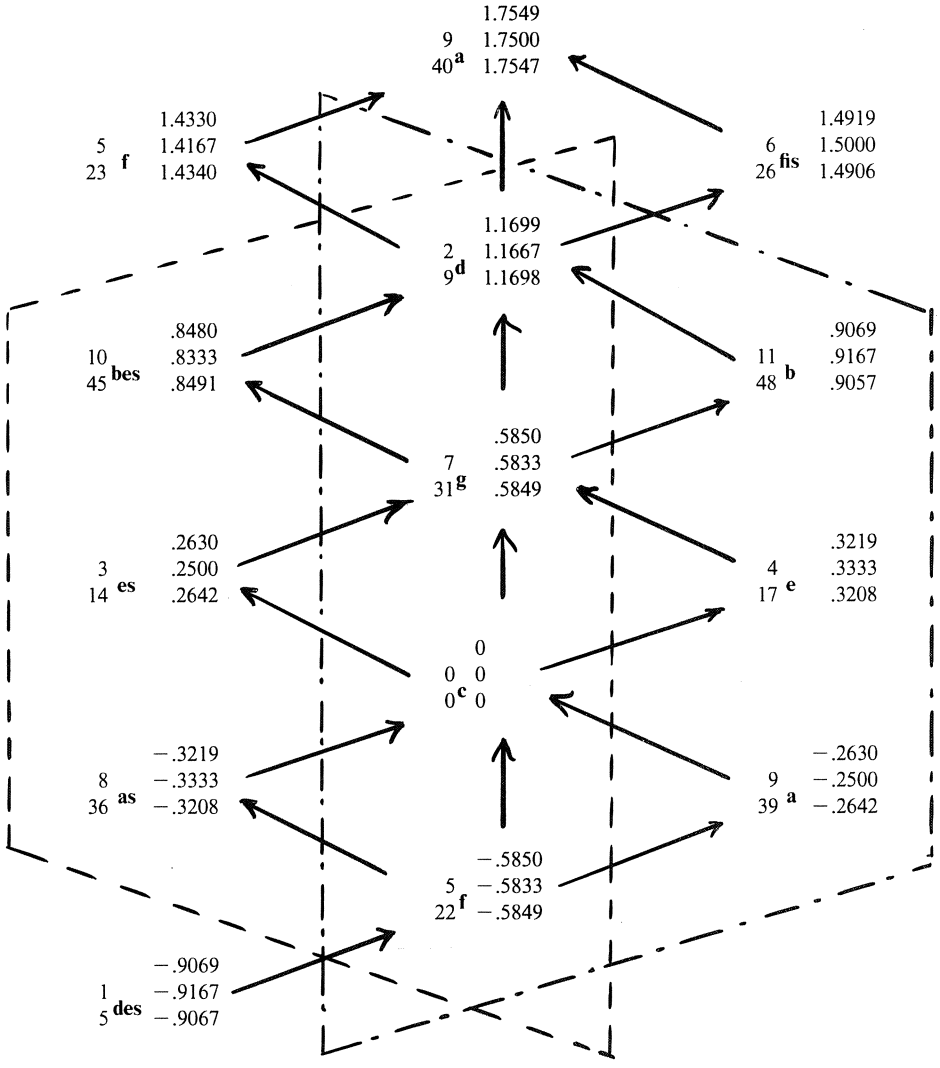
R. KANNAN & L. LOVÁSZ, Annals Math. 128 (1988) pp. 577-602.

L. BABAI, Combinatorica 6 (1986) pp. 1-13.

Toonsprongen: ↑ kwint hoger
↗ grote terts hoger
↖ kleine terts hoger

Toonfrequenties: logarithmische waarden met basis 2

	natuurtonen	12-toonstelsel	53-toonstelsel
↑	+0,5850	+0,5833	+0,5849
↗	+0,3219	+0,3333	+0,3208



Het getal links van de noot geeft aan de hoeveelste noot in het octaaf het betreft (uitgaande van $c = 0$), respectievelijk in het 12-toonstelsel en het 53-toonstelsel. De getallen rechts geven respectievelijk de logarithmische toonfrequenties volgens de natuurtoon, in het 12-toonstelsel en het 53-toonstelsel.

Modulair worteltrekken en fraudebestendige identiteitsdocumenten

J. van de Craats
Koninklijke Militaire Academie
Vakgroep Wiskunde en Operations Research
Postbus 90154
4800 RG Breda

Vrijwel iedereen beschikt tegenwoordig over een hele serie identificatiepapieren: paspoort, rijbewijs, bankpas, giropas, toegangsbewijzen, uitleenpasjes, credit cards. Allemaal kunnen ze vervalst worden, vaak met buitengewoon onplezierige gevolgen voor de rechtmatige eigenaar en de instantie die ze uitgeeft. De paspoortaffaire heeft aangetoond hoe moeilijk het is werkelijk fraudebestendige identiteitsdocumenten te maken. Giromaatpasjes met magneetstrip en pincode zijn evenmin honderd procent veilig. Een principiëel bezwaar van de meeste systemen is dat zodra je je met zo'n document bij een "tegenpartij" identificeert, je de ander (of iemand die meeluistert) informatie in handen geeft om een vals document te maken. Dat is gevaarlijk als je niet weet of je de tegenpartij kunt vertrouwen. Gegevens op paspoort en rijbewijs kunnen gecopiëerd worden. Magneetstripgegevens en pincodes kunnen worden afgetapt, en daarmee kan een malafide tegenpartij een valse kaart produceren en ongestraft je rekening plunderen.

Zero-knowledge proofs

De moderne chipkaarttechnologie, gecombineerd met de praktische onoplosbaarheid van bepaalde wiskundige problemen, maakt het mogelijk werkelijk fraudebestendige identificatiedocumenten te maken. Daarmee lijkt een waterdichte oplossing gevonden te zijn voor het "wachtwoordprobleem": hoe overtuig je iemand ervan dat je het juiste wachtwoord kent, zonder het wachtwoord zelf bekend te maken. De sleutel ligt in het begrip *zero-knowledge proof,* dat in 1985 geïntroduceerd werd door S. Goldwasser, S. Micali en C. Rackoff [4]. Zo'n zero-knowledge proof verloopt via een *protocol,* dat wil zeggen een voorschrift voor een vraag-en-antwoordspel tussen twee partijen, die we in het vervolg Anton en Vera zullen noemen. Anton wil iets *aantonen,* bijvoorbeeld dat hij iets weet of kent, of dat hij toegangsrecht heeft tot

bepaalde locaties, bepaalde gegevens, of, via een betaalautomaat, tot een bepaalde bankrekening. Vera moet *verifiëren* dat Antons aanspraken terecht zijn. Zij vertrouwt Anton niet: hij zou best een bedrieger kunnen zijn. Maar Anton vertrouwt Vera ook niet: hij is bang dat zij, of iemand anders die het protocol afluistert, zich later wederrechtelijk voor hem uit zal geven.

Wat te doen om uit dit dilemma te geraken? Dat lijkt een onoplosbaar probleem. Immers, hoe verifiëer je of Anton iets weet? Door het hem te vragen. Of door steekproeven te nemen als die kennis zeer omvangrijk is. Dat is ook de praktijk bij de meeste examens: je vraagt niet alles, maar kiest min of meer willekeurig wat onderwerpen uit. Maar bij zo'n examen wordt informatie overgedragen, en iemand die genoeg uitwerkingen van geslaagde kandidaten verzamelt, kent de stof op den duur ook op z'n duimpje.

Bij zero-knowledge proofs doet zich echter de paradoxale situatie voor dat de examinator de kandidaat na afloop een 10 moet geven, zonder dat hij zelf iets over de examenstof weet of te weten komt. In de oorspronkelijke opzet van GOLDWASSER, MICALI en RACKOFF heeft de "examenstof" betrekking op abstracte "talen". Het gaat daarbij om de vraag of bepaalde "woorden" W behoren tot een "taal" L. Anton overtuigt Vera ervan dat W tot L behoort zonder iets te onthullen over de manier waarop dat bewezen kan worden. Het enige waarvan Vera na afloop overtuigd is, is dat W tot L moet behoren, en dat Anton weet hoe hij dat kan bewijzen. In 1986 hebben O. GOLDREICH, S. MICALI en A. WIGDERSON [3] de "examenstof", dat wil zeggen de problemen waarvoor zero-knowledge proofs gegeven kunnen worden, uitgebreid tot een veel grotere klasse.

Om een eenvoudig voorbeeld te geven: bij een variant van het handelsreizigersprobleem gaat het er om bij een gegeven wegennet uit te zoeken of er een route is die alle steden aandoet en een totale lengte heeft die beneden een opgegeven bovengrens M blijft. Bij uitgebreide wegennetten kan dat voor bepaalde waarden van M een lastig probleem zijn. Stel nu dat Anton een oplossingsroute kent. Hij wil Vera daarvan overtuigen zonder die route te verraden. Dat kan via een zero-knowledge proof. Vera is na afloop overtuigd, maar over de betreffende route is zij niets te weten gekomen.

ZERO-KNOWLEDGE PROOFS OF KNOWLEDGE

In 1988 modificeerden U. FEIGE, A. FIAT en A. SHAMIR [2] deze techniek op zo'n manier dat Anton Vera nu niet overtuigt van de *waarheid* van een uitspraak ("er is een route met lengte kleiner dan M"), maar alleen maar van het feit *dat hij weet of die uitspraak waar is of niet.* In het zojuist genoemde voorbeeld was Vera na afloop van het "examen" overtuigd van het bestaan van een route met een totale lengte kleiner dan M. Maar het kan natuurlijk ook zo zijn dat er helemaal geen route korter dan M bestaat. Bij de nieuwe methode wordt ze er alleen maar van overtuigd dat Anton *weet* of er zo'n route bestaat. Maar verder komt ze helemaal niets te weten, zelfs niet of de route bestaat of niet.

PASJESSYSTEMEN

Paradoxale en intrigerende zaken, inderdaad, maar hebben ze ook praktisch nut? Jazeker: met zero-knowledge proofs is onder andere het wachtwoord-probleem oplosbaar, en de toepassingsmogelijkheden daarvan zijn legio. FEIGE, FIAT en SHAMIR gaven bijvoorbeeld aan hoe je met deze methode een pasjessysteem kunt opzetten dat voor honderd procent veilig is, althans zolang een bepaald wiskundig probleem praktisch onoplosbaar blijft. Bij dat systeem krijgt Anton, en elke andere gebruiker, een pasje dat voorzien is van een chip. Met zo'n pasje kan hij zich identificeren zonder dat Vera (of een spion) in staat is het pasje na te maken, in de eerste plaats omdat tijdens het identificatieprotocol geen andere informatie wordt overgedragen dan de boodschap "Dit is een geldig pasje", en in de tweede plaats omdat het genereren van geldige pasjes alleen door de bevoegde instantie kan gebeuren. Elk van die twee eigenschappen berust op de praktische onoplosbaarheid van hetzelfde wiskundige probleem: het ontbinden van grote getallen in priemfactoren.

Dank zij de moderne chipkaart-technologie is zo'n systeem praktisch goed uitvoerbaar. We zullen er hier een vereenvoudigde versie van presenteren (afkomstig van J. BUHLER [1]), en aandacht besteden aan de getaltheoretische achtergronden ervan.

