STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZC 46

Capita selecta uit de getallentheorie.
incompl.

H.J.A. Duparc.

1958

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.

ATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM-O.

Capita Selecta uit de Getallentheorie

door

H.J.A. Duparc

Cursusjaar 1957-'58 te 's-Gravenhage

§ 1. Inleiding, grondbegrippen

Voor een belangrijk deel worden in de getallentheorie eigenschappen van gehele getallen bestudeerd. Alvorens tot deze studie over te gaan, is het nuttig om van de het meest gebruikte eigenschappen een overzicht te geven.

Zijn a en b gehele getallen, dan is dat ook het geval met a+b, a-b en ab. Het quotiënt $\frac{a}{b}$ (met $b \neq 0$) is echter niet noodzakelijkerwijze geheel. Is dit wel het geval, dan zegt men dat b deelbaar is op a; men schrijft dan $b|a$. In het vervolg worden onder getallen verstaan gehele getallen, tenzij het tegendeel wordt vermeld.

Bij willekeurige a en positieve b is het steeds mogelijk een getal q en een getal r te bepalen, zodanig dat $a=qb+r$; $0 \leq r < b$ ("delen met rest"). Is ook a positief, dan is het getal q het grootste gehele getal dat $\leq \frac{a}{b}$ is; men schrijft wel $q=\left[\frac{a}{b}\right]$.

Een natuurlijk getal heet ondeelbaar of priem, als het precies twee positieve delers bezit (nl. 1 en zichzelf). Niet-ondeelbare natuurlijke getallen heten samengesteld.

Hoofdstelling. Elk natuurlijk getal is op één en slechts één wijze in ondeelbare factoren te ontbinden (de volgorde der factoren speelt hierbij geen rol). Wij schrijven wel $n=p_1^{r_1}\ldots p_s^{r_s}$, waarbij elk tweetal der getallen $p_1,\ldots,p_s$ verschillend ondersteld is en $r_1,\ldots,r_s$ natuurlijke getallen voorstellen. De hier gegeven ontbinding van het getal n noemt men wel de canonieke ontbinding.

De hoofdstelling wordt bewezen met gebruikmaking van de volgende belangrijke

Hulpstelling. Als het priemgetal p deelbaar is op een product ab, dan is het deelbaar op ten minste één der factoren a en b.

Uit de canonieke ontbinding van twee natuurlijke getallen m en n zijn gemakkelijk hun gemeenschappelijke delers en dus ook hun grootste gemeenschappelijke deler, aan te geven met (m,n), te bepalen. Analoge overwegingen voeren tot het begrip kleinste gemene veelvoud. Voor twee getallen a en b is dat gelijk aan $\frac{ab}{(a,b)}$.

Een belangrijk onderdeel van de getallentheorie is de leer der congruenties. Met $a \equiv b \pmod m$ bedoelt men $m \mid a-b$. Men zegt, dat a en b tot dezelfde restklasse mod m behoren. Uit $a \equiv b \pmod m$ en $c \equiv d \pmod m$ volgen de formules $a \pm b \equiv c \pm d \pmod m$ en $ac \equiv bd \pmod m$, dus voor natuurlijke m ook $a^n \equiv b^n \pmod m$.
Uit $a \equiv b \pmod m$ volgt voor een gemeenschappelijke deler d van a en b niet noodzakelijk $\frac{a}{d} \equiv \frac{b}{d} \pmod m$; men kan slechts concluderen tot $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{(d,m)}}$.

Men gaat gemakkelijk na, dat, als $m > 0$ en $(a,m)=1$, de congruentie $ax \equiv b \pmod m$ precies een gehele oplossing x met $0 \leq x < m$ bezit. In het bijzonder is dit dan het geval met $ax \equiv 1 \pmod m$; de oplossing hiervan wordt wel geschreven in de gedaante a^{-1}.

In het algemeen rekent men bij een congruentie $f(x) \equiv 0 \pmod m$ (veelal stelt daarbij f(x) een veelterm in x voor met gehele coëfficiënten) twee oplossingen x_1 en x_2 als dezelfde als ze tot dezelfde restklasse mod m behoren. Zo beschouwd kan zo'n congruentie niet meer dan m oplossingen bezitten.

Is x_1 een wortel van de congruentie $f(x) \equiv 0 \pmod m$, waarbij f(x) een veelterm is met gehele coëfficiënten, dan geldt

$$f(x) \equiv (x-x_1)g(x) \pmod m,$$

waarbij ook g(x) een veelterm is met gehele coëfficiënten. In het geval dat m een priemgetal is vindt men alle oplossingen van de oorspronkelijke congruentie door op te lossen $x-x_1 \equiv 0 \pmod m$ en $g(x) \equiv 0 \pmod m$. Bij samengestelde m is de zaak gecompliceerder.

§ 2. Over zekere bijna- of pseudo-priemgetallen.

Wij gaan uit van de eigenschap

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

geldig voor alle a, die niet deelbaar zijn door het priemgetal p. Hoewel de eigenschap bekend is, geven wij er hier een kort bewijs van. Het stel van p-1 getallen 1,2,...,p-1 gaat na vermenigvuldiging met a

over in weer een stel van p-1 getallen, die twee aan twee incongruent zijn met p (immers $ah \equiv ak \pmod p$ impliceert $h \equiv k \pmod p$), en dus in een permutatie van zichzelf. Bijgevolg vindt men na product-nemen

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

waaruit (1) volgt.

Wij vragen ons thans of of uit

$$a^{m-1} \equiv 1 \pmod m$$

volgt dat m priem is. Gemakkelijk blijkt uit een tegenvoorbeeld, dat dit niet het geval is, b.v. $3^{90} \equiv 1 \pmod{91}$, reden om de zaak aan een nader onderzoek te onderwerpen.

Ieder samengesteld m dat voldoet aan $m \mid a^{m-1}-1$, zullen we een bijna-priemgetal (met betrekking tot a) noemen.

Stelling. Bij elke $a > 1$ bestaat er een bijna-priemgetal m (met betrekking tot a).

Opmerking. De bewering dat bij elke samengestelde m een $a > 1$ bestaat met $m \mid a^{m-1}-1$ is voor even m kennelijk onjuist (zoals b.v. blijkt door $m=6$ te nemen) en voor oneven m triviaal.

Bewijs:

1°. Bij $a=2$ neme men $m=341=11.31$. Inderdaad heeft men $341 \mid 2^{10}-1 \mid 2^{340}-1$.

2°. Is a een oneven priemgetal, dan neme men $m = \frac{a^{2a}-1}{a^2-1}$. Kennelijk is m samengesteld. Verder heeft men

$\frac{a^{2a-2}-1}{a^2-1} = a^{2a-4} + \ldots + a^2 + 1 \equiv 1 + \ldots + 1 + 1 = a-1 \equiv 0 \pmod 2$, dus

$2(a^2-1) \mid a^{2a-2}-1$, dus $2a \mid \frac{a^{2a}-a^2}{a^2-1} = m-1$, dus $m \mid a^{2a}-1 \mid a^{m-1}-1$.

3°. Zij a samengesteld. Nu neme men $m = \frac{a^a-1}{a-1}$ en ook nu is m samengesteld. Men heeft dan $m-1 = \frac{a^a-a}{a-1}$ en $a \mid \frac{a^a-a}{a-1} = m-1$, dus $m \mid a^a-1 \mid a^{m-1}-1$.

Opmerking. In elk der drie gevallen voldoet het gevonden getal m aan $(m, a-1)=1$.

Bewijs: Voor $a=2$ en $m=341$ is dit evident.

In het tweede geval heeft men voor een willekeurige priemdeler p van $a-1$ de relatie $a \equiv 1 \pmod p$, dus

$$m = a^{2a-2} + \ldots + a^2 + 1 \equiv 1 + \ldots + 1 + 1 = a \equiv 1 \pmod p,$$

derhalve $p \nmid m$ en $(m, a-1)=1$.

In het derde geval heeft men voor een willekeurige priemdeler p van a-1 eveneens $a \equiv 1 \pmod p$, dus

$$m = a^{a-1}+\ldots+a+1 \equiv 1+\ldots+1+1=a \equiv 1 \pmod p,$$

en dus ook nu $p \nmid m$ en $(m,a-1)=1$.

Van het in de opmerking gevondene zullen we verderop nog gebruik maken.

Stelling. Bij elke $a > 1$ zijn er oneindig veel bijna-priemgetallen m (met betrekking tot a).

Bewijs: Wij weten reeds, dat er zeker één zo'n getal m bestaat en dat dat bovendien nog voldoet aan $(m,a-1)=1$. Wij laten nu zien dat bij ieder bijna-priemgetal m met $(m,a-1)=1$ een nieuw bijna priemgetal M te vinden is met eveneens $(M,a-1)=1$. Daarmee zal dan het bewijs geleverd zijn.

Wij nemen thans $M = \frac{a^m-1}{a-1}$ en merken allereerst op, dat, als m samengesteld is, dit ook het geval is met M. Verder heeft men $m \mid a^{m-1}-1 \mid a^m-a=(a-1)(M-1)$. Wetens $(m,a-1)=1$ geldt dan $m \mid M-1$. Bij gevolg $M \mid a^m-1 \mid a^{M-1}-1$.

Om ten slotte aan te tonen dat de bijvoorwaarde $(M,a-1)=1$ vervuld is, beschouwe men een willekeurige priemdeler p van a-1, welke dus niet deelbaar is op m.
Daarvoor vindt men dan

$$M=a^{m-1}+\ldots+a+1 \equiv 1+\ldots+1+1=m \not\equiv 0 \pmod p.$$

Opmerking. Heeft m juist s verschillende priemfactoren, dan bezit M er ten minste s+1. Onze hierboven gegeven afleiding leert ons dus tevens, dat er bijna-priemgetallen zijn met willekeurig veel priemfactoren.

