STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZC 35

Getallentheorie.

Cursus Eindhoven 1955/56.

H.J.A.Duparc.

1956

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

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

GETALLENTHEORIE 1955/56

door

H.J.A. Duparc

§1. Inleiding

Reeds eeuwen lang zijn velen, zowel mathematici als leken, geboeid geweest door fascinerende eigenschappen van de rij der natuurlijke getallen 1,2,3,... Doordat deze rij wel een der meest eenvoudige rijen der wiskunde is, is het mogelijk dat de probleemstelling van tal van haar curieuze eigenschappen, zowel door wiskundigen als door niet-wiskundigen kan worden begrepen. In het algemeen echter blijkt dat de bewijzen dezer eigenschappen, met hoeveel verve en toewijding ook door leken gezocht, niet binnen hun bereik liggen, ja zelfs soms nauwelijks en zelfs soms (laten wij hopen: nog) niet binnen dat van de mathematicus.

Juist door de simpelheid der probleemstelling hebben vele problemen in dit gebied een wereldvermaardheid verkregen en, wellicht ten dele hierdoor gegrepen, hebben tal van mathematici naar oplossingen van die problemen gezocht. Dat daarbij soms een geheel nieuw gebied der wiskunde ontgonnen werd was voor de leek minder tot vreugde dan het de wiskundige tot droefheid stemde dat zelfs met deze nieuwgesmede hulpmiddelen hij nog niet tot een oplossing van de vraagstukken kwam. Door dit gebeuren echter kwamen delen van verwante vakken als algebra en analyse tot grote ontwikkeling, welke ontwikkeling vaak haar vruchten weer had in haar bijdrage tot de oplossing van geheel andere vraagstukken.

Eeuwen lang is men in het onzekere geweest of de bewering van Fermat dat hij een kort bewijs had gevonden van de stelling dat er geen gehele x,y,z en $n(n \geq 3)$ bestaan waarvoor geldt $x^n+y^n=z^n$, juist was of niet. Tot dusverre is er voorzover mij bekend is nog geen wiskundige geweest, die van de juistheid of onjuistheid van dit spectaculair geworden vermoeden een bewijs, laat staan een kort bewijs, heeft gegeven. In zijn zoeken naar oplossingen maakte in het midden van de vorige eeuw Kummer een fout, welke na door hem te zijn onderkend, leidde tot de ontwikkeling der ideaaltheorie, een toen nieuwe tak der algebra. Ook wij zullen bij bepaalde bewijzen wel eens van deze theorie gebruik maken.

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

Evenmin als bij het probleem van Fermat weet men thans of het vermoeden van Goldbach juist is. Dit vermoeden luidt dat elk even getal te schrijven zou zijn als de som van twee priemgetallen. Hier werd veelal de analyse te hulp geroepen, waarbij een speciale tak der analyse, zo men wil : der toegepaste analyse, n.l. de analytische getallentheorie tot ontwikkeling kwam. In dit kader past tevens de vermelding van het vermoeden van Riemann dat de functie $\zeta(s)$ welke voor Re $s>1$ gedefinieerd is als $\sum_{n=1}^{\infty} n^{-s}$ en verder daaruit door analytische voortzetting wordt gevonden, afgezien van haar nulpunten $-2,-4,\ldots$ slechts nulpunten s heeft op de rechte Re $s=\frac{1}{2}$. Is dit vermoeden juist dan heeft het belangrijke consequenties voor de getallentheorie,met name voor de verdeling der priemgetallen.

§ 2. Ontbinding

In het vervolg zal voornamelijk worden beschouwd de rij der natuurlijke getallen, soms echter ook haar uitbreiding tot de verzameling der gehele getallen. Beide getalverzamelingen hebben de eigenschap dat met a en b ook $a+b$ en ab ertoe behoren, waarbij voldaan is aan de volgende eigenschappen

A1 $a+0=0+a=a$
A2 $a+b=b+a$
A3 $(a+b)+c=a+(b+c)$

M1 $a.1=1.a=a$
M2 $ab=ba$
M3 $(ab)c=a(bc)$
M4 $a(b+c)=ab+ac$

A4. Bij de tweede der genoemde verzamelingen bezit bovendien de vergelijking $a+x=b$ voor alle a en b een ondubbelzinnig bepaalde oplossing x; men schrijft $x=b-a$.
Het kan voorkomen, dat er bij twee gehele getallen a en b een geheel getal c bestaat, zodanig dat $a=bc$ is. Dan schrijft men wel $b|a$. Is er geen zo'n geheel getal c te vinden, dan schrijft men $b \nmid a$. Een verzameling die voldoet aan de eigenschappen A1-4, M1, M3, M4 noemt men een ring; is tevens voldaan aan M2, dan heet ze een commutatieve ring. De verzameling der gehele getallen is dus een commutatieve ring.

Een zeer belangrijk begrip is het begrip priemgetal. Een priemgetal is een getal dat geen andere factoren bezit dan het getal 1 en zichzelf. De fundamentele stelling welke wij thans als eerste grondresultaat willen afleiden is de stelling dat ieder natuurlijk getal op één en slechts één wijze (afgezien van hun volgorde) te schrijven is als een product

van priemgetallen. Hierbij worden factoren 1 genegeerd. De stelling geldt ook in het gebied der gehele getallen, waarbij nog om de ondubbelzinnigheid te kunnen handhaven een verdere afspraak nodig is, b.v. dat ontbindingen die slechts daarin verschillen dat één of meer factoren door hun tegengestelde zijn vervangen of waarvan het aantal factoren -1 verschilt, als dezelfde worden gerekend.

Men kan zich nu gezien het feit dat de gehele getallen een ring vormen afvragen of een stelling als de hiergenoemde ook geldt voor willekeurige ringen. Het antwoord zal daarbij ontkennend zijn, zoals een tegenvoorbeeld zal leren.

Eerst geven wij nu een bewijs van de grondstelling voor de verzameling der natuurlijke getallen. Daarna laten wij zien dat bij een bepaald type van ringen de stelling ook geldt. Is vervolgens aangetoond dat de verzameling der gehele getallen tot dat type ringen behoort, dan is dus een tweede bewijs gevonden.

Zoëven was sprake van een speciaal type ringen. Dit suggereert al dat de hierboven opgesomde eigenschappen (van ringen of van de natuurlijke getallen) ontoereikend zijn om de grondstelling te bewijzen. Bij ons directe bewijs van de stelling voor de verzameling der natuurlijke getallen gebruiken wij nog iets anders van deze verzameling, n.l. het feit dat ze geordend is, d.w.z.:

Bij ieder tweetal getallen a en b geldt één en slechts één der relaties $a < b$, $a = b$, $b < a$. Men heeft $a < b$ dan en slechts dan als er een natuurlijk getal x bestaat zodanig dat $b = a + x$ is. Gemakkelijk bewijst men nu dat $a < b$ en $b < c$ leiden tot $a < c$, en meer dergelijke eigenschappen (b.v. $a = bc$, $b > 1$ leidt tot $a > c$). Voorts schrijft men voor $b < a$ ook wel $a > b$.

Dat elk natuurlijk getal a een priemontbinding bezit is nu duidelijk. Men heeft wegens bovenstaande opmerking voor een ontbinding $a = bc$ slechts alle natuurlijke getallen b te proberen die $< a$ zijn. Na eindig veel stappen weet men dus of a een factor $< a$ bezit. Is dit niet het geval dan is a zelf priem en is een priemontbinding gevonden die uit slechts één factor bestaat. Is een deler $b < a$ gevonden, waarbij dus $a = bc$ geldt met natuurlijke c, dan herhale men het onderzoek met b resp. c in plaats van a, enz. Juist omdat $b < a$, $c < a$ loopt het verdere onderzoek voor b en c, hun delers, de delers van hun delers enz. na een eindig aantal stappen af en is daarmee dus een priemontbinding van a gevonden. Het bedroevende is dat men in de practijk vrijwel over geen betere methode van ontbinding van een getal beschikt dan de primitieve hier geschetste.

De ondubbelzinnigheid van ontbinding van een natuurlijk getal is echter lastiger te bewijzen. Daarvoor leiden wij enige lemma's af.

Lemma 1. Bij ieder paar natuurlijke getallen a en d is een getal r te vinden met $a=qd+r$, q geheel ≥ 0 en $0 \leq r < d$. ("delen met rest").

Bewijs: Allereerst merken we op dat $(a+1)d \geq a+1 > a$ is, en dat bij $g > a+1$ ook $gd > a$ is. Bijgevolg blijven voor q slechts de eindig veel getallen $0,1,\ldots,a$ over en q is dan het grootste dezer getallen waarvoor $qd \leq a$ is. Immers dan is $r=a-qd \geq 0$ en wegens $(q+1)d > a$ heeft men $r=a-qd < d$.

Lemma 2. Ieder paar natuurlijke getallen a en b bezit een grootste gemeenschappelijke deler d. Deze is te schrijven in de gedaante $d=au+bv$, waarbij u en v geheel zijn.

Bewijs: Daar ieder getal slechts eindig veel delers bezit, bezit ieder tweetal getallen slechts eindig veel gemeenschappelijke delers en dus één grootste gemeenschappelijke deler.

Om nu het tweede deel der bewering af te leiden onderstellen wij $a \geq b$ en gebruiken lemma 1 herhaaldelijk om een rij getallen $q_1,q_2,\ldots$, $r_1,r_2,\ldots$ te bepalen met

$$a=q_0b+r_1, \quad 0 \leq r_1 < b, \quad q_0 \geq 0 ;$$

$$b=q_1r_1+r_2, \quad 0 \leq r_2 < r_1, \quad q_1 \geq 0 ;$$

$$r_1=q_2r_2+r_3, \quad 0 \leq r_3 < r_2, \quad q_2 \geq 0 ;$$

Daar elke rest kleiner is dan de voorafgaande is er een eerste rest die 0 is. Laat dit r_n zijn. Dan heeft men dus

$$r_{n-2}=q_{n-1}r_{n-1}.$$

Het is duidelijk dat iedere deler van a en b ook deler is van b en r_1, dus van r_1 en r_2 enz., van r_{n-1} en 0, d.w.z. van r_{n-1}. Omgekeerd is iedere deler van r_{n-1} ook deler van a en b. Bijgevolg is r_{n-1} de grootste gemeenschappelijke deler van a en b. Verder heeft men $r_{n-1}=r_{n-3}-q_{n-2}r_{n-2}$ en r_{n-2} uitdrukkende in getallen r met lagere indices vindt men zo voortgaande dat r_{n-1} een lineair compositium is van a en b met gehele coëfficiënten.

Lemma 3. Als een priemgetal deelbaar is op een product van twee factoren maar niet op een der factoren, dan is het deelbaar op de andere factor.

Bewijs: Zij p priem en deelbaar op ab, maar niet op a. Dan is de G.G.D. van a en p gelijk aan 1. Volgens lemma 2 bestaan er de gehele getallen u en v met $1=au+pv$. Derhalve $b=abu+pbv$. Daar in het rechterlid beide termen deelbaar zijn door p is ook het linkerlid deelbaar door p.

Grondstelling. Elk natuurlijk getal bezit een ondubbelzinnige (canonieke) ontbinding in priemfactoren.(Hierbij gelden twee ontbindingen als identiek indien zij slechts in de volgorde der factoren verschillen).

Bewijs: Dat ieder getal een ontbinding in priemfactoren bezit is reeds bewezen. Stel nu dat er twee ontbindingen waren

(1) $p_1 \ldots p_s = q_1 \ldots q_t$.

Omdat q_t deelbaar is op $p_1 \ldots p_s$ moet q_t deelbaar zijn op zeker één der factoren $p_1, \ldots, p_s$, b.v. p. Noemt men de overige factoren $p_1' \ldots p_{s-1}'$, dan vindt men dus $p_1' \ldots p_{s-1}' p = q_1 \ldots q_t$, d.w.z. $p_1' \ldots p_{s-1}' = q_1 \ldots q_{t-1}$. Herhaalt men nu dit procédé met q_{t-1} inplaats van q_t enz. dan vindt men successievelijk dat alle factoren van het rechterlid overeenstemmen met die van het linkerlid van (1) en dat s=t is.

Opmerking. Bij de canonieke ontbinding van een getal m pleegt men gelijke priemfactoren samen te nemen. Men schrijft dan $m = p_1^{r_1} \ldots p_s^{r_2}$.

Wij kunnen niet nalaten nu voor ringen in het algemeen een onderzoek naar de grondstelling in te stellen. Eerst moeten wij daarbij nog een en ander preciseren. In het vervolg beschouwen wij een voorlopig willekeurige commutatieve ring, zonder nuldelers, d.w.z. een ring, waarbij ab=0 slechts kan gelden als òf a=0 òf b=0. Zo'n ring heet een integriteitsgebied.

Definitie. Een eenheid is een getal dat deelbaar is op het getal 1.

Voorbeeld: -1 is een eenheid.

Stelling: Een eenheid bezit een inverse; omgekeerd, bezit een getal een inverse dan is het een eenheid.

Immers zij u een eenheid, dan bestaat er een getal v met uv=1; dit getal v is het inverse van u.

Is omgekeerd gegeven dat een getal u een inverse (v) bezit, dan geldt uv=1, dus u is een eenheid.

Opgave 1. Het product van twee eenheden is weer een eenheid; elke macht (met gehele exponent) van een eenheid is weer een eenheid.

Definitie. Twee getallen heten geassocieerd als hun quotiënt een eenheid is.

Stelling: Als a|b en b|a, dan zijn a en b geassocieerd. Immers uit b=qa en a=rb volgt b=qrb, dus (qr-1)b=0, dus qr=1 als $b \neq 0$. Dus q is een eenheid.

Is b=0, dan is a=0 en ook dan zijn a en b kennelijk geassocieerd.

Bij het beschouwen van de grondstelling voor willekeurige ringen dient men - om de eenduidigheid der ontbinding te kunnen handhaven - allereerst af te spreken, dat twee ontbindingen, die slechts daarin verschillen dat een of meer der factoren door hun geassocieerde zijn vervangen en een of meer eenheden zijn toegevoegd (of weggelaten), als dezelfde worden gerekend. (Dit merkten wij hierboven al op bij de ontbinding van gehele getallen, b.v. 21=3.7, maar ook 21=(-3)(-7) en 21=(-1)(-3)7 enz.) Wij gaan nu met deze afspraak over aequivalentie van

ontbindingen de grondstelling nader onderzoeken.

Allereerst geven wij een voorbeeld dat niet in iedere ring zonder nuldelers de grondstelling geldt. Immers beschouw de verzameling der getallen a+bj, waarbij a en b willekeurig geheel zijn en $j=\sqrt{-6}$ is.

Opgave 2. Toon aan dat deze getallen een integriteitsgebied vormen.

Wij laten thans zien dat het getal 10 in deze verzameling twee verschillende priemontbindingen heeft, allereerst de welbekende 10=2.5 en verder 10=(2+j)(2-j).

Het bewijs is geleverd als wij aantonen dat elk der vier getallen 2,5,2+j en 2-j priem is en geen tweetal hunner geassocieerd is.

Stel 2 was samengesteld en $a+bj \mid 2$. Dan ook $a-bj \mid 2$.

Opgave 3. Bewijs dat.

Dus $a^2+6b^2 \mid 4$. Hieruit volgt direct b=0, a= ± 1 of ± 2.

Opgave 4. Toon evenzo aan dat 5 priem is in deze verzameling.

Was voorts 2+j samengesteld dan leidde $a+bj \mid 2+j$ tot $a-bj \mid 2-j$ dus $a^2+6b^2 \mid 10$. Kennelijk is $b \neq 0$, dus $b^2 \geq 1$, dus $a^2 \leq 4$. Men vindt dan $a=\pm 2$, $b=\pm 1$, waarvan slechts 2+j en -2-j voldoen. Evenzo blijkt 2-j priem te zijn.

Dat tenslotte geen twee der getallen 2,5,2+j,2-j geassocieerd zijn volgt gemakkelijk door deling.

Opgave 5. Voer dit uit.

Na het bovenstaande is het zonder meer duidelijk, dat een extra-voorwaarde aan een integriteitsgebied moet worden opgelegd wil erin de grondstelling gelden.

Om deze te kunnen formuleren voeren wij een nieuw begrip in: het begrip ideaal.

Definitie. Een ideaal is een deelverzameling van een ring met de volgende eigenschappen:

Behoren a en b ertoe, dan ook a-b;

behoort a ertoe en r tot de ring, dan behoort ra tot het ideaal.

Gevolg. Met a en b behoort ook a-a=0, dus 0-b=-b, dus a-(-b)=a+b tot het ideaal.

Opmerking. Bezit de ring een eenheidselement dan mag men in de definitie van ideaal in de eerste regel de uitdrukking a-b vervangen door a+b. Immers als a en b tot het ideaal behoren dan ook (-1)b en dus a+(-1)b= =a-b.

Voorbeelden. Bij de ring der gehele getallen vormen alle even getallen een ideaal. Bij de ring der veeltermen (met b.v. willekeurige complexe coëfficiënten) in één veranderlijke x vormen alle door x deelbare veeltermen een ideaal.

Opgave 6. Bewijs dat.

Onder de idealen zijn er bijzondere waarvan alle elementen veelvouden zijn van één element uit het ideaal. Zulke idealen heten hoofdidealen. Zijn alle elementen veelvouden van a, dan geeft men zo'n ideaal aan met (a).

Nu bestaan er ringen waarbij ieder ideaal hoofdideaal is. Zulke ringen noemt men hoofdideaalringen. Wij zullen nu de volgende stelling afleiden:

In een hoofdideaalring geldt de grondstelling over ontbinding.

Bewijs: eerst tonen wij de mogelijkheid van de ontbinding van een element van onze ring aan, daarna de eenduidigheid (met inachtneming van de bekende hierbovengenoemde afspraken).

Wij merken eerst op dat een priemgetal zeker een priemontbinding bezit. Beschouw nu een element a van de ring dat niet in priemfactoren te ontbinden is. Dan is a niet priem, dus zeker van de gedaante a_1b_1, waarbij ten minste een der getallen a_1 en b_1 niet te schrijven is als een product van priemelementen en de ander geen eenheid is.

Laat de ene a_1 en de andere b_1 zijn. Handel daarna met a_1 evenzo; d.w.z. $a_1=a_2b_2$, waarbij a_2 niet als een product van priemelementen te schrijven is en $b_2$geen eenheid is. Zo voortgaande vinden wij $a=a_nb_nb_{n-1}\ldots b_1$, waarbij a_n niet als product van priemelementen te schrijven is,enz. Beschouw nu alle elementen u van onze ring die veelvouden zijn van minstens een der getallen $a_1,a_2,\ldots$ Het is direct in te zien, dat deze getallen een ideaal vormen.

Opgave 7. Bewijs dat.

Op grond van het feit dat de beschouwde ring hoofdideaalring is is het hier geconstrueerde ideaal een hoofdideaal, d.w.z. er bestaat een element u zodat het ideaal de gedaante (u) bezit. Daar u tot het ideaal behoort is er een a_n met $a_n|u$. Daar a_{n+1} ook tot het ideaal behoort is $u|a_{n+1}$. Dus $a_n|a_{n+1}$. Daar ook $a_{n+1}|a_n$ zou b_{n+1} een eenheid zijn, in strijd met de onderstelling dienaangaande. Een onontbindbaar element a van onze ring bestaat er dus niet. Thans onderzoeken wij de eenduidigheid der ontbinding. Hiertoe tonen wij ook nu weer lemma 3 aan, waarna de ondubbelzinnigheid der ontbinding geheel zo als hierboven volgt.

Laat dan een priemelement p van de ring deelbaar zijn op een product ab, maar niet op a. Beschouw de verzameling der getallen van de gedaante ua+vp, waarbij u en v tot de grondring behoren. Deze verzameling is een ideaal.

Opgave 8. Bewijs dat.

De verzameling is dus een hoofdideaal, d.w.z. alle elementen ervan zijn veelvouden van een element g van het ideaal. Daar p tot het ideaal behoort is g, afgezien van eenheden, gelijk aan p of 1. Daar ook a tot

dit ideaal behoort, maar volgens onderstelling niet een veelvoud is van p moet g=1 zijn. Bijgevolg bestaan er elementen x en y uit de ring met 1=xa+yp. Dan heeft men b= ab+yp en wegens p|ab vinden wij dan p|b.

Het onderzoek naar de geldigheid der grondstelling kan dus soms geschieden door na te gaan of de beschouwde verzameling een hoofdideaalring is. Voor het onderzoek naar dit laatste is nog een ander begrip van belang.

Men noemt een ring Euclidisch als bij elk element een niet negatief geheel getal bestaat (dat men de norm of de waardering van a noemt en dat wordt aangegeven met $|\ |$ of soms met $\|a\|$) met de volgende eigenschappen:

1. $|0|=0$, $|a|>0$ als $a\neq 0$;
2. $|ab|\leqq|a|\,|b|$;
3. bij elk stel elementen a en b met $b\neq 0$ bestaan elementen q en r zodanig dat $a=qb+r$, $|r|<|b|$.

Wij laten nu zien dat een Euclidische ring een hoofdideaalring is.

Beschouw daartoe een willekeurig ideaal uit de ring. Beschouw verder een element b uit het ideaal met minimale positieve norm. Dan is dus $b\neq 0$. Zij nu a een willekeurig element van het ideaal. Dan bepale men volgens 3° elementen q en r van de ring zodanig dat $a=qb+r$ en $|r|<|b|$. Ondat a en b tot het ideaal behoren, behoort $r=a-qb$ er ook toe. Op grond van de onderstellingen over $|b|$ moet $|r|=0$ zijn, dus $r=0$ en $a=qb$. Het ideaal is dus het ideaal (b).

Opgave 9. Bewijs dat bij een ideaal in een Euclidische ring alle elementen met minimale positieve norm geassocieerd zijn.

Wij besluiten nu deze paragraaf met enige voorbeelden van Euclidische ringen, dus hoofdideaalringen, dus ontbindingsringen.

Als eerste voorbeeld mogen wij de verzameling der gehele getallen noemen.

Opgave 10. Bewijs dit. Bepaal tevens alle eenheden in deze verzameling.

Een verder voorbeeld is de ring van Gauss, dat is de verzameling der getallen $\alpha=a+bi$, waarbij a en b geheel zijn.

Hier voeren wij in $|a+bi|=a^2+b^2=\alpha\bar{\alpha}$. Voor twee elementen α en β van deze ring geldt $|\alpha\beta|=|\alpha|\,|\beta|$. Immers $|\alpha\beta|=\alpha\beta\overline{\alpha\beta}=\alpha\beta\bar{\alpha}\bar{\beta}=$ $=\alpha\bar{\alpha}\beta\bar{\beta}=|\alpha||\beta|$.

Wij tonen nu aan, dat bij willekeurige α en β met $\beta\neq 0$ elementen κ en ϱ van de ring van Gauss bestaan zodanig dat $\alpha=\kappa\beta+\varrho$, $|\varrho|<|\beta|$. Daartoe bepalen wij het quotient $\frac{\alpha}{\beta}=\gamma=c+di$ waarbij c en d rationaal zijn. Zijn k en h de meest nabijzijnde gehele getallen van c resp. d, dan neme men $\kappa=k+hi$, dus $\gamma=\kappa+\lambda$ met $\lambda=c-k+(d-h)i$, derhalve $|\lambda|\leqq(c-k)^2+(d-h)^2\leqq(\frac{1}{2})^2+(\frac{1}{2})^2=\frac{1}{2}$. Bijgevolg is $\alpha=\beta\gamma=\beta\kappa+\beta\lambda=\beta\kappa+\varrho$

met $\varrho = \beta\lambda$ en $|\varrho| = \frac{1}{2}|\beta| < |\beta|$, waarmede de bewering bewezen is. Hiermede is dus tevens aangetoond dat in de ring van Gauss de grondstelling geldt, een feit dat wij later nog zullen uitbuiten.
Geheel op dezelfde wijze is het bewijs te leveren dat de ring $R(i\sqrt{2})$, dat is de verzameling der getallen $a+bi\sqrt{2}$ met gehele a en b Euclidisch is, zodat ook daar de grondstelling geldt.
Opgave 11. Voer dit uit.
Opgave 12. Toon aan dat de ringen $R(\sqrt{2})$ en $R(\frac{1}{2}+\frac{1}{2}i\sqrt{3})$ Euclidisch zijn. Als norm van een getal $a+b\sqrt{2}$ neme men $|a^2-2b^2|$ en van een getal $\alpha=a+b(\frac{1}{2}+\frac{1}{2}i\sqrt{3})$ neme men $a^2-ab+b^2=\alpha\bar{\alpha}$. Gezien het feit dat de getallen van $R(i\sqrt{6})$ zoals hierboven bleek geen ondubbelzinnige priemontbinding bezitten rijst nu de vraag voor welke m de ring $R(\sqrt{m})$ wel en voor welke m niet Euclidisch is. Hierbij zij nog opgemerkt dat als $m \equiv 1 \pmod 4$ is, men om bepaalde redenen niet de ring $R(\sqrt{m})$ maar de ring $R(\frac{1}{2}+\frac{1}{2}\sqrt{m})$ beschouwt. Vergelijk de volgende
Opgave 13. Toon aan dat in de ring $R(i\sqrt{3})$ de grondstelling niet geldt.

Het antwoord op bovengestelde vraag is door samenvoeging van tal van op dit gebied gevonden resultaten tenslotte eerst onlangs gegeven. Het is gebleken, dat er slechts 21 waarden van m zijn waarvoor $R(\sqrt{m})$ resp. $R(\frac{1}{2}+\frac{1}{2}\sqrt{m})$ Euclidisch is. Verre van hier die moeizaam verkregen resultaten af te leiden volstaan wij tot besluit van dit hoofdstuk met de opsomming dezer 21 waarden. Het bleken te zijn
m=-11,-7,-3,-2,-1,2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73.

§3. Klassieke problemen over priemgetallen.

Reeds Euclides bewees dat er oneindig veel priemgetallen bestaan. Zijn bewijs verliep als volgt. Stel dat men de rij der priemgetallen $p_1=2, p_2=3, p_3=5, \ldots$ kent tot en met het n^e priemgetal p_n. Beschouw dan de uitdrukking $P=p_1p_2\ldots p_n+1$. Kennelijk is deze niet deelbaar door een der priemgetallen $p_1,\ldots p_n$. Is ze zelf priem dan is hiermede een nieuw priemgetal gevonden; is ze samengesteld dan is elk harer priemdelers een nieuw priemgetal.

Hierbij valt op te merken, dat men in plaats van P in het geschetste procédé ook de uitdrukking P-2 kan nemen, of zelfs een willekeurig compositum

$$\lambda q_1 \ldots q_r + \mu q_{r+1} \ldots q_n ,$$

waarbij de getallen $q_1,\ldots q_n$ een permutatie der getallen $p_1,\ldots,p_n$ zijn en λ en μ gehele getallen, die slechts zo behoeven te worden gekozen dat dit compositum niet deelbaar is op enige macht van $q_1 \ldots q_n$.