DE CHIPKAART

Eerst iets over de chipkaart. Dat is een klein technisch wonder. Een goudkleurig schijfje ter grootte van een kwartje zit ingebakken in een plastic kaart met het formaat van een betaalpas. Het gouden schijfje bevat een chip waarin zich bijvoorbeeld een 8-bits microcomputer, een 128 bits RAM (werkgeheugen) en enige kilobytes ROM (read only memory) en EPROM (electronically programmable read only memory) kunnen bevinden. In die laatste geheugens kunnen bij fabricage en bij uitgifte van de kaart programma's en geheime gegevens worden opgeslagen die daarna niet meer gewijzigd kunnen worden. Alleen door de chip open te breken zou je de precieze inhoud van de geheugens dan nog kunnen trachten te achterhalen. Maar de chip kan zo geprogrammeerd zijn, dat hij bij zo'n aanval zichzelf vernietigt. Zomaar kopiëren van zo'n chipkaart, zoals dat bij magneetstripkaarten kan, is dus uitgesloten, en hetzelfde geldt voor knoeien met het geheime geheugen. Diefstal blijft natuurlijk wel een probleem, maar dat is op allerlei manieren op te lossen: een gecodeerde foto, handtekening, vingerafdruk, stemanalyse of DNA-patroon kan de koppeling tussen kaart en persoon tot stand brengen, maar in de praktijk zal een pincode van vier cijfers meestal voldoende waarborgen bieden. Juist doordat de kaart een computer bevat, kan hij mislukte pincodepogingen registreren, en zich na bijvoorbeeld drie van die pogingen ongeldig maken.

SNELLE ALGORITMEN

Het zal inmiddels duidelijk zijn dat Anton en Vera bij hun identificatieprotocol computers nodig hebben. Anton's computer zit in zijn chipkaart, en Vera's computer zit in een kastje. Als Anton zich wil identificeren, stopt hij z'n kaart in het kastje, waarna de beide computers gaan rekenen. Ze passen daarbij

bepaalde algoritmen toe, en daarom moeten we eerst iets zeggen over snelle en langzame algoritmen.

De rekentijd van een algoritme hangt meestal af van de lengte van de invoer. Een algoritme dat bijvoorbeeld twee gehele getallen met elkaar vermenigvuldigt, zal er langer over doen naarmate die getallen groter zijn. We zullen een algoritme *snel* noemen als de uitvoeringstijd begrensd wordt door een polynomiale functie van de *lengte* van de invoer. Als die invoer bestaat uit een natuurlijk getal n, gerepresenteerd in het tweetallig stelsel, dan wordt de lengte ervan gegeven door het getal

$$l = [\log_2 n] + 1 = [(1\mathrm{n}\, n)/(1\mathrm{n}\, 2)] + 1.$$

Een algoritme dat als invoer een vast aantal natuurlijke getallen heeft, is dus snel wanneer de rekentijd begrensd wordt door een macht van de logaritme van het grootste invoergetal. Er zijn snelle algoritmen voor de gebruikelijke rekenoperaties: optellen, aftrekken, vermenigvuldigen, machtsverheffen en delen met rest. Ook het bekende algoritme van Euclides waarmee men de grootste gemene deler (ggd) van twee natuurlijke getallen bepaalt, is een snel algoritme. In het vervolg zullen we vaak *modulair* rekenen met een natuurlijk getal M als modulus. Belangrijk daarbij is het feit dat er ook snelle algoritmen bestaan voor modulair optellen, aftrekken, vermenigvuldigen, machtsverheffen en delen (voor zover het laatste gedefiniëerd is).

Niet alle algoritmen zijn snel. Het bovengenoemde handelsreizigersprobleem kan bijvoorbeeld algoritmisch opgelost worden door gewoon systematisch alle mogelijke routes te proberen. De rekentijd die dat kost neemt exponentiëel toe met het aantal steden in het net, zoals men gemakkelijk kan bewijzen. Dat algoritme is dus niet snel in de boven gedefiniëerde zin. Inderdaad is het algoritme zelfs voor betrekkelijk kleine aantallen steden al volstrekt onuitvoerbaar door de enorme hoeveelheid rekentijd die het vergt.

Primaliteitstesten en factoriseren

Voor sommige problemen zijn er wel algoritmen bekend, maar geen snelle algoritmen. Het handelsreizigersprobleem is daar een voorbeeld van. Een ander voorbeeld is het *factorisatieprobleem*: ontbind een gegeven (groot) natuurlijk getal n in z'n priemfactoren. Het algoritme gaat in grote trekken als volgt: kijk of n een priemgetal is. Zo ja, dan ben je klaar, zo nee, zoek dan een ontbinding in twee factoren (groter dan 1). Kijk of die factoren priem zijn, enzovoort. Na eindig veel stappen heb je n volledig gefactoriseerd. Het proces bestaat blijkbaar uit twee soorten stappen:

1. testen op primaliteit
2. zoeken van factoren.

Dat zijn wezenlijk verschillende stappen, want er zijn primaliteitstesten die vertellen dat n *geen* priemgetal is zonder dat ze factoren van n leveren. Veel primaliteitstesten bestaan uit verschillende rondes waarbij n door de mand kan vallen als n samengesteld is: als n zo'n testronde niet doorstaat, is n zeker geen priemgetal; als n de ronde wel passeert, neemt de kans dat n priem is, toe. Met zulke *probabilistische* primaliteitstesten kan men in korte tijd met vrijwel

honderd procent zekerheid vaststellen of n een priemgetal is of niet. Er zijn ook deterministische primaliteitstesten die volledige zekerheid geven, maar die werken niet zo snel. De huidige stand van zaken is dat men van willekeurige getallen van 300 cijfers in een paar minuten kan vaststellen of ze priem zijn of niet.

Factoriseren van samengestelde getallen lijkt een veel moeilijker probleem. Snelle factorisatie-algoritmen, probabilistisch of deterministisch, zijn niet bekend. Thans ligt de grens van het bereikbare zo ongeveer bij getallen van 100 cijfers. In oktober 1988 werd door de gezamenlijke inspanning van 400 computers uit 12 onderzoekscentra over de gehele wereld een "moeilijk" getal van 100 cijfers, waarvan bekend was dat het geen priemgetal is, ontbonden in z'n priemfactoren. Het ging om het getal

$$(11^{104} + 1)/(11^8 + 1).$$

Dit bleek het product te zijn van een getal van 60 en een getal van 41 cijfers. Het project stond onder leiding van onze landgenoot Arjen Lenstra (thans werkzaam aan de Universiteit van Chicago) en Mark Manasse van Digital Equipment Corporation in Palo Alto (Californië); de benodigde rekentijd bedroeg bijna een maand.

Geheim

Dit alles betekent dat als iemand twee priemgetallen P en Q bepaalt van ongeveer 100 cijfers (dat gaat snel) en hun product $M = P \cdot Q$ berekent en bekend maakt (M is dan een getal van ongeveer 200 cijfers), maar P en Q zelf geheim houdt, hij een geheim bezit dat niemand hem op slinkse wijze kan ontfutselen. Dit gegeven is een van de pijlers van veel cryptografische systemen; onder andere het bekende RSA public key cryptosystem dat in 1978 ontwikkeld is door R.L. Rivest, A. Shamir en L.M. Adleman [6] ("RSA" komt van de initialen van hun achternamen). Ook het identificatieprotocol van Feige, Fiat en Shamir berust op de praktische onmogelijkheid om M te ontbinden als P en Q geheim gehouden worden.

Modulair worteltrekken

Twee gehele getallen a en b heten *congruent modulo m* wanneer hun verschil een geheel veelvoud is van m. Notatie:

$$a \equiv b \bmod m.$$

Het getal m heet de *modulus*, en in het vervolg nemen we steeds aan dat m een geheel getal groter dan 1 is. Bij een gegeven modulus m is congruentie een equivalentierelatie; er zijn precies m equivalentieklassen, we noemen ze *restklassen modulo m*. De verzameling van restklassen wordt aangegeven met $\mathbb{Z}/m\mathbb{Z}$. De m getallen $0, 1, 2, \ldots, m-1$ zitten in verschillende klassen; ze vormen een volledig stel representanten. In het vervolgd zullen we ze vaak met hun restklasse identificeren. De elementaire rekenkundige bewerkingen met gehele getallen: optellen, aftrekken, vermenigvuldigen, machtsverheffen, kunnen we direct overplanten naar $\mathbb{Z}/m\mathbb{Z}$. Op deze wijze wordt *modulair rekenen*

in $\mathbb{Z}/m\mathbb{Z}$ gedefiniëerd. Nemen we bijvoorbeeld $m=10$, dan geldt

$$5+9=4$$

$$5-9=6$$

$$5\cdot 9=5$$

$$5^9=5.$$

Delingen gaan niet altijd op. Enerzijds is

$$5/9=5 \text{ (want } 5=5\cdot 9)$$

maar de deling 9/5 kan niet uitgevoerd worden omdat er geen restklasse x is waarvoor geldt dat $x\cdot 5=9$.
Kwadrateren is altijd mogelijk: de kwadraten van 0, 1, 2, ... , 9 zijn resp. 0, 1, 4, 9, 6, 5, 6, 9, 4, 1.
Worteltrekken daarentegen lukt niet altijd: de vergelijking in x

$$x^2=a$$

heeft modulo 10 alleen oplossingen als a een van de genoemde kwadraten is, en soms is er dan 1 oplossing (als $a=0$ of 5), en soms 2 (in alle andere gevallen).

REKENEN MODULO EEN PRIEMGETAL

De situatie is zeer overzichtelijk als de modulus een priemgetal $p>2$ is. Dan gelden namelijk de volgende eigenschappen:

E-1. Elke deling

$$x=a/b$$

met $b\neq 0$ heeft precies één oplossing x.

E-2. Er is een snel algoritme om delingen uit te voeren.

E-3. Er zijn precies $(p-1)/2$ kwadraten ongelijk aan 0.

E-4. Elk kwadraat ongelijk aan 0 heeft precies twee wortels; als x de ene wortel is, dan is $p-x$ de andere.

E-5. Er is een snel algoritme om te bepalen of een getal een kwadraat is of niet.

E-6. Er is een snel algoritme om de wortels van een kwadraat te bepalen.

REKENEN MODULO $M=P\cdot Q$

In het vervolg nemen we aan dat P en Q twee verschillende zeer grote priemgetallen zijn (om de gedachten te bepalen: ongeveer 100 cijfers elk), en dat $M=P\cdot Q$.
Voor rekenen modulo M geldt:

E-7. Als b geen geheel veelvoud is van P of Q dan heeft elke deling

$$x=a/b$$

precies één oplossing x.

E-8. Er is een snel algoritme om delingen uit te voeren.

E-9. Als $a \neq 0$ een kwadraat is, dan heeft a twee of vier wortels; het aantal wortels is vier d.e.s.d. als ggd$(a,M) = 1$.

E-10. Als men de priemfactoren P en Q van M kent, kan men met een snel algoritme bepalen of een getal een kwadraat is of niet.

E-11. Als men de priemfactoren P en Q van M kent, kan men met een snel algoritme de wortels van willekeurige kwadraten bepalen.