Wij geven thans een tweede bewijs van het bestaan van oneindig veel bijna-priemgetallen.

Hiertoe beschouwe men de getallen $u_h=(a^{a^h}-1):(a^{a^{h-1}}-1)$ voor $h=1,2,\ldots$. Allereerst merken wij op dat voor $h \neq k$ geldt $(u_h,u_k)=1$. Immers zij $h < k$ en p een willekeurige priemfactor van u_h. Wegens $k-1 \geq h$ heeft men dan $p \mid u_h \mid a^{a^h}-1 \mid a^{a^{k-1}}-1$, dus $u_k=a^{a^{k-1}}(a-1)+\ldots+a^{a^{k-1}}+1 \equiv 1+\ldots+1+1=a \not\equiv 0 \pmod p$.

Thans beschouwen wij twee getallen u_h en u_k met $h < k \leq a^{h-1}$. Dan heeft men

$$a^k \mid a^{a^h}-a^{a^{h-1}} \mid u_h-1 \text{ en } a^h \mid a^{a^k}-a^{a^{k-1}} \mid u_k-1$$

en uiteraard $a^k \mid u_k - 1$ en $a^h \mid u_h - 1$.

Dus
$$u_k \mid a^{a^k} - 1 \mid a^{u_h - 1} - 1 \text{ en } u_h \mid a^{a^h} - 1 \mid a^{u_k - 1} - 1$$

en uiteraard
$$u_k \mid a^{a^k} - 1 \mid a^{u_k - 1} - 1 \text{ en } u_h \mid a^{a^h} - 1 \mid a^{u_h - 1} - 1.$$

Bijgevolg geldt wegens $(u_h, u_k) = 1$
$$u_h u_k \mid a^{u_h - 1} - 1; \quad u_h u_k \mid a^{u_k - 1} - 1 \mid a^{u_h u_k - u_h} - 1 \quad .$$

Dus
$$u_h u_k \mid a^{u_h u_k - 1} - 1$$

en $u_h u_k$ is een bijna-priemgetal.

Ten slotte geven wij een derde bewijs van de stelling, dat er oneindig veel bijna-priemgetallen zijn met betrekking tot een gegeven getal a.

Stelling. Zij p een oneven priemgetal, dat niet deelbaar is op $a^2 - 1$. Dan is $m = \frac{a^{2p} - 1}{a^2 - 1}$ een bijna-priemgetal.

Bewijs. Wij laten eerst zien, dat m-1 even is.

In het geval dat a even is, is m kennelijk oneven, dus m even. Is echter a oneven, dan heeft men

$$m = a^{2p-2} + \ldots + a^2 + 1 \equiv 1 + \ldots + 1 + 1 = p \equiv 1 \pmod 2.$$

Dus $2 \mid m-1$. Verder $p \mid a^{p-1} - 1 \mid a^{2p-2} - 1$, dus $p \mid m-1$, want $p \nmid a^2 - 1$. Bij gevolg $2p \mid m-1$ en men vindt

$$m \mid a^{2p} - 1 \mid a^{m-1} - 1.$$

Dat m ten slotte niet priem is volgt uit $m = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1}$.

§ 3. Getallen van Carmichael

In het voorafgaande werden samengestelde getallen m gevonden, die bij gegeven a voldeden aan $m \mid a^{m-1}-1$. Thans stellen wij ons de vraag of er samengestelde getallen m bestaan, die deze relatie vervullen voor alle a. Het antwoord is kennelijk ontkennend. Immers in het bijzonder zou dan gelden $m \mid m^{m-1}-1$, wat echter niet het geval is. Wij zullen onze vraag dus iets anders moeten formuleren en dan een bevestigend antwoord op onze vraag verkrijgen.

Definitie. Een getal m dat voldoet aan $m \mid a^{m-1}-1$ voor alle a, die onderling ondeelbaar zijn met m, heet een getal van Carmichael.

Alvorens een nader onderzoek te doen naar dergelijke getallen geven wij eerst een aantal eigenschappen, die bij het verdere onderzoek zullen worden gebruikt.

Hulpstelling. Als een getal m voldoet aan $m \mid a^{r}-1$ en $m \mid a^{s}-1$, dan voldoet het ook aan $m \mid a^{(r,s)}-1$.

Bewijs: Wij weten dat de G.G.D. (r,s) van r en s te schrijven is in de gedaante $(r,s)=ur+vs$ met gehele u en v. Dan volgt uit $a^{r} \equiv 1 \pmod m$ en $a^{s} \equiv 1 \pmod m$ ook $a^{ur+vs} \equiv 1 \pmod m$. Q.e.d.

Gevolg. Bij elk paar getallen m en a met $(a,m)=1$ is er een kleinste positieve exponent g met $a^{g} \equiv 1 \pmod m$. Deze wordt genoemd de primitieve exponent of kortweg dé exponent van a mod m.

Verder geldt: Voor iedere h, die voldoet aan $a^{h} \equiv 1 \pmod m$, geldt $g \mid h$. Immers stel $h=qg+r$ met $0 \leq r < g$, dan vindt men

$$a^{r} \equiv a^{qg} a^{r} \equiv a^{h} \equiv 1 \pmod m,$$

dus op grond van de minimaliteit van g vindt men r=0. In het bijzonder heeft men dus $g \mid \varphi(m)$.

Definitie. Een getal a heet primitieve wortel mod m als het hierboven ingevoerde getal g gelijk is aan $\varphi(m)$. Zo is b.v. 3 een primitieve wortel voor m=7 en ook voor m=14 en m=49.

Wij maken thans gebruik van een belangrijke stelling, waarvan wij, om ons onderzoek niet verder te onderbreken, het bewijs achterwege laten.

Stelling. Elk oneven priemgetal p bezit ten minste één primitieve wortel; ook elk getal van het type p^{r}.

Opmerking. Uit deze stelling volgt direct, dat er $\varphi(p-1)$ primitieve wortels zijn. Is nl. f een primitieve wortel, dan is dit ook het ge-

val met f^e, waarbij $(e,p-1)=1$ is.

Thans keren wij terug tot het onderzoek naar getallen van Carmichael. Stel m even, $m=2^r n$, waarbij n oneven is. Zij p een oneven priemdeler van n. Kies nu voor a een primitieve wortel mod p. Dan heeft men $a^{m-1}\equiv 1 \pmod m$, dus $a^{m-1}\equiv 1 \pmod p$, dus $\varphi(p)\mid m-1$. Wegens $2\mid\varphi(p)$ geldt $2\mid m-1$ en $r=0$. Dus m is oneven, tenzij dat m geen dergelijke priemdeler p bezit. In dat geval is $m=2^r$. Voor $a=3$ eist men dan enerzijds $a^{m-1}\equiv 1 \pmod m$, anderzijds blijkt dé exponent van a mod 2^r voor $r\geq 3$ gelijk te zijn aan 2^{r-2}. Dus $2^{r-2}\mid m-1$ in strijd met $r\geq 3$. Ook $m=4$ blijkt uitgesloten te zijn, want $3^3\not\equiv 1 \pmod 4$.

Dus m is oneven. Zij $m=p_1^{r_1}\ldots p_s^{r_s}$ de canonieke ontbinding van m. Laat a_1 een primitieve wortel zijn mod $p_1^{r_1}$ en verder $(a,m/p_1^{r_1})=1$. Dus uit $a^{m-1}\equiv 1 \pmod m$ volgt $a^{m-1}\equiv 1 \pmod{p_1^{r_1}}$, dus $\varphi(p_1^{r_1})\mid m-1$, dus $p_1^{r_1-1}(p_1-1)\mid m-1$. Wegens $p_1\mid m$ heeft men $r_1-1=0$ en evenzo $r_2=\ldots=r_s=1$.

Verder vinden we nog uit het bovenstaande, dat $p_1-1\mid m-1$, dus, als men $m=m_i p_i$ $(i=1,\ldots,s)$ stelt, $p_1-1\mid m_1(p_1-1)+m_1-1$ en bijgevolg $p_1-1\mid m_1-1$. Algemeen evenzo $p_i-1\mid m_i-1$ $(i=1,\ldots,s)$.

Wij bewijzen nu $s\geq 3$. Inderdaad, als $s=2$ was, had men $m_1=p_2$, $m_2=p_1$ en $p_1-1\mid p_2-1$, $p_2-1\mid p_1-1$, in strijd met $p_1\neq p_2$.

Dus $s\geq 3$.

Omgekeerd leidt $p_i-1\mid m_i-1$ tot $p_i-1\mid m-1$, dus $p_i\mid a^{p_i-1}-1\mid a^{m-1}-1$ en derhalve $m\mid a^{m-1}-1$.

Wij willen het bovenstaande verder uitwerken voor het geval $s=3$ en inderdaad daarbij Carmichaelgetallen vinden.

Wij proberen dus $m=pqr$ en mogen, zonder de algemeenheid te schaden, onderstellen, dat $p>q>r$ is. Er zijn dan gehele x,y en z met

$$qr-1=x(p-1)\ ;\ pr-1=y(q-1)\ ,\ pq-1=z(r-1)\ ;\ x<y<z.$$

Oplossing van de eerste twee relaties leert

$$p-1=\frac{(y+r)(r-1)}{xy-r^2}\quad ;\quad q-1=\frac{(x+r)(r-1)}{xy-r^2}\ .$$

Verder heeft men wegens $p>q$, dus $p\geq q+2$,

$$x=\frac{qr-1}{p-1}\leq\frac{qr-1}{q+1}=r-\frac{r+1}{q+1}\ ,$$

dus $x\leq r-1$ (want x is geheel). Hieruit volgt, dat

$$q-1\leq\frac{(2r-1)(r-1)}{xy-r^2}\leq(2r-1)(r-1),$$

zodat bij gegeven r slechts eindig veel mogelijkheden voor q bestaan en wegens $p-1 \mid qr-1$ ook slechts eindig vele voor p. Wij vinden dus, dat er bij gegeven r slechts eindig veel getallen pqr van Carmichael bestaan met $p > q > r$.