Een volgende vraag, die men zich zou kunnen stellen, betreft de

dichtheid der priemgetallen, welke hierop neer komt dat men het gedrag van p_n als functie van n wil bepalen of omgekeerd n als functie van p_n. In het laatste geval zoekt men dus naar een betrekking voor het aantal $\pi(u)$ der priemgetallen dat $\leq u$ is. Wij kunnen hier reeds, uitgaande van Euclides' bewijs, een zeer grove schatting voor p_n maken, nl. $p_n \leq 2^{2^{n-1}}$. Immers voor n=1 is deze juist. Zij nu de relatie bewezen voor alle natuurlijke getallen $\leq n$, dan vindt men

$$p_{n+1} \leq p_1 \cdots p_n + 1 \leq 2^{2+\ldots+2^{n-1}} + 1 = 2^{2^n - 1} + 1 < 2^{2^n}.$$

Voorts vindt men hieruit voor $\pi(u)$ de schatting $\pi(u) > {}^2\log {}^2\log u$. Immers bepaal het grootste natuurlijke getal m met $2^{2^m} \leq u$. Dan geldt $u < 2^{2^{m+1}}$ en verder $\pi(u) \geq \pi(2^{2^m}) > m+1 > {}^2\log {}^2\log u$.

Wij zullen spoedig veel scherpere schattingen voor p_n en $\pi(u)$ geven zonder echter het scherpe resultaat $\pi(u)$ is $\frac{u}{\log u}$ af te leiden.

Eerst echter willen wij het procédé van Euclides toepassen om aan te tonen dat er oneindig veel priemgetallen bestaan die een viervoud +3 zijn. Hiertoe beschouwe men niet de hierboven genomen uitdrukkung P maar de uitdrukking $Q = 4p_1 \ldots p_n - 1$. Daar het product van viervouden +1 weer een viervoud +1 is, moet er in Q ten minste één factor zitten die een viervoud +3 is. Uit het feit dat deze kennelijk verschilt van elk der getallen $p_1, \ldots, p_n$, dus zeker van alle priemgetallen $\leq p_n$, die een viervoud +3 zijn, volgt nu de bewering direct.

Op volkomen analoge wijze toont men aan dat er oneindig veel priemgetallen bestaan, die een zesvoud -1 zijn.

Opgave 1. Voer dit uit.

Beide bovenstaande resultaten zijn bijzondere gevallen van de beroemde stelling van Dirichlet, welke zegt dat iedere rekenkundige reeks, waarvan het verschil en de eerste term onderling ondeelbaar zijn, oneindig veel priemgetallen bevat. Wij zullen het klassieke bewijs van deze stelling dat essentieel gebruikt maakt van functietheorie en verder van nog tal van eerst later in te voeren getallentheoretische begrippen, hier uiteraard niet geven. Van deze stelling, evenals van het resultaat $\pi(u) \backsim \frac{u}{\log u}$, zijn in 1950 elementaire (maar meer moeizame) bewijzen gegeven door A. Selberg en P. Erdös.

Wij willen thans nog een ander bewijs geven van Euclides' eerste resultaat, dat er oneindig veel priemgetallen zijn. Hiertoe voeren wij in de getallen $F_n = 2^{2^n} + 1$ van Fermat. Voor $n \neq m$ geldt $(F_n, F_m) = 1$. Immers stel $m > n$. Dan is $m \geq n+1$. Dus $2^{n+1} \mid 2^m$ (lees: 2^{n+1} is deler van 2^m), dus $2^{2^{n+1}} - 1 \mid 2^{2^m} - 1$. Zij nu p een priemdeler van F_n. Dan $p \mid 2^{2^n} + 1 \mid 2^{2^{n+1}} - 1 \mid 2^{2^m} - 1 = F_m - 2$. Dus $p \nmid F_m$ (lees: p is niet deelbaar op F_m). Bijgevolg moet ieder element der rij $F_0, F_1, F_2, \ldots$ een nieuwe priemdeler bezitten, waarmee de stelling opnieuw bewezen is.

De getallen van Fermat spelen in de wiskunde nog verder een rol. Gauss heeft bewezen dat regelmatige veelhoeken met p zijden (waarbij p= een oneven priemgetal is) dan en slechts dan te construeren zijn als p gelijk is aan een macht van 2 vermeerderd met 1. De vraag komt dan op welke van dergelijke getallen priem zijn. Dat 2^a+1 in het geval dat a niet een macht is van 2 samengesteld is, is evident; immers als $2 \nmid p \mid a$, dan $2^{a/p}+1 \mid 2^a+1$. Het onderzoek voert dus tot het bepalen van de priemgetallen in de rij $F_0, F_1, \ldots$. Ver is men hiermee nog niet gevorderd. De resultaten voor F_0 en F_1 zijn bekend en bij het middelbaar en gymnasiaal onderwijs uitgebuit. Voor $p=F_2=17$ gaf Gauss in 1806 een eenvoudige constructie der bijbehorende regelmatige veelhoek. Ook $F_3=257$ en zelfs $F_4=65537$ zijn behandeld. Reeds Euler bewees echter dat $F_5=2^{32}+1$ samengesteld is (nl. de deler 641 bevat). Dit is gemakkelijk te verifieren (maar lastiger vast te stellen). Immers voor $q=641$ heeft men $q=5.2^7+1$, dus $q \mid 5^3.2^{21}+1 \mid 625.2^{21}+5$, dus $q \mid -2^4.2^{21}+5$ d.w.z. $q \mid 2^{25}-5$; dan $q \mid 2^{32}-5.2^7=2^{32}-640$, waaruit de bewering volgt.

Enigermate verwant met de getallen van Fermat zijn die van Mersenne $M_n=2^n-1$. Kennelijk is M_n samengesteld als n het is. Mersenne meende dat M_n priem is voor

$$n=2,3,5,7,13,17,19,31,67,127 \text{ en } 257.$$

Latere onderzoekingen leerden dat dit het geval is voor

$$n=2,3,5,7,13,17,19,31,61,89,107,127,521,607,127,2203,2281,$$

waarmede niet gezegd is dat voor alle tussengelegen priemwaarden van n het gedrag van M_n beslist is. Het getal $M_{2281}=2^{2281}-1$ was in 1954 het grootste officieel bekende priemgetal. Het getal $2^{8191}-1$, om bepaalde redenen onderzocht, bleek samengesteld te zijn. Het onderzoek maakt gebruik van een methode van Lucas, waarop wij nog nader terugkomen.

De getallen van Mersenne spelen een rol in het klassieke probleem naar het zoeken van volmaakte getallen, dat zijn getallen die gelijk zijn aan de som van hun delers (waarbij het getal zelf niet maar de deler 1 wèl wordt meegeteld). Men kan ook zeggen, dat zo'n getal gelijk is aan de helft van de som van al zijn delers. Wij bewijzen dat een even getal dan en slechts dan volmaakt is, als het van de gedaante $m=\frac{1}{2}p(p+1)$ is, waarbij p een priemgetal van Mersenne is.

Zij nl. $p=2^n-1$ priem dan is $m=2^{n-1}(2^n-1)$. De delers van m zijn de getallen $1,2,\ldots,2^{n-1}$ en $p,2p,\ldots 2^{n-1}p$ met som $(p+1)(1+\ldots 2^{n-1}) = (p+1)(2^n-1)=p(p+1)=2m$. Omgekeerd zij m volmaakt en even. Stel $m=2^n u$, waarbij $n \geq 1$ en u oneven is. Alle delers van m vindt men door alle delers van u te nemen en die te vermenigvuldigen resp. met $1,2,\ldots,2^n$. Geeft men, zoals gebruikelijk is, de som der delers van u aan met $\sigma(u)$, dan heeft men dus

$$2m=(1+2+\ldots+2^n)\,\sigma(u)=(2^{n+1}-1)\,\sigma(u),$$

dus

$$\sigma(u)=\frac{2^{n+1}u}{2^{n+1}-1}=u+\frac{u}{2^{n+1}-1}\ .$$

Hieruit volgt allereerst $2^{n+1}-1 \mid u$. Nu is $\sigma(u)\geq u+1$, dus $u\geq 2^{n+1}-1$. Was $u>2^{n+1}-1$ dan bezat u nog een andere deler dan $2^{n+1}-1$, hetgeen echter zou leiden tot $\sigma(u)>u+\frac{u}{2^{n+1}-1}$. Bijgevolg $u=r^{n+1}-1$ en $m=2^n(2^{n+1}-1)$, waarbij $2^{n+1}-1$ alleen zichzelf en 1 tot delers mag hebben, zodat $2^{n+1}-1$ een Mersenne priemgetal is.

Het is onbekend of er oneven volmaakte getallen bestaan.

Aan het bovenstaande willen wij nu nog een methode van Tchebycheff toevoegen, die ons een veel betere schatting van $\pi(n)$ levert dan de hier gevondene. Allereerst geven wij een hulpeigenschap, die zegt dat het aantal priemfactoren p dat in de uitdrukking m! bevat is, gelijk is aan $\left[\frac{m}{p}\right]+\left[\frac{m}{p^2}\right]+\left[\frac{m}{p^3}\right]+\ldots$, waarbij de reeks uiteraard afbreekt.

Hierbij stelt het symbool $[u]$ (lees: u entier) het grootste natuurlijke getal $\leq u$ voor; het kleinste natuurlijke getal $\geq u$ geeft men soms wel met $\{u\}$ aan. Wij laten het bewijs gaarne aan de lezers over.

Wij gaan nu uit van een natuurlijk getal n en beschouwen de binomiaalcoëfficiënt $N=\binom{2n}{n}=\frac{(2n)!}{n!\,n!}$. Het product P van alle priemgetallen tussen n en 2n is kennelijk deelbaar op N. Het aantal dezer priemgetallen is juist gelijk aan $\pi(2n)-\pi(n)$, dus $N\geq n^{\pi(2n)-\pi(n)}$ (hierbij is elk dier priemfactoren door n geminoreerd). Anderzijds ziet men gemakkelijk in dat $N=\binom{2n}{n}<2^{2n}$.

<u>Opgave 2</u>. Bewijs dit.

Bijgevolg heeft men $2^{2n}>n^{\pi(2n)-\pi(n)}$, dus

$$(1)\qquad \pi(2n)-\pi(n)<\frac{2n\log 2}{\log n}=\frac{n\log 4}{\log n}\ .$$

Zij nu m een willekeurig natuurlijk getal. Bepaal het grootste natuurlijke getal t met $2^t\leq m$. Dus $m<2^{t+1}$ en $t\leq\frac{\log m}{\log 2}$. Pas nu relatie (1) toe met $n=2^2,2^3,\ldots,2^t$. Na optelling der zo gevonden resultaten vindt men

$$\pi(2^{t+1})-\pi(4)<\log 4\sum_n\frac{n}{\log n}=\log 4\sum_{s=2}^{t}\frac{2^s}{s\log 2}=\sum_{s=2}^{t}\frac{2^{s+1}}{s}=$$

$$=2\sum_{s=2}^{t}\frac{(\frac{4}{3})^s(\frac{3}{2})^s}{s}\ .$$

Nu is de functie $\frac{(\frac{3}{2})^s}{s}$ monotoon stijgend voor $s\geq 3$ en $\frac{(\frac{3}{2})^3}{3}=\frac{(\frac{3}{2})^2}{2}$.

Opgave 3. Bewijs de eerste dezer beweringen.

Men vindt dan

$$\pi(2^{t+1})-\pi(4) < 2.\frac{(\frac{3}{2})^t}{t} \cdot \sum_{s=2}^{t}(\frac{4}{3})^s < \frac{(\frac{3}{2})^t.6}{t}.(\frac{4}{3})^{-t+1} = 8.\frac{2^t}{t} < 8.\frac{2^r}{r}$$

met $r=\frac{\log m}{\log 2} \geqq t$ (want ook $\frac{2^t}{t}$ is monotoon stijgend voor $t \geqq 2$).

Dus

$$\pi(2^{t+1})-\pi(4) < 8.\frac{2^{\frac{\log m}{\log 2}}}{\log m} = \frac{8m}{\log m} .$$

en

$$\pi(m) \leqq \pi(2^{t+1}) < \frac{8m}{\log m} + 2.$$

Wij geven thans ook een ongelijkheid voor $\pi(m)$ in de andere richting. Beschouw daartoe wederom de uitdrukking $N=\binom{2n}{n}$. Ontbinding van N leert $N=\prod_p p^v$, uitgestrekt over alle priemdelers van N, waarvoor uiteraard slechts de $\pi(2n)$ priemgetallen $< 2n$ in aanmerking komen. De exponent v van zo'n priemdeler p vinden wij uit de hierboven gegeven hulpstelling. Hiervoor geldt

$$v=\sum_{j=1}^{s}\left\{\left[\frac{2n}{p^j}\right] -2\left[\frac{n}{p^j}\right]\right\} ,$$

waarbij uiteraard deze som niet verder behoeft te worden uitgestrekt dan het grootste natuurlijke getal s waarvoor $p^s \leqq 2n$. Het is voorts duidelijk dat elke term der som $\leqq 1$ is.

Opgave 4. Bewijs dit.

Bijgevolg geldt $v \leqq s$ en dus $p^v \leqq p^s \leqq 2n$. Wij gebruiken nu nog de relatie $2^n \leqq \binom{2n}{n}$.

Opgave 5. Bewijs deze.

Wij verkrijgen dan

$$2^n \leqq \binom{2n}{n} = \prod_p p^v \leqq \prod_p (2n) = (2n)^{\pi(2n)} .$$

Hieruit volgt $\pi(2n) > \frac{n \log 2}{\log(2n)}$.

Zij nu m een willekeurig natuurlijk getal en t het grootste natuurlijke getal met $2^t \leqq m$. Dus als boven $m < 2^{t+1}$ en $t \leqq \frac{\log m}{\log 2} = r < t+1$.

Dan vindt men

$$\pi(m) \geqq \pi(2^t) > \frac{2^{t-1}\log 2}{\log 2^t} = \frac{2^{t-1}}{t} = \frac{2^{t+1}}{4(t+1)} > \frac{2^r}{4r}$$

$$= \frac{1}{4} \cdot \frac{m \log 2}{\log m} = \frac{\log 2}{4} \cdot \frac{m}{\log m} .$$

De resultaten samenvattende vinden wij dus

$$\frac{\log 2}{4}\,\frac{m}{\log m} < \pi(m) < \frac{8m}{\log m} + 2,$$

waaruit volgt dat $\frac{\pi(m)}{m/\log m}$ voor $m \to \infty$ begrensd blijft. Hier blijkt die grens tussen $\frac{\log 2}{4}$ en 8 te liggen; met scherpere methoden vindt men het hier niet te bewijzen resultaat dat de uitdrukking voor $m \to \infty$ een limiet 1 bezit.

§4. Congruenties, restklassen.

Beschouwen wij eerst de verzameling der gehele getallen. Hierin definieert men $a \equiv b \pmod m$ (lees: a congruent met b modulo m) als $m \mid a-b$. Het hier ingevoerde congruentiebegrip is een aequivalentiebegrip.

Opgave 1. Bewijs dat.

Voor congruenties gelden de volgende belangrijke eigenschappen. Uit $a_i \equiv b_i \pmod m$ $(i=1,2)$ volgt $a_1+a_2 \equiv b_1+b_2 \pmod m$, $a_1-a_2 \equiv b_1-b_2 \pmod m$ en $a_1a_2 \equiv b_1b_2 \pmod m$.

Opgave 2. Bewijs deze drie eigenschappen.

In het bijzonder leert de laatste eigenschap dat uit $a \equiv b \pmod m$ volgt $ac \equiv bc \pmod m$. Omgekeerd echter volgt uit $ac \equiv bc \pmod m$ niet noodzakelijk $a \equiv b \pmod m$. Immers uit $m \mid ac-bc = c(a-b)$ volgt slechts dat $a-b$ die factoren van m bevat voorzoveel ze niet in c bevat zijn, d.w.z. men vindt niet dat m deelbaar is op a-b, maar dat $\frac{m}{(m,c)}$ het is, d.w.z. men vindt $a \equiv b \pmod{\frac{m}{(m,c)}}$.

Verder volgt nog uit $a \equiv b \pmod m$ voor veeltermen $f(u)$ de relatie $f(a) \equiv f(b) \pmod m$, waarbij alle coëfficiënten van $f(u)$ geheel ondersteld zijn.

Opgave 3. Bewijs dit.

Onder een compleet restsysteem mod m verstaat men een m-tal gehele getallen, waarvan er geen twee congruent zijn mod m. Een compleet restsysteem mod m is b.v. het stel getallen $0,1,\ldots,m-1$. Ieder ander m-tal getallen dat congruent is resp. met deze m getallen noemt men ook een compleet restsysteem. Zo vormen b.v. de getallen $0,2^0,2^1,2^2,\ldots,2^{10}$ een compleet restsysteem mod 11.

Opgave 4. Ga dit na.

Wij willen nu, nog steeds bij gegeven m, alle mod m onderling congruente getallen samen beschouwen. Men zegt dat deze één restklasse mod m vormen. Deze is bepaald door één harer elementen, die dan als vertegenwoordiger of representant der restklasse optreedt. In bovenstaand voor-

beeld met m=11 stelt b.v. 2^6 dezelfde restklasse voor als 9. De verzameling der gehele getallen valt dus mod m uiteen in m restklassen, elk kennelijk bestaande uit oneindig veel elementen. De verzameling dier m restklassen geeft men, als men de verzameling der gehele getallen met R aanduidt, wel aan met R/(m).

Ook in de algebra komt een dergelijk begrip voor. Is R een willekeurige ring en I een ertoe behorend ideaal, dan voert men in de restklassenverzameling R/I. Twee elementen a en b van R behoren tot dezelfde restklasse als hun verschil in I ligt. Men schrijft ook hier $a \equiv b \pmod{I}$. Is dit niet het geval, dan behoren ze tot verschillende elementen. Als a en b en ook b en c tot dezelfde restklasse mod I behoren, dan liggen zowel a-b als b-c in I, dus op grond van een der grondeigenschappen van idealen, ligt ook hun som a-c in I, dus ook a en c behoren tot dezelfde restklasse. De andere grondeigenschap van idealen leert dat als a en b tot eenzelfde restklasse mod I behoren, ook ac en bc tot eenzelfde restklasse mod I behoren. Bij bovenstaand voorbeeld over restklassen mod m is voor I het hoofdideaal (m) genomen.

Wij willen hier volstaan met de vermelding van deze algebraïsche generalisatie zonder er thans een essentieel verder gebruik van te maken. Wij keren dus nu terug tot het vertrouwde domein der gehele getallen.

Zoals in de algebra naast relaties vergelijkingen optreden, zo treden in de getallentheorie naast congruenties van het hier geschetste soort ook congruenties op van het type $f(x) \equiv 0 \pmod{m}$. Wij willen enige eigenschappen van dergelijke congruenties onderzoeken.

Onderstel dat f(x) een veelterm is met gehele coëfficiënten, (wij noemen voortaan dergelijke veeltermen kortweg geheel), dan behoeft men, omdat zoals zoëven bleek, bij $x \equiv u \pmod{m}$ geldt $f(x) \equiv f(u) \pmod{m}$, slechts van de natuurlijke getallen $0,1,\ldots,m-1$ te onderzoeken welke aan de congruentie voldoen. Vindt men onder deze één oplossing, dan zegt men dat de gegeven congruentie één wortel (of oplossing) bezit.

Thans geven wij beschouwingen, die herinneren aan de reststelling uit de algebra. Wij beschouwen een geheel polynoom $f(x)=\sum_{n=0}^{N} c_n x^n$. Dan geldt $f(x)-f(a)=\sum_{n=0}^{N} c_n(x^n-a^n)=\sum_{n=0}^{N} c_n(x-a)(x^{n-1}+\ldots+a^{n-1})=(x-a)g(x)$, waarbij ook g(x) gehele coëfficiënten bezit. Gevolg: Is a een wortel der congruentie $f(x) \equiv 0 \pmod{p}$, waarbij p een priemgetal is, dan is $f(a) \equiv 0 \pmod{p}$, dus $(x-a)g(x) \equiv 0 \pmod{p}$. Juist omdat p een priemgetal is is deze congruentie slechts te vervullen door hetzij $x-a \equiv 0 \pmod{p}$, hetzij $g(x) \equiv 0 \pmod{p}$ te nemen. Is een wortel b van deze laatste congruentie bekend, dan volgt daaruit op analoge wijze het bestaan van een

gehele veelterm h(x), zodanig dat $g(x) \equiv (x-b)h(x) \pmod p$ is. Zo voortgaande ziet men gemakkelijk in dat wij hier tot het volgende analogon van de hoofdstelling van de algebra komen: Voor een gehele veelterm f(x) van de n^e graad en een priemgetal p bezit de congruentie $f(x) \equiv 0 \pmod p$ ten hoogste n oplossingen.

Dat de restrictie dat p een priemgetal is nodig is, blijkt uit het volgende tegenvoorbeeld: De congruentie $x^2-1 \equiv 0 \pmod 8$ bezit 4 oplossingen (nl. 1,3,5 en 7). Dat voorts de woorden "ten hoogste" in tegenstelling tot in de algebra niet mogen worden weggelaten, leert ons het voorbeeld $x^2+1 \equiv 0 \pmod 3$; deze congruentie bezit nl. geen oplossingen.

Opgave 5. Bewijs dit.

Wij willen nu allereerst de eerste graadscongruentie

$$ax \equiv b \pmod p \qquad (a \text{ en } b \text{ geheel})$$

oplossen. Wij onderstellen daarbij uiteraard dat p niet deelbaar is op a. Laat nu x een volledig restsysteem mod p, bv. de rij der getallen 0,1,2,...,p-1 doorlopen. Dan doorloopt ax ook zo'n systeem. Immers elk tweetal getallen ax' en ax" is incongruent mod p, want als $p \mid ax'-ax" = a(x'-x")$ dan volgt uit $p \nmid a$ direct dat $p \mid x'-x"$, in strijd met de onderstelling over x' en x". De p getallen ax zijn dus twee aan twee incongruent mod p en vormen derhalve inderdaad een volledig restsysteem mod p. Dan moet er dus precies één getal x zijn dat mod p congruent is met b. Dit is dus de enige oplossing onzer congruentie. Men schrijft deze wel als $a^{-1}b$ mod p of ba^{-1} mod p. Kennelijk is dus a^{-1} de oplossing der congruentie $ax \equiv 1 \pmod p$. Zo is bv. 3^{-1} mod 5 gelijk aan het getal 2, 7^{-1} mod 11 gelijk aan 8. In het bovenstaande is echter geen constructieve methode gegeven om het getal a^{-1} mod p te bepalen. Een ietwat omslachtige methode volgt uit een overweging die nauw aansluit aan bovenstaand bewijs. Beschouw nl. eens alle p-1 getallen 1,2,...,p-1. Dan vormen als $p \nmid a$ is, de p-1 getallen a,2a,...(p-1)a, afgezien van het getal 0, ook een volledig restsysteem mod p. De elementen van dit nieuwe restsysteem zijn dus in een of andere volgorde mod p congruent met de getallen 1,2,...,p-1; bijgevolg vindt men na product nemen

$$1.2. \ldots (p-1) \equiv a.2a. \ldots (p-1)a \pmod p$$

dus

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

Omdat $p \nmid (p-1)!$ volgt hieruit de bekende

Stelling van Fermat: Als een priemgetal p niet deelbaar is op een geheel getal a, dan geldt

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

Nu kan men a^{-1} mod p gemakkelijk bepalen; immers men heeft $a.a^{p-2} \equiv 1$ (mod p) en mag dus voor a^{-1} nemen het getal a^{p-2}.
Voorbeeld. Bepaal 5^{-1} mod 37. Men heeft $5^{-1} \equiv 5^{35}$ (mod 37). Dus is $5^3 \equiv 14$ (mod 37), dus $5^6 \equiv 14^2 \equiv 11$ (mod 37), dus $5^{12} \equiv 11^2 \equiv 10$ (mod 37), dus $5^{36} \equiv 10^3$ (mod 37) en $5^{35} \equiv 200 \equiv 15$ (mod 37).

Bijgevolg is 5^{-1} mod 37 gelijk aan 15 (inderdaad $5.15 \equiv 1$ (mod 37)).
Tevens ziet men dat uit $u \equiv v$ (mod p-1) voor willekeurige gehele u en v volgt dat

$$a^u \equiv a^v \pmod{p}.$$

(Het omgekeerde is niet steeds juist; bv. uit $2^5 \equiv 2^8$ (mod 7) volgt niet $5 \equiv 8$ (mod 6)). Met het bovenstaande is het gemakkelijk om vraagstukken van het volgende type op te lossen. Bepaal de rest bij deling van 100^{100} door 7. Men heeft $100^{100} = 10^{200}$ en de rest bij deling door 6 van 200 is 2. Dus $10^{200} \equiv 10^2 \equiv 2$ (mod 7).
Een ander zeer belangrijk resultaat is, dat als men op een of andere wijze van een natuurlijk getal m vindt dat bv. $m \nmid 2^{m-1}-1$, men dan mag concluderen dat m samengesteld is, zonder dat men ook maar een enkele priemfactor van m behoeft te hebben gevonden.
Voorbeeld: m=1001. Reduceer 2^{1000} mod 1001. Men heeft (de modulus 1001 voor het gemak weglatende) $2^{10} \equiv 24$, dus $2^{20} \equiv 576$, $2^{40} \equiv 576^2 = 331776 \equiv 445$, dus $2^{80} \equiv 445^2 = 198025 \equiv 828$, $2^{160} \equiv 828^2 = 685584 \equiv 900$, $2^{320} \equiv 900^2 = 810000 \equiv 191$; $2^{640} \equiv 191^2 = 36481 \equiv 445$. Dan is $2^{1000} = 2^{640+320+40} \equiv 445.191.445 \equiv 191.445^2 \equiv$ $\equiv 191.828 = 158148 \equiv 991 \not\equiv 1$, dus 1001 is samengesteld. Voor het onderzoek naar samengesteldheid van grote "natuurlijke"getallen m is dit een der aangewezen wegen. Wij komen hierop later nog terug.

Hierboven voerden wij het begrip volledig restsysteem mod m in. Thans beschouwen wij ook het belangrijke begrip gereduceerd restsysteem mod m. Dit ontstaat uit een volledig restsysteem mod m door daaruit die restklassen mod m weg te laten welke een factor ($\neq \pm 1$) met m gemeen hebben. Is p een priemgetal, dan bevat het gereduceerde restsysteem mod p juist p-1 elementen, die vertegenwoordigd kunnen worden door de getallen 1,2,...,p-1. Van dit gereduceerde restsysteem hebben wij hierboven reeds gebruik gemaakt om de congruentie $ax \equiv b$ (mod p) (met (a,p)=1) op te lossen. Wij willen nu bij willekeurige m de congruentie $ax \equiv b$ (mod m) (met (ab,m)=1 oplossen. Hiertoe gaan wij uit van alle elementen $x_1,\ldots,x_k$ van een gereduceerd restsysteem mod m en beschouwen daarna de elementen $ax_1,\ldots,ax_k$. Geen twee dezer elementen behoort tot dezelfde restklasse mod m. Immers anders waren er indices i en j met $m \mid a(x_i-x_j)$. Zij $m=p_1^{r_1}\ldots p_s^{r_s}$. Dan volgt uit (m,a)=1 zeker $(m,p_\sigma)=1$, dus $p_\sigma^{r_\sigma} \mid x_i-x_j$ ($\sigma=1,\ldots,s$). Derhalve $m \mid x_i-x_j$ in strijd met de veronderstelling. Verder heeft men $(m,ax_i)=1$ want $(m,a)=1$ en $(m,x_i)=1$ (i=1,...,k).