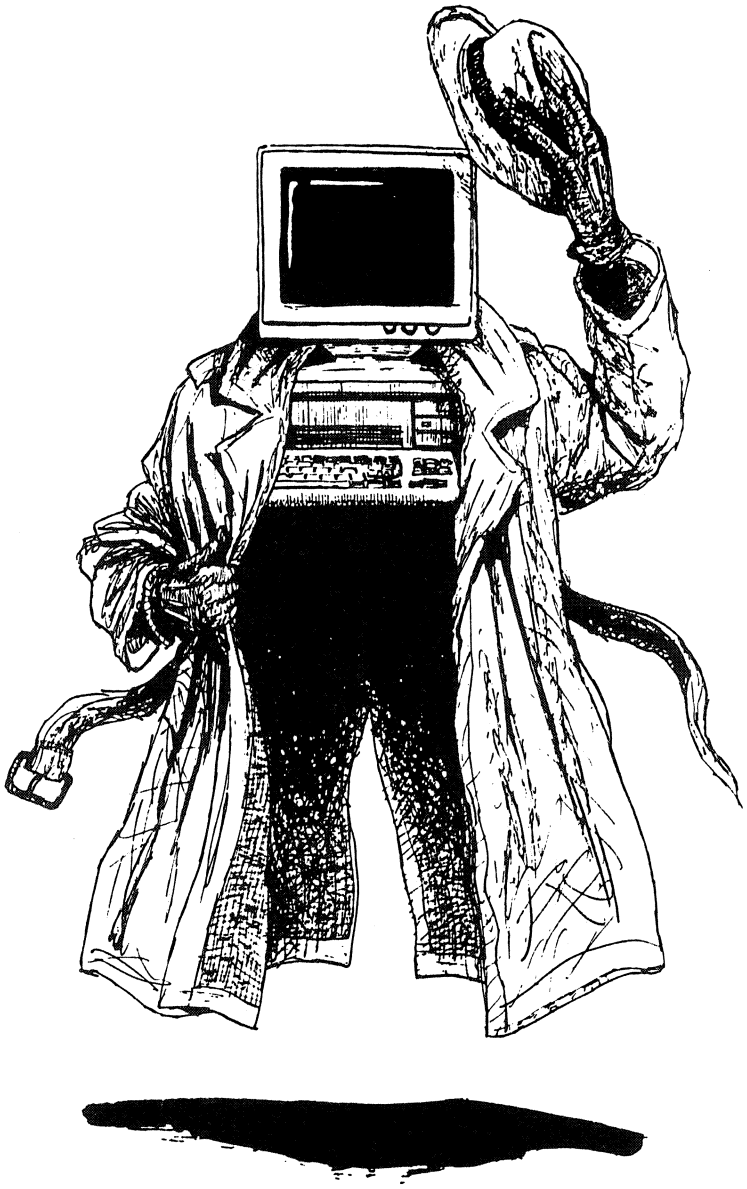
E-12. Als men de priemfactoren P en Q van M *niet* kent en het bepalen van P en Q is praktisch onmogelijk, dan is ook het bepalen van wortels van een willekeurig kwadraat a praktisch onmogelijk.

Bewijzen van het bovenstaande zijn o.a. te vinden in het boek van N. KOBLITZ [5]. De bewijzen van E-1 t.e.m. E-4 en E-7 t.e.m. E-9 zijn heel elementair; de andere bewijzen vereisen wat meer voorkennis en techniek.

KAARTUITGIFTE

Na deze getaltheoretische voorbereidingen kunnen we beginnen met het door BUHLER vereenvoudigde identificatiesysteem van FEIGE, FIAT en SHAMIR. We nemen aan dat er een door alle partijen te vertrouwen hoofdkwartier (HQ) is dat het systeem beheert en de chipkaarten uitgeeft. Denk bijvoorbeeld aan het hoofdkantoor van een bank of een credit-card-organisatie, of aan een ministerie. Het HQ laat z'n computer twee grote priemgetallen P en Q bepalen van ongeveer 100 cijfers elk. De priemgetallen P en Q worden geheim gehouden, maar het product $M = P \cdot Q$ wordt bekend gemaakt. Omdat M zo groot is, kan verder niemand de priemfactoren P and Q te weten komen. Alle gebruikers gaan werken met de modulus M. De klanten kunnen nu komen.

Stel dat Anton zich meldt met het verzoek om een chipkaart te ontvangen. Hij vult een aanvraagformulier in met daarop alle benodigde gegevens (naam, leeftijd, adres, geboortedatum, burgerlijke staat, kredietwaardigheid, enz.). Na controle worden die gegevens in een rij getallen omgezet. Om Anton's privacy te beschermen, kan de rij ook nog vercijferd worden, bijvoorbeeld met behulp van DES, een bekend vercijferalgoritme. Met willekeurige getallen wordt de rij vervolgens aangevuld tot een groot getal I met net zo veel cijfers als M. Hierbij zorgt HQ ervoor dat het getal I een kwadraat modulo M wordt. Dat kan met een snel algoritme op een betrekkelijk eenvoudige wijze gebeuren, juist omdat HQ de priemfactoren P en Q kent (eigenschap E-10). Het getal I is Anton's *openbare identificatienummer.* Hij hoeft het niet geheim te houden, integendeel, alle I's van alle deelnemers mogen worden gepubliceerd. Het getal I wordt ook in het geheugen van Anton's chipkaart geplaatst. Maar HQ zet ook een ander getal in het geheime deel van het geheugen, namelijk een *wortel* i van I, dat wil zeggen een getal i dat gekwadrateerd modulo M precies I oplevert. HQ kan zo'n wortel bepalen met behulp van P en Q (eigenschap E-11). Anton krijgt die geheime priemgetallen niet te zien. Alleen het resultaat i



van het worteltrekken is in zijn chip gezet. Het getal i is Anton's *geheime identificatienummer.* De rol van HQ is nu uitgespeeld: Anton kan zijn kaart gaan gebruiken.

Het gebruik van de kaart

Hoe gaat dat in z'n werk? Als Anton zich ergens wil identificeren, presenteert hij de kaart. Vera, die de identiteit van Anton moet verifiëren, stopt de kaart in haar computer. Zij kent de modulus M, maar het is nergens voor nodig dat haar computer in verbinding staat met de centrale computer van HQ. De onafhankelijkheid van grote computernetwerken is een van de grote voordelen van dit systeem. Alle berekeningen kan Vera zelfstandig uitvoeren. Anton heeft Vera via zijn kaart zijn openbare identificatienummer I gegeven. Vera moet verifiëren dat Anton's kaart in het ontoegankelijke geheugendeel een getal i bevat waarvoor geldt dat $i^2 \equiv I \bmod M$. Maar als i bekend wordt, kan Vera de kaart van Anton vervalsen. Daarom doen ze het anders. Een groot aantal malen (bijvoorbeeld honderd keer) herhalen ze het volgende vraag-en-antwoordspel:

1. Anton kiest een willekeurig getal x en bepaalt het kwadraat $X \equiv x^2 \bmod M$. Hij deelt dat kwadraat X aan Vera mede.
2. Vera mag één van de volgende vragen stellen (maar niet beide!):
   a. Wat is x?
   b. Wat is $x \cdot i$?
   Anton beantwoordt de gestelde vraag.
3. Vera verifiëert Anton's antwoord door in geval (a) te controleren of $x^2 \equiv X$, en in geval (b) of $(x \cdot i)^2 \equiv X \cdot I$, alles mod M.

In werkelijkheid wordt het hele spel natuurlijk zelfstandig door de chip van Anton en de computer van Vera gespeeld. Het geheel duurt slechts een paar seconden.

Bedrieger

Stel dat Anton een bedrieger is die i niet kent. Hoe groot is dan de kans dat hij zo'n test doorstaat? Hij kan gokken welke keuze Vera gaat doen. Gokt hij op (a), dan kan hij in stap 1 de normale procedure kiezen. Als Vera inderdaad (a) kiest, zit hij goed. Verwacht hij dat Vera (b) kiest, dan kan hij bij stap 1 een getal y kiezen, het kwadraat $Y \equiv y^2 \bmod M$ berekenen, en dan aan Vera het quotient $X \equiv Y/I$ mededelen. Kiest Vera inderdaad vraag (b), dan zit hij goed als hij het antwoord y geeft, want Vera verifiëert dan dat $y^2 \equiv Y \equiv X \cdot I$. Maar in beide gevallen valt hij door de mand als Vera de andere vraag stelt. Zijn overlevingskans bij één ronde is dus 1 op 2. De overlevingskans bij *honderd* rondes is echter slechts 1 op twee-tot-de-honderdste! Vera hoeft dus niet bang te zijn dat Anton een bedrieger is als hij alle tests doorstaat. Zij verklaart Anton's identiteitskaart dan geldig.

Maar weet ze na afloop iets over Anton's geheime nummer i? De keren dat ze vraag (a) koos, speelde i helemaal geen rol, en de keren dat ze vraag (b)

koos, was i veilig verpakt in het produkt $x \cdot i$; omdat ze x niet kende, kon ze i ook niet achterhalen. Voor Anton is het van groot belang de keuzen van x op een onvoorspelbare manier uit te voeren: alleen in dat geval zijn de getallen $x \cdot i$ vanuit Vera's standpunt bezien volstrekt willekeurige getallen, zodat ze niets over i te weten kan komen. In het extreme geval dat hij zo dom is om Vera twee maal dezelfde x te presenteren, kan Vera door beide vragen te stellen zowel x als $x \cdot i$ te weten komen, en dan kent ze na deling ook i.

PRAKTISCHE BRUIKBAARHEID

Het bovenstaande geeft in grote lijnen het protocol weer van een zero-knowledge proof of identity. Door kleine modificaties kan men de snelheid van de procedure nog aanzienlijk verhogen.

Hoe bruikbaar is zo'n systeem in de praktijk? Chipkaarten zijn duurder dan magneetstrippasjes, maar de kosten vormen geen onoverkomelijk probleem. Bij massaal gebruik zullen die kosten ook sterk dalen. Wel is het nodig dat overal waar met deze systemen gewerkt wordt verificatiecomputertjes aanwezig zijn. Maar die hoeven slechts een simpele rekenchip te bevatten; verbindingen met een centrale computer en grote geheugencapaciteiten zijn niet vereist. Grote kosten zijn daar dus niet aan verbonden. Het enige grote gevaar dat de methode bedreigt komt van de wiskunde zelf. Mischien lukt het slimme wiskundigen om snelle ontbindingsalgoritmen te ontwerpen. Dan stort de veiligheid van het systeem in elkaar, want kun je M in z'n priemfactoren P en Q ontbinden, dan wordt worteltrekken modulo M een fluitje van een cent. Als dat gebeurt, zijn er echter nog allerlei andere wiskundige problemen voorhanden die voor deze zelfde cryptografische doeleinden gebruikt kunnen worden. Er zal waarschijnlijk steeds een rivaliteit blijven bestaan tussen de wiskundigen die nieuwe systemen ontwerpen en de wiskundigen die ze zullen trachten te kraken.

LAATSTE NIEUWS (JUNI 1990):

Inmiddels hebben Lenstra en Manasse een nog veel groter "moeilijk" getal ontbonden, namelijk het negende *Fermat-getal*

$$F_9 = 2^{(2^9)} + 1.$$

Van dit getal van 155 cijfers was bekend dat het deelbaar is door het priemgetal 2424833, maar van de overblijvende factor van 148 cijfers wist men alleen dat het geen priemgetal is. In samenwerking met honderden werkstations over de gehele wereld verspreid, zijn binnen twee maanden de priemfactoren gevonden: een priemgetal van 49 cijfers en een priemgetal van 99 cijfers

7455602825647884208337395736200454918783366342657

en

7416400626275308015247871419019374740599407810975190239058213 16 \

1444157595047050080928187116939407 37.

Hoewel bij de ontbinding gebruik gemaakt is van de speciale structuur van het Fermat-getal, meent men dat cryptosystemen die gebaseerd zijn op moduli tot 512 bits (getallen van 155 decimale cijfers) thans niet meer als absoluut veilig beschouwd kunnen worden.

LITERATUUR

1. J. BUHLER (1986): Zero-Knowledge Proofs, Focus - The Newsletter of the M.A.A., vol 6, nummer 5, p. 1, 6, 7.
2. U. FEIGE, A. FIAT, A. SHAMIR (1988): Zero-Knowledge Proofs of Identity, Journal of Cryptology 1, pp. 77-94.
3. O. GOLDREICH, S. MICALI, A. WIGDERSON (1986): Proofs that Yield Nothing but Their Validity and a Methodology of Cryptographic Protocol Design, Proceedings of FOCS, pp. 174-187.
4. S. GOLDWASSER, S. MICALI, C. RACKOFF (1985): Knowledge complexity of Interactive Proof Systems, Proceedings of STOC, pp. 291-304.
5. N. KOBLITZ (1987): A course in Number Theory and Cryptography, Springer Verlag, New York, etc., 208 p.
6. R.L. RIVEST, A. SHAMIR, L.M. ADLEMAN (1978): A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21, pp. 120-126.

OEFENOPGAVEN

1. Toon aan dat $N=(11^{104}+1)/(11^8+1)$ een geheel getal is.

2. a. Bereken $d=\text{ggd}(a,b)$ voor $a=21890$, $b=47760$.
   b. Schrijf d in de vorm $d=k\cdot a+l\cdot b$ met $k,l\in\mathbb{Z}$.