Op geheel analoge wijze ziet men in, dat er slechts eindig veel getallen van Carmichael $p_1p_2 \ldots p_s$ bestaan met $p_1 > p_2 > \ldots > p_s$, waarvoor $r=p_3p_4 \ldots p_s$ gegeven is.

Wij passen het bovenstaande eens toe voor r=3, en bepalen dus Carmichaelgetallen van het type m=3pq met $p > q > 3$. Allereerst heeft men te zorgen voor $3-1 \mid pq-1$, hetgeen uiteraard automatisch vervuld is. Verder leert het bovenstaande ons, dat $q-1 \leqq (2r-1)(r-1)$, dus $q-1 \leqq 10$, dus $q \leqq 11$. Wij hebben dus slechts te onderzoeken q=5, q=7 en q=11. Nu geldt verder $p > q$ en $p-1 \mid qr-1$, dus in het eerste geval $p-1 \mid 14$, hetgeen tot niets voert. De tweede mogelijkheid leert $p-1 \mid 20$, dus slechts p=11. Maar het getal 6 (nl.q-1) is niet deelbaar op pr-1 (nl.32). Rest het geval q=11, dus $p-1 \mid 32$. Slechts is dit vervulbaar voor p=17 en inderdaad blijkt nu ook te gelden, dat $q-1 \mid pr-1$. Het enige Carmichaelgetal van de gedaante 3pq (p en q priem) is dus 3.11.17=561).

Opmerking. Voor (a,561)=1 is het getal 561 dan tevens een pseudopriemgetal ten opzichte van a.

Curiositeitshalve geven wij hier een tabel van enige getallen van Carmichael van het type pqr ($p > q > r$) met r=3 tot en met 23 (en priem). Het rekenwerk kan door enkele verdere overwegingen nog wat worden bekort.

3.11.17 = 561	13.37.61 = 29341
5.13.17 = 1105	13.37.97 = 46657
5.17.29 = 2465	13.37.241 = 115921
5.29.73 = 10585	13.61.397 = 314821
7.13.19 = 1729	13.97.421 = 530881
7.13.31 = 2821	17.41.233 = 162401
7.19.67 = 8911	17.353.1201 = 7207201
7.23.41 = 6601	19.43.409 = 334153
7.31.73 = 15841	19.199.271 = 1024651
7.73.103 = 52633	23.199.353 = 1615681

§ 4. De ring van Gauss

In deze paragraaf worden complexe getallen $z=x+iy$ (x en y reëel) beschouwd, waarvoor de bekende regels van optellen, aftrekken, vermenigvuldigen en delen (mits niet door 0) bestaan en de antwoorden weer complexe getallen zijn.

In navolging van Gauss stellen we de complexe getallen meetkundig voor door punten; met het getal $z=x+iy$ correspondeert het punt met rechthoekige coördinaten (x,y). Het meetkundige verband tussen de punten, voorgesteld door de drie complexe getallen z_1, z_2 en z_1+z_2 (een "vectoroptelling") onderstellen wij bekend; ook dat tussen de getallen z_1, z_2 en $z_1 z_2$.

Naast het getal $z=x+iy$ beschouwt men wel het toegevoegd complexe getal $\overline{z}=x-iy$; de X-as (of reële as) is middenloodlijn van het lijnstuk met uiteinden z en $\overline{z}$ (mits $y\neq 0$). Een getal z is dan en slechts dan reëel als $z=\overline{z}$ en dan en slechts dan zuiver imaginair (d.w.z. gelegen op de Y-as, hier genoemd imaginaire as) als $z=-\overline{z}$.

Verder heeft men $z\overline{z}=x^2+y^2$; deze uitdrukking stelt voor het quadraat van de lengte $|z|$ van het lijnstuk dat 0 en z verbindt. Dus $|z|^2=z\overline{z}$. Men kan een complex getal ook vastleggen door de modulus $|z|$ en het argument $\arg z = \angle zOX$. Men heeft $\overline{z+w}=\overline{z}+\overline{w}$; $\overline{zw}=\overline{z}\,\overline{w}$; $|\overline{z}|=|z|$; $\arg \overline{z} = -\arg z$.

Uit de verzameling van alle complexe getallen lichten wij nu uit de gehele complexe getallen, dat zijn de getallen $z=x+iy$, waarbij x en y gehele reële getallen zijn. Deze verzameling heet de ring van Gauss. Het is duidelijk, dat som, verschil en product van twee gehele complexe getallen weer zo'n getal is. Bij de deling behoeft dit uiteraard niet zo te zijn. Men bedoelt met $w|z$ (w is een deler van z) bij gehele w en z, dat $z=sw$, waarbij s een geheel complex getal is. Vb. $2+i|3-i$; $3+2i|13$; $3i|9$.

Alle gehele complexe getallen d, die voldoen aan $d|z$ noemt men delers van z. Gevolg: Als d een deler is van z zijn ook $-d$, id en $-id$ delers van z. De getallen $1,-1$, i en $-i$ zijn delers van elk geheel complex getal.

Definitie. Een eenheid is een deler van 1.

Wij bepalen thans alle eenheden. Nu geldt voor een eenheid $e=f+ig$ de relatie $es=1$ (met gehele s), dus $\overline{e}\,\overline{s}=1$ en $e\overline{e}\;s\overline{s}=1$, dus $(f^2+g^2)\,s\overline{s}=1$, dus f^2+g^2 is een reële deler van 1. Bijgevolg is $f^2+g^2=1$, d.w.z. $f^2=1$ en $g=0$ of $g^2=1$ en $f=0$. Hieruit blijkt dat de

enige eenheden zijn de vier getallen 1,-1, i en -i.

Bij de verzameling der gehele reële getallen zijn de enige eenheden de getallen 1 en -1, bij die der natuurlijke getallen is de enige eenheid het getal 1.

Twee complexe getallen heten geassocieerd als hun quotiënt een eenheid is. De geassocieeerden van w zijn w,-w, wi en -wi. Als $z|w$ en $w|z$, dan zijn w en z geassocieerd (bewijs dit). De eenheden zijn die getallen, die geassocieerd zijn met 1 (bewijs dit).

Elk geheel complex getal z bezit als triviale delers de getallen z,-z, zi, -zi, 1,-1, i en -i. Een getal z dat geen andere (maar precies deze acht) delers bezit heet bij definitie priem (of ondeelbaar). Een niet ondeelbaar getal heet samengesteld. Zo zijn de getallen 2, 4 en 5 samengesteld, maar 3 is priem; ook 1 is niet priem (evenals bij de reële getallen).

Nu eenmaal het begrip priemgetal is ingevoerd, komt direct de vraag naar voren, of elk geheel complex getal te schrijven is als een product van priemfactoren en verder of deze schrijfwijze (afgezien van de volgorde der factoren en van vervanging van factoren door hun geassocieerden) ondubbelzinnig is.

Ons onderzoek wordt vereenvoudig door invoering van het begrip norm. Onder de norm N_z van het getal $z=x+iy$ verstaat men het getal $N_z=|z|^2=z\bar{z}=x^2+y^2$. Men heeft voor alle z de betrekking $N_z \geq 0$ en $N_z=0$ komt slechts voor bij $z=0$. Verder geldt

$$N_{zw} = (zw)(\overline{zw}) = zw\,\bar{z}\,\bar{w} = z\bar{z}\,w\bar{w} = N_z N_w.$$

Bijgevolg leidt $s|w$ tot $N_s|N_w$. Wil men dus alle delers van een gegeven geheel complex getal w opsporen, dan bepale men eerst alle positieve echte delers d van N_w en daarna alle $s=p+qi$ met $N_s=d$, dus $p^2+q^2=d$. Beide problemen bezitten maar eindig veel oplossingen. De zo verkregen oplossingen s moet men nog rechtstreeks controleren op $s|w$. Vb. $w=3+i$. $N_w=3^2+1^2=10$. Men probere s met $N_s=2$ en $N_s=5$. $N_s=2$ leidt tot $p^2+q^2=2$, dus $s=\pm1\pm i$, en $N_s=5$ levert $p^2+q^2=5$, dus $s=\pm2\pm i$ of $s=\pm1\pm2i$. De enige wezenlijk te onderzoeken s (waarbij na het onderzoek van een s niet ook nog het nodeloze onderzoek met de geassocieerde geschiedt) zijn 1+i, 2+i, 2-i, waarna men vindt $3+i = (2-i)(1+i)$. De gevonden factoren zijn niet nog verder te ontbinden. Hiertoe helpt ons de <u>stelling</u>: Is de norm van een getal een priemgetal, dan is het priem. Immers uit $s|w$ volgt $N_s|N_w$ en als N_w

priem is, vindt men $N_s=1$, dus s is een eenheid, of wel $N_s=N_w$, dus $N_{w/s}=1$ en w/s is een eenheid, dus w en s zijn geassocieerd.

Het omgekeerde der stelling geldt niet; immers het getal 3 is een ondeelbaar geheel complex getal (ga dit na!), maar $N_3=9$ is niet priem.

Om ons onderzoek naar de ondubbelzinnige ontbindbaarheid nu te voltooien, hebben wij enige tussenresultaten nodig.

Hulpstelling 1. Bij iedere w en z zijn er gehele q en r met $w=qz+r$ en $N_r < N_z$ ("delen met rest").