Dus de getallen $ax_1,\ldots,ax_k$ vormen ook een gereduceerd restsysteem mod m. Hieruit volgen twee belangrijke resultaten.

Allereerst blijkt er dus precies één element van dit restsysteem gelijk te zijn aan b, d.w.z. de congruentie $ax\equiv b \pmod m$ heeft precies één oplossing als $(ab,m)=1$, een resultaat dat ook wel op andere wijze voor de dag zal komen.

Verder vindt men na vermenigvuldigen

$$x_1\ldots x_k\equiv a^k x_1\ldots x_k \pmod m,$$

waaruit wegens $(x_1\ldots x_k,m)=1$ volgt dat $a^k\equiv 1 \pmod m$.
Het hierbij optredende getal k, dat van m afhangt, is gelijk aan het aantal getallen die tussen 0 en m liggen en onderling ondeelbaar zijn met m. Men is gewoon dit getal met $\varphi(m)$ (ook genoemd de indicator van m) aan te geven en vindt dan de

Stelling van Euler.

Als $(a,m)=1$, dan geldt $a^{\varphi(m)}\equiv 1 \pmod m$.

Hieruit is, evenals zoeven bij priemgetallen, de waarde van $a^{-1} \pmod m$ gemakkelijk te bepalen. Men neme er slechts voor $a^{\varphi(m)-1}$. Ook hier vindt men uit $u\equiv v \pmod{\varphi(m)}$ voor willekeurige gehele u en v het resultaat $a^u\equiv a^v \pmod m$ en ook hier behoeft het omgekeerde niet te gelden (het geldt zelfs in tal van gevallen zeker niet).
Voorbeeld. Bepaal $2^{-1} \bmod 35$. Hiertoe moet eerst $\varphi(35)$ worden bepaald. Vooruitlopende op een later resultaat geven wij nu al aan hoe $\varphi(35)$ te vinden is: men schrappe van de rij der getallen $1,\ldots,34$ alle 5-vouden (dat zijn er 6) en alle 7-vouden (dat zijn er 4). Dus $\varphi(35)=34-6-4=24$ en $2^{-1}\equiv 2^{23} \pmod{35}$. Nu geldt, alles mod 35 nemende, $2^5\equiv -3$, dus $2^{10}\equiv 9$, dus $2^{20}\equiv 81\equiv 11$, dus $2^{23}\equiv 88\equiv 18$.
Opmerking. Voor priemgetallen p heeft men $\varphi(p)=p-1$ (ga dit na!), waarna de stelling van Fermat als bijzonder geval van die van Euler verkregen kan worden.

De congruentie $ax\equiv b \pmod m$ is nu onder de minder vergaande restrictie $(a,m)=1$ op te lossen. Immers dan bestaat $a^{-1} \bmod m$ en de congruentie is aequivalent met de haar oplossing meteen gevende relatie $x\equiv a^{-1}b \pmod m$. In het geval dat $(a,m)=d\neq 1$ is kan men de congruentie $ax\equiv b \pmod m$ slechts oplossen als $d\mid b$. Immers uit $d\mid a$ en $d\mid m$ volgt $d\mid b$. Is aan deze relatie voldaan, dan vindt men $a=da'$, $b=db'$, $m=dm'$ en als nieuwe congruentie $a'x\equiv b' \pmod{m'}$, waarbij $(a',m')=1$. Deze bezit precies één oplossing mod m'. Dan bezit de oorspronkelijke precies d oplossingen mod m.
Opgave 6. Ga dit na.

Samenvattende vinden wij dus dat de congruentie $ax \equiv b \pmod m$ dan en slechts dan oplosbaar is als $(a,m) \mid b$; het aantal oplossingen is gelijk aan (a,m).

Stelling. De vergelijking $a_1x_1+\ldots+a_nx_n=b$, waarbij $a_1,\ldots,a_n$ en b gegeven gehele getallen zijn (uiteraard $a_1\ldots a_n \neq 0$) heeft dan en slechts dan een gehele oplossing $(x_1,\ldots,x_n)$ als de GGD $g=(a_1,\ldots,a_n)$ deelbaar is op b.

Bewijs: Zij nl. de congruentie oplosbaar. Dan is kennelijk $g \mid b$. Zij omgekeerd $g \mid b$. Wij bewijzen nu de oplosbaarheid met volledige inductie en wel naar de uitdrukking $h = \sum_{\nu=1}^{n} |a_\nu|$. Voor h=1 is de bewering zeker juist.

Opgave 7. Ga dat na.

Onderstel nu dat de bewering juist is voor alle natuurlijke getallen $< h$. Zonder de algemeenheid te schaden mogen wij onderstellen dat $|a_n| \geq |a_{n-1}|$ is. Dan heeft één der getallen a_n+a_{n-1}, a_n-a_{n-1} een modulus die kleiner is dan $|a_n|$. Geef dat getal aan met $a_n+\varepsilon a_{n-1}$. Dus $\varepsilon = +1$ of -1. Beschouw nu de vergelijking $a_1x_1+\ldots+a_{n-2}x_{n-2}+a_{n-1}y+(a_n+\varepsilon a_{n-1})x_n=b$. Hiervoor is de som der moduli der coëfficiënten op grond van de keuze van ε zeker $< h$, terwijl de GGD der coëfficiënten gelijk is aan g. Bij inductie weet men dat deze vergelijking oplosbaar is. Uit een oplossing $(x_1,\ldots,x_{n-2},y,x_n)$ vindt men dan direct de oplossing $(x_1,\ldots,x_{n-2},y+\varepsilon x_n,x_n)$ der oorspronkelijke.

Bijzonder geval. De vergelijking $ax+by=c$ bezit bij gehele a,b en c met $(a,b) \mid c$ een oplossing.

Wij vinden nu opnieuw dat de congruentie $ax \equiv b \pmod m$ oplosbaar is als $(a,m) \mid b$. Immers men kan deze congruentie ook in de gedaante $ax+mv=b$ schrijven en wij weten dat deze oplosbaar is indien $(a,m) \mid b$.

Chinese reststelling. Als de getallen $m_1,\ldots,m_k$ onderling ondeelbaar zijn dan bestaat er bij ieder stel gehele getallen $a_1,\ldots,a_k$ een geheel getal x zodanig dat

$$x \equiv a_K \pmod{m_K} \qquad (K=1,\ldots,k)$$

Bewijs: Voor k=1 is de bewering triviaal. Zij nu de stelling bewezen voor k-1 in plaats van k en daarbij een oplossing y gevonden, die voldoet aan

$$y \equiv a_\lambda \pmod{m_\lambda} \quad (\lambda=1,\ldots,k-1).$$

Dan neme men $x=y+tm_1\ldots m_{k-1}$ waarbij het gehele getal t zo wordt bepaald dat

$$x=y+tm_1\ldots m_{k-1} \equiv a_k \pmod{m_k}.$$

Hiertoe behoeft men slechts de congruentie $tm_1\ldots m_{k-1} \equiv a_k-y \pmod{m_k}$ op te lossen en dat kan omdat $(m_1\ldots m_{k-1},m_k)=1 \mid a_k-y$.

Wij onderzoeken nu algemeen het oplossen van congruenties van congruenties van het type $f(x)\equiv 0 \pmod m$. Zij $m=p_1^{r_1}\ldots p_s^{r_s}$ de canonieke ontbinding van m. Uit $f(x)\equiv 0 \pmod m$ volgt dan $f(x)\equiv 0 \pmod{p_\sigma^{r_\sigma}}$ $(\sigma=1,\ldots,s)$ en omgekeerd. Zij x_σ een willekeurige oplossing van $f(x)\equiv 0 \pmod{p_\sigma^{r_\sigma}}$ $(\sigma=1,\ldots,s)$. Dan voldoet x aan de oorspronkelijke congruentie dan en slechts dan als $x\equiv x_\sigma \pmod{p_\sigma^{r_\sigma}}$ $(\sigma=1,\ldots,s)$. Juist op grond van de Chinese reststelling vindt men dat er zo'n getal x te vinden is; immers de s hier optredende moduli zijn twee aan twee onderling ondeelbaar. Wij kunnen zelfs nog verder gaan en opmerken dat twee oplossingen x en x' dan en slechts dan mod m verschillen als tenminste één σ bestaat waarvoor de bijbehorende x_σ en x'_σ verschillen. Bijgevolg bezit de oorspronkelijke congruentie $n_1\ldots n_s$ oplossingen als de congruentie

$$f(x)\equiv 0 \pmod{p_\sigma^{r_\sigma}}$$

er n_σ bezit $(\sigma=1,\ldots,s)$.

Als voorbeeld merken wij op dat van de congruentie $x^2\equiv 1 \pmod{24}$ het aantal oplossingen 2x4=8 bedraagt; de congruentie $x^2\equiv 1 \pmod 3$ heeft er nl. 2 en de congruentie $x^2\equiv 1 \pmod 8$ heeft er 4. De congruentie $x^2\equiv -1 \pmod{15}$ heeft daarentegen geen oplossingen, want weliswaar bezit $x^2\equiv -1 \pmod 5$ oplossingen, maar $x^2\equiv -1 \pmod 3$ heeft er geen. Wij behandelen thans een tweetal stellingen, waarvan de ene ons een formule over $\varphi(m)$ zal geven.

Stelling. Als (a,b)=1 en als x en y volledige restsystemen resp. mod b en mod a doorlopen, dan doorloopt ax+by een volledig restsysteem mod ab.

Inderdaad, men verkrijgt hier ab getallen van de gedaante ax+by. Geen twee hiervan behoren tot dezelfde restklasse mod ab, want uit $ax+by\equiv ax'+by' \pmod{ab}$ volgt $ax\equiv ax' \pmod b$, dus $x\equiv x' \pmod b$ en ook $by\equiv by' \pmod a$ dus $y\equiv y' \pmod a$. Omgekeerd als $x\equiv x' \pmod b$ en $y\equiv y' \pmod a$ is $ax+by\equiv ax'+by' \pmod{ab}$.

Stelling. Als (a,b)=1 en x en y gereduceerde restsystemen resp. mod b en mod a doorlopen, dan doorloopt ax+by een gereduceerd restsysteem mod ab.

Bewijs: Wij hebben aan te tonen dat $(ax+by, ab)\neq 1$ aequivalent is met: $(x,b)\neq 1$ of $(y,a)\neq 1$. Als $(ax+by, ab)=g$ dan bezit g een priemfactor $\neq 1$ gemeen met zeker een der getallen a en b. Zij dit bv. een p met $p\mid a$. Dan is $p\mid g\mid ax+by$, $p\mid a\mid ax$, dus $p\mid by$. Wegens (a,b)=1 en $p\mid a$ is $p\nmid b$. Dus $p\mid y$ en $(a,y)\neq 1$. Omgekeerd is $(a,y)\neq 1$, dan is er een p met $p\mid a\mid ax$ en $p\mid y\mid by$, dus $p\mid ax+by$ en ook $p\mid ab$.

Bijgevolg verdwijnen door voor x en y van gewone op gereduceerde restsystemen over te gaan uit het volledige restsysteem mod ab van de getallen ax+by juist die waarvoor $(ax+by,ab)\neq 1$ is. Hiermede is de stelling bewezen.

Als toepassing ziet men dat het aantal elementen uit het gereduceerde restsysteem mod ab (met $(a,b)=1$) gelijk is aan het product van de aantallen elementen uit de gereduceerde restsystemen mod a en mod b, anders gezegd: als $(a,b)=1$, dan is $\varphi(ab)=\varphi(a)\,\varphi(b)$.

Als onmiddellijk gevolg hiervan ziet men dat voor $m=p_1^{r_1}\ldots p_s^{r_s}$ geldt $\varphi(m)=\varphi(p_1^{r_1})\ldots\varphi(p_s^{r_s})$.

Om nu een formule voor $\varphi(m)$ te vinden is het voldoende er een af te leiden voor $m=p^r$, waarbij p een priemgetal is. Nu verkrijgt men alle getallen ≥ 0 en $< p^r$ die relatief priem zijn met p^r (d.w.z. met p) door alle p-vouden hieruit weg te laten. Dat zijn er p^{r-1} stuks, zodat men vindt $\varphi(p^r)=p^r-p^{r-1}=p^{r-1}(p-1)$. Bijgevolg geldt voor $m=p_1^{r_1}\ldots p_s^{r_s}$ de formule

$$\varphi(m)=\prod_{\sigma=1}^{s} p_\sigma^{r_\sigma-1}\,(p_\sigma-1)=m\prod_{\sigma=1}^{s}\left(1-\frac{1}{p_\sigma}\right).$$

Men heeft bv. $\varphi(24)=\varphi(2^3.3)=2^2.2=8$, dus wegens Fermat $a^8\equiv 1 \pmod{24}$ voor alle a met $(a,24)\neq 1$, d.w.z. voor alle oneven a, die niet deelbaar zijn door 3.

Opgave 7. Bepaal m zodat $2\nmid\varphi(m)$.

Opgave 8. Bepaal m zo dat $\varphi(m)=\frac{1}{2}m$.

Opgave 9. Bepaal de rest bij deling van 9^{9^9} door 77; ook van $7^{7^{7^7}}$ door 99.

Het bepalen van m uit de waarde van $\varphi(m)$ is een probleem waarvoor i.h.a. geen direct oplossingsprocédé bestaat.

Tot slot van deze paragraaf geven wij nog de

Stelling van Wilson. Als p een priemgetal is, dan geldt

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

Bewijs: De getallen $1,\ldots,p-1$ kunnen op een enkele uitzondering na in paren worden verdeeld, zodanig dat het product der elementen van zo'n paar $\equiv 1 \pmod{p}$ is. Immers men neme zo'n element a en bepale volgens het bovenstaande b zo dat $ab\equiv 1 \pmod{p}$ is. Uitzonderingen zijn hierbij die getallen waarbij b=a wordt, hetgeen optreedt bij $a^2\equiv 1 \pmod{p}$, dus $p\mid(a+1)(a-1)$, dus bij a=1 en a=p-1. Wij vinden dus $\frac{p-1}{2}-2$ paren van het eerstgenoemde type. Hiervan is het product $\equiv 1 \pmod{p}$. Om nu $(p-1)!$ te krijgen moeten wij dat product nog met $1.(p-1)$ vermenigvuldigen. Dan vindt men

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

waarmee de stelling bewezen is.

Men heeft zich afgevraagd of zowel de congruentie $a^{p-1}\equiv 1 \pmod{p}$ (bij vaste gegeven a) als de relatie $(p-1)!\equiv -1 \pmod{p}$ soms ook geldt modulo een hogere macht van p. Wat de eerste betreft is dit bv. bij a=2 onderzocht o.a. door Beeger. De kleinste waarden van p waarvoor geldt

$2^{p-1} \equiv 1 \pmod{p^2}$, zijn p=1093 en p=3511. Men kan hier een samenhang tussen dit resultaat en het vermoeden van Fermat afleiden nl. als er natuurlijke x,y,z en p (met $p>2$) bestaan, waarvoor $x^p+y^p=z^p$ en tevens $p \nmid xyz$, dan geldt $2^{p-1} \equiv 1 \pmod{p^2}$. Dat de laatste relatie echter niet de vervulbaarheid van de vergelijking van Fermat garandeert blijkt bv. daaruit dat bewezen is dat voor p=1093 en p=3511 ja zelfs voor geen enkele p met $p < 253747889$ en $p \nmid xyz$ de relatie $x^p+y^p=z^p$ te vervullen is. In 1953 bewezen van Wijngaarden en Duparc dat hieruit volgt dat elk der getallen x ,y en z minstens gelijk moet zijn aan $10^{6\times10^9}$. Overigens is nog aangetoond dat het getal p, indien hiervoor "Fermat zal gelden", ook moet voldoen aan $3^{p-1} \equiv 1 \pmod{p^2}$. Een eenvoudige oplossing hiervan is gemakkelijk te vinden, nl. p=11. Uit "Fermat" volgt echter niet dat ook nog moet gelden $5^{p-1} \equiv 1 \pmod{p^2}$.

Van de congruentie $(p-1)! \equiv -1 \pmod{p^2}$ kent men tot nu toe nog slechts enkele oplossingen waarvan wij noemen p=5, p=13.

Een ander bewijs van de stelling van Wilson volgt door een geheel ander soort beschouwing. Wij vonden hierboven dat als p een priemgetal is en de congruentie

$$f(x) = x^k + a_1x^{k-1} + \ldots + a_k \equiv 0 \pmod{p}$$

de wortels $x_1,\ldots,x_k$ bezit, men heeft

$$f(x) \equiv (x-x_1)\ldots(x-x_k) \pmod{p}.$$

Dus $a_1 \equiv -\sum_i x_i \pmod{p}$, $a_2 \equiv \sum_{i<j} x_ix_j \pmod{p}$, enz.

Neemt men nu $f(x)=x^{p-1}-1$. Wij weten op grond van de stelling van Fermat dat $f(x) \equiv 0 \pmod{p}$ de wortels $1,2,\ldots,p-1$ bezit. Hieruit volgen door vergelijken van coëfficiënten tal van resultaten. Neemt men de laatste dan vindt men $-1 \equiv 1.2\ldots.(p-1) \pmod{p}$, waarmee de stelling van Wilson opnieuw bewezen is.

Een ander resultaat luidt

$$0 \equiv \sum_{n=1}^{p-1} n = 1 + 2 + \ldots + (p-1) \quad (\text{mits } p>2).$$

Dit is overigens triviaal. Voor $p>3$ heeft men verder

$$0 \equiv \sum_{0<n<m<p} nm \pmod{p}.$$

Dus geldt ook $\sum_{n=1}^{p-1} n^2 = (\sum_{n=1}^{p-1} n)^2 - 2\sum_{n<m} nm \equiv 0-0=0 \pmod{p}$.

Hieruit volgt nog een belangrijke formule.

Beschouw daartoe de teller t van de als onvereenvoudigbare breuk geschreven uitdrukking

$$U = \sum_{n=1}^{p-1} \frac{1}{n} .$$

Wij tonen aan dat deze deelbaar is door p^2. Nu heeft men

$$2U = \sum_{n=1}^{p-1} \frac{1}{n} + \sum_{n=1}^{p-1} \frac{1}{p-n} = \sum_{n=1}^{p-1} \frac{p}{n(p-n)} ,$$

zodat het voldoende is om aan te tonen dat $\sum_{n=1}^{p-1} \frac{1}{n(p-n)}$ een teller heeft die door p deelbaar is.

Beschouwt men bij elke n die niet deelbaar is door p ook het getal n' met $0<n'<p$ en $nn' \equiv 1 \pmod p$ dan is $p \mid \frac{1}{n}$ aequivalent met $p \mid n'$ en zo doorgaande:

$$p \mid \sum_{n=1}^{p-1} \frac{1}{n(p-n)} \text{ is aequivalent met } p \mid \sum_{n'} n'(p-n)' .$$

Uit $n \not\equiv m \pmod p$ volgt $n' \not\equiv m' \pmod p$; dus als $n=1,\ldots,p-1$ wordt genomen doorloopt n' een permutatie dezer getallen. Verder is $(p-n)' \equiv -n' \pmod p$, dus $\sum_{n'} n'(p-n)' \equiv -\sum_{n'} n'^2 = -\sum_{n=1}^{p-1} n^2 \equiv 0 \pmod p$, waarmee de bewering bewezen is.

Dus $p^2 \mid \sum_{n=1}^{p-1} \frac{1}{n}$ voor priemgetallen $p>3$ (stelling van Wolstenholme).

Of er een priemgetal p bestaat, waarvoor toevallig $p^3 \mid \sum_{n=1}^{p-1} \frac{1}{n}$ geldt, is niet bekend. Zeker moet gelden $p \geq 367$.

§ 5 Quadraatresten.

Definitie. Een getal a heet quadraatrest van (of mod) een priemgetal p als er een getal k niet deelbaar door p bestaat zodanig dat $a \equiv k^2 \pmod p$.

Bestaat zo'n getal k, niet deelbaar door p, niet, dan heet a een nietrest.

Als a quadraatrest is van m is elk getal dat mod p congruent is met a het ook. Hetzelfde geldt ten aanzien van nietresten. Om alle quadraatresten mod p te bepalen is het dus voldoende de p-1 getallen $1,\ldots,p-1$ te onderzoeken.

Voor p=2 laten wij het onderzoek aan de lezer over. Zij nu p een priemgetal >2. Beschouw de tussen 0 en p gelegen getallen x_i met $x_i \equiv i^2 \pmod p$ $(i=1,\ldots,\frac{1}{2}(p-1))$. Geen twee dezer getallen zijn gelijk. Immers $x_i = x_j$ leidt tot $p \mid i^2-j^2=(i+j)(i-j)$ hetgeen wegens $0<i,j<\frac{1}{2}(p-1)$ uitgesloten is. Voor i tussen $\frac{1}{2}p$ en p heeft men verder kennelijk $x_{p-i} \equiv i^2 \pmod p$. Bijgevolg vinden wij dat er precies $\pi = \frac{1}{2}(p-1)$ quadraatresten bestaan. Er moeten dus ook $\frac{1}{2}(p-1)$ (nl. $p-1-\frac{1}{2}(p-1)$) nietresten zijn.

Stelling. Het product van twee quadraatresten is een quadraatrest; van een quadraatrest en een nietrest is een nietrest en van twee nietresten is een quadraatrest.

Bewijs: Zijn a en b quadraatresten, dan bestaan er getallen h en k met $a \equiv k^2 \pmod p$, $b \equiv h^2 \pmod p$, dus $ab \equiv (kh)^2 \pmod p$ en ab is quadraatrest.

Is a quadraatrest en b nietrest, dan leidt de onderstelling dat ab ook quadraatrest is tot een contradictie. Immers er bestaan dan getallen h en k met $a \equiv k^2 \pmod p$, $ab \equiv h^2 \pmod p$, dus $a^2b \equiv (hk)^2 \pmod p$ en $b \equiv (hka^{-1})^2 \pmod p$, in strijd met de onderstelling over b.

Laat tenslotte b een vaste nietrest zijn. Beschouw de verzameling der p-1 onderling mod p incongruente getallen x, waarbij x=1,2,...,p-1. De getallen xb zijn dan ook onderling incongruent en de $\frac{1}{2}(p-1)$ getallen van dit stel voor welke x een quadraatrest is zijn, zoals wij zojuist zagen, nietresten. Dan moeten de overige $\frac{1}{2}(p-1)$ getallen (welke dus producten zijn van twee nietresten) juist de $\frac{1}{2}(p-1)$ quadraatresten opleveren.

Definitie. Onder het symbool van Legendre $(\frac{a}{p})$ verstaat men:

het getal +1 als a quadraatrest is mod p;
het getal -1 als a nietrest is mod p;
het getal 0 als a deelbaar is door p.

De voorafgaande stelling, aangevuld met eenvoudige overwegingen voor gevallen waarin het symbool van Legendre nul is, levert ons de volgende formule:

$$(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p}).$$

Deze formule geldt ook voor het priemgetal 2.

Opgave 1. Bewijs dit.

Euler heeft een criterium gegeven om bij gegeven oneven priemgetal p uit te maken of een getal a quadraatrest of nietrest is. Dit luidt als volgt:

Als a quadraatrest mod p is, geldt $a^{\frac{1}{2}(p-1)} \equiv +1 \pmod p$;
als a nietrest mod p is, geldt $a^{\frac{1}{2}(p-1)} \equiv -1 \pmod p$.

Waar hiermede alle gevallen met $p \nmid a$ zijn uitgeput, gelden ook de omkeringen van deze beweringen.

Bewijs: Zij a quadraatrest mod p. Er is dan een getal h met $a \equiv h^2 \pmod p$, dus

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

waarbij de laatste congruentie die van Fermat is. Beschouw thans de congruentie $x^{p-1} \equiv 1 \pmod p$, met haar p-1 wortels 1,2,...,p-1. We schrijven nu

$$(x^{\frac{1}{2}(p-1)}-1)(x^{\frac{1}{2}(p-1)}+1) \equiv 0 \pmod p.$$

Elk dezer factoren moet nu $\frac{1}{2}(p-1)$ nulpunten bezitten, want geen van beide kan er meer hebben dan zijn graad bedraagt en samen hebben ze er p-1.

De eerste factor heeft als nulpunten de $\frac{1}{2}(p-1)$ quadraatresten mod p, zodat de laatste juist de $\frac{1}{2}(p-1)$ nietresten als nulpunten moet bezitten. Wij kunnen het resultaat ook anders formuleren:

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

Immers beide leden nemen tegelijk een der waarden +1, -1 of 0 (de enige ervoor mogelijke waarden) aan.

Deze laatste congruentie geldt ook weer voor p=2.

Opgave 2. Bewijs dit.

Wij kunnen nu reeds nagaan van welke priemgetallen -1 een quadraatrest is. Immers $(\frac{-1}{p}) \equiv (-1)^{\frac{1}{2}(p-1)} \pmod{p}$ en het rechterlid is +1 als $p \equiv 1 \pmod{4}$ is en -1 als $p \equiv 3 \pmod{4}$ is. Dus -1 is een quadraatrest van alle viervouden +1, mits die priem zijn en nietrest van de priemgetallen die viervouden +3 zijn.

Hieruit zijn tal van belangrijke conclusies te trekken. Allereerst tonen wij aan dat er oneindig veel ondeelbare getallen zijn, die een viervoud +1 zijn.

Bewijs: Zijn $p_1,\ldots,p_n$ de eerste n ondeelbare getallen, die viervouden +1 zijn, dan beschouwe men het getal

$$u = 4p_1^2 \ldots p_n^2 + 1.$$

Is u priem dan is hiermee een nieuw ondeelbaar viervoud +1 gevonden. Is u samengesteld, laat dan p een priemfactor van u zijn. Dan heeft men

$$4p_1^2 \ldots p_n^2 \equiv -1 \pmod{p},$$

dus $(\frac{-1}{p})=1$ en p is een viervoud +1, kennelijk ongelijk aan de al bekende priemgetallen $p_1,\ldots,p_n$.

Opmerking. Wij vinden hier nog iets meer, nl. dat alle (priem)delers van een getal van de gedaante $4m^2+1$ zeker viervouden +1 zijn. Dit resultaat hangt samen met een tweede belangrijke toepassing die wij van het bovenstaande willen geven.