3. Bewijs: als $\text{ggd}(a,m)=1$ dan is er precies één b met $0\leqslant b<m$ en $a\cdot b\equiv 1 \bmod m$.

4. a. Bereken x met $0\leqslant x<1990$ met $x\cdot 7\equiv 1 \bmod 1990$.
   b. Bereken x met $0\leqslant x<1990$ met $x\cdot 7\equiv 4 \bmod 1990$.

5. a. Geef een lijst van alle kwadraten modulo 37.
   b. Geef een lijst van alle kwadraten modulo 35; geef daarbij aan welke kwadraten 2, en welke 4 wortels hebben.

6. Stel dat a en b gegeven gehele getallen zijn. Bewijs dat er precies één geheel getal x met $0\leqslant x<M$ is waarvoor geldt

$$x\equiv a \bmod P \text{ en } x\equiv b \bmod Q.$$

(Dit is een bijzonder geval van de zg. *Chinese reststelling*.)
Bewijs ook dat x berekend kan worden met een snel algoritme.

7. Bewijs de eigenschappen E-3 en E-4.

8. Bewijs eigenschap E-9.

9. a. Toon aan dat het aantal kwadraten modulo M met twee wortels gelijk is aan $P+Q-2$.

   b. Toon aan dat het aantal kwadraten modulo M met vier wortels gelijk is aan $(P-1)(Q-1)/4$.

   Geef een schatting voor de verhouding tussen de beide aantallen als P en Q beide getallen zijn van 100 cijfers.

10. Bewijs E-11 onder gebruikmaking van E-6.

11. Waarom is het belangrijk dat in het behandelde identificatiesysteem het openbare identificatienummer I van Anton echte persoonsgebonden gegevens bevat en niet zo maar een willekeurig getal kleiner dan M is?

12. Stel Anton kent twee getallen a,b met $a \not\equiv \pm b \bmod M$ en $a^2 \equiv b^2 \bmod M$. Laat zien hoe hij dan op een snelle manier P en Q kan berekenen.

13. Ciska zegt een snel algoritme te hebben waarmee ze van willekeurige kwadraten modulo M één wortel kan berekenen. Laat zien hoe ze daarmee op een snelle probabilistische manier de ontbinding $M=P\cdot Q$ kan berekenen.

14. Anton beweert de ontbinding $M=P\cdot Q$ te kennen. Hij wil Vera daarvan overtuigen zonder P en Q prijs te geven. Vera stelt het volgende voor:
    Zij stuurt Anton 100 verschillende random getallen kleiner dan M. Als Anton van minstens 20 van die getallen een wortel kan produceren, gelooft ze hem.

    a. Heeft Vera gelijk als ze Anton na zo'n test gelooft?

    b. Is het voor Anton verstandig op het voorstel in te gaan?

(Telefonisch tossen.) Anton en Ciska staan via een datalijn met elkaar in verbinding. Ze hebben een rekening gekregen voor een gezamenlijk etentje, en besluiten te tossen wie er betalen moet. Omdat ze elkaar niet kunnen zien, kunnen ze niet op de gebruikelijke wijze een muntje opgooien. Daarom doen ze het volgende:
Ciska kiest twee priemgetallen p en q van 100 cijfers en zendt Anton het product $m = p \cdot q$. Anton kiest een groot natuurlijk getal a kleiner dan m en zendt Ciska het getal b kleiner dan m waarvoor geldt dat $b \equiv a^2 \bmod m$. Ciska berekent (met behulp van p en q) de wortels van b, en zendt Anton één van die wortels. Zij zegt te zullen betalen als Anton haar nu de ontbinding $m = p \cdot q$ kan mededelen. Kan hij dat niet, dan moet hij betalen.

Is dit een eerlijke procedure?

De priemtoets van Lucas

H.-J.A. Duparc
Insulindeweg 26
2612 EM Delft

1. Inleiding

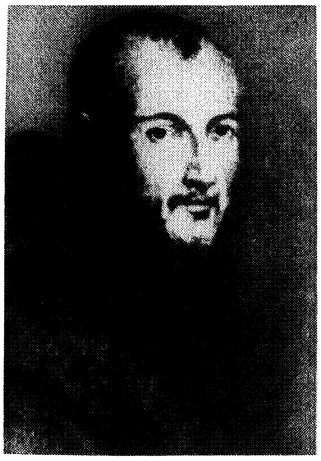
Sinds de dagen van Euclides (of al langer?) is bekend dat er oneindig veel priemgetallen bestaan. Het daarvan door Euclides gegeven bewijs heeft echter een (overigens niet door alle wiskundigen gevoeld) nadeel: het is niet constructief. Men weet wel dat er bij elk bekend priemgetal een groter priemgetal bestaat maar men beschikt niet over een bruikbare methode om het eerstvolgende priemgetal te vinden. En ook met de moderne rekenapparatuur gelukt dat (nog steeds) niet.

Een analoog (hier niet verder te behandelen) probleem doet zich voor bij de vraag naar het ontbinden in priemfactoren van grote getallen.

In verschillende gebieden van de toegepaste wiskunde blijkt men de laatste jaren duidelijk de behoefte te hebben aan grote priemgetallen. Geregeld leest men zelfs in de dagbladpers dat er een nieuwe recordhouder is gevonden; waarmee men dan eventueel zijn voordeel kan doen. Een en ander is te danken aan twee zaken: aan een ruim een eeuw geleden door E. Lucas gevonden stelling over bepaalde priemgetallen en aan de komst van moderner steeds sneller werkende rekenapparatuur. Het prettige feit doet zich daarbij voor dat die stelling van Lucas zich bijzonder goed leent voor verwerking met rekentuig.

Lucas beschouwde getallen van het type $M_s = 2^s - 1$, ook wel getallen van Mersenne genoemd. De kracht van zijn stelling ligt daarin dat die een nodige en voldoende voorwaarde geeft voor het ondeelbaar zijn van zo'n getal. Nu is elke lezer wel in staat een nodige voorwaarde voor het ondeelbaar zijn van zo'n getal M_s te geven; immers het getal s zal daartoe zelf ondeelbaar moeten zijn. Maar helaas die voorwaarde is niet voldoende. Euler leerde ons al dat het getal M_{11} samengesteld is.

Opgave 1. Ga dit na.



M. Mersenne
(1588 - 1648)

En bij dat ene voorbeeld blijft het niet.

OPGAVE 2. Bepaal nog meer dergelijke tegenvoorbeelden.

De stelling van Lucas legt verband tussen getallen van Mersenne en elementen van de (geassocïerde) rij van Fibonacci.

Ter verduidelijking, de (gewone) rij $\{u_n\}$ van Fibonacci is door de inductieformule

$$u_{n+2}=u_{n+1}+u_n\ , \quad (n\in\mathbb{N})$$

en de beginvoorwaarden $u_0=0$, $u_1=1$ bepaald. De geassocïeerde rij $\{v_n\}$ voldoet aan dezelfde inductieformule maar heeft als beginvoorwaarden $v_0=2$, $v_1=1$.

Zijn α en β de wortels van de (verwante) vierkantsvergelijking

$$x^2-x-1=0$$

dan valt (bijvoorbeeld met volledige inductie) te bewijzen dat

$$u_n=\frac{\alpha^n-\beta^n}{\alpha-\beta};\quad v_n=\alpha^n+\beta^n.$$

OPGAVE 3. Ga dit na.

Voorts gelden de verdubbelingsformules

$$u_{2n}=u_nv_n;\quad v_{2n}=v_n^2-2(-1)^n.$$

OPGAVE 4. Bewijs deze formules.

Deze verdubbelingsformules vertonen een zekere analogie met die van sin x en cos x, en dat is geen wonder.

De stelling van Lucas luidt nu als volgt:

Een getal $M_s=2^s-1$ met $s\equiv 3 \pmod 4$ is dan en slechts dan ondeelbaar als het zelf deelbaar is op het element $v_{2^{s-1}}$ van de geassocïerde rij van Fibonacci.

Wij geven twee simpele voorbeelden.

Enerzijds is $M_3=2^3-1=7$ deelbaar op $v_4=7$, anderzijds is $M_{11}=2^{11}-1=2047$ niet deelbaar op $v_{2^{10}}=v_{1024}$.

OPGAVE 5. Ga dit laatste na onder gebruikmaking van de verdubbelingsformule voor de v-rij.

De stelling van Lucas heeft het nadeel dat deze slechts betrekking heeft op getallen $M_s=2^s-1$ met $s\equiv 3 \pmod 4$. Het is daarom beter met een iets andere rij te werken, waarbij men dan uitsluitsel krijgt over het ondeelbaar zijn van M_s voor alle oneven s. Dit wordt in het volgende hoofdstuk gedaan.

2. INLEIDENDE EIGENSCHAPPEN VAN EEN BEPAALDE RECURRENTE RIJ

In het vervolg beschouwen we de recurrente rij $\{u_n\}$ die is gedefiniëerd door

$$u_{n+2}=4\,u_{n+1}-u_n\ ,\quad (n\in\mathbb{N})$$

met wederom de beginvoorwaardem $u_0=0$ en $u_1=1$ en verder de geassociëerde rij $\{v_n\}$ die voldoet aan dezelfde recurrente relatie en aan de beginvoorwaarden $v_0=2$, $v_1=4$. De voor deze rij gemodificeerde stelling van Lucas luidt als volgt:

Een getal $M_s=2^s-1$ met oneven s is dan en slechts dan ondeelbaar als het deelbaar is op het element $v_{2^{s-2}}$ van de zoëven gedefiniëerde v-rij.

Eerst gaan wij voor de hier gedefiniëerde rijen enige hulpeigenschappen afleiden. Daarbij maken we gebruik van de wortels $\alpha=2+\sqrt{3}$ en $\beta=2-\sqrt{3}$ van de (verwante) vierkantsvergelijking

$$x^2-4x+1=0.$$

Hierbij gelden wederom de formules

$$u_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}\ \text{en}\ v_n=\alpha^n+\beta^n.$$

OPGAVE 6. Bewijs deze formules.

OPGAVE 7. Bewijs de verdubbelingsformules

$$u_{2n}=u_n v_n\ \text{en}\ v_{2n}=v_n^2-2.$$

Verder geldt voor het getal α de hieronder te gebuiken formule

$$(\alpha-2)^n\ =\ 3^{\frac{1}{2}n}.$$

Nu worden twee gevallen onderscheiden.

1° : Laat p een priemgetal zijn en laat 3 kwadraatrest mod p zijn.

Dan heeft men successievelijk

$$3^{\frac{1}{2}(p-1)}\equiv 1 \pmod p$$

$$(\alpha-2)^{p-1}\equiv 1 \pmod p$$

$$\alpha^p-2^p\equiv(\alpha-2)^p\equiv\alpha-2 \pmod p$$

$$\alpha^p\equiv\alpha \pmod p$$

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

Evenzo bewijst men

$$\beta^{p-1} \equiv 1 \pmod{p}$$

dus

$$u_{p-1} = \frac{\alpha^{p-1} - \beta^{p-1}}{\alpha - \beta} \equiv 0 \pmod{p}.$$

Dit resultaat, hier voor de volledigheid behandeld, speelt geen rol in het vervolg.