Bewijs: Beschouw het niet noodzakelijk gehele getal $\frac{w}{z}=h+ki$ (h en k zijn niet noodzakelijk geheel). Zij m het meest nabijzijnde gehele reële getal bij h; n dat bij k. Dan is $|m-h| \leqq \frac{1}{2}$; $|n-k| \leqq \frac{1}{2}$. Stel $m+ni=q$; $h-m+i(k-n)=t$. $\frac{w}{z} = q + t$, dus $w=qz+tz$. Omdat qz geheel is, is ook $r=tz$ geheel en verder geldt

$$N_r = N_t N_z = \left\{ (h-m)^2 + (k-n)^2 \right\} N_z \leqq \left(\frac{1}{4} + \frac{1}{4}\right) N_z < N_z, \quad \text{q.e.d.}$$

Nu eenmaal het "delen met rest" mogelijk blijkt, is de algorithme van Euclides ter bepaling van de "G.G.D." van twee getallen w en z te imiteren.

Stel nl. $w = q_1 z + r_1$ met $N_{r_1} < N_z$

$z = q_2 r_1 + r_2$ met $N_{r_2} < N_{r_1}$

$r_1 = q_3 r_2 + r_3$ met $N_{r_3} < N_{r_2}$, enz.

De rij getallen $N_z, N_{r_1}, N_{r_2}, \ldots$ is dalend. Omdat elke norm $\geqq 0$ is, moet er een index n zijn, van waaraf geldt $N_{r_n}=0$, dus $r_n=0$. Ons schema eindigt dan met de regels

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$$

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

Het is duidelijk dat iedere gemeenschappelijke deler van w en z ook deler is van r_1, dus ook een gemeenschappelijke deler is van z en r_1, dus evenzo van r_1 en r_2, enz. Elke gemeenschappelijke deler van w en z is dus gemeenschappelijke deler van r_{n-2} en r_{n-1}, dus deler van r_{n-1}. Omgekeerd ziet men, het schema van beneden naar boven vervolgende, dat iedere deler van r_{n-1} een gemeenschappelijke deler is van w en z.

Definitie. Die gemeenschappelijke deler van w en z, waarop alle gemeenschappelijke delers van w en z deelbaar zijn, heet grootste gemeenschappelijke deler van w en z.

We schrijven voor de grootste gemeenschappelijke deler van w en z wel (w,z). Het bovenstaande leert ons dan, dat $r_{n-1}=(w,z)$ en geeft ons tegelijkertijd een methode om (w,z) te bepalen.

Tenslotte merken wij nog op, dat uit het bovenstaande volgt, dat er gehele u en v zijn met (w,z)=uw+vz. Inderdaad, men heeft $r_1=1.w-q_1.z$; dus $r_2=z-q_2r$ is ook een dergelijke combinatie van w en z; evenzo r_3 enz. Dus ook $r_{n-1}=(w,z)$.

Lemma (2e hulpstelling): Als p een ondeelbaar geheel complex getal is en $p|ab$, $p\nmid a$, dan geldt $p|b$.

Bewijs: Zij d de GGD van a en p. Omdat $p\nmid a$ is, is d=1, dus wegens het bovenstaande bestaan er u en v met 1=up+va. Dus b=upb+vab. Uit $p|ab$ volgt dan $p|b$.

Hoofdstelling. Elk geheel complex getal is op één en slechts één wijze te ontbinden in dergelijke ondeelbare getallen (met de bekende restricties ten aanzien der volgorde der factoren en vervanging van factoren door hun geassocieerden).

Bewijs: Zij $m=p_1p_2\ldots p_s=q_1q_2\ldots q_t$, waarbij alle factoren p_i en q_j ondeelbaar zijn. Dan geldt $q_t|m$, dus q_t moet op een der factoren $p_1,p_2,\ldots,p_s$ deelbaar zijn (op grond van het lemma). Zonder de algemeenheid te schaden mogen wij onderstellen, dat $q_t|p_s$, dus q_t en p_s zijn geassocieerd. Beschouw nu m/q_t en handel evenzo met q_{t-1} enz. Men vindt dan s=t en verder ziet men, dat de factoren p_i en q_i twee aan twee geassocieerd zijn. Q.e.d.

Opgave. Ontbind in priemfactoren de getallen 8+i en 50.

Wij passen het gevondene toe op het vinden van quadraatsplitsingen der natuurlijke getallen, dat is om te onderzoeken of er bij gegeven n gehele x en y bestaan met $n=x^2+y^2$. Zonder de algemeenheid te schaden mag men onderstellen $x\geq 0$, $y\geq 0$. Men mag verder onderstellen, dat (x,y)=1, want (x,y)=d voert tot de splitsing $(\frac{x}{d})^2+(\frac{y}{d})^2$ van het getal $\frac{n}{d^2}$. Wij behoeven dus slechts quadraatvrije getallen op hun splitsbaarheid te onderzoeken.

Is $n=x^2+y^2$ en $m=u^2+v^2$, dan heeft men voor z=x+iy en w=u+iv de relaties $n=z\bar{z}$, $m=w\bar{w}$, dus $mn=z\bar{z}.w\bar{w}=(zw)(\overline{zw})$. Stel zw=s+it, dan geldt $mn=s^2+t^2$ en mn blijkt splitsbaar als m en n het zelf zijn.

Alvorens het onderzoek voort te zetten bekijken wij eens een reëel priemgetal p. Voor $p=2=1^2+1^2$ heeft men precies één splitsing.

Is p oneven en splitsbaar, dan leidt $p=x^2+y^2$ tot $(x,y)=1$, dus $(y,p)=1$ (ga na) en, als men $ry \equiv 1 \pmod p$ stelt,

$$r^2x^2 \equiv -r^2y^2 \equiv -1 \pmod p.$$

Het getal -1 is dus quadraatrest mod p, waarna de theorie der quadraatresten ons leert, dat p een viervoud + 1 is. Dit levert allereerst de conclusie dat ieder reëel ondeelbaar viervoud +3 ook in de ring van Gauss ondeelbaar is (ga dit precies na!). Een reëel ondeelbaar viervoud +1 is steeds splitsbaar (en dus samengesteld). Immers zij $p \equiv 1 \pmod 4$ en reëel en ondeelbaar. Dan is er een x met $x^2 \equiv -1 \pmod p$, dus $p \mid x^2+1=(x+i)(x-i)$. Stel, dat p in de ring van Gauss ondeelbaar was, dan moest de priemfactor p op tenminste een der factoren x+i en x-i deelbaar zijn. Stel $p \mid x+i$. Dan geldt $\overline{p} \mid x-i$, dus wegens $p=\overline{p}$ ook $p \mid x-i$, derhalve $p \mid 2i$, in strijd met $p \equiv 1 \pmod 4$ en p priem. Bijgevolg moet ieder reëel ondeelbaar viervoud +1 in de ring van Gauss samengesteld zijn. Zij nu w een complexe deler van p, dan is $\overline{w}$ ook een complexe deler van p (nl. van $\overline{p}$), dus wegens $(w,\overline{w})=1$ (ga dat na) $w\overline{w} \mid p$. Zelfs volgt nu uit de reële primaliteit van p, dat $p=w\overline{w}=u^2+v^2$, dus p is splitsbaar. Wij vinden dus (onder gebruikmaking van de eigenschappen van de ring van Gauss), dat ieder ondeelbaar viervoud +1 te schrijven is in de gedaante u^2+v^2.

Voorbeelden:

$5=1^2+2^2$	$53=2^2+7^2$	$109=3^2+10^2$
$13=2^2+3^2$	$61=5^2+6^2$	$113=7^2+8^2$
$17=1^2+4^2$	$73=3^2+8^2$	$137=4^2+11^2$
$29=2^2+5^2$	$89=5^2+8^2$	$149=7^2+10^2$
$37=1^2+6^2$	$97=4^2+9^2$	$157=6^2+11^2$
$41=4^2+5^2$	$101=1^2+10^2$	$173=2^2+13^2$

Opmerking. Dat de ondeelbare viervouden +3 geen quadraatsom zijn, is ook direct duidelijk. Stel $p \equiv 3 \pmod 4$ en $p=u^2+v^2$. Kennelijk is een dergetallen u en v even, het andere oneven (ga dat na!). Dus $p=u^2+v^2$ is een viervoud +1 (ga dat ook na) in strijd met de onderstelling over p.

Als een reëel getal meer dan één quadraatsplitsing bezit, is het samengesteld. Immers zij $m=u^2+v^2=x^2+y^2=w\overline{w}=z\overline{z}$ met $w \neq z$, $w \neq \overline{z}$.

Omdat m op slechts één wijze te ontbinden is kunnen w, $\overline{w}$, z en $\overline{z}$ niet allen priem zijn. Stel zonder de algemeenheid te schaden, w samengesteld en zij t een echte deler van w. Dan is $\overline{t}$ een echte deler van $\overline{w}$ en dus is het reële getal $t\overline{t}$ een echte deler van $m=w\overline{w}$.

Zo volgt uit $10001=100^2+1^2=65^2+76^2$, dat het getal 10001 samengesteld is. Inderdaad is $10001=73.137$.

Opgave. Ga na of er een rechtstreeks procédé is, dat uit de gegeven splitsingen van 10001 de factoren 73 en 137 kan opleveren.

Wij kunnen niet nalaten om de gevonden resultaten iets uit te breiden.

Laat n een vast gegeven quadraatvrij natuurlijk getal zijn. Een geheel getal m noemen wij splitsbaar als het te schrijven is in de gedaante $m=u^2+nv^2$ met gehele u en v.

Beschouw thans een priemgetal p met $(\frac{-n}{p})=-1$. Dan is p niet splitsbaar. Immers een relatie $p=u^2+nv^2$ leidt tot

$$u^2 \equiv -nv^2 \pmod p, \text{ dus } (uv_1)^2 \equiv -n \pmod p,$$

waarbij v_1 het reciproke mod p is van v (v_1 bestaat omdat $(p,v)=1$) in strijd met $(\frac{-n}{p})=-1$.