Stelling. Elk ondeelbaar 4voud +1 is te schrijven als som van twee quadraten.

1e Bewijs:

Wij leiden eerst een paar hulpeigenschappen af.

I. Het product van twee quadraatsommen is weer een quadraatsom.

II. Als een ondeelbare quadraatsom deelbaar is op een andere, dan is het quotiënt weer een quadraatsom.

Ad I. $(a^2+b^2)(A^2+B^2) = (aA+bB)^2 + (aB-bA)^2 = (aA-bB)^2 + (aB+bA)^2$.

Anders: $\alpha = a+bi$, $\beta = A+Bi$. Dan geldt

$$(a^2+b^2)(A^2+B^2) = \alpha\bar{\alpha}\,.\,\beta\bar{\beta} = \alpha\beta.\bar{\alpha}\bar{\beta} = \alpha\beta.\overline{\alpha\beta}$$

en het laatste en voorlaatste lid is als norm van een "geheel" complex getal weer een quadraatsom.

Ad II. Zij $p=a^2+b^2 \mid A^2+B^2$. Dan geldt

$$q = \frac{A^2+B^2}{a^2+b^2} = \frac{(a^2+b^2)(A^2+B^2)}{p^2} = \frac{(aA\pm bB)^2+(aB\mp bA)^2}{p^2}$$

$$= \left(\frac{aA\pm bB}{p}\right)^2 + \left(\frac{aB\mp bA}{p}\right)^2$$

Nu is hetzij aA+bB, hetzij aA-bB deelbaar door p. Immers hun product is

$$a^2A^2-b^2B^2 \equiv a^2A^2+a^2B^2 = a^2(A^2+B^2) \equiv 0 \pmod{p}.$$

Anders: Uit de onderstelling volgt in de bij I gebruikte notatie dat $\alpha\bar{\alpha} \mid \beta\bar{\beta}$. Omdat $p=\alpha\bar{\alpha}$ priem is, is α priem in de ring van Gauss.

Opgave 3. Bewijs dat.

Omdat de ring van Gauss een ontbindingsring is, is dan α deelbaar hetzij op β, hetzij op $\bar{\beta}$. Onderstel bv. $\alpha \mid \beta$. Dan is er een γ in de ring van Gauss met $\alpha\gamma=\beta$. Men heeft dan $\alpha\bar{\alpha}\gamma\bar{\gamma}=\beta\bar{\beta}$ en het gezochte quotiënt is van de gedaante $\gamma\bar{\gamma}$, dus een quadraatsom.

Nu het bewijs van de stelling zelf. Zij het priemgetal $p\equiv -1 \pmod 4$. Dan is er een even u met $u^2 \equiv -1 \pmod p$, waarbij wij zonder de algemeenheid te schaden mogen onderstellen dat $0 < u \leq \frac{1}{2}(p-1)$. Dus $u^2+1=pv$ met $v<p$. Van het getal v is elke priemdeler q, zoals wij al zagen, een viervoud +1 en tevens geldt $q<p$. Bij inductie nemen wij aan dat de stelling bewezen is voor alle ondeelbare 4vouden +1, die $<p$ zijn, d.w.z. elke q is een quadraatsom. Wegens I is dan v als product van quadraatsommen ook een quadraatsom. Deze laatste is een deler van de quadraatsom u^2+1. Dus wegens II is ook p een quadraatsom.

2e Bewijs: Zij p een ondeelbaar 4voud +1. Er is dan een getal u met $u^2 \equiv -1 \pmod p$. Dus $p \mid u^2+1 = \alpha\bar{\alpha}$ met $\alpha = u+i$. Er zijn nu twee gevallen mogelijk: 1° p is ondeelbaar in de ring van Gauss of p is aldaar samengesteld. In geval 1° moet p op zeker één der factoren α en $\bar{\alpha}$ deelbaar zijn. Onderstel bv. $p \mid \alpha$. Maar dan geldt $\bar{p} \mid \bar{\alpha}$, d.w.z. $p \mid \bar{\alpha}$. Dus $p \mid \alpha-\bar{\alpha}=2i$, in strijd met $p \equiv 1 \pmod 4$. Bijgevolg geldt 2°, dus p is samengesteld in de ring van Gauss. Omdat p priem is in de verzameling

der gehele getallen moet p zeker een complexe (niet reële)deler β bezitten. Maar uit $\beta|p$ volgt dan $\bar{\beta}|p$. Dus $p=\beta\bar{\beta}$, d.w.z. p is een quadraatsom. Het is nl. uitgesloten dat p meer complexe delers bezit.

Opgave 4. Bewijs dit.

3e bewijs: Evenals hierboven ziet men in dat er een u bestaat met $u^2+1=vp$. Zij m de kleinste positieve waarde van v waarvoor vp de som van twee quadraten is. Dan heeft men $mp=x^2+y^2$ en $m<p$. Zij $x'\equiv x \pmod m$, $y'\equiv y \pmod m$, zodanig dat $0\leq|x'|\leq\frac{1}{2}m$, $0\leq|y'|\leq\frac{1}{2}m$. Dan geldt $0\leq x'^2+y'^2\leq\frac{1}{2}m^2$ en $x'^2+y'^2\equiv x^2+y^2\equiv 0 \pmod m$, dus $x'^2+y'^2=mn$ met $0\leq n\leq\frac{1}{2}m$. Stel nu dat $n>0$ was. Dan gold $m^2np=(x^2+y^2)(x'^2+y'^2)=z^2+w^2$ met $z=xx'+yy'\equiv x^2+y^2\equiv 0 \pmod m$; $w=xy'-x'y\equiv xy-xy=0 \pmod m$, dus $np=(\frac{z}{m})^2+(\frac{w}{m})^2$ in strijd met de minimaliteitsdefinitie van m. Bijgevolg is n=0, dus x'=y'=0 en m|x, m|y. Derhalve $m^2|x^2+y^2=mp$, d.w.z. m|p en m=1. Q.e.d.

Opmerking. Een bewijs, analoog aan dit derde, zal later worden gegeven voor de stelling dat elk getal te schrijven is als de som van vier quadraten.

Met behulp van de stelling van Wilson kan men voor $p\equiv 1 \pmod 4$ gemakkelijk de oplossingen geven van $x^2\equiv -1 \pmod 4$. De getallen $x=\pm(\frac{1}{2}(p-1))!$ voldoen nl. Immers men heeft $1\equiv-(p-1)$, $2\equiv-(p-2)$,...,$k\equiv-(p-k)$, dus $x=(\frac{1}{2}(p-1))!=1.2.\ \ldots\ \frac{1}{2}(p-1)\equiv(-)^{\frac{1}{2}(p-1)}(p-1)(p-2)\ldots\frac{1}{2}(p+1)\equiv(p-1)(p-2)\ldots\frac{1}{2}(p+1)$ en wegens Wilson geldt dan inderdaad $x^2\equiv -1 \pmod p$.

Opgave 5. Ga na tot welk resultaat deze methode voert bij een priemgetal $p\equiv 3 \pmod 4$.

Om iets naders over het symbool van Legendre te vinden, leiden wij thans af het

Lemma van Gauss. Zijn p en q twee verschillende priemgetallen en $p\neq 2$. Reduceert men de $\frac{1}{2}(p-1)$ getallen $1.q, 2.q, \ldots, \frac{1}{2}(p-1).q$ tot hun absoluut kleinste resten mod p, dan voldoet het aantal N dier negatieve kleinste resten aan $(\frac{q}{p})=(-)^N$.

Bewijs: Zij $j.q\equiv r_j \pmod p$, waarbij r_j de te beschouwen absoluut kleinste rest is. De $\frac{1}{2}(p-1)$ getallen $|r_1|,\ldots|r_{\frac{1}{2}(p-1)}|$ vormen dan een permutatie der getallen $1,\ldots,\frac{1}{2}(p-1)$, want $p\nmid r_j-r_k$ en $p\nmid r_j+r_k$ voor alle mogelijke paren j en k met $j\neq k$. Immers $r_j\pm r_k=q(j\pm k)$ is wegens $0<j$, $k<\frac{1}{2}(p-1)$ niet deelbaar door p. Bijgevolg heeft men $|r_1\ldots r_{\frac{1}{2}(p-1)}|=(\frac{1}{2}(p-1))!$, d.w.z.

$$(\tfrac{1}{2}(p-1))!\ q^{\frac{1}{2}(p-1)}\equiv(-)^N\ r_1\ldots r_{\frac{1}{2}(p-1)}=(\tfrac{1}{2}(p-1))! \pmod p,$$

dus wegens het criterium van Euler:

$$(\tfrac{q}{p})\equiv q^{\frac{1}{2}(p-1)}\equiv(-)^N \pmod p,$$

en wegens $p\neq 2$ ten slotte $(\frac{q}{p})=(-)^N$.

Dit lemma maakt het ons inderdaad mogelijk om voor bepaalde waarden van p en q het symbool van Legendre uit te rekenen. Wij geven als voorbeeld het geval q=2.

Zij allereerst $\frac{1}{2}(p-1)$ even (=2s). De te beschouwen absoluut kleinste resten zijn nu $1.2, 2.2, \ldots, s.2; (s+1)2-p, (s+2)2-p, \ldots, 2s.2-p$.

Het aantal N is het aantal uitdrukkingen van de tweede groep en blijkt na uittellen te zijn $s=\frac{1}{4}(p-1)$. Is nu $p\equiv 1 \pmod 8$, dan is s,dus N, even en $(\frac{2}{p})=+1$. Is $p\equiv 5 \pmod 8$, dan is s,dus N, oneven en $(\frac{2}{p})=-1$.

Zij vervolgens $\frac{1}{2}(p-1)$ oneven $(=2s+1)$. Nu zijn de te beschouwen absoluut kleinste resten

$$1.2,2.2,\ldots,s.2;\ (s+1)2-p,\ (s+2)2-p,\ldots,(2s+1)2-p$$

en het aantal N der uitdrukkingen van de tweede groep is nu s+1. Is $p\equiv 3 \pmod 8$, dan is s even, dus N oneven en $(\frac{2}{p})=-1$. Is echter $p\equiv 7 \pmod 8$, dan is s oneven, dus N even en $(\frac{2}{p})=+1$.

Samenvattende vindt men dat 2 quadraatrest is van de priemgetallen p met $p\equiv \pm 1 \pmod 8$ en nietrest is van die met $p\equiv \pm 3 \pmod 8$.

Opgave 6. Bewijs op analoge wijze dat 3 quadraatrest is voor de priemgetallen p met $p\equiv \pm 1 \pmod{12}$ en nietrest voor die met $p\equiv \pm 5 \pmod{12}$.

Opgave 7. Bereken het symbool $(\frac{q}{p})$ van Legendre voor q=-2,-3,6 en -6.

Wij bewijzen thans een beroemd theorema dat ons een algorithme oplevert voor de bepaling van $(\frac{q}{p})$ voor willekeurige ondeelbare p.

Reciprociteitsstelling van Legendre. Indien p en q oneven priemgetallen zijn heeft men $(\frac{q}{p})(\frac{p}{q})=(-)^{\frac{1}{2}(p-1).\frac{1}{2}(q-1)}$

Bewijs: Wij gebruiken bij het bewijs het lemma van Gauss. Eerst beschouwen wij de getallen

$$hp=a_h+qs_h \quad \text{met } 0<a_h<q \quad (h=1,\ldots,\tfrac{1}{2}(p-1)).$$

Men heeft dan $s_h=\left[\frac{hp}{q}\right]$. Telt men deze $\frac{1}{2}(q-1)$ relaties op, dan vindt men

$$(1) \qquad \sum_h hp = \sum_h a_h + q\sum_h \left[\frac{hp}{q}\right],$$

waarbij alle sommen lopen over h van 1 tot en met $\frac{1}{2}(q-1)$. Nu komen er onder de resten a_h een aantal voor die gelegen zijn tussen $\frac{1}{2}q$ en q. Schrijft men deze als $a_h=q+b_h$ dan is b_h een absoluut kleinste rest mod q en het aantal optredende getallen b_h is wegens het lemma van Gauss gelijk aan $M=(\frac{p}{q})$. De overgebleven getallen a_h en de nu juist ingevoerde $|b_h| = -b_h$ vormen een permutatie der getallen $1,\ldots,\frac{1}{2}(q-1)$, dus hun som is gelijk aan $\sum h$, bijgevolg is de som der overgebleven getallen a_h en de getallen b_h, afgezien van een even bedrag, ook gelijk aan $\sum h$. Wij vinden dan uit (1)

$$\sum_h hp \equiv \sum_h h + M.q + q\sum_h \left[\frac{hp}{q}\right] \pmod 2,$$

dus, omdat p-1 en q-1 even zijn,

$$M \equiv \sum_h \frac{hp}{q} \pmod 2.$$

Evenzo vindt men dat het aantal N der absoluut kleinste negatieve resten mod p uit het systeem $q,2q,\ldots,\frac{1}{2}(p-1)q$ voldoet aan

$$N \equiv \sum_k \left[\frac{kq}{p}\right] \pmod 2,$$

waarbij k loopt van 1 tot en met $\frac{1}{2}(p-1)$.
Wij vinden dan

(2) $$M + N \equiv \sum_h \left[\frac{hp}{q}\right] + \sum_k \left[\frac{kq}{p}\right] \pmod 2$$

Meetkundig is gemakkelijk de waarde van het rechterlid van (2) te vinden. Beschouw daartoe in het x,y-vlak de rechthoek R met hoekpunten $(0,0)$, $(0,\frac{1}{2}(q-1))$, $(\frac{1}{2}(p-1),0)$, $(\frac{1}{2}(p-1), \frac{1}{2}(q-1))$. Het aantal erin gelegen roosterpunten (dat zijn punten met gehele coördinaten) dat niet op ten minste een der assen is gelegen is kennelijk gelijk aan $\frac{1}{2}(p-1).\frac{1}{2}(q-1)$. Anderzijds verdele men de rechthoek R in twee gedeelten door de rechte $y=\frac{q}{p}x$. Op deze rechte liggen binnen R geen roosterpunten.
Opgave 8. Bewijs dit.

De rechte verdeelt R in twee gedeelten. Eerst tellen wij het aantal roosterpunten in het onderste deel en wel door dit kolomsgewijze te tellen. Dit aantal in de kolom x=k is juist gelijk aan $\left[\frac{kq}{p}\right]$, zodat het onderste deel juist $\sum_k \left[\frac{kq}{p}\right]$ roosterpunten bezit. Het analoge resultaat voor het bovenste deel leert ons dan dat het rechterlid van (2) gelijk is aan het totale aantal $\frac{1}{2}(p-1).\frac{1}{2}(q-1)$ roosterpunten van R. Dan levert (2) ons

$$M + N \equiv \tfrac{1}{2}(p-1).\tfrac{1}{2}(q-1) \pmod 2,$$

dus

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{M+N} = (-1)^{\frac{1}{2}(p-1).\frac{1}{2}(q-1)}$$

Toepassingen. Als toepassing bepalen wij de waarde van een aantal symbolen van Legendre. Men rechtvaardige ieder hier optredend gelijkteken.

$$\left(\frac{34}{23}\right)=\left(\frac{11}{23}\right)= -\left(\frac{23}{11}\right)=-\left(\frac{12}{11}\right)= -\left(\frac{2}{11}\right)^2\left(\frac{3}{11}\right)= -\left(\frac{3}{11}\right)=\left(\frac{11}{3}\right)=\left(\frac{2}{3}\right)= -1.$$

$$\left(\frac{13}{37}\right)= + \left(\frac{31}{13}\right)= \left(\frac{5}{13}\right)=\left(\frac{13}{5}\right)=\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)= -1.$$

Opmerking. Dat $\left(\frac{3}{11}\right)= +1$ en $\left(\frac{3}{5}\right)= -1$ is, volgt ook direct uit opgave 6.

$$\left(\frac{55}{37}\right) = \left(\frac{5}{37}\right)\left(\frac{11}{37}\right)= \left(\frac{37}{5}\right)\left(\frac{37}{11}\right)=\left(\frac{2}{5}\right)\left(\frac{4}{11}\right)=\left(\frac{2}{5}\right)\left(\frac{2}{11}\right)^2=\left(\frac{2}{5}\right)= -1.$$

Is $p\neq 2$, dan is $\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)$ en als $p \equiv \pm 1 \pmod 5$, dan vindt men voor $\left(\frac{p}{5}\right)$ kennelijk +1, immers $\left(\frac{1}{5}\right)=1$ en $\left(\frac{-1}{5}\right)=1$ omdat $5 \equiv 1 \pmod 4$ is. Is echter $p \equiv \pm 2 \pmod 5$, dan geldt bij p=2 het al gevonden resultaat $\left(\frac{2}{5}\right)=-1$ en bij p=-2 vindt men bv. $\left(\frac{-2}{5}\right)=\left(\frac{2}{5}\right)\left(\frac{-1}{5}\right)=-1.1=-1$. Dus $\left(\frac{5}{p}\right)=+1$ als $p \equiv \pm 1 \pmod 5$ en $\left(\frac{5}{p}\right)=-1$ als $p \equiv \pm 2 \pmod 5$.

Opgave 8. Leid het gevondene van de vorige opgave af met behulp van de reciprociteitsstelling.

Opgave 9. Onderzoek voor welke waarden van p het symbool $(\frac{-5}{p})$ gelijk is aan +1 en wanneer het gelijk is aan -1.

Opgave 10. Hetzelfde voor $(\frac{7}{p})$.

Het symbool van Legendre $(\frac{m}{q})$ is gedefinieerd (en na het voorafgaande in principe te berekenen) voor willekeurige m en priemgetallen q. Het geeft ons tevens uitsluitsel of de congruentie $x^2 \equiv m \pmod q$ oplosbaar is of niet. In principe is hiermee ook het onderzoek der congruentie $x^2 \equiv m \pmod n$ uit te voeren, mits men maar van n de priemontbinding kent en mits men congruenties van het type $x^2 \equiv m \pmod{q^r}$ voor ondeelbare q kan oplossen. Hierop komen wij weldra terug. Toch zou men zich kunnen afvragen of ook een symbool $(\frac{m}{n})$ voor willekeurige m en n in te voeren is en of het van belang is om hiermee uitsluitsel te krijgen over de oplosbaarheid van congruenties van het type $x^2 \equiv m \pmod n$. Het eerste is geschied; het tweede blijkt echter niet het geval te zijn.

Om allereerst het symbool $(\frac{m}{n})$ (van Jacobi) voor samengestelde n in te voeren stellen wij bij $n=q_1^{r_1}\ldots q_s^{r_s}$ bij definitie

$$(\frac{m}{n}) = \prod_{\sigma=1}^{s} (\frac{m}{q_\sigma})^{r_\sigma},$$

waarmee het symbool van Jacobi is teruggebracht tot dat van Legendre.

Men heeft nu

Stelling. $(\frac{-1}{n}) = (-1)^{\frac{1}{2}(n-1)}$; $(\frac{2}{n}) = (-1)^{\frac{1}{8}(n^2-1)}$ $\qquad (2 \nmid n)$

Bewijs: Wij tonen de beweringen aan door volledige inductie naar het aantal priemfactoren van n. Stel n=pn' en stel de relaties gelden reeds voor n'. Dan heeft men

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

want $\frac{1}{2}(p-1)+\frac{1}{2}(n'-1)-\frac{1}{2}(n-1) = -\frac{1}{2}(1-p)(1-n') \equiv 0 \pmod 2$

en verder

$$(\frac{2}{n}) = (\frac{2}{p})(\frac{2}{n'}) = (-1)^{\frac{1}{8}(p^2-1)}(-1)^{\frac{1}{8}(n'^2-1)} = (-1)^{\frac{1}{8}(n^2-1)},$$

want $\frac{1}{8}(p^2-1)+\frac{1}{8}(n'^2-1)-\frac{1}{8}(n^2-1) = -\frac{1}{8}(p^2-1)(n'^2-1) \equiv 0 \pmod 4$.

Stelling. Als $2 \nmid mn$, dan geldt $(\frac{m}{n})(\frac{n}{m}) = (-1)^{\frac{1}{2}(m-1).\frac{1}{2}(n-1)}$.

Bewijs: Wij geven een bewijs door inductie naar de som der aantallen priemfactoren van m en n. Is die som 2 en zijn n en m elk priem dan geldt de relatie volgens de gewone reciprociteitsstelling. Zij de som > 2 en stel zonder de algemeenheid te schaden n=pn' waarbij p priem is en de stelling voor n' en m reeds bewezen verondersteld is. Dan heeft men

$$(\tfrac{m}{n})(\tfrac{n}{m}) = (\tfrac{m}{p})(\tfrac{m}{n'})(\tfrac{p}{m})(\tfrac{n'}{m}).$$

Op grond van de inductieonderstelling is het product van de eerste en derde factor gelijk aan $(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(m-1)}$ en om dezelfde reden is dat van de tweede en vierde gelijk aan $(-1)^{\frac{1}{2}(n'-1).\frac{1}{2}(m-1)}$. Het product van de gevonden uitdrukkingen is $(-1)^{\frac{1}{2}(m-1).\frac{1}{2}(n-1)}$, want

$$\tfrac{1}{2}(p-1).\tfrac{1}{2}(m-1)+\tfrac{1}{2}(n'-1).\tfrac{1}{2}(m-1)-\tfrac{1}{2}(pn-1).\tfrac{1}{2}(m-1)=-\tfrac{1}{2}(p-1)(n'-1).\tfrac{1}{2}(m-1)$$
$$\equiv 0 \pmod 2.$$

Voorbeeld $(\frac{5}{21}) = (\frac{21}{5})=1$. Echter is $x^2\equiv 5 \pmod{21}$ onoplosbaar want $x^2\equiv 5 \pmod 3$ en $x^2\equiv 5 \pmod 7$ zijn het beide. Inderdaad heeft men $(\frac{5}{21})=(\frac{5}{3})(\frac{5}{7})=-1.-1=1$.

Wij besluiten deze paragraaf met de behandeling der quadratische congruentie

$$ax^2 + bx + c \equiv 0 \pmod m.$$

Zoals reeds betoogd is mag men zonder de algemeenheid te schaden het onderzoek terugvoeren tot dat van

$$ax^2 + bx + c \equiv 0 \pmod{p^r},$$

waarbij p een priemgetal is.

Eerst beschouwen wij het geval r=1 en daarbij mogen wij onderstellen dat $p \nmid a$, omdat men anders een reeds behandelde eerstegraadscongruentie verkrijgt. Dan is wegens het bestaan van $a^{-1} \pmod p$ de congruentie terug te voeren tot een van het type

$$x^2 + mx + n \equiv 0 \pmod p.$$

Het geval p=2 is gemakkelijk na te gaan. Men heeft dan trouwens $x^2 \equiv x \pmod 2$.

Opgave 11. Voer dat uit.

Onderstellen wij p oneven dan bestaat $2^{-1} \pmod p$ en men vindt

$$(x + \tfrac{1}{2}m)^2 \equiv \tfrac{1}{4}m^2 - n = D \pmod p.$$

Is nu $(\frac{D}{p})= +1$ dan is de congruentie oplosbaar; is $(\frac{D}{p})=0$ dan eveneens. Is echter $(\frac{D}{p})=-1$ dan is de congruentie, dus zeker ook die met modulus p^r voor $r>1$, onoplosbaar.

Het onderzoek van de congruentie

$$f(x) = x^2 + mx + n \equiv 0 \pmod{p^r}$$

voor $r\geq 2$ behoeft dus slechts te worden verricht als die voor r=1 oplosbaar is. Wij geven nu een procédé aan waarmee men de congruentie mod p^{r+1} kan oplossen als dat mod p^r reeds is geschied. De gezochte oplossing x moet dan mod p^r zeker overeenstemmen met een der oplossingen, zeg u, van de congruentie mod p^r. Stel de oplossing $x=u+vp^r$. Dan heeft

men

$$(3)\quad f(x) = f(u) + vp^r f'(u) + \tfrac{1}{2}v^2p^{2r} f''(u),$$

dus wij hebben wegens $2r \geqq r+1$ en $p \neq 2$ te zorgen voor

$$f(u) + vp^r f'(u) \equiv 0 \pmod{p^{r+1}},$$

d.w.z.

$$\frac{f(u)}{p^r} + v f'(u) \equiv 0 \pmod{p}.$$

Is $p \nmid f'(u)$ dan voldoet $v \equiv -\frac{f(u)}{p^r f'(u)} \pmod{p}$ en dus $x \equiv u - \frac{f(u)}{p^r f'(u)} \pmod{p^{r+1}}$; men vergelijke hiermee het benaderingsprocédé van Newton bij vergelijkingen. In het geval dat $f'(u) \equiv 0 \pmod{p}$ heeft men wegens (3)

$$f(x) \equiv f(u) \pmod{p^{r+1}}$$

en slechts als $p^{r+1} \mid f(u)$ vindt men dan een oplossing (en wel $x=u$).

In het geval tenslotte dat voor de congruentie $ax^2+bx+c \equiv 0 \pmod{p^r}$ geldt $p^s \mid a$ met $1 \leqq s < r$ losse men eerst op de congruentie $bx+c \equiv 0 \pmod{p^s}$. De oplossingen der oorspronkelijke congruentie moeten zeker mod p^s overeenstemmen met die der nieuwe, waarna daaruit op de hierboven aangegeven wijze successievelijk oplossingen der oorspronkelijke congruentie met modulus $p^{s+1}, p^{s+2}, \ldots, p^r$ kunnen worden gevonden.

Ons resteert nog het onderzoek van de congruentie

$$ax^2 + bx + c \equiv 0 \pmod{2^r},$$

hetwelk wij echter gaarne aan de lezer overlaten. Er worde hierbij nog gewezen op het feit dat in het geval dat b even is een oplossing voor de modulus 4 niet uit een voor de modulus 2 te vinden is, maar rechtstreeks moet worden bepaald. Dit geldt dus in het bijzonder voor de congruentie $x^2 \equiv a \pmod{2^r}$.

Opgave 12. Los op de congruentie

$$x^6 - 1 \equiv 0 \pmod{49}.$$

Opgave 13. Eveneens

$$x(x-1)(x-2)(x-3) \equiv 0 \pmod{2400}.$$

Opgave 14. Onderzoek voor welke priemgetallen p de congruentie

$$x^2 - x - 1 \equiv 0 \pmod{p}$$

oplosbaar is.

Opgave 15. Bewijs dat voor alle gehele a de uitdrukking $a^{15}-a^3$ deelbaar is door 32760.

Opgave 16. Bepaal het aantal nullen waarop het getal 19! eindigt en ook welke twee cijfers aan die nullen voorafgaan.