2° : Laat p een priemgetal zijn en 3 niet-rest mod p. Dan heeft men successievelijk

$$3^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$$

$$(\alpha-2)^{p-1} \equiv -1 \pmod{p}$$

$$\alpha^p - 2^p \equiv (\alpha-2)^p \equiv 2-\alpha \pmod{p}$$

$$\alpha^p \equiv 4-\alpha = \beta \pmod{p}$$

$$\alpha^{p+1} \equiv \alpha\beta = 1 \pmod{p}. \tag{1}$$

Evenzo heeft men

$$\beta^{p+1} \equiv 1 \pmod{p}$$

dus

$$u_{p+1} = \frac{\alpha^{p+1} - \beta^{p+1}}{\alpha - \beta} \equiv 0 \pmod{p}.$$

Verder heeft men successievelijk (op grond vam $2^{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod{p}$)

$$(\alpha-1)^2 = 2\alpha$$

$$(\alpha-1)^{p-1} = 2^{\frac{1}{2}(p-1)}\,\alpha^{\frac{1}{2}(p-1)} \equiv \pm\,\alpha^{\frac{1}{2}(p-1)} \pmod{p}$$

$$\beta - 1 \equiv \alpha^p - 1 \equiv (\alpha-1)^p \equiv \pm\,\alpha^{\frac{1}{2}(p-1)}\,(\alpha-1) \pmod{p}$$

$$\alpha^{\frac{1}{2}(p-1)} \equiv \pm\frac{\beta-1}{\alpha-1} = \pm\frac{(\beta-1)^2}{(\alpha-1)(\beta-1)}$$

$$= \pm\frac{\beta^2-2\beta+1}{1-4+1} = \pm\frac{2\beta}{-2} = \mp\beta \pmod{p}$$

$$\alpha^{\frac{1}{2}(p+1)} \equiv \mp\,\alpha\beta = \mp 1 \pmod{p}$$

waaruit andermaal de formule (1) is af te leiden. Evenzo heeft men

$$\beta^{\frac{1}{2}(p+1)} \equiv \mp 1 \pmod{p}$$

dus

$$u_{\frac{1}{2}(p+1)} = \frac{\alpha^{\frac{1}{2}(p+1)} - \beta^{\frac{1}{2}(p+1)}}{\alpha - \beta} \equiv 0 \pmod{p}$$

en

$$v_{\frac{1}{2}(p+1)} = \alpha^{\frac{1}{2}(p+1)} + \beta^{\frac{1}{2}(p+1)} \equiv \mp 2 \pmod{p}.$$

Voor $p \equiv -1 \pmod 8$, waarbij de bovenste tekens in bovenstaande formules gelden, vindt men dan

$$v^2_{\frac{1}{4}(p+1)} - 2 \equiv v_{\frac{1}{2}(p+1)} \equiv -2 \pmod{p}$$

dus

$$v_{\frac{1}{4}(p+1)} \equiv 0 \pmod{p}.$$

OPGAVE 6. Wat krijgt men in het geval $p \equiv 3 \pmod 8$?

3. BEWIJS VAN DE GEMODIFICEERDE STELLING VAN LUCAS

Onderstel nu dat het getal $M_s = 2^s - 1$ ondeelbaar is. Voor dit getal $p = M_s$ geldt dan: s is oneven, dus $p \equiv -1 \pmod 8$ en verder $p = 2^s - 1 \equiv 2 - 1 = 1 \pmod 3$, dus $p \equiv 7 \pmod{12}$, dus 3 is niet-rest mod p. Uit het hierboven afgeleide resultaat

$$p \mid v_{\frac{1}{4}(p+1)}$$

volgt dan

$$2^s - 1 \mid v_{2^{s-2}}$$

waarmee het eerste deel van de bedoelde stelling is bewezen.

Zij thans omgekeerd gegeven dat het getal $M_s = 2^s - 1$ deelbaar is op $v_{2^{s-2}}$. Dan voldoet elke priemdeler q van M_s aan

$$v_{2^{s-2}} \equiv 0 \pmod{q}. \tag{2}$$

Omdat voor oneven s met $s \geqslant 3$ geldt $2^s - 1 \equiv 7 \pmod{12}$ moet het getal M_s ten minste één priemdeler p hebben die voldoet aan

$$p \equiv \pm 7 \pmod{12}.$$

OPGAVE 7. Ga dit na.

Derhalve is het getal 3 niet-rest mod p en het getal p voldoet dan aan (1).

Vervolgens beschouwen we het kleinste natuurlijke getal C waarvoor geldt $\alpha^C \equiv 1 \pmod p$. Uit (1) volgt dan

$$C \mid p + 1. \tag{3}$$

OPGAVE 8. Bewijs dit.

Anderzijds heeft men op grond van relatie (2)

$$\alpha^{2^{s-2}}+\beta^{2^{s-2}}\equiv 0(\mathrm{mod}\,p)$$

successievelijk

$$\alpha^{2^{s-2}}\equiv-\beta^{2^{s-2}}\ (\mathrm{mod}\,p)$$
$$\alpha^{2^{s-1}}\equiv-\alpha^{2^{s-2}}\beta^{2^{s-2}}=-1\ (\mathrm{mod}\,p)$$
$$\alpha^{2^{s}}\equiv+1\ (\mathrm{mod}\,p).$$

Daaruit volgt dat het getal C voldoet aan

$$C \mid 2^s\ ,\quad C \nmid 2^{s-1}$$

dus $C=2^s$. En (3) leert dan dat $2^s \mid p+1$. Stelt men nog $M_s=Np$, dan komt men tot $Np+1 \mid p+1$ en daaruit volgt kennelijk $N=1$, dus $M_s=p$, waarmee het tweede deel van de gemodificeerde stelling van Lucas is bewezen.

Ter illustratie geven we hier de tot nu toe bekende priemgetallen van Mersenne, met het jaar van ontdekking en de naam van de ontdekker.

Lijst van bekende priemgetallen van Mersenne: 2^p-1

Exponent p	Jaar van ontdekking	Auteur
2, 3, 5, 7, 13	$-\infty$?	?
17, 19	$\sim$ 1600	Cataldi
31	1750	Euler
61	1883, 1886	Pervouchine, Seelhoff
89	1911	Powers
107	1911	Powers
127	1876	Lucas
521, 607	1952	Robinson
1279, 2203, 2281	1952	Lehner
3217	1958	Riesel
4253, 4423	1962	Hurwitz & Selfridge
9689, 9941, 11213	1963	Gillies
19937	1971	Tuckermann
21701	1978	Nickel & Noll
23209, 44497	1979	Slowinsky & Nelson
86243, 132049	1983	Slowinsky

Men zal zich afvragen: "Zijn er nog meer priemgetallen van Mersenne en - zo ja - hoe groot zijn die dan wel ?" Hierover bestaan interessante voorspellingen. In de Mathematical Intelligencer van het najaar 1983 komt een artikel voor van Manfred Schroeder (Math. Int. Vol. 5, Nr. 3, 1983), getiteld: "Where is the Next Mersenne Prime Hiding?" Zonder op de détails in te gaan vermelden we slechts de conclusie. Deze betreft in principe de verdeling van de te verwachten afstanden tussen twee opvolgende Mersenne-priemgetallen:

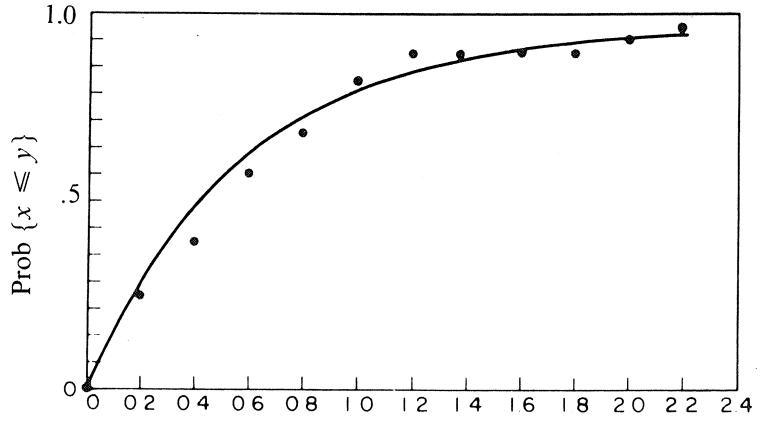
$M(n+1)-M(n)$, met als steeds $M(n)=2^{p_n}-1$. In plaats van de intervallen zelf wordt de aandacht gericht op de waarden ${}^2\log({}^2\log M(n+1))-{}^2\log({}^2\log M(n))$, dus ten naaste bij ${}^2\log p_{n+1}-{}^2\log p_n$ oftewel ${}^2\log\frac{p_{n+1}}{p_n}$.

Op grond van waarschijnlijkheidstheoretische overwegingen rees het vermoeden dat de cumulatieve verdeling van deze intervallen zich zou gedragen als $P(d)=1-e^{-Kd}$, waarin voor de constante K geldt: $K=e^{\gamma}$, met daarin γ de constante van Euler: $\gamma=\lim(1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{n}-\log n)$.

Voor de 28 op dat ogenblik bekende priemgetallen van Mersenne bleek dit aardig te kloppen (zie onderstaande afbeelding).

Maar nu komt het: op grond van deze overwegingen werd het eerstvolgende Mersenne-priemgetal vermoed in de buurt van $2^{130.000}$.

Kort daarop vond Slowinsky voor het 29e Mersenne-priemgetal $M(29)=2^{132.049}-1$.



$$x={}^2\log({}^2\log M(n+1))-{}^2\log({}^2\log M(n))$$

Tot slot valt nog op te merken dat de stelling van Lucas kan worden gegeneraliseerd waarbij het gaat om een analoog criterium voor het ondeelbaar zijn van getallen van de gedaante $a.\,2^s-1$, dit onder bepaalde woorwaarden voor het oneven getal a ($\neq 1$). De huidige recordhouder van dit type is

$$391581*2^{216193}-1 \quad \text{(Amdahl, 1990).}$$

Het Vermoeden van Fermat: Recente Resultaten

F. Beukers
Rijksuniversiteit Utrecht
Faculteit Wiskunde en Informatica
Postbus 80010, 3508 TA Utrecht

1. Inleiding

De historie rond het vermoeden van Fermat is reeds vele malen verteld en misschien heeft u het ook al vele malen gehoord. In dat geval kunt u meteen doorgaan naar paragraaf 2 van deze tekst. Voor de volledigheid geven we in deze paragraaf een korte beschrijving van het Fermat-vermoeden.

Het is bekend dat er kwadraten zijn waarvan de som weer een kwadraat is. Bekende voorbeelden zijn $3^2+4^2=5^2$, $5^2+12^2=13^2$ en nog vele andere die geproduceerd kunnen worden door in de identiteit $(a^2-b^2)^2+(2ab)^2=(a^2+b^2)^2$ willekeurige gehele waarden van a en b in te vullen. Automatisch rijst de vraag of er ook twee positieve derde machten bestaan waarvan de som weer een derde macht is, of algemener, of er twee positieve n-de machten ($n\geqslant 3$) bestaan waarvan de som een n-de macht is. Enig proberen, al of niet met de computer, levert geen voorbeelden op. De flauwe oplossing $0^n+1^n=1^n$ laten we buiten beschouwing door alleen naar *positieve* oplossingen te vragen. Het uitblijven van niet-triviale voorbeelden bracht de Franse wiskundige Pierre de Fermat er rond 1640 toe het volgende vermoeden te formuleren.

(Vermoeden van Fermat) Zij n een geheel getal groter dan 2. Dan heeft de vergelijking $x^n+y^n=z^n$ geen oplossingen met positieve gehele x,y,z.

Fermat bewees zijn vermoeden voor het speciale geval $n=4$. Tevens claimde Fermat in het bezit te zijn van een wonderbaarlijk bewijs voor algemene n. Het ongeluk wilde dat de kantlijn van Bachet's vertaling van Diophantos' 'Arithmetica', waarin Fermat deze opmerking schreef, te smal was om het bewijs te bevatten. Dit is jammer want het is nog steeds niet bekend of Fermat inderdaad een correct bewijs bezat. Velen betwijfelen dit, omdat ondanks de enorme

Fermat, l'un des géomètres dont les travaux contribuèrent le plus à accélérer la découverte des nouveaux calculs, cultiva avec un grand succès la science des nombres, et s'y fraya des routes nouvelles. On a de lui un grand nombre de théorèmes intéressants, mais il les a laissés presque tous sans démonstration. C'était l'esprit du temps de se proposer des problèmes les uns aux autres. On cachait le plus souvent sa méthode, afin de se réserver des triomphes nouveaux tant pour soi que pour sa nation; car il y avait surtout rivalité entre les géomètres français et les anglais. De là il est arrivé que la plupart des démonstrations de Fermat ont été perdues, et le peu qui nous en reste nous fait regretter d'autant plus celles qui nous manquent.