Zij thans p een oneven priemgetal met $(\frac{-n}{p})=1$. De situatie is nu niet noodzakelijkerwijze analoog aan die bij de ring van Gauss, waar in dit geval wel tot splitsbaarheid van p mocht worden besloten. Wij kunnen hier voorlopig slechts het volgende vaststellen.

Stelling. Als de ring der getallen $x+y\sqrt{-n}$ (x,y geheel) een ontbindingsring is (d.w.z. een ondubbelzinnige ontbinding toelaat), dan is een priemgetal p met $(\frac{-n}{p})=1$ splitsbaar.

Bewijs. Omdat $(\frac{-n}{p})=1$ is, is er een gehele x met $x^2 \equiv -n \pmod p$, dus $p \mid (x+\sqrt{-n})(x-\sqrt{-n})$. Was p priem in de beschouwde ring, dan was p deelbaar op ten minste een der uitdrukkingen $x+\sqrt{-n}$, $x-\sqrt{-n}$. Zonder de algemeenheid te schaden mogen wij onderstellen, dat men had $p \mid x+\sqrt{-n}$, dus $\overline{p} \mid x-\sqrt{-n}$. Wegens $p=\overline{p}$ had men dan $p \mid 2\sqrt{-n}$ in strijd met de onderstellingen. Dus p is deelbaar in de beschouwde ring. Zij $w=u+v\sqrt{-n}$ een priemdeler van p, dan is $\overline{w}$ het ook, dus wegens $(w,\overline{w})=1$ (was $(w,\overline{w})\neq 1$, dan was p geen gewoon priemgetal) geldt $w\overline{w} \mid p$ en wegens de "gewone" ondeelbaarheid van p vindt men $p=w\overline{w}=u^2+nv^2$.

Voorbeeld. De ring der getallen $a+b\sqrt{-2}$ (a,b geheel) is een ontbindingsring.

Opgave. Ga dit na door aan te tonen, dat hier(op dezelfde wijze als in de ring van Gauss) in de ring een Euclidische algorithme bestaat.

Gevolg: Alle p met $(\frac{-2}{p})=1$, d.w.z. alle p met $p \equiv 1$ of 3 (mod 8) zijn splitsbaar in de gedaante u^2+2v^2. Is een priemgetal $p \equiv 5$ of 7 (mod 8), dan is het niet splitsbaar op die wijze. Een natuurlijk getal met verschillende splitsingen is samengesteld.

Bevat een natuurlijk getal tenminste een priemfactor p, die mod 8 congruent is met 5 of 7, in een oneven macht, dan is het niet splitsbaar.

Dit laatste is het gevolg van de eigenschap
Als $p \equiv 5$ of 7 (mod 8) en $p \mid u^2+2v^2$, dan is $p \mid u$ en $p \mid v$, dus $p^2 \mid u^2+2v^2$.

Opgave. Bewijs deze eigenschap.

Wij beschouwen thans de getallen $x+y\sqrt{-3}$ (x,y geheel). Deze vormen geen ontbindingsring. Immers $4=(1+\sqrt{-3})(1-\sqrt{-3})=2^2$, en elk der factoren $1+\sqrt{-3}$, $1-\sqrt{-3}$ en 2 is ondeelbaar in deze ring.

Toch is hier nog wel de stelling van kracht, dat het getal p als het een oneven priemgetal is met $(\frac{-3}{p})=1$, splitsbaar is (in de gedaante u^2+3v^2). Daarvoor zijn verschillende bewijzen mogelijk, waarvan wij er een noemen.

De getallen van de gedaante $x+y\varepsilon$ (x,y geheel; $\varepsilon=-\frac{1}{2}+\frac{1}{2}i\sqrt{3}$) vormen een ontbindingsring (ring van Eisenstein). Het bewijs gaat weer op de gebruikelijke wijze via de algorithme van Euclides. Wij merken hierbij op dat voor $z=x+y\varepsilon$ als norm te nemen valt

$$N_z=z\overline{z}=(x+y\varepsilon)(x+y\overline{\varepsilon})=(x-\tfrac{1}{2}y+\tfrac{1}{2}yi\sqrt{3})(x-\tfrac{1}{2}y-\tfrac{1}{2}yi\sqrt{3})=x^2-xy+y^2.$$

Zij nu p een priemgetal met $(\frac{-3}{p})=1$. Er is dus een x met $x^2 \equiv -3$ (mod p), dus $p \mid x^2+3=z\overline{z}$ met $z=x-1-2\varepsilon$; $\overline{z}=x-1-2\overline{\varepsilon}$. Was p priem in de ring van Eisenstein, dan was p deelbaar op tenminste een der getallen z en $\overline{z}$.

Zonder de algemeenheid te schaden mogen wij aannemen $p \mid z$. Dus $\overline{p} \mid \overline{z}$, dus $p \mid \overline{z}$, dus $p \mid z-\overline{z}=4\varepsilon$, hetgeen tot een contradictie voert. Derhalve is p samengesteld in de ring van Eisenstein, d.w.z. er is een $w=u+\varepsilon v$ met $w \mid p$, dus $\overline{w} \mid p$ en, evenals vroeger, $\overline{w} \neq w$, $p=w\overline{w}=u^2-uv+v^2$. Tenslotte vindt men dan $p=(u-\frac{1}{2}v)^2+3(\frac{1}{2}v)^2$ als v even is en $p=(v-\frac{1}{2}u)^2+3(\frac{1}{2}u)^2$ als u even is en $p=(\frac{1}{2}u+\frac{1}{2}v)^2+3(\frac{1}{2}u-\frac{1}{2}v)^2$ als noch u noch v even is. Tenslotte heeft men nog de eigenschap
Als een natuurlijk getal m twee verschillende splitsingen x^2+3y^2 en u^2+3v^2 bezit, is het samengesteld.(Ga dit na).

Als laatste voorbeeld beschouwen wij getallen, die splitsbaar zijn in de gedaante x^2+5y^2. De priemgetallen p, waarvoor geldt $(\frac{-5}{p})=1$, zijn congruent met 1,3,7 of 9 mod 20. Thans blijkt echter, dat niet ieder dergelijk getal splitsbaar is, b.v. 3,7,23 en 47 zijn niet splitsbaar, trouwens geen enkel getal dat congruent is met 3 of 7 mod 20, is splitsbaar (ga dat na). Wel blijkt, dat ieder

priemgetal, dat congruent 1 of 9 is mod 20, splitsbaar is.

Een elementair bewijs hiervan kan op de volgende wijze geschieden. Zij $p \equiv 1$ of 9 (mod 20). Dan is $(\frac{-5}{p})=1$, dus er bestaat een x met $x^2 \equiv -5$ (mod p). Van dit getal x mogen wij onderstellen dat het positief, even en kleiner dan p is. Dus $x^2+5 \leq (p-1)^2+5<p^2$ mits $p>3$ (wat kennelijk het geval is). Dus $x^2+5=pn$ met $n<p$. Laat de ontbinding van n luiden $n=p_1p_2\ldots p_s$. Wegens $x^2 \equiv -5$ (mod p_i) geldt $(\frac{-5}{p_i})=1$, dus $p_i \equiv 1,3,7$ of 9 (mod 20) (geldig voor $i=1,\ldots,s$).

Wij geven het bewijs nu door inductie en onderstellen dat elk getal m met $m<p$ en $m \equiv 1$ of 9 (mod 20), dat slechts priemfactoren $\equiv 1,3,7$ of 9 (mod 20) bezit, splitsbaar is.

Allereerst dient een beginpunt voor de volledige inductie te worden gevonden. Kennelijk vindt men dit uit

$$9 = 2^2+5.1^2;\ 21=4^2+5.1^2,\ 29=3^2+5.2^2$$

(echter niet al deze relaties zijn nodig als springplank voor de inductie).

Wij weten nu dat $pn=x^2+5$ splitsbaar is. Beschouw eerst een priemgetal $p_i \equiv 1$ of 9 (mod 20). Bij inductie is dat ook splitsbaar (u^2+5v^2). Dan is $\frac{pn}{p_i} = \frac{x^2+5}{u^2+5v^2} = \frac{(x^2+5)(u^2+5v^2)}{p_i^2} =$

$$= \frac{(xu+5v)^2+5(xv-u)^2}{p_i^2} = \frac{(xu-5v)^2+5(xv+u)^2}{p_i^2}.$$

Nu is

$$(xu+5v)(xu-5v) = x^2u^2-25v^2 \equiv x^2u^2+5u^2 \equiv 0 \text{ (mod } p_i),$$

dus p_i is deelbaar op tenminste een der factoren xu+5v en xu-5v. Dat leidt er toe dat ook $\frac{pn}{p_i}$ splitsbaar is. Dit zetten wij voort en vinden dan tenslotte, dat $g=\frac{pn}{p_1\ldots p_r} = pQ$ splitsbaar is, waarbij Q slechts priemfactoren van het type $\equiv 3$ of 7 (mod 20) bevat en uit $g \equiv 1$ of 9 (mod 20) en $p \equiv 1$ of 9 (mod 20) volgt, dat $Q \equiv 1$ of 9 (mod 20 is). Omdat $Q<n<p$ is en Q slechts priemfactoren bezit, die $\equiv 3$ of 7 zijn mod 20, is bij inductie het getal Q splitsbaar. Ook g is het. Het getal $gQ=pQ^2$ is dan ook splitsbaar $(=a^2+5b^2)$. Zij nu q een priemdeler van Q. Dan is bij inductie q^2 splitsbaar, $q^2=c^2+5d^2$.