§ 6 Primitieve wortels

De hierboven gevonden congruentie van Euler luidde

$$a^{\varphi(m)} \equiv 1 \pmod{m}, \quad \text{mits } (a,m) = 1.$$

Men kan deze desgewenst ook zo interpreteren, dat elk element x van het gereduceerde restsysteem mod m voldoet aan $x^{\varphi(m)} \equiv 1 \pmod{m}$. Natuurlijk is het mogelijk dat er een positieve exponent e is die kleiner is dan $\varphi(m)$ en waarvoor een getal a ook reeds voldoet aan $a^e \equiv 1 \pmod{m}$. De kleinste positieve exponent c waarvoor geldt $a^c \equiv 1 \pmod{m}$ zullen wij noemen de primitieve periode of de primitieve exponent (of DE periode of de periode of DE exponent of de exponent) van a mod m. Wij geven deze wel aan met $c_a(m)$, soms kortweg met c(m) of zelfs met c.

Stelling. Als $a^n \equiv 1 \pmod{m}$, dan geldt $c \mid n$.

Bewijs: Stel $n=qc+r$ met gehele q en $0 \leq r < c$. Dan geldt $a^c \equiv 1 \pmod{m}$, dus $a^{qc} \equiv 1 \pmod{m}$, dus $a^r \equiv a^{qc+r} = a^n \equiv 1 \pmod{m}$, dus $r=0$, op grond van de minimaliteitsdefinitie van c. Derhalve $c \mid n$.

Opmerking. Omgekeerd als $c \mid n$ geldt uiteraard $a^n \equiv 1 \pmod{m}$. De getallen n, die aan deze congruentie voldoen vormen dus het hoofdideaal (c).

Gevolg. In het bijzonder geldt dus $c \mid \varphi(m)$.

Stelling. Als $a^h \equiv 1 \pmod{m}$ en $a^k \equiv 1 \pmod{m}$, dan geldt voor $g=(h,k)$ ook $a^g \equiv 1 \pmod{m}$.

Bewijs: Voor de GGD g van h en k geldt de schrijfwijze $g=uh+vk$, waarbij u en v passend gekozen gehele getallen zijn. Dan heeft men, in aanmerking nemende dat $(a,m)=1$ is en dus a^{-1} mod m bestaat,

$$a^g = a^{uh+vk} = (a^h)^u (a^k)^v \equiv 1 \pmod{m}.$$

Toepassing. Gevraagd zij a^p-1 te factoriseren.

Uiteraard geldt $a-1 \mid a^p-1$. Wij nemen aan dat de factorisatie van a-1 bekend is.

Een priemfactor q van $d = \frac{a^p-1}{a-1} = a^{p-1}+\ldots+1$ voldoet aan $a^p \equiv 1 \pmod{q}$. Voldoet ze ook aan $a \equiv 1 \pmod{q}$, dan heeft men $0 \equiv d \equiv a^{p-1}+\ldots+1 \equiv 1+\ldots+1 = p \pmod{q}$, dus $q=p$ en $p \mid a-1$. Om nu andere priemfactoren r van d te vinden dan diegene die deelbaar zijn op a-1 merken wij op dat uit $a^p \equiv 1 \pmod{r}$ volgt dat de exponent van a mod r een deler is van p, dus gelijk aan 1 of p. Wegens $r \nmid a-1$ moet die exponent dus p zijn. Ander-

zijds geldt $a^{r-1} \equiv 1 \pmod r$, dus $p \mid r-1$ en $r \equiv 1 \pmod p$; zelfs wegens $2 \mid r-1$ ook $r \equiv 1 \pmod{2p}$ (mits $p \neq 2$ is).

Voorbeeld. Ontbind $2^{11}-1$. Men onderzoeke alle priemgetallen die voldoen aan $p \equiv 1 \pmod{22}$. Reeds $p=23$ voldoet en $2^{11}-1=23.89$.

Opgave 1. Als q en $p=2q+1$ beide priem zijn en $(\frac{2}{p})=1$, dan geldt $p \mid 2^q-1$. Toon verder aan dat dit slechts kan optreden als $p \equiv -1 \pmod{24}$ is.

Opgave 2. Als a, b en n natuurlijke getallen zijn en p een priemdeler is van a^n-b^n, maar niet van a^m-b^m met $0 < m < n$, dan geldt $p \equiv 1 \pmod n$.

Opgave 3. Ontbind in factoren $3^{11}-2^{11}$; ook $5^{20}-3^{20}$.

Definitie. Een getal g heet primitieve wortel mod m als zijn primitieve exponent gelijk is aan $\varphi(m)$.

Voor een primitieve wortel mod m vormen de getallen $1=g^0, g, g^2, \ldots, g^{\varphi(m)-1}$ kennelijk een gereduceerd restsysteem mod m.

Opgave 4. Bewijs dit.

Stelling. Als g een primitieve wortel mod m is, dan is de exponent c van $h=g^n$ mod m gelijk aan $\frac{\varphi(m)}{d}$, waarin $d=(n, \varphi(m))$.

Bewijs: Uit $g^{\varphi(m)} \equiv 1 \pmod m$ volgt $g^{\frac{n\varphi(m)}{d}} \equiv 1 \pmod m$, dus $h^{\frac{\varphi(m)}{d}} \equiv 1 \pmod m$, dus $c \mid \frac{\varphi(m)}{d}$.

Uit $h^c \equiv 1 \pmod m$ volgt $g^{nc} \equiv 1 \pmod m$. Omdat g een primitieve wortel is mod m vindt men $\varphi(m) \mid nc$, dus

$$\frac{\varphi(m)}{d} \mid \frac{n}{d} c, \text{ dus } \frac{\varphi(m)}{d} \mid c. \text{ Bijgevolg } c = \frac{\varphi(m)}{d}.$$

Gevolg. Het getal $h=g^n$ is een primitieve wortel mod m als maar $(n, \varphi(m))=1$ is. Zodra dus voor een getal m het bestaan van één primitieve wortel is aangetoond, blijkt dat er precies $\varphi(\varphi(m))$ primitieve wortels bestaan.

Thans gaan wij onderzoeken welke getallen m primitieve wortels bezitten. Hiertoe tonen wij aan dat m geen primitieve wortels bezit als m door 4 deelbaar is en $\neq 4$ is, en ook als m tenminste twee verschillende oneven priemfactoren bezit.

Immers in het eerste gevalstelle men $m=2^r n$; n oneven. Is $n=1$, dus $r \geq 3$ dan heeft men voor elke oneven a de relatie $a^{2^{r-2}} \equiv 1 \pmod{2^r}$.

Opgave 5. Bewijs deze relatie.

Wegens $2^{r-2} = \frac{1}{2}\varphi(2^r)$ is a dus geen primitieve wortel.
Is $n \neq 1$, dan heeft men voor a met $(a,m)=1$ de relatie $a^{\varphi(n)} \equiv 1 \pmod n$, waarbij $\varphi(n)$ even is. Dus in verband met $a^{2^{r-1}} \equiv 1 \pmod{2^r}$ (geldig voor $r \geq 2$) vindt men $a^{2^{r-2}\varphi(n)} \equiv 1 \pmod m$ en a is geen primitieve wortel wegens $2^{r-2}\varphi(n) = \frac{1}{2}\varphi(m)$.

In het tweede geval gelden voor $m=p^r n$ (n oneven en $\neq 1$, niet deelbaar door het priemgetal p) en a met $(a,m)=1$ de relaties $a^{p^{r-1}(p-1)} \equiv 1 \pmod{p^r}$, en $a^{\varphi(n)} \equiv 1 \pmod{n}$, waarbij $\varphi(n)$ weer een even natuurlijk getal is. Dus $a^{\frac{1}{2}p^{r-1}(p-1)\varphi(n)} \equiv 1 \pmod{m}$ en a is wederom geen primitieve wortel wegens $\frac{1}{2}p^{r-1}(p-1)\varphi(n)=\frac{1}{2}\varphi(m)$.

De enige gevallen waarin m dus een primitieve wortel kán bezitten zijn $m=2$, $m=4$, $m=p^r$ en $m=2p^r$, waarbij p een oneven priemgetal is. Inderdaad bezitten 2 en 4 resp. de primitieve wortels 1 en 3. Zij verder g een primitieve wortel mod p^r, dan is datgene van de getallen g en p^r+g, dat oneven is, een primitieve wortel mod $2p^r$.

Opgave 6. Bewijs dat.

Het is dus nog voldoende om het bestaan van een primitieve wortel mod p^r aan te tonen. Wij doen dat eerst voor het geval $r=1$.

Wij bewijzen eerst de stelling door nu iets meer aan te tonen, nl.: Zij d een deler van $p-1$, dan bezit de congruentie

$$x^d \equiv 1 \pmod{p}$$

juist $\varphi(d)$ oplossingen met periode d.

Bewijs: Voor $d=1$ is de bewering triviaal. Zij $d>1$ en de bewering juist voor elke deler d' van d met $d'<d$. Het aantal oplossingen met periode d is dan gelijk aan $d-\sum_{\substack{d' \mid d \\ d' \neq d}} \varphi(d')$, welke uitdrukking, zoals men gemakkelijk inziet (en zoals in de volgende paragraaf nog wordt aangetoond), gelijk is aan $\varphi(d)$.

Opgave 7. Bewijs de gebruikte relatie.

Het gewenste resultaat vindt men nu door $d=p-1$ te nemen.

Tenslotte tonen wij door inductie naar r aan dat $m=p^r$ ook primitieve wortels bezit.

Hiertoe merken wij eerst op, dat p een primitieve wortel g bezit die voldoet aan $g^{p-1} \not\equiv 1 \pmod{p^2}$. Immers p bezit zeker een primitieve wortel f. Stel dat $f^{p-1} \equiv 1 \pmod{p^2}$, dan geldt volgens het binomium van Newton voor $g=f+p$

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

Thans laten wij (door inductie naar r) zien dat voor het nu gevonden getal g geldt

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

De eerste relatie is triviaal. Verder volgt voor $r \geq 1$ uit $g^{p^{r-1}(p-1)} \not\equiv 1 \pmod{p^{r+1}}$ dat $g^{p^{r-1}(p-1)}=1+vp^r$ met $p \nmid v$. Dus alweer gebruik makende van het binomium van Newton en van $2r+1 \geq r+2$

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

Hiermede is de hulpeigenschap bewezen. Voor de exponent c mod p^r van g heeft men dan $c \mid p^{r-1}(p-1)$, $p-1 \mid c$ (omdat $g^c \equiv 1 \pmod{p^r}$ voert tot $g^c \equiv 1 \pmod{p}$ en omdat g een primitieve wortel is mod p) en $c \nmid p^{r-2}(p-1)$. Bijgevolg is $c = p^{r-1}(p-1) = \varphi(p^r)$ en g een primitieve wortel mod p^r.

Voor getallen van de gedaante $m=2^r$ bestaat er, als $r \geq 3$ is, geen primitieve wortel. Het is van belang op te merken dat er wel een getal g bestaat met exponent $\frac{1}{2}\varphi(m) = 2^{r-2}$.
Immers voor $r=3$ neme men het getal 5. Het getal 5 voldoet bovendien aan $5^2 \not\equiv 1 \pmod{16}$. Evenals hierboven is nu door volledige inductie naar r aan te tonen dat het getal 5 ook voldoet aan

$$5^{2^{r-2}} \equiv 1 \pmod{2^r}, \quad 5^{2^{r-2}} \not\equiv 1 \pmod{2^{r+1}}.$$

Opgave 8. Ga dat na.
Daaruit volgt dan dat het getal 5 de gewenste eigenschap bezit.
Opgave 9. Bewijs dat.
Opgave 10. Als $a \equiv 1 \pmod 4$ is, dan bestaat bij gegeven r een exponent n met $5^n \equiv a \pmod{2^r}$.
Wij geven thans een toepassing van de gevonden resultaten over het bestaan van primitieve wortels.

Stelling. Als m een primitieve wortel bezit dan geldt

$$\prod_{\substack{n=1 \\ (n,m)=1}}^{m} n \equiv -1 \pmod m;$$

heeft m geen primitieve wortel dan is dat product $\equiv 1 \pmod m$.

Bewijs: Wij weten dat in het eerste geval de te beschouwen getallen n op m-vouden na van de gedaante g^r zijn, waarbij g een primitieve wortel is van m en r de waarden $0,1,\ldots, \varphi(m)-1$ doorloopt. Dus het gezochte product is mod m congruent met $g^{\frac{1}{2}\varphi(m)(\varphi(m)-1)}$. Omdat g een primitieve wortel is geldt $g^{\varphi(m)} \equiv 1 \pmod m$, $g^{\frac{1}{2}\varphi(m)} \equiv -1 \pmod m$.

Opgave 11. Deze conclusie, normaliter geldig voor priemgetallen m, mag hier worden getrokken op grond van de bijzondere gedaante van m als getal dat primitieve wortels bezit. Bewijs dit.

Omdat $\varphi(m)-1$ oneven is (behalve als $m=2$ is, maar dat geval is irrelevant) heeft men $g^{\frac{1}{2}\varphi(m)(\varphi(m)-1)} \equiv -1 \pmod m$.

In het geval dat m geen primitieve wortels bezit treedt als eerste mogelijkheid op het geval dat $m=2^r$ is.

Dan geldt (verg.opgave 10)

$$\prod_{\substack{n=1\\ 2\nmid n}}^{2^r} n = \prod_{s=0}^{\frac{1}{2}\varphi(2^r)} 5^s(2^r-5^s) \equiv \prod_{s=0}^{\frac{1}{2}\varphi(2^r)} (-5^{2s}) =$$

$$= (-)^{\frac{1}{2}\varphi(2^r)}\, 5^{\varphi(2^r)(\frac{1}{2}\varphi(2^r)-1)} = 1 \pmod{2^r}.$$

In de verdere gevallen heeft men voor elke oneven priemfactor p van m, onderstellende $m=p^r k$ met $p\nmid k$, $k\neq 1$, $k\neq 2$,

$$\prod_{\substack{n=1\\ (n,m)=1}}^{m} n \equiv \left(\prod_{\substack{n=1\\ (n,p)=1}}^{p^r} n\right)^{\varphi(k)} \equiv (-1)^{\varphi(k)} = 1 \pmod{p^r}$$

en voor de eventuele priemfactor 2 van m, onderstellende $m=2^r k$, $2\nmid k$, $r \geq 2$

$$\prod_{\substack{n=1\\ (n,m)=1}}^{m} n \equiv \left(\prod_{\substack{n=1\\ (n,2)=1}}^{2^r} n\right)^{\varphi(k)} \pmod{2^r}.$$

Is $r \geq 3$ dan is het laatste lid $\equiv (+1)^{\varphi(k)} = 1 \pmod{2^r}$. Is $r=2$ dan is $k\neq 1$, dus het laatste lid is dan $\equiv (-1)^{\varphi(k)} = 1 \pmod{2^r}$. Het gevondene samenvattende vindt men ten slotte

$$\prod_{\substack{n=1\\ (n,m)=1}}^{m} n \equiv 1 \pmod{m}$$

als m geen primitieve wortels bezit.

Opmerking. Dat het beschouwde product slechts de waarde +1 of -1 kan aannemen blijkt ook uit de volgende beschouwing (herinnerende aan die welke bij het bewijs van de stelling van Wilson werd gegeven).

Naast elke n is een n' te vinden met $nn' \equiv 1 \pmod{m}$. Alle zo verkregen paren mogen dus bij de berekening mod m van het product worden weggelaten, zodat dit product slechts gelijk blijkt te zijn aan het product van die getallen n met $n^2 \equiv 1 \pmod{m}$. Om hun product te vinden merke men op dat bij $n^2 \equiv 1 \pmod{m}$ ook geldt $(m-n)^2 \equiv 1 \pmod{m}$, zodat naast elke oplossing n ook een oplossing m-n optreedt. Omdat $n \neq m-n$ is (afgezien van het geval m=2; immers (m,n)=1) vindt men alle producten slechts uitstrekkende over de n met $n^2 \equiv 1 \pmod{m}$

$$\prod_{n=1}^{m} n \equiv \prod_{n=1}^{\frac{1}{2}m} n(m-n) \equiv \prod_{n=1}^{\frac{1}{2}m} -n^2 = \prod_{n=1}^{\frac{1}{2}m} (-1) = \pm 1 \pmod{m}.$$

Wij geven een tweede toepassing van het gevondene over primitieve wortels. Op blz. 17 vroegen wij ons af of uit $2^{m-1} \equiv 1 \pmod m$ volgt dat m priem is. Dat dit niet zo is blijkt bv. uit de keuze $m=341=11.31$. Men heeft nl. $2^{10} \equiv 1 \pmod{31}$, $2^{10} \equiv 1 \pmod{11}$, dus $2^{10} \equiv 1 \pmod m$, dus $2^{m-1} \equiv 1 \pmod m$. Zelfs zijn er oneindig veel samengestelde getallen en die voldoen aan $2^{m-1} \equiv 1 \pmod m$. Is nl. eenmaal één zo'n getal m bekend (en wij kennen er nu zo een), dan heeft $M=2^m-1$ ook deze eigenschap. Immers $m \mid 2^{m-1}-1$ leidt tot

$$M = 2^m-1 \mid 2^{2^{m-1}-1}-1 \mid 2^{2^m-2}-1 = 2^{M-1}-1.$$

P.Poulet heeft een lijst gemaakt waarin alle samengestelde getallen m van dit type die kleiner zijn dan 10^8 optreden *). Met behulp van deze lijst is een toets op primaliteit voor elk getal $< 10^8$ gemakkelijk met eenvoudige vermenigvuldigapparaten uit te voeren.

Voor elk natuurlijk getal a bestaan er voorts oneindig veel samengestelde getallen m met $m \mid a^{m-1}-1$.

Immers, zij m een samengesteld getal dat hieraan voldoet en verder aan $(m,a-1)=1$. Dan heeft men voor $M=\frac{a^m-1}{a-1}$ dezelfde relaties. Immers zij $p \mid a-1$, dan $M=a^{m-1}+\ldots+a+1 \equiv 1+\ldots+1+1=m \pmod p$, dus $p \nmid M$ en $(a-1,M)=1$. Verder heeft men

$$M = \frac{a^m-1}{a-1} \mid a^m-1 \mid a^{a^{m-1}-1}-1 \mid a^{a^m-a}-1 = a^{(M-1)(a-1)}-1$$

Ook bleek $M \mid a^m-1$. Dus $M \mid a^g-1$ met $g=(m,(M-1)(a-1))=(m,M-1)$.

Bijgevolg $M \mid a^{M-1}-1$. Als begin -m van de rij die hier wordt geconstrueerd neme men bv. $m=\frac{a^{2a}-1}{a^2-1}$, een getal dat kennelijk samengesteld is. Hiervoor geldt $(m,a-1)=1$, want als $p \mid a-1$, dan $m=a^{2a-2}+\ldots+a^2+1 \equiv 1+\ldots+1+1=2a \equiv 2 \pmod p$, dus $p \nmid m$. Verder

$$m = \frac{a^{2a}-1}{a^2-1} \mid a^{2a}-1 \mid a^{\frac{a^{2a}-a^2}{a^2-1}}-1 = a^{m-1}-1,$$

waarmede de bewering is bewezen.

De vraag rijst nu of er samengestelde getallen m bestaan, waarbij voor elke a met $(a,m)=1$ geldt $a^{m-1} \equiv 1 \pmod m$ (Carmichael getallen). Deze zijn te vinden onder de Poulet getallen en in Poulet's tabel aangegeven. Wij leiden hier enige eigenschappen van deze getallen af.

---

*) P.Poulet, Table des nombres composés verifiant le théorème de Fermat pour le module 2 jusqu'à 100000000. Sphinx 8(1938), 42-52.

Zij $m=p^r n$, $2 \nmid p \nmid n$. Kies nu voor a een primitieve wortel mod p. Dan vindt men uit $a^{m-1} \equiv 1 \pmod{p^r}$, dat $p^{r-1}(p-1) \mid m-1$, dus r=1 en $p-1 \mid m-1$. Omgekeerd geldt voor elke priemfactor p van m de relatie $p-1 \mid m-1$, dan heeft men voor elke q met (q,m)=1 de betrekking $a^{p-1} \equiv 1 \pmod{p}$, dus $a^{m-1} \equiv 1 \pmod{p}$, dus $a^{m-1} \equiv 1 \pmod{m}$. De nodig en voldoende voorwaarde dat m een Carmichael getal is is dus dat m quadraatvrij is en dat elke oneven priemfactor p van m voldoet aan $p-1 \mid m-1$.

Verder is m oneven. Immers was $m=2^r n$, dan gold voor elke (oneven) priemfactor p van n de relatie $p-1 \mid m-1$, maar p-1 is even en m-1 oneven. Het geval $m=2^r$ is ook uitgesloten want men heeft $a^{2^{r-2}} \equiv 1 \pmod{2^r}$, dus $a^{2^r} \equiv 1 \pmod{2^r}$, dus $a^{2^r-1} \equiv 1 \pmod{2^r}$ zou dan leiden tot $a \equiv 1 \pmod{2^r}$, wat echter voor de toelaatbare keuze a=3 niet vervuld is.

Het geval m=pq is onmogelijk, want $p-1 \mid m-1$ en $q-1 \mid m-1$ leiden resp. tot $p-1 \mid q-1$ en $q-1 \mid p-1$. Elk Carmichael getal is dus een quadraatvrij oneven product van tenminste drie factoren. Dat er zulke getallen bestaan blijkt uit het voorbeeld m=561=3.11.17 (het kleinste Carmichael getal).

Opgave 12. Controleer dit.

Wij geven nog een enkele eigenschap van Carmichael getallen, waarbij men een typisch getallentheoretische werkwijze in de afleiding ontmoet.

Laat M=pq m een Carmichael getal zijn met $p < q$. Nodig is dan dat de priemgetallen p en q voldoen aan $p-1 \mid M-1$, d.w.z. $p-1 \mid qm-1$ en $q-1 \mid M-1$, d.w.z. $q-1 \mid pm-1$. Er bestaan dus gehele u en v met $pm-1=u(q-1)$, $qm-1=v(p-1)$. Kennelijk is $u > 1$, $v > 1$ en $u < v$. Wegens $q \geq p+2$ heeft men $u \leq \frac{pm-1}{p+1} = m - \frac{m+1}{p+1} < m$, dus $u \leq m-1$.

Uit de beide relaties volgt na oplossing

$$p-1 = \frac{(m-1)(m+u)}{uv-m^2}, \qquad q-1 = \frac{(m-1)(m+v)}{uv-m^2}.$$

Voorts is $uv-m^2 \geq 1$ (als geheel en positief getal). Bijgevolg

$$p-1 \leq (m-1)(m+u) \leq (m-1)(2m-1)$$

en dus

$$q-1 \leq \tfrac{1}{2}(pm-1) \leq \tfrac{1}{2}(m-1)(2m^2-m+1).$$

Dit leert ons, dat er slechts eindig veel Carmichael getallen zijn, waarvan alle priemfactoren, afgezien van de grootste twee gegeven zijn.

Voorbeeld. m=3, dus $p \leq 11$, d.w.z. p=5,7 of 11. Wegens $p-1 \mid qm-1$ is $(p-1,m)=(p-1,3)=1$, dus $p \neq 7$. Het geval p=5 leidt tot $q-1 \mid 14$, wat uitgesloten is. Tenslotte voert p=11 tot $q-1 \mid 32$ met als enige mogelijkheid q=17. Inderdaad blijkt 3.11.17=561 een Carmichael getal te zijn (en zelfs het kleinste).

§ 7. Rekenkundige functies en reeksen van Dirichlet.

In deze paragraaf onderzoeken wij bepaalde eigenschappen van rekenkundige functies, dat zijn functies $f(n)$ die voor alle natuurlijke n gedefinieerd zijn.

Definitie. Een rekenkundige functie $f(n)$ heet multiplicatief als $f(ab) = f(a)\,f(b)$ indien $(a,b)=1$.

Een multiplicatieve rekenkundige functie is bepaald voor alle natuurlijke getallen zodra zij het is voor de machten der priemgetallen.

Stelling. Als $f(n)$ en $g(n)$ multiplicatief zijn, is de functie

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

het ook.

Bewijs. Als $(n_1,n_2)=1$ heeft men

$$h(n_1n_2) = \sum_{d|n_1n_2} f(d)\, g\left(\frac{n_1n_2}{d}\right) = \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1)f(d_2)g\left(\frac{n_1}{d_1}\right)g\left(\frac{n_2}{d_2}\right)$$

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

waarbij gebruik gemaakt is van het feit dat elke deler d van n_1n_2 ondubbelzinnig te schrijven is in de gedaante $d=d_1d_2$ met $d_1|n_1$, $d_2|n_2$, dus $(d_1,d_2)=1$.

Van deze stelling zijn vele toepassingen te geven. Bij een aantal ervan zullen wij $g(n)=1$ nemen. Daar deze functie kennelijk multiplicatief is heeft men: Is $f(n)$ multiplicatief, dan is $F(n)= \sum_{d|n} f(d)$ het ook.

Als voorbeeld zien wij door $f(n) = n$ te nemen dat $\sigma(n)= \sum_{d|n} f(d) = \sum_{d|n} d$, d.w.z. de som der delers van n, een multiplicatieve functie is. Hiermede is $\sigma(n)$ gemakkelijk te bepalen. Immers $n=p^r$ heeft als delers de getallen $1,p,p^2,\ldots,p^r$, dus $\sigma(p^r)= \frac{p^{r+1}-1}{p-1}$ en bijgevolg is $\sigma(n) = \prod_{\sigma=1}^{s} \frac{p_\sigma^{r_\sigma+1}-1}{p_\sigma-1}$, waarbij $n=p_1^{r_1}\ldots p_s^{r_s}$ de kanonieke ontbinding van n zij. (Indien hierover verder niets wordt gezegd zal steeds worden ondersteld dat dit de kanonieke ontbinding is van n).

Opgave 1. Bewijs dat $\sigma_a(n)$, de som der a^e machten der delers van n een multiplicatieve functie is en bepaal deze functie voor willekeurige n.

In het geval dat men $f(n)=1$ neemt vindt men voor $F(n)= \sum_{d|n} f(d)= \sum_{d|n} 1$ het aantal delers van n, veelal aangegeven door $d(n)$. Deze functie is dus ook multiplicatief. Verder geldt $d(p^r)=r+1$,

dus $d(n) = \prod_{\sigma=1}^{s} (r_\sigma+1)$.

Opgave 2. Bewijs deze formules.

Opgave 3. Bepaal $d(n)$ ook als $\lim_{a \to 0} \sigma_a(n)$.

Een zeer belangrijke multiplicatieve functie is de functie $\mu(n)$ van Möbius, gedefinieerd als volgt: $\mu(1) = 1$;
$\mu(n) = 0$, als n niet quadraatvrij is;
$\mu(n)=(-)^r$ als n een product is van r verschillende priemfactoren.

Opgave 4. Bewijs dat $\mu(n)$ multiplicatief is.