Passage uit het voorwoord van Legendre's "Essai sur la Théorie des Nombres", 1e editie, Deel I, 1798.

ontwikkeling van de getaltheorie en de vele mensuren die er in zijn gestoken, er nog niemand in geslaagd is een bewijs van het Fermat-vermoeden te leveren.

2. Oude resultaten

Hoewel het algemene Fermat-vermoeden onbewezen is, zijn er veel speciale waarden van n waarvoor het vermoeden bevestigd is. Euler bewees in 1753 het geval $n=3$, Dirichlet (1828) het geval $n=5$ en Lamé (1839) het geval $n=7$. Merk op dat het geval $n=6$ uit het geval $n=3$ volgt. Immers $x^6+x^6=z^6 \Rightarrow (x^2)^3+(y^2)^3=(z^2)^3$. Dus een oplossing van het geval $n=6$ geeft een oplossing voor het geval $n=3$. We weten sinds Euler dat er bij $n=3$ geen positieve oplossingen zijn, en dus voor $n=6$ ook niet. In het algemeen zien we dat als het Fermat-vermoeden waar is voor de exponent n, dan is het ook waar voor ieder veelvoud van n. In de praktijk is het dus voldoende te kijken naar het geval dat de exponent n priem is.

De gebruikte oplossingsmethoden beginnen allemaal als volgt. Zij p een priemgetal en stel $\zeta=e^{2\pi i/p}$. Dan kan $x^p+y^p=z^p$ herschreven worden als

$$(x+y)(x+\zeta y)\ \cdots\ (x+\zeta^{p-1}y) = z^p. \tag{2.1}$$

De linkerzijde van onze vergelijking is dus in factoren ontbonden. De prijs die hiervoor betaald wordt is dat we niet meer in $\mathbf{Z}$ werken maar in de getallenring $\mathbf{Z}[\zeta]=\{a_0+a_1\zeta+\cdots+a_{p-1}\zeta^{p-1} | a_i \in \mathbf{Z}\}$. Als we in $\mathbf{Z}$ twee getallen a en b hebben met grootste gemene deler 1 en waarvan het produkt een p-de macht is, dan zijn a en b zelf ook p-de machten. Algemener, als het product $a_1 \cdots a_r$ een p-de macht is en $\text{ggd}(a_i,a_j)=1$ voor alle $i \neq j$, dan is elk van de getallen a_i een p-de macht. Dit is een gevolg van het feit dat we in $\mathbf{Z}$ éénduidige priemontbinding hebben. Om Fermat te bewijzen zouden we graag uit (2.1) iets dergelijks concluderen. Links hebben we namelijk een produkt van getallen in $\mathbf{Z}[\zeta]$ en rechts staat een p-de macht. We zouden graag willen dat elk van de faktoren links p-de macht is van een element uit $\mathbf{Z}[\zeta]$. Het is op dit punt dat zich één van de voetangels voordoet bij het oplossen van het Fermat-probleem. In $\mathbf{Z}[\zeta]$ geldt namelijk niet altijd éénduidige priemontbinding. Zou dit wel zo zijn, dan kon het Fermat vermoeden bewezen worden (hoewel het in dat geval nog steeds niet gemakkelijk is). Helaas hebben we in algebraïsche getallenringen de éénduidige priemontbinding niet en moet er iets voor in de plaats komen. Dit soort problemen vormde een belangrijke stimulans voor de ontwikkeling van de algebraïsche getaltheorie in de 19e eeuw. Rond 1847 zag E. Kummer kans om de volgende frappante stelling te bewijzen.

Stelling. *Zij $B_0,B_1,B_2,\ldots$ de rij Bernoulli-getallen. Als het oneven priemgetal p geen deler is van de tellers van $B_2,B_4,B_6,\ldots,B_{p-3}$ dan heeft $x^p+y^p=z^p$ geen oplossing in positieve gehele getallen.*

Opmerking. De *Bernoulli-getallen* $B_0,B_1,B_2,\ldots$ worden gegeven door de Taylorreeks

$$\frac{x}{e^x-1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}.$$

Het is gemakkelijk te zien dat $B_n=0$ als n oneven en groter dan 1 is. Enkele waarden:

$$B_2 = 1/6$$
$$B_4 = -1/30$$
$$B_6 = 1/42$$
$$B_8 = -1/30$$
$$B_{10} = 5/66$$
$$B_{12} = -691/2730$$
$$B_{14} = 7/6$$
$$B_{16} = -3617/510$$
$$B_{18} = 43867/798$$
$$B_{20} = -174611/330.$$

Uit dit rijtje getallen en Kummer's stelling kunnen we al direkt zien dat het Fermat-vermoeden waar is voor alle n met $2<n<29$. Met behulp van de computer en verfijningen van het Kummer criterium weten we nu, dat het Fermat vermoeden waar is voor alle n met $2<n<150000$. Voor meer details over de geschiedenis en bewijzen van Kummer's theorie verwijzen we naar de boeken van P. Ribenboim (13 Lectures on Fermat's Last Theorem, Springer Verlag, 1979) en H.M. Edwards (Fermat's Last Theorem, Springer Verlag, 1977). In de periode tussen 1850 en 1980 zijn er, behalve allerlei verfijningen van bestaande resultaten, weinig nieuwe ontwikkelingen rond het Fermat-vermoeden geweest. Na 1980 veranderde dit en een aantal volkomen nieuwe resultaten heeft sindsdien het licht gezien. In de volgende paragrafen trachten we hier een overzicht van te geven.

3. Het Mordell-vermoeden

We maken even een kleine uitstap naar algemenere diophantische vergelijkingen. Kies een polynoom $P(X,Y)$ met gehele coëfficienten. Gevraagd wordt het volgende probleem op te lossen

$$P(x,y) = 0 \text{ met } x,y \in \mathbf{Q}. \tag{3.1}$$

Dat de oplossingsverzameling zeer grillig van P af kan hangen moge blijken uit de voorbeelden $x^3+y^3=4$, die geen oplossingen $x,y\in\mathbf{Q}$ heeft, en $x^3+y^3=22$ die er oneindig veel heeft. Trouwens, zonder geschikte voorkennis zijn beide uitspraken zeer lastig te bewijzen. Probeer het maar. Het is duidelijk dat het Fermat probleem ook onder dit type valt. De vergelijking $x^n+y^n=z^n$ kan immers als $(x/z)^n+(y/z)^n-1=0$ worden herschreven en het polynoom P is in dit geval X^n+Y^n-1. Eén van de faktoren waarvan de grootte van de oplossingsverzameling kan afhangen is de meetkundige struktuur van de algebraïsche kromme $\mathcal{C}=\{(x,y)\in\mathbf{C}^2 | P(x,y)=0\}$. Laten we allereerst aannemen dat $\mathcal{C}$ irreducibel is, dat wil zeggen, $P(X,Y)$ is geen produkt van twee niet-constante polynomen met coëfficienten in $\mathbf{C}$. Een belangrijke invariant van een

irreducibele algebraïsche kromme is het *geslacht* g, dat op vele manieren berekend kan worden. We zullen hier volstaan met een korte typering van de gevallen $g=0$, $g=1$ en $g\geqslant 2$.

Algebraïsche krommen van geslacht 0 zijn precies die krommen waarvoor een tweetal niet-constante rationale funkties $f(t),g(t)$ bestaat zó dat $P(f(t),g(t))=0$. Met andere woorden, $\mathcal{C}$ heeft een rationale parametrisatie $x=f(t)$, $y=g(t)$ en $\mathcal{C}$ zelf noemen we dan een rationale kromme. Een voorbeeld is $x^2+y^2=1$ met als parametrisatie $x=(t^2-1)/(t^2+1), y=2t/(t^2+1)$. Kiezen we in dit voorbeeld $t=2$ dan krijgen we het bekende punt (3/5, 4/5). Door t willekeurige andere waarden in $\mathbf{Q}$ te geven kunnen we oneindig veel rationale oplossingen van $x^2+y^2=1$ genereren. Zo kunnen we ook in het algemeen, als de coëfficienten van $f(t)$, $g(t)$ in $\mathbf{Q}$ zitten, oneindig veel oplossingen $x,y\in\mathbf{Q}$ van $P(x,y)=0$ construeren. Dit neemt niet weg dat er ook krommen van geslacht 0 zijn waarvoor $P(x,y)=0$, $x,y\in\mathbf{Q}$, geen oplossingen heeft, zoals $x^2+y^2=3$. Blijkbaar zijn er in dit geval geen parametrisaties met coëfficienten in $\mathbf{Q}$ te vinden.

Algebraïsche krommen van geslacht 1 zijn precies de krommen die geparametriseerd kunnen worden door niet-constante elliptische funkties. Een voorbeeld is $x^3+y^3=1$. We zullen hier verder niet al te veel over uitweiden, maar merken op dat in dit geval er ook oneindig veel rationale oplossingen kunnen zijn zoals bij $x^3+y^3=22$.

Voorbeelden van algebraïsche krommen van geslacht $\geqslant 2$ zijn $x^n+y^n=1$ met $n\geqslant 4$. Het geslacht is dan $(n-1)(n-2)/2$. In 1922 spak L.J. Mordell het volgende vermoeden uit:

Als $g\geqslant 2$, dan heeft $P(x,y)=0$ hooguit eindig veel oplossingen $x,y\in\mathbf{Q}$.

Dit vermoeden heeft lange tijd als één van de hoofdproblemen in de theorie van de diophantische vergelijkingen te boek gestaan, totdat in 1983 een bewijs werd geleverd door G. Faltings. Helaas is het bewijs zeer lastig en slechts toegankelijk voor specialisten in de arithmetische algebraïsche meetkunde. Gelukkig ziet het er naar uit, dat door het werk van Vojta, Faltings en Bombieri alternatieve bewijzen geleverd kunnen worden die toegankelijk zijn voor grotere groepen wiskundigen.

Keren we terug naar het Fermat probleem dan zien we dat Faltings' stelling impliceert dat $x^n+y^n=1$ hooguit eindig veel oplossingen $x,y\in\mathbf{Q}$ heeft als $n\geqslant 4$. Na uitvermenigvuldiging van eventuele noemers kunnen we ook zeggen dat $x^n+y^n=z^n$ voor $n\geqslant 4$ hoogstens eindig veel oplossingen $x,y,z\in\mathbf{Z}$ heeft met $\mathrm{ggd}(x,y,z)=1$. De laatste conditie is erbij gevoegd om te voorkomen dat we naast een oplossing (x,y,z) ook de oplossingen $(2x,2y,2z)$, $(3x,3y,3z)$, etc. gaan meetellen. Hoewel Fermat's vermoeden hiermee nog niet bewezen is, is het wel een stap in de goede richting. Een ander gevolg van Faltings' stelling is de volgende frappante uitspraak, die onafhankelijk door A. Granville en R. Heath-Brown in 1985 werd bewezen.

Plimpton 322

Pierre de Fermat
(1601 - 1665)

STELLING 3.1. *De verzameling van exponenten n waarvoor het Fermat-vermoeden waar is heeft dichtheid 1 in de natuurlijke getallen.*

OPMERKING. Zij A een deelverzameling van de natuurlijke getallen $\mathbb{N}$. We zeggen dat A dichtheid δ in $\mathbb{N}$ heeft als

$$\lim_{x\to\infty} \frac{\sharp\{n\in A \mid n\leqslant x\}}{x}$$

bestaat en gelijk is aan δ. De dichtheid, indien deze bestaat, van een verzameling $A\subset\mathbb{N}$ zullen we voortaan aangeven met $\delta(A)$. Intuïtief gezien beslaat een verzameling met dichtheid δ een fraktie δ van de natuurlijke getallen. Zijn nu A en B een tweetal verzamelingen van natuurlijke getallen waarvan de dichtheid bestaat. Dan gelden de volgende eigenschappen, die men zelf eenvoudig kan nagaan

i. $\delta(A)\leqslant 1$
ii. $\delta(A^C)$ bestaat en is gelijk aan $1-\delta(A)$
iii. als A en B slechts een eindig aantal elementen verschillen, dan is $\delta(A)=\delta(B)$
iv. als $A\cap B=\varnothing$, dan bestaat $\delta(A\cup B)$ en is gelijk aan $\delta(A)+\delta(B)$
vi. als A een rij deelverzamelingen $B_1,B_2,B_3,\ldots$ bevat zó dat $\lim_{r\to\infty}\delta(B_r)=1$, dan bestaat de dichtheid van A en is gelijk aan 1.