Dus

$$\frac{pQ^2}{q^2} = \frac{(a^2+5b^2)(c^2+5d^2)}{q^4} = \frac{(ac+5bd)^2+5(ad-bc)^2}{q^4} = \frac{(ac-5bd)^2+5(ad+bc)^2}{q^4}$$

Wegens

$$(ac+5bd)(ac-5bd)=a^2c^2-25b^2d^2 \equiv a^2c^2+5b^2c^2 \equiv 0 \pmod{q^2}$$

en omdat ac+5bd en ac-5bd geen factor q gemeen hebben, moet een der factoren ac+5bd en ac-5bd deelbaar zijn door q^2, dus $\frac{pQ^2}{q^2}$ is splitsbaar. Zo doorgaande met alle verdere priemdelers van Q vindt men tenslotte, dat p splitsbaar is.

Tenslotte merken wij op, dat een getal m, dat twee verschillende splitsingen bezit, samengesteld is.
Zij nl. $m=u^2+sv^2=x^2+5y^2$ met $(u^2-x^2)(v^2-y^2)\neq 0$. Onderstel, dat m priem was, dan was

$$m^2=(ux+5vy)^2+5(uy-vx)^2=(ux-5vy)^2+5(uy+vx)^2.$$

Verder geldt $(ux+5vy)(ux-5vy)=u^2x^2-25v^2y^2 \equiv u^2x^2+5v^2x^2 \equiv 0 \pmod{m}$.

Dus m is deelbaar op tenminste een der factoren ux+5vy en ux-5vy. Zonder de algemeenheid te schaden mogen wij aannemen dat m deelbaar is op ux+5vy (anders vervange men v door -v). Dan heeft men

$$1 = A^2 + 5B^2 \text{ met } A = \frac{ux+5vy}{m} \; ; \; B = \frac{uy-vx}{m},$$

waarbij A en ook B geheel zijn. Dus $A=\pm 1$, $B=0$, d.w.z.

$$ux + 5vy = \pm m, \quad uy = vx.$$

Dan geldt $\pm my = uxy + 5vy^2 = vx^2+5vy^2=vm$, dus $v=\pm y$, in strijd met de onderstelling. Het getal m is dus samengesteld.

Een analoge redenering voor splitsingen van het type x^2+7y^2 $(x>0,\ y>0)$ leert ons, dat elk priemgetal, dat $\equiv 1,9$ of $25 \pmod{28}$ is, splitsbaar is en verder dat elk samengesteld getal, dat $\equiv 1,9$ of $25 \pmod{28}$ is en dat alleen maar priemdelers bezit, die $\equiv 1,9,11,15,23$ of $25 \pmod{28}$ (d.w.z. $\equiv 1,9$ of $11 \pmod{14}$) zijn, eveneens splitsbaar is. Het blijkt, dat men hier zelfs iets verder kan gaan: elk priemgetal $\equiv 1,9$ of $11 \pmod{14}$ is nl. splitsbaar.

De priemgetallen $\equiv 1,9$ of $25 \pmod{14}$ zijn op slechts één wijze splitsbaar.

Tot slot maken wij nog enige opmerkingen over enkele typen van algebraïsche getallen en de daarbij behorende ringen.

De beschouwde soorten getallen zijn bijzonderegevallen van het algemene type $z=\frac{a+b\sqrt{n}}{c}$ met gehele a,b,c ($c>0$) en n en quadraatvrije n. Dergelijke getallen die kennelijk aan een vierkantsvergelijking met gehele coëfficiënten voldoen, nl. aan

$$(cz-a)^2-b^2n = 0$$

noemt men geheel algebraïsch als die vierkantsvergelijking van het type $z^2+Az+B=0$ is met gehele A en B. Voor ons betekent dit, dat $c^2|2ac$; $c^2|a^2-b^2n$. De eerste relatie leert $c|a$ of $c=2\not|a$. Als $c|a$ heeft men $c^2|b^2n$ en, omdat n quadraatvrij is, $c|b$, dus $z=x+y\sqrt{n}$ met gehele x en y. Is echter $c=2$ en a oneven, dan is $4|a^2-b^2n$, dus b^2n oneven. Wegens $a^2\equiv 1 \pmod 4$, $b^2\equiv 1 \pmod 4$ moet dan ook gelden $n\equiv 1 \pmod 4$, dus $z=\frac{a+b\sqrt{n}}{2}$ met $4|n-1$, $2|a-b$. Men kan dan ook schrijven $z=u+v(\frac{1}{2}+\frac{1}{2}\sqrt{n})$ met gehele u en v. Beide typen schrijven wij in de vorm $x+y\sqrt{n}$, waarbij x en y noodzakelijk geheel zijn als $n\equiv 2$ of $3 \pmod 4$ is en in het geval, dat $n\equiv 1 \pmod 4$ is, 2x en 2y en x-y geheel moeten zijn.

Neemt men als norm van $z=x+y\sqrt{n}$ de uitdrukking $N_z=|x^2-y^2n|$, dan is die onder alle omstandigheden geheel en niet negatief; $N_z=0$ impliceert $z=0$ (ga dat na!).

Wij sommen nu een paar gevallen op.

Het geval $n=-1$ levert de ring van Gauss, waarin de hoofdstelling over de ontbinding in priemfactoren geldt. Ook bij $n=-2$ is de bijbehorende ring Euclidisch (zie boven).

Voor $n=-3$ heeft men de ring van Eisenstein, waarin eveneens de hoofdstelling geldt.

Voor $n=-5$ is dat niet het geval (b.v. $2.3=(1+\sqrt{-5})(1-\sqrt{-5})$). Het is bewezen dat de enige ontbindingsringen van het beschouwde type met negatieve n die ringen zijn, waarbij -n gelijk is aan 1,2,7, 11,19,43,67 en 163 en ten hoogste verder nog één. De enige waarbij een Euclidische algorithme geldt, zijn die met $-n=$ 1,2,3,7 en 11.

Voor positieve n ligt de situatie geheel anders. Het is alleen al van belang om eens naar eenheden te zoeken.

Wij nemen als voorbeeld het geval $n=2$ en bepalen alle eenheden van het type $x+y\sqrt{2}$, dus alle x en y met $x^2-2y^2=\pm 1$. En passant houdt dit in dat wij een zeer speciaal type vergelijkingen oplossen, genoemd vergelijking van Pell (ten onrechte) of Fermat (vrij ongebruikelijk).

Het is duidelijk dat met $x+y\sqrt{2}$ ook $x-y\sqrt{2}$, $-x+y\sqrt{2}$ en $-x-y\sqrt{2}$ eenheden zijn, zodat wij ons zullen beperken tot de gevallen dat $x>0$, $y>0$ (de gevallen $x=0$ resp. $y=0$ zijn gemakkelijk direct uit te zoeken).

Kennelijk is $\varepsilon=1+\sqrt{2}$ een eenheid. Ook zijn alle getallen ε^n bij natuurlijke n eenheden. Het zijn trouwens de enige positieve eenheden $\neq 1$. Immers, stel $u+v\sqrt{2}$ is een eenheid. Wegens $\lim \varepsilon^n=\infty$ is er een natuurlijke n met $\varepsilon^n < u+v\sqrt{2} < \varepsilon^{n+1}$, dus $1 < x+y\sqrt{2} < \varepsilon$, waarbij $x+y\sqrt{2}=(u+v\sqrt{2})\,\varepsilon^{-n}$ ook een eenheid is. Uit $1 < x+y\sqrt{2}$ volgt in de onderstelling $x>y\sqrt{2}$ de relatie $x-y\sqrt{2} < x^2-2y^2=1$, dus $2x < 1+\varepsilon < 3$, dus $x=1$, dus $y\sqrt{2} < \sqrt{2}$, dus $y=0$ tegen de onderstelling. Is echter $x<y\sqrt{2}$, dan geldt $2x<\varepsilon<2$, dus $x=0$, eveneens tegen de onderstelling. Behalve de getallen ε^n is er dus geen positieve eenheid $\neq 1$. Alle eenheden blijken dan van de gedaante $\pm\varepsilon^n$ (n willekeurig geheel te zijn).

Soortgelijke overwegingen gelden bij andere dergelijke ringen. Bij $n=3$ b.v. zijn alle eenheden van de gedaante $\pm(2+\sqrt{3})^n$, bij $n=5$ van de gedaante $\pm(\frac{1}{2}+\frac{1}{2}\sqrt{5})^n$.

Men heeft nagegaan, dat bij positieve n de enige ringen, waarbij een Euclidische algorithme geldt, die zijn met $n=2,3,5,6,7,11,13,17,19,21,29,33,37,41,57$ en 73. Hoewel bij $n=23$ geen Euclidische algorithme geldt, blijkt de ring der getallen $x+y\sqrt{23}$ (x en y geheel) wel een ontbindingsring te zijn.

Opgave. Ontbind in factoren in de betreffende ringen:

$$11+13i\ ;\quad 11+13\sqrt{2}\ ;\quad 11+13\sqrt{-2}\ ;\quad \frac{13}{2}+\frac{11}{2}\sqrt{-3}\ .$$

Bepaal alle gehele oplossingen (x,y) van de vergelijking $x^2-3y^2=4$.

§ 5. Splitsing in vier quadraten.

Wij bewijzen in deze paragraaf de stelling, dat elk natuurlijk getal de som is van vier quadraten van gehele getallen.

Hiertoe hebben wij enige hulpresultaten nodig.

Hulpstelling 1.

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

met
$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$$
$$z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3$$
$$z_3 = x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2$$
$$z_4 = x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1 .$$

Het bewijs wordt geleverd door uitcijferen (of met behulp van de theorie der quaternionen).

Gevolg. Is eenmaal aangetoond, dat ieder priemgetal de som is van 4 quadraten, dan geldt de bewering ook voor elk samengesteld getal.

Wij behoeven de stelling dus nog slechts aan te tonen voor priemgetallen. Voor p=2 is ze evident ($2=1^2+1^2+0^2+0^2$), zodat ze nog slechts voor oneven priemgetallen p behoeft te worden nagegaan.