Voor de functie $\mu(n)$ geldt de belangrijke eigenschap $\sum_{d|n} \mu(d) =$
$= \begin{cases} 1 \text{ als } n=1; \\ 0 \text{ als } n\neq 1. \end{cases}$

Bewijs: Omdat $\mu(n)$ multiplicatief is, is $M(n)= \sum_{d|n} \mu(d)$ het ook.
Men heeft $M(1) = \mu(1) = 1$ en verder $M(p^r)= \sum_{d|p^r} \mu(d)=\mu(1)+\mu(p)=$
$=1-1=0$. Bijgevolg $M(1)=1$, $M(n)=0$ als $n\neq 1$.
Het is ons nu mogelijk om niet alleen $F(n)= \sum_{d|n} f(d)$ uit te drukken in $f(d)$ maar omgekeerd ook $f(n)$ in $F(d)$. Dit geschiedt met behulp van de

Omkeerformule van Möbius. Als $F(n) = \sum_{d|n} f(d)$, dan geldt
$f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d})$.

Bewijs: Men heeft $\sum_{d|n} F(d)\mu(\frac{n}{d}) = \sum_{d|n} \sum_{d'|d} f(d')\mu(\frac{n}{d}) =$

$= \sum_{d'|n} \sum_{d''|\frac{n}{d'}} f(d')\mu(d'') = \sum_{d'|n} f(d') \sum_{d''|\frac{n}{d'}} \mu(d'')$.

De laatste som is op grond van het voorafgaande 0 of 1 en wel slechts één als $\frac{n}{d'} = 1$, dus het laatste lid is gelijk aan $f(n)$. Q.e.d.

Opgave 5. Bewijs $\sum_{d|n} \mu(d)\sigma_a(\frac{n}{d}) = n^a$.

Het is duidelijk dat bij $F(n) = \sum_{d|n} f(d)$ en $f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d})$ men door nogmaals toepassen van de omkeerformule van Möbius weer $F(n)$ moet terugvinden, d.w.z. dat

$$F(n) = \sum_{d_1|n} \mu(\frac{n}{d_1}) \sum_{d|d_1} F(d)\mu(\frac{d_1}{d}).$$

Opgave 6. Bewijs deze formule rechtstreeks.

Uit vroegere beschouwingen kennen wij de functie $\varphi(n)$ van Euler, gedefinieerd door $\varphi(n)= \sum_{\substack{i=1 \\ (n,i)=1}}^{n} 1$. Wij vonden toen reeds dat deze func-

tie multiplicatief is. Thans tonen wij aan dat $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$. Een eerste bewijs gaat direct. Bij $n = p_1^{r_1} \ldots p_s^{r_s}$ vindt men dat het rechterlid der te bewijzen formule een som is van uitdrukkingen van de gedaante

$$\frac{(-)^j}{p_{s_1} \cdots p_{s_j}}$$ en dus gelijk is aan $\prod_{\sigma=1}^{s} (1 - \frac{1}{p_\sigma})$, waarmee de formule bewezen is. Omdat $\mu(n)$ multiplicatief is, is $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$ het ook, waarmee de multiplicativiteit van $\varphi(n)$ is teruggevonden. Omgekeerd is een tweede bewijs van onze formule gemakkelijk met behulp van die multiplicativiteit te verkrijgen. Immers men heeft de formule slechts voor $n = p^r$ te verifieren.

Opgave 7. Voer dit uit.

Beschouwen we de gevonden formule als het resultaat van toepassen van de omkeerformule van Möbius, dan vindt men dat als uitgangsformule gegolden heeft

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

een formule die wij reeds on blz. 34 hebben gebruikt en toen direct bewezen.

Opgave 8. Bewijs $\sum_{d|n} \mu(d) \log d = 0$.

Opgave 9. Als het getal n ten minste t verschillende priemfactoren bevat bewijze men

$$\sum_{d|n} \mu(d) \log^t d = 0.$$

Er is een nauwe samenhang tussen de hier ontwikkelde theorie en de theorie der reeksen van Dirichlet welke in zekere zin kunnen worden beschouwd als voortbrengende functies van multiplicatieve rekenkundige functies.

Een reeks van Dirichlet is een reeks van het type $\sum_{n=1}^{\infty} a_n n^{-z}$. Evenals men een machtreeks $\sum_{n=0}^{\infty} a_n z^n$ kan opvatten als voortbrengende functie van een getallenrij $a_0, a_1, \ldots$ kan men de hiergenoemde reeks van Dirichlet ook wel opvatten als voortbrengende functie (maar dan dus in iets andere zin) van de rij $a_1, a_2, \ldots$

Wij geven eerst een paar convergentieeigenschappen van reeksen van Dirichlet. Als zo'n reeks absoluut convergeert voor zekere z, convergeert ze ook voor alle z met Re $z \geq$ Re z_0. Immers

$$\sum_{n=1}^{\infty} a_n n^{-z} < \sum_{n=1}^{\infty} |a_n| n^{-x_0}.$$

Er geldt echter meer: Als de reeks convergeert voor zekere z_o convergeert ze voor alle z met Re $z \geq$ Re z_o. Immers zij $\sum_{n=1}^{\infty} a_n n^{-z_o}$ convergeert. Stel $\sum_{n=N}^{\infty} a_n n^{-z_o} = \varepsilon_N$. Dan heeft men $\lim_{N \to \infty} \varepsilon_N = 0$. Verder heeft men voor Re $z >$ Re z_o

$$\sum_{n=h}^{k} a_n n^{-z} = \sum_{n=h}^{k} a_n n^{-z_o} n^{z_o - z} = \sum_{n=h}^{k} (\varepsilon_n - \varepsilon_{n+1}) n^{z_o - z}$$

$$= \sum_{n=h}^{k} \varepsilon_n (-(n-1)^{z_o - z} + n^{z_o - z}) + \varepsilon_h (h-1)^{z_o - z} - \varepsilon_{k+1} k^{z_o - z}.$$

Wegens Re $z >$ Re z_o worden bij voldoende grote h en willekeurige k met $k > h$ de laatste twee termen willekeurig klein, terwijl de som wegens $(n-1)^{z_o - z} - n^{z_o - z} = O(n^{x_o - x - 1})$ en wegens $\mathrm{Re}(z+1-z_o) > 1$ dan eveneens willekeurig klein wordt. Op grond van het criterium van Cauchy vindt men hieruit de gewenste convergentie.

De laatste eigenschap geeft na gebruikelijke overwegingen het bestaan van een convergentie abscis, d.i. een reëel getal α met de eigenschap dat de reeks convergeert voor Re $z > \alpha$, divergeert voor Re $z < \alpha$, terwijl het gedrag voor Re $z = \alpha$ in eerste instantie onbeslist is.

Reeds bij het bovenstaande ziet men dat zich bij het convergentie onderzoek van de reeks van Dirichletreeks $D(z) = \sum_{n=1}^{\infty} a_n n^{-z}$ analoge verschijnselen voordoen als bij dat van de zgn. faculteitenreeksen

$$A(z) = \sum_{n=0}^{\infty} \frac{a_n (-)^n}{n!} \cdot \frac{\Gamma(z-n)}{\Gamma(z)} \text{ en } B(z) = \sum_{n=0}^{\infty} \frac{a_n \, n! \, \Gamma(z)}{\Gamma(z+n+1)}.$$

(verg. blz. DE 49 e.v.). Wij bewijzen thans dat de drie reeksen A(z), B(z) en D(z) dezelfde convergentieabscis bezitten. Van de reeksen A(z) en B(z) is dit reeds bekend, zodat wij hier ons b.v. kunnen beperken tot het vergelijken van de reeksen B(z) en D(z).

Onderstel allereerst dat D(z) convergent is, d.w.z. $\lim_{N \to \infty} \varepsilon_N = 0$, waarbij $\varepsilon_N = \sum_{n=N}^{\infty} a_n n^{-z}$. Dan heeft men

$$\sum_{n=N}^{M} a_n \frac{n! \, \Gamma(z)}{\Gamma(z+n+1)} = \sum_{n=N}^{M} (\varepsilon_n - \varepsilon_{n-1}) \frac{n! \, n^z \, \Gamma(z)}{\Gamma(z+n+1)}$$

$$= \sum_{n=N}^{M} \varepsilon_n \frac{n! \, n^z \, \Gamma(z)}{\Gamma(z+n+1)} - \sum_{n=N}^{M} \varepsilon_{n+1} \frac{(n+1)! (n+1)^z \, \Gamma(z)}{\Gamma(z+n+2)} +$$

$$-\varepsilon_{N-1}\frac{N!\,N^z\,\Gamma(z)}{\Gamma(z+N+1)}+\varepsilon_M\frac{(M+1)!\,(M+1)^z\,\Gamma(z)}{\Gamma(z+M+2)}$$

$$=\sum_{n=N}^{M} p_n - r_N + r_{M+1}$$

met $r_{M+1}=\varepsilon_M\frac{(M+1)!(M+1)^z\,\Gamma(z)}{\Gamma(z+M+2)}=\varepsilon_M\left(\frac{M+1}{M+2}\right)^z\Gamma(z)\left(1+O\left(\frac{1}{M}\right)\right)$

$$\longrightarrow 0 \text{ als } N\longrightarrow\infty \text{ en } M\geqslant N,$$

dus met $r_N\longrightarrow 0$ als $N\longrightarrow\infty$ en verder met

$$p_n=\varepsilon_n\frac{\Gamma(z)n^z\,n!}{\Gamma(z+n+1)}\left(1-\frac{(n+1)\left(1+\frac{1}{n}\right)^z}{z+n+1}\right)=\varepsilon_n\Gamma(z)\left(1+\frac{1}{n}\right)^{-z}\cdot$$

$$-\frac{z(z+1)}{2n^2}\left(1+O\left(\frac{1}{n}\right)\right)$$

$$=-\varepsilon_n\Gamma(z)\frac{z(z+1)}{2n^2}\left(1+O\left(\frac{1}{n}\right)\right), \text{ dus } \sum_{n=N}^{M} p_n << \varepsilon \text{ als } N, \text{ dus}$$

$M\geqslant N$, voldoende groot wordt gekozen. Hierbij is gebruik gemaakt van de bekende asymptotische formule (vgl. blz. DE 51) $\frac{\Gamma(z+c)}{\Gamma(z)}=z^c\left(1+O\left(\frac{1}{\mathrm{Re}\,z}\right)\right)$. Bijgevolg leidt convergentie van D(z) tot die van B(z). Op geheel analoge wijze, eveneens door gebruik te maken van partiële sommatie, is af te leiden dat convergentie van B(z) voert tot convergentie van D(z).

Opgave 10. Voer dat uit.

Bijgevolg geldt voor de convergentieabscis van de reeks van Dirichlet dezelfde formule als die van de faculteitenreeks. De formule daarover is in de cursus Differentierekening afgeleid (en zou trouwens op geheel analoge wijze rechtstreeks voor de Dirichletreeksen zijn af te leiden) en luidt (vgl blz. FE 52 e.v.) $\lambda=\alpha$ als $\lambda\geqslant 0$ en $\lambda=\beta$ als $\lambda<0$, waarbij

$$\alpha=\overline{\lim_{N\to\infty}}\frac{\log\left|\sum_{n=1}^{N}a_n\right|}{\log N};$$

$$\beta=\overline{\lim_{N\to\infty}}\frac{\log\left|\sum_{n=N}^{\infty}a_n\right|}{\log N}.$$

Voorbeeld. Voor de ζ-functie $\sum_{n=1}^{\infty} n^{-z}$ heeft men (omdat men hier kennelijk in het eerste geval, nl. $\lambda=\alpha$, verkeert) $\lambda=\alpha=$

$$=\overline{\lim}\frac{\log\sum_{n=1}^{N}1}{\log N}=1.$$

Opgave 11. Bepaal de convergentieabscis van de reeksen

$$\sum_{n=1}^{\infty} \log n.\, n^{-z} \text{ en } \sum_{n=1}^{\infty} (-1)^n\, n^{-z};$$

bepaal van de laatste reeks ook de abscis van absolute convergentie.

Wij beschouwen thans de Dirichletreeksen nader van getallentheoretisch standpunt. In de punten z waar ze worden genomen onderstellen we, als niet het tegendeel wordt meegedeeld, convergent.

Als $f(z) = \sum_{n=1}^{\infty} a_n n^{-z}$ en $g(z) = \sum_{n=1}^{\infty} b_n n^{-z}$, dan geldt

$$f(z)g(z) = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} a_n b_m n^{-z} m^{-z} = \sum_{N=1}^{\infty} \sum_{n|N} a_n b_{N/n} N^{-z} = \sum_{N=1}^{\infty} c_N N^{-z},$$

waarbij $c_N = \sum_{n|N} a_n b_{N/n}$. Zijn a_n en b_n multiplicatieve functies, dan blijkt dat dus ook het geval te zijn met de coëfficiënten van de productreeks van de reeksen, welke door a_n resp. b_n worden voortgebracht.

Om nadere toepassingen te kunnen geven voeren wij in de reeks

$$\zeta(z) = \sum_{n=1}^{\infty} n^{-z} \quad (\zeta\text{-functie van Riemann}),$$

waarvan alle coëfficiënten $a_n = 1$ zijn en welke kennelijk de convergentieabscis 1 bezit.

Opgave 12. Bewijs dit.

Als a_n nu een multiplicatieve functie is, dan is dat ook het geval met $A_n = \sum_{d|n} a_d$ en deze getallen brengen een functie F(z) voort, welke voldoet aan $F(z) = \zeta(z)f(z)$, waarbij $f(z) = \sum_{n=1}^{\infty} a_n n^{-z}$. Een eenvoudige toepassing is het geval $f(z) = \zeta(z)$, dus $F(z) = \zeta^2(z)$. Men vindt

$$\zeta^2(z) = \sum_{n=1}^{\infty} d(n) n^{-z}.$$

Opgave 13. Bewijs dit.

Verder heeft men

$$\zeta(z)\zeta(z-1) = \sum_{n=1}^{\infty} n^{-z} \sum_{m=1}^{\infty} m.m^{-z} = \sum_{N=1}^{\infty} c_N N^{-z}$$

met $c_N = \sum_{m|N} m = \sigma(N)$, dus

$$\zeta(z)\zeta(z-1) = \sum_{n=1}^{\infty} \sigma(n) n^{-z}.$$

Opgave 14. Bewijs

$$\zeta(z)\zeta(z-a) = \sum_{n=1}^{\infty} \sigma_a(n)\, n^{-z}.$$

Thans bepalen wij op twee manieren de "Dirichletontwikkeling van $\frac{1}{\zeta(z)}$. Bij de eerste manier merken wij op dat

$$(1-2^{-z})\,\zeta(z) = \sum_{\substack{n=1\\(n,2)=1}}^{\infty} n^{-z},$$

verder dat

$$(1-2^{-z})(1-3^{-z})\,\zeta(z) = \sum_{\substack{n=1\\(n,6)=1}}^{\infty} n^{-z}$$

enz., dus als p het m^e priemgetal voorstelt

$$(1-2^{-z})(1-3^{-z})\ldots(1-p^{-z})\,\zeta(z) = \sum_{\substack{n=1\\(n,2.3.\ \ldots p)=1}}^{\infty} n^{-z},$$

waarbij de reeks in het rechterlid te majoreren is door

$$1 + \sum_{n=p}^{\infty} n^{-x} < 1 + \int_{p-1}^{\infty} u^{-x}\,du = 1 + \frac{u^{1-x}}{1-x}\Big|_{p-1}^{\infty} = 1 + \frac{(p-1)^{1-x}}{x-1},$$

en dus voor $m \longrightarrow \infty$ de limiet 1 bezit. Bijgevolg heeft men

$$\prod_p (1-p^{-z})\,\zeta(z) = 1,$$

waarbij bedoeld is dat p de rij van alle priemgetallen doorloopt. Dus

$$\frac{1}{\zeta(z)} = \prod_p (1-p^{-z}).$$

Ontwikkelt men dit product verder dan vindt men de Dirichletreeks $\sum_{n=1}^{\infty} c_n n^{-z}$, waarbij $c_1=1$, $c_n=0$ als n niet quadraatvrij is en $c_n=(-)^s$ als n een product is van s verschillende priemfactoren. Bijgevolg is $c_n=\mu(n)$ en

$$\frac{1}{\zeta(z)} = \sum_{n=1}^{\infty} \mu(n) n^{-z}.$$

<u>Toepassing</u>. Als $f(z) = \sum_{n=1}^{\infty} a_n n^{-z}$ en $A_n = \sum_{d|n} a_d$, dan vonden wij $F(z) = f(z)\,\zeta(z) = \sum_{n=1}^{\infty} A_n n^{-z}$. Anderzijds geldt $f(z) = \frac{1}{\zeta(z)} F(z)$, dus de Dirichlet coëfficiënten $\mu(n)$ van $\frac{1}{\zeta(z)}$ voldoen aan $a_n = \sum_{d|n} A_d \mu(\frac{n}{d})$, waarmee de omkeerformule van Möbius is teruggevonden.

Het tweede bewijs van de formule voor $\frac{1}{\zeta(z)}$ volgt juist uit de om-

keerformule van Möbius. Men heeft nl. $1 = \zeta(z)\frac{1}{\zeta(z)}$, dus als men de Dirichlet-coëfficiënten van $\frac{1}{\zeta(z)}$ voorlopig b_n noemt, heeft men

$\sum_{d|n} b_d = e_n$ met $e_1=1$ en $e_n=0$, als $n\neq 1$. Kennelijk is de functie e_n multiplicatief.

Opgave 15. Bewijs dit.

Bijgevolg geldt $b_n = \sum_{d|n}\mu(\frac{n}{d})e_d = \mu(n)$, waarmee de formule voor $\frac{1}{\zeta(z)}$ opnieuw is gevonden.

Om na te gaan welke functie wordt voorgesteld door $f(z) = \sum_{n=1}^{\infty}\varphi(n)n^{-z}$ merken wij op dat wegens $\sum_{d|n}\varphi(d)=n$ geldt

$$\sum_{n=1}^{\infty} n.n^{-z} = f(z)\zeta(z),$$

dus $f(z) = \frac{\zeta(z-1)}{\zeta(z)} = \sum_{n=1}^{\infty}\varphi(n)n^{-z}$.

Verder volgt uit $\frac{1}{\zeta(z)} = \prod_p (1-p^{-z})$ na logarithmisch differentieren

$$\frac{-\zeta'(z)}{\zeta(z)} = \sum_p \frac{p^{-z}\log p}{1-p^{-z}} = \sum_p \sum_{m=1}^{\infty} p^{-mz}\log p = \sum_{n=1}^{\infty} c_n n^{-z}$$

met $\begin{cases} c_n=0 \text{ als } n \text{ ten minste twee verschillende priemgetallen bezit;} \\ c_n = \log p, \text{ als } n=p^r. \end{cases}$

Men noemt deze functie wel $\Lambda(n)$. Anderzijds heeft men $\zeta'(z) = -\sum_{n=1}^{\infty}\log n.n^{-z}$ en wegens $\frac{1}{\zeta(z)} = \sum_{n=1}^{\infty}\mu(n)n^{-z}$ dat

$\Lambda(n) = \sum_{d|n}\log d.\mu(\frac{n}{d})$, dus ook $\mu(n) = \sum_{d|n}\Lambda(d)$. Ten slotte levert de formule voor $\frac{1}{\zeta(z)}$ na differentiatie $\frac{\zeta'(z)}{\zeta^2(z)} = \sum_{n=1}^{\infty}\mu(n)\log n.n^{-z}$,

dus $\zeta'(z) = \sum_{m=1}^{\infty} d(m).m^{-z}\sum_{n=1}^{\infty}\mu(n)\log n.n^{-z}$,

waaruit volgt $\log n = -\sum_{m|n}\mu(m)\log m.\, d(\frac{n}{m})$.

Tenslotte beschouwen wij nog de reeksen van Lambert, dat zijn reeksen van de gedaante $\sum_{n=1}^{\infty} a_n \frac{z^n}{1-z^n}$. Dergelijke reeksen zijn natuurlijk naar machten van z te ontwikkelen. Men vindt dan

$$\sum_{n=1}^{\infty} a_n \frac{z^n}{1-z^n} = \sum_{n=1}^{\infty} \sum_{k=1}^{\infty} a_n z^{nh} = \sum_{m=1}^{\infty} A_m z^m,$$

met $A_m = \sum_{n|m} a_n$. Hier ontmoeten wij dezelfde samenhang als hierboven tussen de coëfficiënten van $f(z) = \sum_{n=1}^{\infty} a_n n^{-z}$ en $f(z)\zeta(z)$.
Wij vinden door bv. alle $a_n=1$ te nemen de relatie

$$\sum_{n=1}^{\infty} \frac{z^n}{1-z^n} = \sum_{m=1}^{\infty} d(m) z^m.$$

Opgave 16. Ontwikkel de functie $\sum_{n=1}^{\infty} \frac{n^k z^n}{1-z^n}$ naar machten van z.

Opgave 17. Sommeer de reeks $\sum_{n=1}^{\infty} \frac{\varphi(n) z^n}{1-z^n}$.

§8. Splitsing in quadraten.

Reeds eerder vonden wij dat ieder ondeelbaar viervoud + 1 te schrijven is als de som van twee quadraten. Wij willen thans eens onderzoeken op hoeveel manieren het mogelijk is om een willekeurig natuurlijk getal n te schrijven als som van twee quadraten en bovendien uit het resultaat een interessante formule afleiden.

Wij beginnen met de

Stelling. Zij x een irrationaal getal en n een vast gegeven getal. Dan bestaat er een onvereenvoudigbare breuk $\frac{a}{b}$ met $a < b < n$ en $|x - \frac{a}{b}| < \frac{1}{nb}$.

Bewijs. Beschouw de n getallen $\nu x = a_\nu + \vartheta_\nu$, waarbij $0 \leqq \vartheta_\nu < 1$, dus $a_\nu = [\nu x]$ $(\nu=1,\ldots,n)$. De n twee aan twee verschillende getallen $\vartheta_1,\ldots,\vartheta_n$ zijn allen >0 en <1, dus er moeten er twee zijn, laten wij zeggen ϑ_i en ϑ_j, met $0 < \vartheta_i - \vartheta_j < \frac{1}{n}$.

Opgave 1. Bewijs dat $\vartheta_h \neq \vartheta_k$ als $h \neq k$.

Derhalve $(i-j)x = a_i - a_j + \frac{\vartheta}{n}$ met $0 < \vartheta < 1$ en

$$x = \frac{a_i - a_j}{i-j} + \frac{\vartheta}{n(i-j)} = \frac{a}{b} + r,$$

waarbij $a=(a_i-a_j)b/(i-j)$, $b = |i-j|/g$, $g=(a_i-a_j, |i-j|)$. Dus $r = \frac{\vartheta}{n|i-j|} = \frac{\vartheta}{nbg} < \frac{1}{nb}$ en $0 < b \leqq |i-j| < n$.

De hier afgeleide stelling geeft ons een (in zekere zin niet constructieve)methode van approximatie van irrationale getallen x door rationale $\frac{a}{b}$. Ook voor approximatie van rationale getallen $x = \frac{t}{m}$ (met $(t,m)=1$) is een dergelijke stelling af te leiden. Deze luidt als volgt.

Stelling. Zij $x = \frac{t}{m}$ met $(t,m)=1$ en n een vast gegeven getal met $0 < n \leqq m$. Dan bestaat er een onvereenvoudigbare breuk $\frac{a}{b}$ met $0 < b < n$ en $|x - \frac{a}{b}| < \frac{1}{nb}$.

Bewijs. Analoog aan de voorafgaande stelling beschouwen wij nu de n+1 getallen $\nu x = a_\nu + \vartheta_\nu$, waarbij $0 \leq \vartheta_\nu < 1$, dus $a_\nu = [\nu x]$ $(\nu = 0,1,\ldots,n)$. Geen twee getallen ϑ_h en ϑ_k met $h \neq k$ zijn gelijk; immers anders had men $(h-k)\frac{t}{m} = a_h - a_k$, dus het linkerlid was geheel. Wegens $(t,m)=1$ had men $m \mid h-k$; echter $0 < |h-k| \leq n \leq m$, hetgeen een contradictie oplevert. De n+1 getallen $\vartheta_0,\ldots,\vartheta_n$ zijn dus twee aan twee ongelijk en allen ≥ 0 en < 1, zodat er zeker twee zijn, laten wij zeggen ϑ_i en ϑ_j met $0 < \vartheta_i - \vartheta_j < \frac{1}{n}$. Dan geldt

$$(i-j)x = a_i - a_j + \frac{\vartheta}{n} \quad \text{met } 0 < \vartheta < 1,$$

waaruit evenals hierboven voor x de gewenste benadering $\frac{a}{b}$ wordt gevonden.

Van dit laatste resultaat geven wij thans een zeer belangrijke toepassing. Wij nemen nl. voor m een deler van het getal t^2+1 (dus zeker $(m,t)=1$) en $n = [\sqrt{m}] + 1$, dus zeker $n \leq m$.

Opgave 2. Ga dat na.

Er bestaat dan dus een getal $\frac{a}{b}$ met $(a,b)=1$ en $\left|\frac{t}{m} - \frac{a}{b}\right| < \frac{1}{nb}$, d.w.z. het getal $c = |bt-am|$ voldoet aan $c < \frac{m}{n} < \sqrt{m}$. Nu heeft men $b < n \leq [\sqrt{m}] + 1$, dus $b \leq [\sqrt{m}]$ en $b^2+c^2 < 2m$. Verder is $b^2+c^2 \equiv b^2+b^2t^2 = b^2(1+t^2) \pmod m$, dus $m \mid b^2+c^2$; derhalve $b^2+c^2 = m$. Wij vinden dus:
Als $m \mid t^2+1$ dan bestaan er natuurlijke getallen b en c met $b^2+c^2=m$, $c \equiv bt \pmod m$. Er bestaat trouwens maar één zo'n stel getallen. Was nl. B en C nog zo'n stel dan had men

$$m^2 = (b^2+c^2)(B^2+C^2) = (bB+cC)^2 + (bC-cB)^2.$$

Nu is $bC \equiv bBt \equiv Bc \pmod m$, dus $m^2 \mid (bC-cB)^2$. Wegens $(bB+cC)^2 \geq 1$ geldt dan $(bC-cB)^2 = 0$, dus $bC = cB$. Uit $b^2+c^2 = B^2+C^2$ vindt men tenslotte $b=B, c=C$. Omgekeerd, als b en c gegeven zijn bestaat er precies één stel natuurlijke getallen m en t met $m = b^2+c^2$ en $c \equiv bt \pmod m$.

Opgave 3. Bewijs dit.

Er is dus een eeneenduidige toevoeging tussen de paren b,c met $(b,c)=1$ en m,t met het verband $m = b^2+c^2$, $c \equiv bt \pmod m$, d.w.z. er is een eeneenduidige toevoeging tussen de oplossingen b,c van $m = b^2+c^2$ met $(b,c)=1$ en de getallen t tussen 0 en m met $c \equiv bt \pmod m$, d.w.z. $t^2 \equiv -1 \pmod m$. Nu is dit aantal getallen t gemakkelijk te bepalen en daarmee dus ook het aantal splitsingen van $m = b^2+c^2$.