Voordat we Stelling 3.1 bewijzen hebben we een lemma nodig over priemgetallen,

LEMMA 3.2. *Zij $p_1,p_2,\ldots,p_r,\ldots$ de rij opeenvolgende oneven priemgetallen. Met D_r geven we de verzameling natuurlijke getallen aan, die deelbaar zijn door een oneven priemgetal $\leqslant p_r$. Dan geldt*

$$\delta(D_r) = 1-(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r}) \qquad (i)$$

en

$$\lim_{r\to\infty}(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r}) = 0. \qquad (ii)$$

BEWIJS van (i). Dit kan door induktie naar r.

$r=1$: $\delta(D_1)=1/p_1=1-(1-1/p_1)$. Dit is duidelijk, want de fraktie van de natuurlijke getallen die deelbaar zijn door p_1 is $1/p_1$.

$r>1$ en stel (induktie hypothese)

$$\delta(D_{r-1}) = 1-(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_{r-1}}). \qquad (3.2)$$

Merk op dat D_r uit D_{r-1} ontstaat door alle natuurlijke getallen toe te voegen die deelbaar zijn door p_r en niet door een kleiner priemgetal. Noem deze

verzameling X. Merk op dat X ontstaat door de elementen van het complement van D_{r-1} met p_r te vermenigvuldigen. Dus, $\delta(X)=\delta(D_{r-1}^C)/p_r=(1-\delta(D_{r-1}))/p_r$. Verder geldt dat $\delta(D_r)=\delta(D_{r-1})+\delta(X)$. Vullen we hier onze uitdrukking voor $\delta(X)$ in, en vervolgens (3.2), dan levert enig rekenwerk ons de gewenste formule voor $\delta(D_r)$.

BEWIJS van (ii). Merk allereerst op dat

$$(1-\frac{1}{p_1})^{-1}\ \cdots\ (1-\frac{1}{p_r})^{-1}=(1+\frac{1}{p_1}+\frac{1}{p_1^2}+\cdots)\ \cdots\ (1+\frac{1}{p_r}+\frac{1}{p_r^2}+\cdots).$$

Na wegwerking van de haakjes in het rechtse produkt houden we een som over die de inversen $1/1,1/3,1/5,...,1/p_r$ bevat. Omdat de som van deze termen naar oneindig gaat als $p_r\to\infty$ (som van de inverse oneven natuurlijke getallen is oneindig !) volgt hieruit dat ook het produkt $(1-1/p_1)^{-1}\cdots(1-1/p_r)^{-1}$ naar oneindig gaat. De inverse van dit produkt gaat dus naar 0.

BEWIJS VAN STELLING 3.1. Het basis idee komt hierop neer. Gegeven een oneven priemgetal p. Dan gaan we een getal $M(p)$ aangeven, zodat het Fermat-vermoeden waar is voor alle exponenten mp met $m\geqslant M(p)$. We weten namelijk dat $x^p+y^p=z^p$ slechts eindig veel oplossingen $x,y,z\in\mathbf{N}$ heeft met $\text{ggd}(x,y,z)=1$. Zij N het grootste getal zodat de z van minstens één van deze oplossingen een N-de macht is. Het duidelijk dat we nu $M(p)=N+1$ kunnen kiezen.

We houden de notaties van Lemma 3.2 aan. Kies $M_r=\max(M(p_1),...,M(p_r))$ voor elke $r\in\mathbf{N}$ en definiëer de verzameling $F_r=\{n\in D_r|n>M_r p_r\}$. Dan volgt uit bovenstaande opmerking dat het Fermat-vermoeden waar is voor alle elementen uit F_r, en dit voor elke r. Omdat F_r en D_r slechts een eindig aantal elementen verschillen, hebben ze dezelfde dichtheid. Verder volgt uit Lemma 3.2 dat $\lim_{r\to\infty}\delta(D_r)=1$. Dus gaat $\delta(F_r)$ ook naar 1 als $r\to\infty$. Conclusie, de dichtheid van de exponenten waarvoor het Fermat-vermoeden waar is, is 1.

4. HET TANIYAMA-WEIL VERMOEDEN

Een zeer verrassend en belangrijk resultaat uit 1987 is dat van K. Ribet dat zegt dat de juistheid van het Fermat-vermoeden volgt uit de juistheid van het zogenaamde Taniyama-Weil vermoeden. Dit laatste vermoeden geeft een wonderbaarlijke karakterisatie van algebraïsche krommen van de vorm $y^2=x^3+Ax^2+Bx+C$ (de zogenaamde *elliptische krommen*) met $A,B,C\in\mathbf{Z}$. We hebben niet de illusie dat we hier kunnen uitleggen wat het Taniyama-Weil vermoeden precies behelst, noch wat het verband met het Fermat vermoeden is. Wat mischien wel duidelijk gemaakt kan worden is een verschil van smaak van beide vermoedens. Als we bijvoorbeeld het vermoeden uitspreken dat $x^{37}+y^{37}=z^{37}$ geen oplossing in natuurlijke getallen heeft, kunnen we niet veel doen. Het heeft weinig zin om numeriek naar oplossingen te zoeken omdat we vermoeden dat ze niet bestaan. Het enige wat gedaan kan worden is het vermoeden bewijzen, wat dan ook gedaan is. Als we daarentegen het Taniyama-

Weil vermoeden voor bijvoorbeeld $y^2=x^3+7x-1$ willen nagaan, dan kunnen we aan de slag. Na enig rekenwerk krijgen we doorgaans een bevestigend antwoord. Het grote aantal elliptische krommen waarvoor het Taniyama-Weil vermoeden is bevestigd wekt vertrouwen en is dus ook, na het werk van G. Frey en K. Ribet, een nieuwe aanwijzing voor de juistheid van het Fermat-vermoeden.

5. Het Fermat-probleem over andere getalsystemen

Als in de wiskunde een vraag niet beantwoord kan worden heeft men vaak de neiging deze vraag enigszins te veranderen om vervolgens te proberen deze nieuwe vraag op te lossen. Soms gebeurt het dat een oplossing voor het gewijzigde probleem inzichten verschaft in het oorspronkelijke probleem. In deze paragraaf zullen we ter vermaak de vergelijking $X^n+Y^n=Z^n$ oplossen in polynomen $X(t), Y(t), Z(t)$.

Stelling 5.1. *Stel $n>2$ en zij $A(t)$, $B(t)$, $C(t)$ een drietal polynomen zodat $A^n+B^n=C^n$ en* ggd$(A,B,C)=1$. *Dan zijn A, B, C constant.*

Eerste bewijs. Stel dat er een niet-constante oplossing $A(t),B(t),C(t)$ is. Voor het gemak nemen we aan dat gr(A)$\geqslant$gr(B),gr(C). (gr(P) is een afkorting voor de *graad* van P). Voor de andere gevallen gaat het bewijs analoog. We differentiëren de gelijkheid

$$A^n+B^n = C^n \tag{5.1}$$

éénmaal aan beide zijden en delen door n

$$A^{n-1}A'+B^{n-1}B' = C^{n-1}C'. \tag{5.2}$$

Vermenigvuldig (5.1) met C', (5.2) met C en trek ze van elkaar af. We krijgen $A^{n-1}(CA'-C'A)+B^{n-1}(CB'-C'B)=0$. Hieruit volgt dat A^{n-1} een deler is van $B^{n-1}(CB'-C'B)$ en omdat ggd$(A,B)=1$ is A^{n-1} een deler van $CB'-C'B$. We onderscheiden twee gevallen.

Geval 1, $CB'-C'B$ is het nul-polynoom. Dan geldt $(B/C)'=(CB'-C'B)/B^2=0$, met andere woorden, B/C is constant. Omdat ggd$(B,C)=1$, volgt dat B,C en dus ook A constant zijn.

Geval 2, $CB'-C'B$ is niet identiek nul. In dit geval zijn B,C niet beide constant, en omdat gr$(A)\geqslant$gr(b),gr(C), geldt gr(A)>0. Het feit dat A^{n-1} deler is van $CB'-C'B$ betekent voor de graden dat

$$(n-1)\text{gr}(A) = \text{gr}(A^{n-1})\leqslant\text{gr}(CB'-C'B)<\text{gr}(B)+\text{gr}(C)\leqslant 2\text{gr}(A).$$

Conclusie, $(n-1)$gr$(A)<2$gr(A) en omdat $n\geqslant 3$ hebben we een tegenspraak. Niet constante oplossingen bestaan blijkbaar niet.

Er is nog een tweede bewijs dat zeer kort is, maar wel van de lezer enige kennis over algebraïsche krommen vereist.

Tweede bewijs. Het bestaan van dergelijke niet-constante polynomen zou betekenen dat de algebraïsche kromme $x^n+y^n=1$ geparametriseerd kan

worden door de rationale funkties $x=A(t)/C(t)$, $y=B(t)/C(t)$. Dus het geslacht is 0. Anderzijds weten we dat het geslacht van de algebraïsche kromme gelijk is aan $(n-1)(n-2)/2$, hetgeen positief is als $n>2$. We hebben een tegenspraak en concluderen dat er geen niet-constante oplossingen zijn.

Er zijn nog vele andere getalsystemen waarin we de vergelijking van Fermat kunnen bestuderen. Eén aardige wil ik nog vermelden. We zullen Fermat's probleem in de vorm $x^n+y^n=1$ nemen. Stel dat we deze vergelijking in kwadratische getallen willen oplossen, dat wil zeggen in getallen van de vorm $a+b\sqrt{d}$, $a,b\in\mathbf{Q}$, waarin $d\in\mathbf{Z}$ verder niet vast ligt. Kunnen er dan oneindig veel oplossingen zijn? Het antwoord is voor gegeven n wederom neen (voor $n>3$). Dit volgt uit zeer recent werk (1989) van Faltings, Harris en Silverman. Er zijn nog nauwelijks voorbeelden van n bekend waarvoor de volledige verzameling oplossingen is bepaald. Voor $n=4$ hebben we

STELLING 5.2. *De enige oplossingen van* $x^4+y^4=1$ *in de kwadratische getallen zijn*

$$(0,\pm 1),\ (0,\pm\sqrt{-1}),\ (\pm\frac{1+\sqrt{-7}}{2},\pm\frac{1-\sqrt{-7}}{2})$$

en de oplossingen hieruit verkregen door x en y te verwisselen.

Het zou heel aardig zijn om de Fermat-vergelijking ook voor andere n in de kwadratische getallen op te lossen, of alleen maar interessante oplossingen te vinden.

MC SYLLABI

1.1 F. Göbel, J. van de Lune. *Leergang besliskunde, deel 1: wiskundige basiskennis.* 1965.

1.2 J. Hemelrijk, J. Kriens. *Leergang besliskunde, deel 2: kansberekening.* 1965.

1.3 J. Hemelrijk, J. Kriens. *Leergang besliskunde, deel 3: statistiek.* 1966.

1.4 G. de Leve, W. Molenaar. *Leergang besliskunde, deel 4: Markovketens en wachttijden.* 1966.

1.5 J. Kriens, G. de Leve. *Leergang besliskunde, deel 5: inleiding tot de mathematische besliskunde.* 1966.

1.6a B. Dorhout, J. Kriens. *Leergang besliskunde, deel 6a: wiskundige programmering 1.* 1968.

1.6b B. Dorhout, J. Kriens, J.Th. van Lieshout. *Leergang besliskunde, deel 6b: wiskundige programmering 2.* 1977.