Hulpstelling 2. Bij elke oneven ondeelbare p bestaan een x en y met $x^2+y^2+1 \equiv 0 \pmod p$.

Bewijs: Beschouw de $\frac{p+1}{2}$ getallen $u_1, u_2, \ldots$ die voldoen aan

$$0 \leqq u < p \text{ en } u_n \equiv -n^2 \pmod p. \qquad (n=0,1,\ldots,\tfrac{p-1}{2}).$$

Deze zijn allen twee aan twee verschillend.

Beschouw ook de $\frac{p+1}{2}$ getallen $v_1, v_2, \ldots$, die voldoen aan

$$0 \leqq v < p \text{ en } v_m \equiv 1+m^2 \pmod p \qquad (m=0,1,\ldots,\tfrac{p-1}{2}).$$

Ook deze zijn twee aan twee verschillend.

Omdat er in totaal p+1 getallen u en v zijn, welke slechts een der p waarden $0,1,\ldots,p-1$ kunnen aannemen, moeten er ten minste twee zijn, die gelijk zijn. Dit impliceert, dat er m en n zijn met $u_n=v_m$, dus met $1+m^2+n^2 \equiv 0 \pmod p$. Q.e.d.

Opmerking: Men heeft ook nog $1+m^2+n^2 \leqq 1+\frac{1}{2}(p-1)^2 < p^2$.

Thans bewijzen wij in navolging van Euler de hoofdstelling voor oneven priemgetallen p.
Bij zo'n p bestaan op grond van de tweede hulpstelling gehele m en n met $1+m^2+n^2=kp$. Op grond van de opmerking geldt ook nog $k<p$. Het getal kp is dus te schrijven als som van vier quadraten. Er bestaat dan een kleinste positief veelvoud ap van p dat ook de som is van vier quadraten,

$$ap = x_1^2 + x_2^2 + x_3^2 + x_4^2 .$$

Voor het getal a geldt verder $0<a\leqq k<p$.
Kies nu $y_i \equiv x_i (\mathrm{mod}\ a)$ met $|y_i| \leqq \frac{a}{2}$ $(i = 1,2,3,4)$.
Dan geldt $y_1^2+y_2^2+y_3^2+y_4^2 \equiv x_1^2+x_2^2+x_3^2+x_4^2 \equiv 0 (\mathrm{mod}\ a)$,
dus

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = ab.$$

Kennelijk geldt $ab \leqq 4$. $\frac{1}{4}a^2 = a^2$, dus $0 \leqq b \leqq a$.
Wij onderscheiden nu 3 gevallen.

1^o: $b=a$. Dan geldt $y_1=y_2=y_3=y_4=\frac{a}{2}$, dus a is even en van de vier grootheden x_1,x_2,x_3 en x_4 hebben twee stel dezelfde pariteit, d.w.z. (na eventueel de nummering dezer grootheden te hebben gewijzigd) $x_1 \equiv x_2 (\mathrm{mod}\ 2)$, $x_3 \equiv x_4 (\mathrm{mod}\ 2)$.
Maar dan geldt

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

in strijd met de minimaliteit van a.

2^o: $b<a$. Overgaande op de in hulpstelling 1 genoemde grootheden z_i vindt men nu

$$a^2pb = z_1^2 + z_2^2 + z_3^2 + z_4^2.$$

Hierbij is

$$z_1 = x_1y_1+x_2y_2+x_3y_3+x_4y_4 \equiv x_1^2+x_2^2+x_3^2+x_4^2 \equiv 0 (\mathrm{mod}\ a)$$

en evenzo $z_2 \equiv z_3 \equiv z_4 (\mathrm{mod}\ a)$, dus

$$pb = u_1^2+u_2^2+u_3^2+u_4^2 \text{ met } au_i = z_i \quad (i=1,2,3,4),$$

wederom in strijd met de minimaliteit van a.

3^{o}: $b=0$, dus $y_1=y_2=y_3=y_4=0$, dus $a \mid x_i$ $(i=1,2,3,4)$.
Dan is $a^2 \mid x_1^2+x_2^2+x_3^2+x_4^2=ap$, dus $a \mid p$. Wegens $a<p$ is dan $a=1$.
Hiermede is de stelling bewezen.

Wij geven nog een toepassing van het gevondene.
Daarbij maken we gebruik van weer een andere identiteit van Euler

$$6(a^2+b^2+c^2+d^2)^2 = (a+b)^4+(a-b)^4+(c+d)^4+(c-d)^4 + (a+c)^4+(a-c)^4+(b+d)^4+(b-d)^4 + (a+d)^4+(a-d)^4+(b+c)^4+(b-c)^4,$$

waarvan het bewijs eveneens door nacijferen gemakkelijk te leveren is.

Zij nu m een willekeurig natuurlijk getal.
Stel $m=6n+r$ $(0 \leq r \leq 5)$. Het natuurlijke getal r is de som van ten hoogste 5 vierde machten $(1^4+1^4+1^4+1^4+1^4)$. Het getal n is dan volgens het bovenstaande de som van ten hoogste vier quadraten $x_1^2+x_2^2+x_3^2+x_4^2$. Eveneens volgens het bovenstaande is x_1 te schrijven als som van ten hoogste 4 quadraten, dus op $6x_1^2 = 6(a_1^2+b_1^2+c_1^2+d_1^2)^2$ is de nieuwe identiteit van Euler van toepassing. Deze leert ons dat $6x_1^2$ te schrijven is als som van ten hoogste 12 vierde machten. Hetzelfde geldt voor $6x_2^2, 6x_3^2, 6x_4^2$, zodat $6n$ de som is van ten hoogste 48 vierde machten en het getal m zelf van ten hoogste $48+5=53$ vierde machten.

In het bovenstaande is voor r genomen een der waarden 0,1,2,3,4 of 5. Zou men n zo bepalen, dat r een der waarden 0,1,2,81, 16 of 17 is (welke allen de som van ten hoogste 2 vierde machten zijn) - dit kan slechts als $m \geq 76$ is - dan ziet men dat elk natuurlijk getal $m \geq 76$ de som is van ten hoogste $48+2=50$ vierde machten. Voor de getallen $m \leq 75$ verifieert men dit eveneens. Bij gevolg is elk natuurlijk getal de som van ten hoogste 50 vierde machten.

Uit het voorafgaande is zelfs iets te zeggen over het aantal 8^{e} machten dat nodig is om een willekeurig natuurlijk getal voor te stellen. Hiertoe gaat men uit van de identiteit

$$5040(a^2+b^2+c^2+d^2)^4 = 6\sum(2a)^8 + 60\sum(a\pm b)^8 + \sum(2a\pm b\pm c)^8 + 6\sum(a\pm b\pm c\pm d)^8,$$

waarbij met de sommen in het rechterlid symmetrische functies van a,b,c en d worden bedoeld, waarvan één karakteriserende term is aangegeven en bij de dubbele tekens de sommen voor elk der neerge-

schreven tekencombinaties moeten worden genomen.

Stel nu $m=5040n+r$, dan is $0 \leqq r \leqq 5039$. Bij nagaan blijkt r de som van ten hoogste 273 achtste machten te zijn. (Het "ergste" getal is $4863=18.2^8+255.1^8$). Het getal n is de som van ten hoogste 50 vierde machten $u_1^4+\ldots+u_{50}^4$. Elke dezer u_i is de som van vier quadraten $u_{i1}^2+u_{i2}^2+u_{i3}^2+u_{i4}^2$, dus 5040n is de som van 50 termen $5040\,(u_{i1}^2+u_{i2}^2+u_{i3}^2+u_{i4}^2)$, die elk volgens de laatste identiteit de som zijn van ten hoogste $6x4+60x12+48+6x8=840$ achtste machten zijn. Bij gevolg is m de som van ten hoogste $50x840+273=42273$ achtste machten. In feite is op dit resultaat heel wat af te dingen; in plaats van met 42273 achtste machten kan men - zoals met verdergaande hulpmiddelen is bewezen - zelfs toe met 279 achtste machten.

§ 6. Het vermoeden van Fermat.

Aan de Franse wiskundige Fermat wordt de bewering toegeschreven, dat hij een bewijs zou hebben gevonden van de stelling, dat de relatie $x^n+y^n=z^n$ onoplosbaar is voor natuurlijke x,y,z en n-2, d.w.z. dat voor natuurlijke x,y,z en n de relatie slechts voor n=1 en 2 oplosbaar is.

Voor n=1 is dit triviaal. Oplossingen voor n=2 vindt men als volgt. Uit $x^2+y^2=z^2$ volgt allereerst, dat als (x,y,z)=1 is, z oneven is en één der getallen x en y even is. Zonder de algemeenheid te schaden mogen wij aannemen 2|x. Dan heeft men $\frac{z-y}{x} = \frac{x}{z+y}$. Stelt men deze breuken gelijk aan $\frac{a}{b}$ (met (a,b)=1 en kennelijk a < b), dan vindt men

$$ax = bz - by, \quad bx = az + ay ,$$

dus $x:y:z = 2ab : (b^2-a^2) : (a^2+b^2)$.

Om te bereiken dat $2ab$, b^2-a^2, a^2+b^2 een onvereenvoudigbaar drietal vormen (d.w.z. een geheel drietal met GGD=1) is het nodig dat

$$(2,b^2-a^2)=1 , \quad (a,b^2-a^2)=1 , \quad (b,b^2-a^2)=1 ,$$

dus allereerst (a,b)=1 en verder $2 \nmid b^2-a^2$, d.w.z. a en b moeten ongelijke pariteit bezitten.

Voorbeeld.

a	b	x	y	z
1	2	4	3	5
2	3	12	5	13
1	4	8	15	17
3	4	24	7	25
2	5	20	21	29
4	5	40	9	41
1	6	12	35	37
5	6	60	11	61
2	7	28	45	53
4	7	56	33	65
6	7	84	13	85

De getallen x,y en z zijn de lengten der zijden van zgn. Pythagoreïsche driehoeken, dat zijn rechthoekige driehoeken met drie gehele zijden.