Het aantal oplossingen A(m) van $t^2 \equiv -1 \pmod m$ is een multiplicatieve functie van m (verg. blz. 20). Men heeft $A(2)=1$, $A(2^r)=0$ als $r \geq 2$. Verder $A(p^r)=2$ als $p \equiv 1 \pmod 4$ (verg.blz. 25 en 30, 31). Tenslotte $A(q^r)=0$ als $q \equiv 3 \pmod 4$ (verg.blz. 25).

Opgave 4. Bewijs de formule voor $A(2^r)$.

Dus als $m=2^r \prod_{\nu=1}^{n} p_\nu^{r_\nu} \prod_{\kappa=1}^{k} q_\kappa^{s_\kappa}$, heeft men

$p_\nu \equiv 1 \pmod 4$ $\quad q_\kappa \equiv 3 \pmod 4$

$A(m) = 0$ als $r \geqslant 2$;

$A(m) = 0$ als $r=0$ of 1 en niet alle $s_\kappa = 0$;

$A(m) = 2^n$ als $r=0$ of 1 en alle $s_\kappa = 0$.

Bijgevolg is het aantal oplossingen van $m=b^2+c^2$, waarbij (b,c) ook $\neq 1$ mag zijn, gelijk aan

$$B(m) = \sum_{d^2 \mid m} A\left(\frac{m}{d^2}\right) = \sum_{d \mid m} f(d)\, A\left(\frac{m}{d}\right),$$

waarbij $f(d)$ gedefinieerd is door

$f(d) = 0$ als d geen quadraat is;

$= 1$ als d een quadraat is.

De functie $f(d)$ is multiplicatief.

Opgave 5. Bewijs dat.

Op grond van de stelling van blz. 39 is dan ook $B(m)$ multiplicatief. Wij kunnen dan $B(m)$ gemakkelijk bepalen.

$$B(2^r) = A(2^r) + A(2^{r-2}) + \ldots + A(4) + A(1) = 1 \text{ als } r \text{ even is;}$$

$$B(2^r) = A(2^r) + A(2^{r-2}) + \ldots + A(8) + A(2) = 1 \text{ als } r \text{ oneven is.}$$

Dus steeds geldt $B(2^r) = 1$.

Verder heeft men voor $p \equiv 1 \pmod 4$

$$B(p^r) = B(p^r) + B(p^{r-2}) + \ldots + B(p^2) + B(1) = 2+2+\ldots+2+1 = r+1$$
als r even is;

$$B(p^r) = B(p^r) + B(p^{r-2}) + \ldots + B(p^3) + B(p) = 2+2+\ldots+2+2 = r+1$$
als r oneven is.

Dus steeds geldt $B(p^r) = r+1$.

Voor $q \equiv 3 \pmod 4$ ziet men direct in dat $B(q^r)$ slechts $\neq 0$ is als r even is en dan vindt men

$$B(q^r) = B(1) = 1.$$

Wij kunnen het resultaat nog iets anders schrijven door in te voeren de functie $\chi(m)$ welke multiplicatief is en voldoet aan

$\chi(m)=0$ als $2 \mid m$; $\chi(m)=-1$ als $m \equiv -1 \pmod 4$, $\chi(m)=1$ als $m \equiv 1 \pmod 4$.

Dan is $B(m) = \sum_{d \mid m} \chi(d)$. Deze formule behoeft slechts te worden geverifieerd (beide leden zijn multiplicatieve functies) voor $m=2^r$, $m=p^r$, $m=q^r$, waarbij $p \equiv +1 \pmod 4$, $q \equiv -1 \pmod 4$ is. En men heeft inderdaad

$$\sum_{s=0}^{r} \chi(2^s) = \chi(1) = 1\ ;\ \sum_{s=0}^{r} \chi(p^s) = \sum_{s=0}^{r} 1 = r+1;\ \sum_{s=0}^{r} \chi(q^s) = 1-1+1-1+\ldots$$

$= 1$ als r even is

$= 0$ als r oneven is.

De in het begin van deze paragraaf beloofde relatie die uit het hier gevonden resultaat volgt, kan nu worden afgeleid.
Beschouw de gelijkheid

$$(1+2x+2x^4+2x^9+\ldots)^2 = 1 + 4\sum_{m=1}^{\infty} B(m)x^m.$$

Opgave 6. Bewijs deze betrekking.

Deze betrekking toont ons dus en passant ook welke functie van de getallen $B(m)$ de voortbrengende functie is. Men heeft verder (verg. de theorie der Lambertreeksen, blz. 47).

$$\sum_{m=1}^{\infty} B(m)x^m = \sum_{m=1}^{\infty} \sum_{d|m} \chi(d)x^m =$$

$$= \sum_{d=1}^{\infty} \chi(d) \sum_{n=1}^{\infty} x^{nd} = \sum_{d=1}^{\infty} \chi(d)\, \frac{x^d}{1-x^d},$$

dus

$$(1+2x+2x^4+2x^9+\ldots)^2 = 1+4\left(\frac{x}{1-x} - \frac{x^3}{1-x^3} + \frac{x^5}{1-x^5} - \frac{x^7}{1-x^7} + \ldots\right).$$

Met behulp van de theorie der ϑ-functies is het mogelijk deze formule rechtstreeks te bewijzen en zo dus opnieuw de formule voor $B(m)$ te vinden. Ook met behulp van die theorie is het mogelijk om een formule af te leiden voor $(1+2x+2x^4+2x^9+\ldots)^4$ en daaruit het aantal manieren $C(m)$ te bepalen waarop een natuurlijk getal m te schrijven is als som van 4 quadraten. Daarbij blijkt het dan dat $C(m) \geqslant 1$ voor alle m, d.w.z. dat elk natuurlijk getal als som van vier quadraten is te schrijven.

Opmerking. Dat niet elk natuurlijk getal te schrijven is als som van drie quadraten blijkt uit de volgende opgave.

Opgave 7. Als $m=4^a n$, waarbij $n \equiv 7 \pmod 8$, dan is m niet te schrijven als som van drie quadraten.

Wij volstaan hier met het bewijs van de stelling dat elk natuurlijk getal te schrijven is als som van vier quadraten en laten de bepaling van het aantal manieren waarop dit kan, achterwege.

Vooraf een paar hulpeigenschappen. Als p een oneven priemgetal is en x en y elk de waarden $0,1,\ldots,\frac{1}{2}(p-1)$ doorlopen, dan zijn er onder de $p+1$ getallen x^2 en $-1-y^2$ twee die modulo p overeenstemmen. Inderdaad kennelijk zijn de $\frac{1}{2}(p+1)$ getallen x^2 onderling incongruent en evenzo de $\frac{1}{2}(p+1)$ getallen $-1-y^2$. Daar er slechts p verschillende restklassen mod p

zijn moeten er een x en y zijn met $x^2 \equiv -1-y^2 \pmod p$, dus ook met $x^2+y^2+1 \equiv 0 \pmod p$.

Verder vermelden wij een identiteit die reeds door Euler is gegeven. Deze luidt

$$(1) \qquad (x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = z_1^2+z_2^2+z_3^2+z_4^2 ,$$

waarbij

$$(2) \qquad \begin{cases} z_1 = x_1y_1+x_2y_2+x_3y_3+x_4y_4 \; ; \; z_2 = x_1y_2-x_2y_1+x_3y_4-x_4y_3 \; ; \\ z_3 = x_1y_3-x_3y_1+x_2y_4-x_4y_2 \; ; \; z_4 = x_1y_4-x_4y_1+x_2x_3-x_3y_2 \; . \end{cases}$$

Het bewijs is te geven door uitcijferen of met behulp van de theorie der quaternionen.

Opgave 8. Bewijs de identiteit.

Om nu de stelling over de splitsing in vier quadraten te geven, is het wegens (1) voldoende haar voor de splitsing van een priemgetal af te leiden. Zij p een oneven priemgetal. Wegens de eerste hulpeigenschap bestaan er dan natuurlijke getallen x en y met $p \mid x^2+y^2+1$. Er bestaat dus een veelvoud hp van p dat de som is van vier (zelfs van drie!) quadraten. Daar men mag onderstellen dat $0 \leq x, \; y \leq \frac{1}{2}(p-1)$ geldt zelfs $h < \frac{1}{2}p$. Laat thans mp het kleinste positieve veelvoud van p zijn dat de som is van vier quadraten. Dan heeft men $mp=x_1^2+x_2^2+x_3^2+x_4^2$ en verder zeker $m < \frac{1}{2}p$. Kies nu de getallen y_i zo dat $y_i \equiv x_i \pmod m$ en $|y_i| \leq \frac{1}{2}m$ $(i=1,2,3,4)$. Dan geldt $y_1^2+y_2^2+y_3^2+y_4^2 \equiv x_1^2+x_2^2+x_3^2+x_4^2 \equiv 0 \pmod m$, dus $y_1^2+y_2^2+y_3^2+y_4^2=mn$. Op grond van de grootte der getallen y_i heeft men $0 \leq n \leq m$. Wij onderscheiden thans de drie gevallen $n=m$, $0 < n < m$, $n=0$.

In het eerste geval is het wegens $y_1^2+y_2^2+y_3^2+y_4^2=m^2$ en $|y_i| \leq \frac{1}{2}m$ direct duidelijk dat $y_1=y_2=y_3=y_4=\frac{1}{2}m$, dus m is even en $mp=x_1^2+x_2^2+x_3^2+x_4^2$ ook. Er is dan een x_j $(j=2,3,4)$ met $x_1 \equiv x_j \pmod 2$ en de overige twee x' en hebben dan ook dezelfde pariteit. Zonder de algemeenheid te schaden mogen wij aannemen dat $j=2$ is. Dan heeft men

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

in strijd met de minimaliteitsdefinitie van m. Dit geval treedt dus niet op.

In het tweede geval heeft men $0 < n < m$. Dan geldt wegens (1)

$$m^2np = mn.mp = \Sigma x_i^2 \,.\, \Sigma y_i^2 = \Sigma z_i^2 .$$

De relaties (2) leren hier

$$z_1 = x_1y_1+x_2y_2+x_3y_3+x_4y_4 \equiv \Sigma x_i^2 \equiv 0 \pmod m;$$
$$z_2 = x_1y_2-x_2y_1+x_3y_4-x_4y_3 \equiv 0 \pmod m$$

en evenzo $z_3 \equiv z_4 \equiv 0 \pmod m$. Dus

$$np = \sum (z_i/m)^2,$$

en dit is wegens $n<m$ weer in strijd met de minimaliteitsdefinitie van m. Ook dit geval treedt dus niet op.

Het enig mogelijke geval is dan het derde, waarbij $n=0$, zodat alle $y_i=0$ zijn en m dus deelbaar is op alle x_i. Maar dan is m^2 deelbaar op $\sum x_i^2 = mp$, dus $m|p$, dus wegens $m<p$ vindt men $m=1$. Q.e.d.

§9. Recurrente rijen. Toets van Lucas.

Wij beschouwen een getallenrij $w_0, w_1, \ldots$ gedefinieerd door haar eerste twee elementen w_0 en w_1 en door de recurrentie relatie

$$w_{n+2} = a\, w_{n+1} + b\, w_n \qquad (n = 0,1,\ldots),$$

waarbij a en b vaste gegeven getallen zijn. Allereerst vragen wij ons af of voor w_n als functie van n een expliciete formule te geven is. Dit kan onder meer door gebruik te maken van de theorie der differentievergelijkingen. Wij vonden dat w_n de gedaante heeft

$$w_n = \omega_1 \alpha^n + \omega_2 \beta^n,$$

waarbij ω_1 en ω_2 willekeurige periodieke functies zijn met periode 1 en α en β de nulpunten van de veelterm $f(x)=x^2-ax-b$, welke de karakteristieke veelterm van de rij wordt genoemd. Voor $n=0$ en 1 vindt men resp.

$$w_0 = \omega_1 + \omega_2, \quad w_1 = \omega_1 \alpha + \omega_2 \beta,$$

dus

$$\omega_1 = \frac{\beta w_0 - w_1}{\beta - \alpha}, \qquad \omega_2 = \frac{\alpha w_0 - w_1}{\alpha - \beta}$$

derhalve

(1) $$w_n = \frac{(w_1 - \beta w_0)\alpha^n + (\alpha w_0 - w_1)\beta^n}{\alpha - \beta}.$$

Door volledige inductie is deze formule ook rechtstreeks te bewijzen zonder gebruik te maken van de theorie der differentievergelijkingen.
In het bijzonder vindt men bij $w_0=0$, $w_1=1$ (de rij dan aanduidende met $u_0, u_1, \ldots$) de relatie

(2) $$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Dat men voor w_n en u_n een symmetrische functie van α en β moet vinden, is evident. De gevonden formules zijn het dan ook. Een nog meer elementair symmetrische functie is de functie $v_n = \alpha^n + \beta^n$. Kennelijk voldoet

deze rij ook aan de oorspronkelijke recurrente betrekking en verder aan $v_o=2$, $v_1=\alpha+\beta=a$. Direct duidelijk zijn de formules

(3) $$u_{2n}=u_n v_n;\quad v_{2n}=v_n^2-2(-b)^n;$$

(4) $$u_{2n+1}=u_n v_{n+1}-(-b)^n=u_{n+1}\,v_n+(-b)^n=\tfrac{1}{2}(u_n\,v_{n+1}+u_{n+1}\,v_n)$$

en

(5) $$v_{2n+1}=v_n\,v_{n+1}-a(-b)^n=Du_n\,u_{n+1}+a(-b)^n;$$

(6) $$w_n=w_1u_n+b\,w_o\,u_{n-1};\quad v_n=b\,u_{n-1}+u_{n+1};$$

(7) $$v_n^2-Du_n^2=4(-b)^n;$$

(8) $$2u_{n+m}=u_nv_m+u_mv_n;$$

en

(9) $$2v_{n+m}=Du_nu_m+v_nv_m,$$

waarbij $D=(\alpha-\beta)^2=a^2+4b$ de discriminant is van de karakteristieke veelterm $f(x)$. Men kan doorgaan met het afleiden van tal van dergelijke formules welke allen gemakkelijk door volledige inductie naar n zijn aan te tonen. Als enige verdere formule noemen wij hier nog

(10) $$\alpha^n=u_n\alpha+bu_{n-1},\quad \beta^n=u_n\beta+bu_{n-1}\,.$$

(11) $$u_n\mid u_m \text{ als } n\mid m;\quad v_n\mid v_m \text{ als } 2\nmid n\mid m.$$

Ten aanzien van formule (10) valt nog op te merken, dat ieder polynoom $g(\alpha)$ in α (resp. β) wegens het feit dat α (resp. β) voldoet aan de quadratische relatie $f(x)=0$ op ondubbelzinnige wijze te schrijven is als lineaire uitdrukking in α (resp. β). Formule (10) geeft de beide coëfficiënten indien $g(x)=x^n$ wordt genomen. Een volkomen aequivalente formulering is

$$x^n\equiv u_nx+bu_{n-1}\pmod{f(x)}.$$

In het geval dat α irrationaal is, is trouwens één der relaties (10) reeds aequivalent met de hier gegeven congruentie. Zijn echter α en β rationaal, dan is pas het tweetal relaties (10) aequivalent met deze congruentie.

In het vervolg is het van belang om deelbaarheidsrelaties van de elementen der beschouwde rijen te onderzoeken. Op grond van (10) is elk polynoom in α (resp. β) terug te brengen op een eerste graads polynoom. Wij definieren nu voor dergelijke polynomen dat

$$r\alpha+s\equiv 0\pmod m,\qquad r\beta+s\equiv 0\pmod m$$

aequivalent is met $r \equiv s \equiv 0 \pmod m$. Zo ziet men bv. dat $\alpha^n \equiv \beta^n \equiv 1 \pmod m$ aequivalent is met

$$u_n \equiv 0 \pmod m, bu_{n-1} \equiv 1 \pmod m$$

ofwel met

$$u_n \equiv 0 \pmod m, \; u_{n+1} \equiv 1 \pmod m.$$

In verband met het bovenstaande zullen wij dit zo nodig ook aangeven met

$$x^n \equiv 1 \pmod{f(x), m}$$

en in het algemeen zij voor een willekeurig polynoom $g(x)$

$$g(x) \equiv 0 \pmod{f(x), m}$$

aequivalent met $g(\alpha) \equiv g(\beta) \equiv 0 \pmod m$ in de zo juist aangegeven zin.

Thans maken wij de veronderstelling dat w_0, w_1, a en b gehele getallen zijn, zodat dat ook het geval is met elk der getallen w_n, u_n en v_n.

Ons interesseert nu het gedrag mod m (waarbij m een willekeurig natuurlijk getal is) van de rij u_n.

Daar ieder element van de rij w_n is bepaald door zijn naaste twee voorgangers volgt uit

(12) $$w_k \equiv w_{k+C} \pmod m \text{ en } w_{k+1} \equiv w_{k+C+1} \pmod m .$$

dat $w_{k+2} \equiv w_{k+C+2} \pmod m$ enz. dus i.h.a. $w_{k+n} \equiv w_{k+C+n} \pmod m$.
Het getal C is dus een periode van de rij w_n zodra er een k is waarvoor (12) geldt. Om die k op te sporen beschouwen wij de rij paren

$$(w_0, w_1), (w_1, w_2), (w_2, w_3), \ldots$$

Het is duidelijk, dat het aantal der mogelijke mod m verschillende paren ten hoogste m^2 is, zodat er dus een $C \leq m^2$ moet bestaan waarvoor (12) geldt. Het kleinste positieve dergelijke getal C zullen wij de periode mod m der rij noemen en aanduiden met C(m) of soms kortweg met C. Op de gebruikelijke wijze toont men aan dat ieder veelvoud van C(m) ook een periode mod m is van de rij en omgekeerd dat iedere periode mod m van de rij een veelvoud is van C(m).

Opgave 1. Ga dat na.

Verder is het ook duidelijk dat voor m|M geldt C(m) | C(M) en dat als (m,M) = 1 het getal C(mM) het kleinste gemene veelvoud is van C(m) en C(M). Om dus C(m) te bepalen is het voldoende om dit te doen voor het geval dat m de gedaante p^r bezit.

Waar wij gecompliceerde uitzonderingen wensen te vermijden zullen wij slechts getallen m beschouwen die relatief priem zijn met b. Uit

$$w_k \equiv w_{k+C} \pmod m, \quad w_{k+1} \equiv w_{k+C+1} \pmod m$$

volgt dan ook (voor $k \geq 1$)

$$w_{k-1} \equiv (w_{k+1} - aw_k)b^{-1} \equiv (w_{k+C+1} - aw_{k+C})b^{-1} \equiv w_{k+C-1} \pmod m,$$

zodat C tevens het kleinste natuurlijke getal is met

$$w_C \equiv w_o \pmod m, \quad w_{C+1} \equiv w_1 \pmod m.$$

Het volgende onderzoek beperkt zich nu tot periodiciteit mod m van de rij u_n. Het getal $C = C(m)$ is nu het kleinste natuurlijke getal waarvoor geldt

$$u_C \equiv 0 \pmod m, \quad u_{C+1} \equiv 1 \pmod m.$$

Bij deze rij valt nog iets interessants op te merken. Er kunnen nl. reeds elementen u_h deelbaar zijn door m, waarvoor $0 < h < C$. Zij $c = c(m)$ het kleinste natuurlijke getal met $m \mid u_c$. Kennelijk is dan voor elk veelvoud kc van c ook u_{kc} deelbaar door m. Omgekeerd zij $u_d \equiv 0 \pmod m$. Stel $d = qc + r$ met $0 \leq r \leq c$. Dan geldt

$$bu_{d-1} \equiv \alpha^d = \alpha^{qc+r} \equiv (bu_c)^q (u_r\alpha + bu_{r-1}) \pmod m,$$

dus wegens $(m,b)=1$ en $(m,u_c) = 1$ (waarom?) vindt men (aangezien deze relatie ook juist is als α door β wordt vervangen) dat $m \mid u_r$, dus $r=0$ en $c \mid d$. Dit leert ons in het bijzonder dat $c \mid C$. Het quotiënt zullen wij met v aanduiden, of om aan te geven dat v afhangt van m, met $v(m)$.

Verder heeft men nog $\alpha^c \equiv bu_{c-1} \equiv u_{c+1} \pmod m$,

dus $1 \equiv \alpha^C = \alpha^{vc} \equiv u_{c+1}^v \pmod m$,

zoodat $v \mid d$, waarbij d de exponent is van u_{c+1} mod m. Ook geldt

$$1 \equiv u_{c+1}^d \equiv \alpha^{dc} \pmod m,$$

dus $dc \mid C$, dwz. $d \mid v$. Uit deze resultaten volgt dat $v = v(m)$ gelijk is aan de exponent d van u_{c+1} mod m.

Van belang is voorts het resultaat

$$u_{c+1}^2 \equiv \alpha^c \beta^c = (-b)^c \pmod m,$$

dus als e de exponent is van -b mod m

$$u_{c+1}^{2e/(e,c)} \equiv (-b)^{2ec/(e,c)} \equiv 1 \pmod m,$$

dus $v \mid 2e/(e,c)$. En ten slotte heeft men

$$(-b)^{vc} = \alpha^{vc}\beta^{vc} \equiv 1 \pmod m, \text{ dus } e \mid vc.$$ Wegens $c \mid vc$ heeft men dan

$$ec/(e,c) \mid vc, \text{ dus } e/(e,c) \mid v$$

en na samenvatting der resultaten:

$$e/(e,c) \mid v \mid 2e/(e,c).$$

Wij kunnen de resultaten nog zo samenvatten, dat C het kleinste natuurlijke getal is waarvoor $\alpha^C \equiv \beta^C \equiv 1 \pmod m$ is en c het kleinste natuurlijke getal is waarvoor $\alpha^c \equiv \beta^c \pmod m$ is.

Opgave 2. Ga dat na.

Door elementaire beschouwingen ziet men gemakkelijk in dat C(mn) het K.G.V. is van C(m) en C(n) en ook dat c(mn) het K.G.V. is van c(m) en c(n). Het is dus voldoende om formules voor $C(p^r)$ en $c(p^r)$, waarbij p een priemgetal voorstelt, af te leiden.

Zij allereerst $(\frac{D}{p})=1$, hetgeen volgens Euler inhoudt $D^{\frac{1}{2}(p-1)} \equiv 1 \pmod p$. Nu geldt

$$4f(x) = 4x^2-4ax-4b = (2x-a)^2-D,$$

dus

$$(2x-a)^2 \equiv D \pmod{f(x)}$$

en

$$2^p x^p - a^p \equiv (2x-a)^p \equiv (2x-a)(2x-a)^{p-1} \equiv (2x-a)D^{\frac{1}{2}(p-1)} \equiv 2x-a \pmod{f(x),p}.$$

Dus

$$2x^p - a \equiv 2x-a \pmod{f(x),p}$$

en omdat $p \neq 2$

$$x^p \equiv x \pmod{f(x),p},$$

d.w.z.

$$x^{p-1} \equiv 1 \pmod{f(x),p}.$$

De laatste overgang wordt bereikt door beide leden te vermenigvuldigen met de inverse x^{-1} van x mod f(x), waarvoor men neme $(x-a)b^{-1} \pmod p$. Uiteindelijk heeft men dan

$$u_{p-1} \equiv 0 \pmod p, \quad u_p \equiv 1 \pmod p,$$

dus

$$C(p) \mid p-1.$$

Is vervolgens $(\frac{D}{p}) = -1$, d.w.z. volgens Euler $D^{\frac{1}{2}(p-1)} \equiv -1 \pmod p$, dan vindt men

$$2x^p-a \equiv 2^p x^p - a^p \equiv (2x-a)^p \equiv -(2x-a) = a-2x \pmod{f(x),p},$$

dus

$$2x^{p+1} \equiv 2ax-2x^2 \equiv -2b \pmod{f(x),p}$$

en

(13) $$x^{p+1} \equiv -b \text{ (modd } f(x),p).$$

Hieruit volgt

(14) $c(p) \mid p+1$ en, als $b \neq -1$, $C(p) \nmid p+1$.

Verder

$$x^{p^2-1} \equiv (-b)^{p-1} \equiv 1 \text{ (modd } f(x),p),$$

dus

$$C(p) \mid p^2-1.$$

In het exceptionele geval dat $(\frac{D}{p})=0$, d.w.z. $p \mid D$, heeft men $4f(x) = (2x-a)^2-D \equiv (2x-a)^2 \pmod p$,

dus

$$(2x-a)^p \equiv 0 \text{ (modd } f(x),p)$$

en

$$2x^p \equiv a \text{ (modd } f(x),p),$$

waaruit volgt $c(p) \mid p$ en dus $c(p)=p$ en verder $C(p)=p$ slechts als $a \equiv 2 \pmod p$. Ook als $p \nmid a-2$ heeft men in ieder geval

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

en

$$C(p) \mid p(p-1).$$

Wij geven nog in principe aan hoe men perioden mod p^r bepaalt. Zij bv. $C=C(p^r)$ bekend, dan heeft men

$$x^C \equiv 1 \text{ (modd } f(x),p^r),$$

d.w.z. er bestaan polynomen s en t met

$$x^C = 1 + s\, f(x) + t\, p^r.$$

Dus mits weer $p \neq 2$,

$$x^{pC} = (1+s\, f(x) + tp^r)^p \equiv (1+tp^r)^p \equiv 1 \text{ (modd } f(x),p^{r+1})$$

en

$$C(p^{r+1}) \mid p\, C(p^r).$$

Analoog is af te leiden dat $c(p^{r+1}) \mid p\, c(p^r)$. Bijgevolg geldt $C(p^{r+1})=C(p^r)$ of $pC(p^r)$ en een analoog resultaat voor $c(p^{r+1})$. In ieder geval is dus bij $(\frac{D}{p})=1$ zeker $C(p^r) \mid p^{r-1}(p-1)$, bij $(\frac{D}{p})=-1$ zeker $C(p^r) \mid p^{r-1}(p^2-1)$ en bij $(\frac{D}{p})=0$ zeker $C(p^r) \mid p^r(p-1)$.
Er bestaan gevallen waarbij $C(p^r)$ minder dan r factoren p bevat. Een nader onderzoek is in te stellen op analoge wijze als op blz. 34. Waar die resultaten hier niet verder nodig zijn, laten wij dat achterwege.

Wij passen het gevondene toe op de rij van Fibonacci, waarbij $f(x)=x^2-x-1$. Hier heeft men $D=5$.
Als $p \equiv \pm 1 \pmod{10}$, dan is $(\frac{D}{p})=1$, dus $c(p) \mid C(p) \mid p-1$.

Als $p \equiv \pm 3 \pmod{10}$, dan is $(\frac{D}{p}) = -1$, dus wegens (14) heeft men $c(p) \mid p+1$ en verder $x^{p+1} \equiv -1 \pmod{p}$, dus $x^{2(p+1)} \equiv 1 \pmod{p}$ en $C(p) \nmid p+1$, $C(p) \mid 2(p+1)$. Tenslotte heeft men voor $p=5$ de relaties $c(5)=5$, $C(5)=20$. Voor $p=2$ is direct te verifiëren dat $c(2)=C(2)=3$.