1.7a G. de Leve. *Leergang besliskunde, deel 7a: dynamische programmering 1.* 1968.

1.7b G. de Leve, H.C. Tijms. *Leergang besliskunde, deel 7b: dynamische programmering 2.* 1970.

1.7c G. de Leve, H.C. Tijms. *Leergang besliskunde, deel 7c: dynamische programmering 3.* 1971.

1.8 J. Kriens, F. Göbel, W. Molenaar. *Leergang besliskunde, deel 8: minimaxmethode, netwerkplanning, simulatie.* 1968.

2.1 G.J.R. Förch, P.J. van der Houwen, R.P. van de Riet. *Colloquium stabiliteit van differentieschema's, deel 1.* 1967.

2.2 L. Dekker, T.J. Dekker, P.J. van der Houwen, M.N. Spijker. *Colloquium stabiliteit van differentieschema's, deel 2.* 1968.

3.1 H.A. Lauwerier. *Randwaardeproblemen, deel 1.* 1967.

3.2 H.A. Lauwerier. *Randwaardeproblemen, deel 2.* 1968.

3.3 H.A. Lauwerier. *Randwaardeproblemen, deel 3.* 1968.

4 H.A. Lauwerier. *Representaties van groepen.* 1968.

5 J.H. van Lint, J.J. Seidel, P.C. Baayen. *Colloquium discrete wiskunde.* 1968.

6 K.K. Koksma. *Cursus ALGOL 60.* 1969.

7.1 *Colloquium moderne rekenmachines, deel 1.* 1969.

7.2 *Colloquium moderne rekenmachines, deel 2.* 1969.

8 H. Bavinck, J. Grasman. *Relaxatietrillingen.* 1969.

9.1 T.M.T. Coolen, G.J.R. Förch, E.M. de Jager, H.G.J. Pijls. *Colloquium elliptische differentiaalvergelijkingen, deel 1.* 1970.

9.2 W.P. van den Brink, T.M.T. Coolen, B. Dijkhuis, P.P.N. de Groen, P.J. van der Houwen, E.M. de Jager, N.M. Temme, R.J. de Vogelaere. *Colloquium elliptische differentiaalvergelijkingen, deel 2.* 1970.

10 J. Fabius, W.R. van Zwet. *Grondbegrippen van de waarschijnlijkheidsrekening.* 1970.

11 H. Bart, M.A. Kaashoek. H.G.J. Pijls, W.J. de Schipper, J. de Vries. *Colloquium halfalgebra's en positieve operatoren.* 1971.

12 T.J. Dekker. *Numerieke algebra.* 1971.

13 F.E.J. Kruseman Aretz. *Programmeren voor rekenautomaten; de MC ALGOL 60 vertaler voor de EL X8.* 1971.

14 H. Bavinck, W. Gautschi, G.M. Willems. *Colloquium approximatietheorie.* 1971.

15.1 T.J. Dekker, P.W. Hemker, P.J. van der Houwen. *Colloquium stijve differentiaalvergelijkingen, deel 1.* 1972.

15.2 P.A. Beentjes, K. Dekker, H.C. Hemker, S.P.N. van Kampen, G.M. Willems. *Colloquium stijve differentiaalvergelijkingen, deel 2.* 1973.

15.3 P.A. Beentjes, K. Dekker, P.W. Hemker, M. van Veldhuizen. *Colloquium stijve differentiaalvergelijkingen, deel 3.* 1975.

16.1 L. Geurts. *Cursus programmeren, deel 1: de elementen van het programmeren.* 1973.

16.2 L. Geurts. *Cursus programmeren, deel 2: de programmeertaal ALGOL 60.* 1973.

17.1 P.S. Stobbe. *Lineaire algebra, deel 1.* 1973.

17.2 P.S. Stobbe. *Lineaire algebra, deel 2.* 1973.

17.3 N.M. Temme. *Lineaire algebra, deel 3.* 1976.

18 F. van der Blij, H. Freudenthal, J.J. de Iongh, J.J. Seidel, A. van Wijngaarden. *Een kwart eeuw wiskunde 1946-1971, syllabus van de vakantiecursus 1971.* 1973.

19 A. Hordijk, R. Potharst, J.Th. Runnenburg. *Optimaal stoppen van Markovketens.* 1973.

20 T.M.T. Coolen, P.W. Hemker, P.J. van der Houwen, E. Slagt. *ALGOL 60 procedures voor begin- en randwaardeproblemen.* 1976.

21 J.W. de Bakker (red.). *Colloquium programmacorrectheid.* 1975.

22 R. Helmers, J. Oosterhoff, F.H. Ruymgaart, M.C.A. van Zuylen. *Asymptotische methoden in de toetsingstheorie; toepassingen van naburigheid.* 1976.

23.1 J.W. de Roever (red.). *Colloquium onderwerpen uit de biomathematica, deel 1.* 1976.

23.2 J.W. de Roever (red.). *Colloquium onderwerpen uit de biomathematica, deel 2.* 1977.

24.1 P.J. van der Houwen. *Numerieke integratie van differentiaalvergelijkingen, deel 1: eenstapsmethoden.* 1974.

25 *Colloquium structuur van programmeertalen.* 1976.

26.1 N.M. Temme (ed.). *Nonlinear analysis, volume 1.* 1976.

26.2 N.M. Temme (ed.). *Nonlinear analysis, volume 2.* 1976.

27 M. Bakker, P.W. Hemker, P.J. van der Houwen, S.J. Polak, M. van Veldhuizen. *Colloquium discretiseringsmethoden.* 1976.

28 O. Diekmann, N.M. Temme (eds.). *Nonlinear diffusion problems.* 1976.

29.1 J.C.P. Bus (red.). *Colloquium numerieke programmatuur, deel 1A, deel 1B.* 1976.

29.2 H.J.J. te Riele (red.). *Colloquium numerieke programmatuur, deel 2.* 1977.

30 J. Heering, P. Klint (red.). *Colloquium programmeeromgevingen.* 1983.

31 J.H. van Lint (red.). *Inleiding in de coderingstheorie.* 1976.

32 L. Geurts (red.). *Colloquium bedrijfsystemen.* 1976.

33 P.J. van der Houwen. *Berekening van waterstanden in zeeën en rivieren.* 1977.

34 J. Hemelrijk. *Oriënterende cursus mathematische statistiek.* 1977.

35 P.J.W. ten Hagen (red.). *Colloquium computer graphics.* 1978.

36 J.M. Aarts, J. de Vries. *Colloquium topologische dynamische systemen.* 1977.

37 J.C. van Vliet (red.). *Colloquium capita datastructuren.* 1978.

38.1 T.H. Koornwinder (ed.). *Representations of locally compact groups with applications, part I.* 1979.

38.2 T.H. Koornwinder (ed.). *Representations of locally compact groups with applications, part II.* 1979.

39 O.J. Vrieze, G.L. Wanrooy. *Colloquium stochastische spelen.* 1978.

40 J. van Tiel. *Convexe analyse.* 1979.

41 H.J.J. te Riele (ed.). *Colloquium numerical treatment of integral equations.* 1979.

42 J.C. van Vliet (red.). *Colloquium capita implementatie van programmeertalen.* 1980.

43 A.M. Cohen, H.A. Wilbrink. *Eindige groepen (een inleidende cursus).* 1980.

44 J.G. Verwer (ed.). *Colloquium numerical solution of partial differential equations.* 1980.

45 P. Klint (red.). *Colloquium hogere programmeertalen en computerarchitectuur.* 1980.

46.1 P.M.G. Apers (red.). *Colloquium databankorganisatie, deel 1.* 1981.

46.2 P.G.M. Apers (red.). *Colloquium databankorganisatie, deel 2.* 1981.

47.1 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60: general information and indices.* 1981.

47.2 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 1: elementary procedures; vol. 2: algebraic evaluations.* 1981.

47.3 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 3A: linear algebra, part I.* 1981.

47.4 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 3B: linear algebra, part II.* 1981.

47.5 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 4: analytical evaluations; vol. 5A: analytical problems, part I.* 1981.

47.6 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 5B: analytical problems, part II.* 1981.

47.7 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 6: special functions and constants; vol. 7: interpolation and approximation.* 1981.

48.1 P.M.B. Vitányi, J. van Leeuwen, P. van Emde Boas (red.). *Colloquium complexiteit en algoritmen, deel 1.* 1982.

48.2 P.M.B. Vitányi, J. van Leeuwen, P. van Emde Boas (red.). *Colloquium complexiteit en algoritmen, deel 2.* 1982.

49 T.H. Koornwinder (ed.). *The structure of real semisimple Lie groups.* 1982.

50 H. Nijmeijer. *Inleiding systeemtheorie.* 1982.

51 P.J. Hoogendoorn (red.). *Cursus cryptografie.* 1983.

CWI SYLLABI

1 Vacantiecursus 1984: *Hewet - plus wiskunde.* 1984.

2 E.M. de Jager, H.G.J. Pijls (eds.). *Proceedings Seminar 1981-1982. Mathematical structures in field theories.* 1984.

3 W.C.M. Kallenberg, et al. *Testing statistical hypotheses: worked solutions.* 1984.

4 J.G. Verwer (ed.). *Colloquium topics in applied numerical analysis, volume 1.* 1984.

5 J.G. Verwer (ed.). *Colloquium topics in applied numerical analysis, volume 2.* 1984.

6 P.J.M. Bongaarts, J.N. Buur, E.A. de Kerf, R. Martini, H.G.J. Pijls, J.W. de Roever. *Proceedings Seminar 1982-1983. Mathematical structures in field theories.* 1985.

7 Vacantiecurus 1985: *Variatierekening.* 1985.

8 G.M. Tuynman. *Proceedings Seminar 1983-1985. Mathematical structures in field theories, Vol.1 Geometric quantization.* 1985.

9 J. van Leeuwen, J.K. Lenstra (eds.). *Parallel computers and computations.* 1985.

10 Vacantiecursus 1986: *Matrices.* 1986.

11 P.W.H. Lemmens. *Discrete wiskunde: tellen, grafen, spelen en codes.* 1986.

12 J. van de Lune. *An introduction to Tauberian theory: from Tauber to Wiener.* 1986.

13 G.M. Tuynman, M.J. Bergvelt, A.P.E. ten Kroode. *Proceedings Seminar 1983-1985. Mathematical structures in field theories, Vol.2.* 1987.

14 Vacantiecursus 1987: *De personal computer en de wiskunde op school.* 1987.

15 Vacantiecursus 1983: *Complexe getallen.* 1987.

16 P.J.M. Bongaarts, E.A. de Kerf, P.H.M. Kersten. *Proceedings Seminar 1984-1986. Mathematical structures in field theories, Vol.1.* 1988.

17 F. den Hollander, H. Maassen (eds.). *Mark Kac seminar on probability and physics. Syllabus 1985-1987.* 1988.

18 Vacantiecursus 1988. *Differentierekening.* 1988.

19 R. de Bruin, C.G. van der Laan, J.R. Luyten, H.F. Vogt. *Publiceren met LATEX.* 1988.

20 R. van der Horst, R.D. Gill (eds.). *STATAL: statistical procedures in Algol 60, part 1.* 1988.

21 R. van der Horst, R.D. Gill (eds.). *STATAL: statistical procedures in Algol 60, part 2.* 1988.

22 R. van der Horst, R.D. Gill (eds.). *STATAL: statistical procedures in Algol 60, part 3.* 1988.

23 J. van Mill, G.Y. Nieuwland (red.). *Proceedings van het symposium wiskunde en de computer.* 1989.

24 P.W.H. Lemmens (red.). *Bewijzen in de wiskunde.* 1989.

25 Vacantiecursus 1989: *Wiskunde in de Gouden Eeuw.* 1989.

26 G.G.A. Bäuerle et al. *Proceedings Seminar 1986-1987. Mathematical structures in field theories.* 1990.

27 Vacantiecursus 1990: *Getallentheorie en haar toepassingen.* 1990.