Opmerking. Door aaneenvoeging van twee Pythagoreïsche driehoeken vindt men driehoeken met gehele zijden en oppervlakte (zgn. Heronische driehoeken). Het procédé levert trouwens alle dergelijke driehoeken op.

Wij bewijzen nu, dat voor $n=4$ de relatie van Fermat onoplosbaar is. Dit geschiedt door het nog iets verdergaande resultaat te bewijzen, dat de relatie $x^4+y^4=z^2$ onoplosbaar is met gehele positieve x,y en z.

Stel nl. dat er wel een dergelijk drietal grootheden te vinden was. Kennelijk moet dan, als wij weer $(x,y,z)=1$ onderstellen, een der grootheden x en y even zijn; laat dit weer x zijn. Op grond van het voorafgaande moeten er gehele a en b zijn met $a < b$, $(a,b)=1$ en

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

waarbij a en b ongelijke pariteit bezitten.

Wegens $y^2+a^2=b^2$ is dan a even en b oneven, dus er bestaan -- alweer volgens het voorafgaande -- gehele c en d met

$$c < d,\ (c,d)=1 \text{ en } a=2cd,\ y=d^2-c^2,\ b=d^2+c^2.$$

Anderzijds leert $x^2=2ab$ met $(a,b)=1$ en $2|a$ dat er gehele e en f zijn met $a=2e^2$, $b=f^2$, dus $f^2=c^2+d^2$. Uit $2e^2=a=2cd$ en $(c,d)=1$ volgt $c=g^2$, $d=h^2$, dus $f^2=g^4+h^4$. Verder is $f \leqq f^2=b \leqq b^2 < z$, zodat een oplossing (x,y,z) tevens een oplossing (g,h,f) zou opleveren met $f < z$. Waar dit tot een contradictie voert, is er geen oplossing van het gewenste type van $x^4+y^4=z^2$ en de relatie van Fermat is dus onoplosbaar voor $n=4$.

Om de onoplosbaarheid der relatie van Fermat voor willekeurige exponent n aan te tonen, is het nu voldoende dit te doen voor ondeelbare n. Immers is $n > 2$ en bevat n een oneven priemdeler p, dan zou een oplossing der relatie voor n tevens een voor de priemexponent p opleveren. Is $n > 2$ en bevat n slechts de priemdeler 2, dus $n=2^r$ met $r \geqq 2$ dan voert een oplossing der relatie voor n tot een met de exponent 4, maar dit is, zoals wij reeds zagen, uitgesloten.

Wij beschouwen dus nu verder de relatie $x^p+y^p=z^p$ met oneven priemexponent p en $(x,y,z)=1$.

Een gemeenschappelijke priemfactor q van $x+y$ en $\frac{x^p+y^p}{x+y} = V(x,y)$

voldoet aan $y \equiv -x \pmod q$, dus aan

$$0 \equiv x^{p-1} - x^{p-2}y + \ldots + y^{p-1} \equiv px^{p-1} \pmod q .$$

Was $q \mid x$, dan $q \mid y$, want $q \mid x+y$. Dit is in strijd met $(x,y,z)=1$. De enige mogelijkheid is dus $q=p$. Dan is dus $p \mid z$. Analoge beschouwingen gelden voor $z^p - y^p$ en $z^p - x^p$.

Wij onderscheiden nu twee gevallen.

I. $p \nmid xyz$.

II. p is deelbaar op precies één der grootheden x, y en z.

In geval I heeft men $z^p = (x+y)V(x,y)$ en $(x+y, V(x,y)) = 1$. Er bestaan dus gehele c en C met $(c,C)=1$, $x+y=c^p$, $V(x,y)=C^p$, en $z=cC$. Evenzo vindt men het bestaan van gehele a, A, b en B met

$$x=aA \ , \ z-y=a^p, \ (a,A)=1;$$
$$y=bB \ , \ z-x=b^p, \ (b,B)=1.$$

Zij nu r een priemdeler van C, dus van z. Dan heeft men $a^p \equiv -y \pmod r$ $b^p \equiv -x \pmod r$, dus $a^{p^2} + b^{p^2} \equiv -x^p - y^p = z^p \equiv d \pmod r$. Verder geldt $a^p + b^p = 2z - x - y \equiv -x - y = -c^p \not\equiv 0 \pmod r$, want $(c,C)=1$. Uit de relaties

$$a^{p^2} + b^{p^2} \equiv 0 \pmod r, \quad a^p + b^p \not\equiv 0 \pmod r$$

volgt nu, dat $r \equiv 1 \pmod{p^2}$. Immers $r \nmid b$ (anders $r \mid x$ en $(x,y,z) \neq 1$), dus $b^{-1} \pmod r$ bestaat en voor $d \equiv -ab^{-1} \pmod r$ heeft men

$$d^{p^2} \equiv 1 \pmod r, \quad d^p \not\equiv 1 \pmod r.$$

Zij e de exponent van d mod r. Kennelijk is $e \mid r-1$. Wegens $e \mid p^2$, $e \nmid p$ geldt $e = p^2$, dus $p^2 \mid r-1$ en $r \equiv 1 \pmod{p^2}$.

Verder volgt nu uit dit resultaat, dat voor iedere priemdeler r van C geldt, dat $C \equiv 1 \pmod{p^2}$, dus $z = cC \equiv c \pmod{p^2}$ en $z^p \equiv c^p = x+y \pmod{p^3}$. Evenzo $x^p \equiv z-y \pmod{p^3}$ en $y^p \equiv z-x \pmod{p^3}$, dus $0 = z^p - x^p - y^p \equiv 2x+2y-2z \pmod{p^3}$ en $z \equiv x+y \pmod{p^3}$. Tenslotte vindt men dan

$$z^p \equiv z \pmod{p^3}, \text{ dus } z^{p-1} \equiv 1 \pmod{p^3} \text{ en evenzo}$$
$$x^{p-1} \equiv 1 \pmod{p^3}, \ y^{p-1} \equiv 1 \pmod{p^3} .$$

Het geval $p=3$ is hiermede iets nader te behandelen. Onderstel $3 \nmid xyz$. Dan heeft men dus $x^2 \equiv y^2 \equiv z^2 \equiv 1 \pmod{27}$. Dus elk der getallen x, y en z kan slechts $\pm 1 \pmod{27}$ zijn. Nu heeft men echter

$z \equiv z^3 = x^3 + y^3 \equiv x+y \pmod{27}$, zodat de onderstelling $3 \nmid xyz$ tot een contradictie voert.

In geval II is p deelbaar op precies een der grootheden x,y en z. Wij onderstellen $p|x$ (het geval $p|y$ gaat geheel analoog en $p|z$ bijna analoog). Laat het getal $x=aA$ precies s factoren p bevatten en het getal z-y precies t stuks. Uit $z=y+p^t u$ (met $p \nmid u$) volgt dan $z^p \equiv y^p + p^{t+1} y^{p-1} u \pmod{p^{2t+1}}$, dus $x^p = z^p - y^p$ bevat precies t+1 factoren p en $t+1=sp$, $t=sp-1$, $z-y=p^{sp-1}u$, waarbij evenals vroeger wordt gevonden dat u de gedaante a^p bezit.

De vorm $V(z,-y)$ bevat dan precies 1 factor p en bezit de gedaante pA^p. De verdere resultaten van het onderzoek bij I leren dat men heeft:

$$x = aAp^s, \quad z-y=p^{ps-1}a^p, \quad (a,A)=1$$
$$y = bB, \quad z-x=b^p, \quad (b,B)=1$$
$$z = cC, \quad x+y=c^p, \quad (c,C)=1.$$

Voor iedere priemdeler r van A heeft men, evenals hierboven $r|x$, dus

$$b^p - c^p \equiv z-y=p^{ps-1}a^p \not\equiv 0 \pmod{r};$$
$$b^{p^2} - c^{p^2} \equiv z^p - y^p = x^p \equiv 0 \pmod{r},$$

dus $r \equiv 1 (p^2)$. Bijgevolg geldt $A \equiv 1 \pmod{p^2}$, $A^p \equiv 1 \pmod{p^3}$. Verder heeft men nog $z \equiv y \pmod{p^{ps-1}}$, dus

$$pA^p = V(z,-y) = z^{p-1} + \ldots + y^{p-1} = pz^{p-1} \pmod{p^{ps-1}}, \text{ dus}$$
$$A^p \equiv z^{p-1} \pmod{p^{ps-2}}.$$

Als nu $ps-2 \geq 3$ (wat zeker optreedt bij $p \geq s$), geldt $z^{p-1} \equiv A^p \equiv 1 \pmod{p^3}$, en evenzo $y^{p-1} \equiv 1 \pmod{p^3}$.

Diverse verdergaande hulpmiddelen leren ons voorts dat voor iedere priemdeler r van x,y en z geldt $r^{p-1} \equiv 1 \pmod{p^2}$. Waar kennelijk r=2 mag worden genomen, geldt dus $2^{p-1} \equiv 1 \pmod{p^r}$ (1^e stelling van Furtwängler). Een tweede stelling van Furtwängler leert o.a. ook nog dat moet gelden $3^{p-1} \equiv 1 \pmod{p^r}$.

Eerstgenoemde congruentie is door Beyer onderzocht. Als kleinste oplossingen vond hij p=1093, p=3511. Geen dezer getallen voldoet aan de tweede (die overigens wel vervuld wordt door p=11).

Met nog weer andere hulpmiddelen beweren H.D. en Emma Lehmer, dat in geval I geldt $p \geq 253747889$; in geval II heeft men gevonden $p \geq 619$.