Wij willen nog één opmerking maken over het getal $v=v(m)$. Wij vonden voor $v=v(m)$ de relaties $e/(e,c) \mid v \mid 2e/(e,c)$. Omdat hier geldt $e=2$ vindt men direct $v \mid 4$, dus $v=1,2$ of 4. Het geval $v=1$ is uitgesloten als c even is. Het is niet moeilijk na te gaan wanneer elk der drie hier gevonden mogelijkheden optreedt. Waar wij dit voor het vervolg niet nodig hebben, laten wij het achterwege.

De gevonden resultaten maken het soms eenvoudig om de ontbinding der getallen u_n te bepalen. Men heeft voor $p \mid n$ wegens (11) de relatie $u_p \mid u_n$. Men kan zich nu afvragen als $n = p_1^{r_1} \ldots p_s^{r_s}$ is, welke factoren u_n verder bezit dan die die reeds op een der getallen u_m met $m \mid n$, $m < n$ deelbaar zijn. Zij p zo'n priemfactor. Dan heeft men $c(p) \mid n$, $c(p) \nmid h$ met $0 < h < n$. Dus $c(p) = n$. Bijgevolg $n \mid p \pm 1$ (mits $(n,D)=1$, is dit niet zo dan onderzoeke men eerst de priemdelers van D op deelbaarheid op u_n); en $p \equiv \pm 1 \pmod{n}$.

Voorbeeld. u_{29}. Men probere priemgetallen $p \equiv \pm 1 \pmod{29}$ en wel: als $p \equiv \pm 1 \pmod{10}$, dan $29 \mid p-1$, dus $p \equiv 1$ of $231 \pmod{290}$; als $p \equiv \pm 3 \pmod{10}$, dan $29 \mid p+1$, dus $p \equiv 117$ of $233 \pmod{290}$. Wegens $u_{29} = 514229$ behoeft men slechts te onderzoeken de getallen p met $p < \sqrt{514229} = 717$ en stelt na een kort onderzoek vast dat u_{29} priem is.

Opgave 3. Ontbind $u_{31} = 1346269$ en $u_{36} = 14930352$.

Het is ons thans mogelijk om aan te geven hoe men - naar een idee van Lucas uit 1879 - tegenwoordig getallen van Mersenne onderzoekt op primaliteit, daarbij gebruik makende van moderne rekenmachines.

Laat $m = 2^p - 1$ het te onderzoeken getal van Mersenne zijn. Met behulp van de rij van Fibonacci verloopt het onderzoek alleen voor de gevallen, dat $m \equiv \pm 3 \pmod{10}$ is, d.w.z. dat $p \equiv 3 \pmod{4}$ is.

Opgave 4. Bewijs dat.

In de andere gevallen dient men een andere rij te nemen dan de rij van Fibonacci. Wij gaan hier nu verder met het onderzoek voor dit geval. Uit $m \equiv \pm 3 \pmod{10}$ volgt wegens (13) dat, als m priem is, geldt

$$x^{2^p} \equiv -1 \pmod{f(x), m},$$

dus $x^{2^{p-1}} + x^{-2^{p-1}} \equiv 0 \pmod{f(x), m}$, d.w.z.

$$m \mid \alpha^{2^{p-1}} + \alpha^{-2^{p-1}} = \alpha^{2^{p-1}} + \beta^{2^{p-1}} = v_{2^{p-1}}.$$

Wij laten nu omgekeerd zien, dat als $m = 2^p - 1 \equiv \pm 3 \pmod{10}$ is en deelbaar is op $v_{2^{p-1}}$, dan m noodzakelijkerwijze ondeelbaar is.

Immers zij $m \mid v_{2^{p-1}}$. Dan geldt wegens (3) ook $m \mid u_{2^p}$, $m \nmid u_{2^{p-1}}$. Dus $c(m) \mid 2^p$, $c(m) \nmid 2^{p-1}$, d.w.z. $c(m)=2^p$. Zij nu $m=p_1^{r_1}\ldots p_s^{r_s}$. Dan is $c(m)=2^p$. Zij nu $m=p_1^{r_1}\ldots p_s^{r_s}$. Dan is $c(m)$ een deler van het KGV der getallen $p_1^{r_1-1}(p_1 \pm 1),\ldots,p_s^{r_s-1}(p_s \pm 1)$, (waarbij de tekens worden gekozen al naar het karakter mod 10 der priemfactoren van m). Dus is dan $c(m)=2^p=m+1$ deelbaar op dit KGV dat ten hoogste gelijk is aan $\frac{1}{2^{s-1}}$ maal hun product, dus

$$m+1 \leq \frac{m}{2^{s-1}} \prod_{\sigma=1}^{s} \frac{p_\sigma \pm 1}{p_\sigma} .$$

Is $s \geq 2$ dan is het laatste product wegens $p_1 \geq 3$, $p_2 \geq 5$,... ten hoogste gelijk aan $\frac{4}{3} \cdot (\frac{6}{5})^{s-1} < 2^{s-2}$ en men vindt de contradictie $m+1 \leq \frac{1}{2}m$. Dus $s=1$ en $m=2^p-1=q^r$. Dus $2^p=m+1=c(m) \mid q^{r-1}(q \pm 1) = \frac{q \pm 1}{q}(2^p-1)$, d.w.z. $\frac{2^p}{2^p-1} = \frac{q \pm 1}{q}$. Hieruit volgt direct $2^p-1=q$, dus $r=1$ en ook nog $c(m) \mid m+1$. Het getal $m=2^p-1$ is dus een priemgetal en het is bovendien van de gedaante $\pm 3 \pmod{10}$.

Om het onderzoek daadwerkelijk uit te voeren moet men het getal $v_{2^{p-1}}$ mod m bepalen. Dit geschiedt het eenvoudigste door gebruik te maken van de relatie (3) welke luidde $v_{2n}=v_n^2-2$. Men heeft

$$v_1=1,\ v_2=3,\ v_4=7,\ v_8=47,\ v_{16}=2207,\ldots \quad \text{(1e rij van Lucas)}.$$

Als dus het $p-1^e$ element van deze rij deelbaar is door 2^p-1, is 2^p-1 priem.
Wij laten eens zien hoe de methode werkt bij het aantonen van de ondeelbaarheid van $m=127=2^7-1$. Men heeft in het tweetallige stelsel rekenende (niet wat de indices betreft!)

$$v_8 = 101111;\ v_{16} = 101111^2 - 10 \equiv 110000;\ v_{32} \equiv 10000;\ v_{64} \equiv 0;$$

dus 127 is ondeelbaar.

Op analoge wijze is het grootste in 1954 bekende priemgetal $2^{2281}-1$ gevonden.

Voor getallen m van de gedaante $m \equiv 1 \pmod 4$ dient men zich, zoals al werd opgemerkt, te bedienen van een andere rij. Hier is een tweede rij van Lucas bruikbaar, welke weliswaar de eigenschap $v_{2n}=v_n^2-2$ bezit, maar een andere v_1 heeft. Deze luidt

$$v_1 = 2,\ v_2 = 4,\ v_4 = 14,\ v_8 = 194,\text{---}$$

De methode is gegeneraliseerd om ook te kunnen worden toegepast bij het onderzoek van getallen $r.2^s \pm 1$ bij bepaalde r en s.

Nog één opmerking willen wij maken over de rij van Fibonacci. Men heeft voor alle priemgetallen p de relatie $v_p \equiv 1 \pmod p$. Immers als $(\frac{D}{p})=1$ is, heeft men $x^{p-1} \equiv 1 \pmod{f(x),p}$, d.w.z. $\alpha^p \equiv \alpha \pmod p$, $\beta^p \equiv \beta \pmod p$, dus $v_p = \alpha^p + \beta^p \equiv \alpha + \beta = 1 \pmod p$. Voor $(\frac{D}{p}) = -1$ vonden wij $x^{p+1} \equiv -1 \pmod{f(x),p}$, d.w.z. $\alpha^p \equiv -\frac{1}{\alpha} = \beta \pmod p$, $\beta^p \equiv \alpha \pmod p$, dus $v_p = \alpha^p + \beta^p \equiv \beta + \alpha = 1 \pmod p$. Is tenslotte $(\frac{D}{p})=0$, dan is p=5 en inderdaad geldt $v_5 \equiv 1 \pmod 5$. Omgekeerd heeft van der Poel zich afgevraagd of (analoog aan hetgeen bij de omkering der stelling van Fermat is gedaan door o.a. Poulet) deze eigenschap karakteriserend is voor priemgetallen. Helaas blijkt dat ook hier niet zo te zijn. Men kan zelfs bewijzen dat er oneindig veel samengestelde getallen m zijn met $v_m \equiv 1 \pmod m$. Een tabel van al deze $m \leq 555200$ is onlangs geconstrueerd *).

§10 Over het vermoeden van Fermat

De wiskundige Fermat heeft in een brief medegedeeld een bewijs te kennen van de stelling dat de relatie

(1) $$x^n + y^n = z^n$$

voor natuurlijke x,y,z en n(met $n \geq 3$) onoplosbaar is. De ruimte in de marge van zijn schrijven was echter onvoldoende om dit bewijs neer te schrijven.

Tot dusverre is men er niet in geslaagd om zijn bewering aan te tonen dan wel te weerleggen. Hoewel men thans het verkrijgen van uitsluitsel hierover meer uit sportief dan uit mathematisch oogpunt van belang acht, heeft het vele weliswaar vruchteloze zoeken hiernaar van tal van mathematici toch zeer zeker zijn goede zijde gehad: al zoekende werden belangrijke nieuwe delen der wiskunde ontwikkeld. Met name valt hier de van Kummer afkomstige ideaaltheorie te noemen.

Wij zullen ons hier niet bezig houden met het vermelden van het vele dat wel aangaande het vermoeden van Fermat is gevonden, evenmin met het vermelden van relaties die bij de lezers de (naar wij hopen niet-) valse hoop kunnen opwekken dat het hun hiermede mogelijk zal zijn om datgene over dit probleem te kunnen doen, dat niemand voordien presteerde. Wij bepalen ons hier tot enkele resultaten en methoden, waardoor men enige indruk krijgt van hetgeen in verband met dit probleem is geprobeerd en bereikt.

Het geval n=1 mogen wij gevoegelijk buiten beschouwing laten.

Voor n=2 geven wij alle oplossingen van het probleem in parametervorm. Men heeft dan nl $\frac{z+y}{x} = \frac{x}{z-y}$. Stelt men elk dezer rationale uitdruk-

---

*) Verg. H.J.A. Duparc, On second order almost-primes, Rapport Math. Centrum ZW 1955-013, 1-13.

kingen gelijk aan $\frac{u}{v}$ met $(u,v)=1$, dan volgt uit

$$ux-vy-vz=0,\quad vx+uy-uz=0,$$

dat x,y en z zich moeten verhouden als $2uv$, u^2-v^2, u^2+v^2, waarmede het probleem is opgelost.

Opgave 1. Laat zien dat uit het gevondene niet noodzakelijk volgt dat x even is.

Wij beschouwen thans het geval $n=4$ en tonen aan dat er dan geen oplossing van (1) bestaat. Wij tonen iets meer aan, nl. dat zelfs de relatie $x^4+y^4=z^2$ geen natuurlijke oplossingen bezit. De hierbij gebruikte methode der descente infinie is van Fermat afkomstig.

Wij stellen dat er wel een oplossing bestond. Dan bestond er ook een kleinste, d.w.z. er is een getal z met

$$z^2=x^4+y^4 \text{ en } u^2\neq v^4+w^4 \text{ voor } 0<u<z.$$

Tevens moeten dan z,x en y twee aan twee relatief priem zijn.

Opgave 2. Bewijs dit.
Op grond van het bovenstaande heeft men dan

$$x^2=2ab,\quad y^2=a^2-b^2,\quad z=a^2+b^2,$$

waarbij a en b natuurlijke getallen zijn met $(a,b)=1$.

Opgave 3. Bewijs de laatste relatie.

Lettende op het karakter mod 4 volgt uit $y^2=a^2-b^2$ en uit het feit dat y oneven is (want x is even) dat a oneven is en b even.

Opgave 4. Bewijs dat.

Stellen wij dan $b=2c$, dan vindt men $x^2=4ac$ en omdat $(a,b)=1$, dus $(a,c)=1$ vindt men dat $a=d^2$, $c=e^2$. Dus $y^2=d^4-4e^4$.

Verder kunnen wij hieruit concluderen dat er gehele getallen g en h met $(g,h)=1$ bestaan, zodanig dat

$$2e^2=2gh,\quad y=g^2-h^2,\quad d^2=g^2+h^2.$$

Wegens $e^2=gh$ en $(g,h)=1$ heeft men $g=k^2$, $h=m^2$, dus $d^2=k^4+m^4$. Uit $d^2=a<a^2<z<z^2$ blijkt dat er een quadraat d^2 zou bestaan dat kleiner is dan z^2 en eveneens de som is van twee vierde machten. Hiermee is een contradictie gevonden.

Uit de gegeven beschouwingen volgt dat de onvervulbaarheid van (1) nu nog "slechts" voor priemgetallen n behoeft te worden onderzocht.

Opgave 5. Ga dat na.

Wij maken thans enige opmerkingen over het geval $n=3$. Zijdelings in verband met de stelling van Fermat staat het

Theorema van Richmond (1923).
Ieder rationaal getal $r\neq 0$ is te schrijven als som van drie derde machten van rationale getallen.

Bewijs: Zonder de algemeenheid te schaden mag men $r>0$ onderstellen. Wij proberen dus rationale u,v en w te vinden met

$$r = u^3+v^3+w^3.$$

Stel $u = \frac{x-y}{t}$, $v = \frac{y-z}{t}$, $w = \frac{z}{t}$, dus

$$t^3r=(x-y)^3+(y-z)^3+z^3 = 3y^2(x-z)+(x^3-3y(x^2-z^2)).$$

Wij zullen niet de meest algemene oplossing (u,v,w) bepalen maar slechts speciale. Dan kunnen wij aan u,v en w, dus aan x,y en z nog een verdere voorwaarde opleggen. Die zal luiden $x^3=3y(x^2-z^2)$, zodat dan $y = \frac{x^3}{3(x^2-z^2)}$, terwijl dan $t^3r=3y^2(x-z)$, dus

$$t^3r = \frac{x^6}{3(x+z)^2(x-z)},$$

dus

$$3r = \left(\frac{x^2}{(x+z)t}\right)^3 \cdot \frac{x+z}{x-z}.$$

Wij kiezen nu $\frac{x+z}{x-z} = 3r$, dus $x=s(3r+1)$, $z=s(3r-1)$, waarna men vindt $t= \frac{x^2}{x+z} = s\frac{(3r+1)^2}{6r}$. Tenslotte vindt men successievelijk $y= \frac{s(3r+1)^3}{36r}$ en

$$(2)\quad u = \frac{36r-(3r+1)^2}{6(3r+1)},\quad v = \frac{(3r+1)^3-36r(3r-1)}{6(3r+1)^2},\quad w = \frac{6r(3r-1)}{(3r+1)^2}.$$

Opgave 6. Verifieer rechtstreeks dat $r=u^3+v^3+w^3$.

Men kan zich nog afvragen of u,v en $w>0$ zijn. Alvorens dit te doen merken wij op dat

$$R = a^3r=(au)^3+(av)^3+(aw)^3 = U^3+V^3+W^3,$$

waarbij

$$(3)\qquad U = au\left(\frac{R}{a^3}\right),\ V = av\left(\frac{R}{a^3}\right),\ W = aw\left(\frac{R}{a^3}\right),$$

zodat wij voor elk rationaal getal R tevens oneindig veel splitsingen vinden door a te laten variëren. Willen wij dan U,V en W positief nemen dan moet men zorgen dat $u(R/a^3)$, $v(R/a^3)$ en $w(R/a^3)$ positief zijn. Wij onderzoeken dus hoe dit wordt bereikt. Nu leidt de eis

$$u(r) > 0 \text{ tot } 9r^2-30r+1 < 0, \text{ dus } \frac{5-2\sqrt{6}}{3} < r < \frac{5+2\sqrt{6}}{3}.$$

De eis $w(r)>0$ leidt tot $r > \frac{1}{3}$, zodat wij alvast nemen $\frac{1}{3} < r < \frac{5+2\sqrt{6}}{3}$. Het onderzoek der veelterm $6(3r+1)^2v=27r^3-81r^2+45r+1$ leert ons dat v positief is voor $r<0{,}76..$ en $r>2{,}26..$, zodat wij dus oneindig veel

oplossingen (3) vinden door a zo te kiezen dat $\frac{1}{3} < \frac{R}{a^3} < 0{,}76..$ ofwel dat $2{,}26.. < \frac{R}{a^3} < \frac{5+2\sqrt{6}}{3}$ dus $1{,}09..\sqrt[3]{R} < a < 1{,}44..\sqrt[3]{R}$ ofwel $0{,}67..\sqrt[3]{R} < a < 0{,}76..\sqrt[3]{R}$. Zoals reeds is opgemerkt vinden wij hier slechts speciale splitsingen van R, nl. die waarvoor $x^3=3y(x^2-z^2)$, dus

(4) $\qquad (U+V+W)^3 = 3(W+V)(U+V+2W)(U+V).$

Opgave 7. Ga dit na.

Opgave 8. Ga na hoe men uit het gevondene ook splitsingen $R=V^3+W^3-U^3$ kan vinden met positieve U,V en W.

In het bijzonder is dus bewezen dat de Diophantische vergelijking

$$x^3+y^3+z^3-Rt^3=0$$

oneindig veel gehele oplossingen bezit. Neemt men voor r zelf een derde macht, dan levert (2) ons gehele oplossingen van

$$a^3+b^3+c^3+d^3=0,$$

bv. r=1 geeft $12^3+1^3=9^3+10^3$. De "kleinste" oplossing $3^3+4^3+5^3=6^3$ is hiermee niet te verkrijgen. Deze voldoet nl. niet aan (4).

Opgave 9. Ga dat na.

Wij keren thans terug tot het vermoeden van Fermat en geven er wat algemenere beschouwingen over.

Wij gaan enige conclusies trekken over getallen x,y,z en p (priem en oneven) waarvoor $x^p+y^p=z^p$ geldt met $(x,y)=(y,z)=(z,x)=1$.

Het linkerlid $(x+y)V(x,y)$, waarbij $V(x,y)=x^{p-1}-x^{p-2}y+\ldots+y^{p-1}$, is dus een p^e macht. Wij onderzoeken eerst of x+y en V(x,y) een factor gemeen kunnen hebben. Stel q is een gemeenschappelijke priemdeler van deze uitdrukkingen, dan vindt men $x \equiv -y \pmod q$, dus $0 \equiv V(x,y) \equiv y^{p-1}+y^{p-1}+\ldots+y^{p-1}=py^{p-1} \pmod q$. Nu geldt $q \nmid y$, want anders $q \mid x$ en $(x,y)\neq 1$. Dus de enige mogelijkheid is dat q=p is.

Een soortgelijke redenering is mogelijk voor $x^p=(z-y)V(z,-y)$ en $y^p=(z-x)V(z,-x)$, zodat er twee mogelijkheden blijken te kunnen optreden:

I. $p \nmid xyz$;

II. p is deelbaar op precies één der drie getallen x,y en z. Wij geven thans een aantal conclusies over geval I. Dan zijn x+y en V(x,y) onderling ondeelbaar en omdat hun product een p^e macht is, bestaan er gehele getallen c_1 en c_2 zodanig dat $x+y=c_1^p$, $V(x,y)=c_2^p$, $z=c_1c_2$. Evenzo heeft men $z-x=b_1^p$, $V(z,-x)=b_2^p$, $y=b_1b_2$, $z-y=a_1^p$, $V(z,-y)=a_2^p$, $x=a_1a_2$ en bijgevolg

(2) $\qquad 2x = a_1^p-b_1^p+c_1^p,\ 2y= -a_1^p+b_1^p+c_1^p,\ 2z=a_1^p+b_1^p+c_1^p.$

Thans tekijken wij enige congruentieëigenschappen. Volgens de stelling van Fermat heeft men

$$z \equiv z^p = x^p + y^p \equiv x+y \pmod{p},$$

waaruit wegens (2) volgt dat

$$a_1^p + b_1^p \equiv c_1^p \pmod{p},$$

dus alweer volgens Fermat

$$c_1 \equiv a_1 + b_1 \pmod{p}.$$

Dan leert (2) verder

$$2c_1c_2 = 2z = a_1^p + b_1^p + c_1^p \equiv a_1 + b_1 + c_1 \equiv 2c_1 \pmod{p},$$

dus $c_2 \equiv 1 \pmod{p}$ en evenzo $a_2 \equiv b_2 \equiv 1 \pmod{p}$.

Hieruit volgt nog dat $x \equiv a_1 \pmod{p}$, dus op de bekende wijze $x^p \equiv a_1^p \pmod{p^2}$. Evenzo $y^p \equiv b_1^p \pmod{p^2}$, $z^p \equiv c_1^p \pmod{p^2}$, dus

$$2x \equiv x^p - y^p + z^p = 2x^p \pmod{p^2}$$

en $x^{p-1} \equiv 1 \pmod{p^2}$. Evenzo $y^{p-1} \equiv 1 \pmod{p^2}$, $z^{p-1} \equiv 1 \pmod{p^2}$, dus ook nog

$$z \equiv z^p = x^p + y^p \equiv x+y \pmod{p^2}.$$

Wij tonen nu nog iets meer aan. Zij r een willekeurige priemdeler van a_2. Dan heeft men allereerst $r \mid x$, $r \nmid a_1$ en verder

$$c_1^p - b_1^p = 2x + y - z \equiv y - z = -a_1^p \not\equiv 0 \pmod{r}$$

terwijl

$$c_1^{p^2} - b_1^{p^2} \equiv (x+y)^p - (z-x)^p \equiv y^p - z^p = -x^p \equiv 0 \pmod{r}.$$

Dus als men $c_1 b_1^{-1} \equiv d \pmod{r}$ stelt,

$$d^p \not\equiv 1 \pmod{r}, \quad d^{p^2} \equiv 1 \pmod{r}.$$

Hieruit volgt gemakkelijk dat $r \equiv 1 \pmod{p^2}$ is. Bij gevolg voldoet iedere priemdeler r van a_2 aan de relatie $r \equiv 1 \pmod{p^2}$. In het bijzonder vindt men dan $a_2 \equiv 1 \pmod{p^2}$, dus $x \equiv a_1 \pmod{p^2}$. Evenzo $y \equiv b_1 \pmod{p^2}$, $z \equiv c_1 \pmod{p^2}$, dus $2x = a_1^p - b_1^p + c_1^p \equiv x^p - y^p + z^p = 2x^p \pmod{p^3}$, dus

$$x^{p-1} \equiv 1 \pmod{p^3}$$

en evenzo

$$y^{p-1} \equiv z^{p-1} \equiv 1 \pmod{p^3}.$$

De hier gevonden resultaten met modulus p^2 zijn nog aanzienlijk te verscherpen. Om dat te bereiken moet de ideaaltheorie worden ingeschakeld, welke theorie haar oorsprong juist aan dit probleem heeft

te danken. Kummer heeft nl bij zijn onderzoekingen over het theorema van Fermat eerst de fout begaan om te menen dat de ring, die uit de ring der gehele getallen ontstaat door adjunctie van een primitieve p^e eenheidswortel, een ontbindingsring is. Nadat hij zijn fout had onderkend probeerde hij zijn redenering te redden door idealen in te voeren met het gevolg dat wel de ideaaltheorie tot ontwikkeling kwam maar niet het theorema van Fermat werd opgelost.

Wij willen hier volstaan met het zonder bewijs vermelden van enige resultaten welke met behulp van ideaaltheorie en zekere onderdelen der zgn. algebraïsche getallentheorie kunnen worden afgeleid.

De eerste stelling van Furtwängler (1912). Uit $x^p+y^p+z^p=0$ met $(x,y)=1$ en $p \nmid x$ volgt voor iedere deler r van x de relatie

$$r^{p-1} \equiv 1 \pmod{p^2}. \tag{6}$$

Gevolg. Daar bij $x^p+y^p=z^p$ zeker een der getallen x,y en z even is vindt men dat onder de veronderstelling $p \nmid xyz$ volgt

$$2^{p-1} \equiv 1 \pmod{p^2}$$ (st.v.Wieferich en Mirimanoff).

Cunningham heeft onderzocht of er priemgetallen zijn die aan deze relatie voldoen; hij bewees dat er geen waren onder de 1000. Hij trof het evenwel niet, want Beeger bewees dat p=1093 wel voldoet (en de kleinste oplossing is) terwijl de volgende oplossing luidt p=3511. Wieferich en Mirimanoff bewezen trouwens ook nog dat p niet een der volgende gedaanten kan hebben: $2^a 3^b \pm 1$, $2^a \pm 3^b$, $3^b - 2^a$ $(a \geq 0,\ b \geq 0)$. Hieruit volgt gemakkelijk dat $p > 100$ is.

De tweede stelling van Furtwängler zegt dat uit $x^p+y^p+z^p=0$ en $p \nmid x^2-y^2$ volgt dat iedere deler r van x-y eveneens voldoet aan (6). Hieruit laat zich nog aantonen dat tevens moet gelden

$$3^{p-1} \equiv 1 \pmod{p^2}.$$

Merkwaardigerwijze blijkt hier dat reeds p=11 voldoet, maar p=1093 en p=3511 niet! Uit Beegers resultaten volgt nu in ieder geval dat $p > 3511$ moet zijn.

In 1941 bewezen H.D. en Emma Lehmer langs andere weg dat in geval I (dus $p \nmid xyz$) moet gelden $p > 253747889$.

Van Wijngaarden en Duparc bewezen hieruit en met gebruikmaking van (5) en enige elementaire ongelijkheden dat x,y en z groter moeten zijn dan $10^{6.10^9}$.

In geval II zijn de gevonden resultaten wat minder vergaand. Onderstel, zonder de algemeenheid te schaden, dat p deelbaar is op z en wel dat z precies k factoren p bezit. Uit onze elementaire overwegingen vindt men dat $(x+y, V_{xy})=p$. Heeft nu x+y juist h factoren p, dus $y = -x+n.p^h (p \nmid n)$, dan vindt men $y^p=(-x+np^h)^p \equiv -x^p+x^{p-1}np^{h+1} \pmod{p^{2h+1}}$ en y^p+x^p heeft precies h+1 factoren p. Bijgevolg bezit V(x,y) precies

één factor p en men vindt

$$x+y=p^{kp-1}c_1^p,\ V(x,y)=pc_2^p,$$

waaruit betrekkingen analoog aan die in (5) te vinden zijn. In het bijzonder vindt men ook nu op elementaire wijze dat

$$x^{p-1}\equiv y^{p-1}\equiv 1 \pmod{p^2}.$$

De stelling van Vandiver die zegt dat deze congruenties ook gelden mod p^3 is echter tot nu toe slechts met gebruikmaking van meer diepgaande hulpmiddelen bewezen.

Met rekenmachines is inmiddels geverifieerd dat in geval II het getal p groter moet zijn dan 2000.