STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZC 22

Colloquium recurrente rijen.

H.J.A.Duparc.

1953

ZC 22

Colloquium Recurrente Rijen.

1952/53

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

1952-1953

Colloquium Recurrente Rijen 1952/53

Hoofdstuk I. Algemeen overzicht

door

H.J.A. Duparc.

§ 1. Inleiding.

In dit colloquium onderzoeken wij het gedrag van bepaalde recurrente rijen. Een recurrente rij is een rij van getallen $u_0, u_1, u_2, \ldots$, waarbij elk element u_n der rij op een voorgeschreven wijze is bepaald door de elementen $u_0, u_1, \ldots, u_{n-1}$ der rij. In het speciale geval dat elk element u_n door de waarden der elementen $u_{n-1}, \ldots, u_{n-k}$ wordt bepaald, waarbij k een vast natuurlijk getal is, is de rij eerst vastgelegd als de waarden der eerste k elementen $u_0, u_1, \ldots, u_{k-1}$ gegeven zijn. Iedere keuze dier k gegeven waarden levert een recurrente rij op. In het vervolg zullen wij ons vrijwel steeds bezighouden met rijen van gehele getallen.

Voorbeelden:

1. $u_0 = 0$; $u_n = u_{n-1} + 1$. Dan is $u_n = n$. Hierbij is het bovengenoemde getal $k = 1$.
2. $u_0 = a$; $u_n = u_{n-1} + v$. Dan is $u_n = a + nv$ (rekenkundige rij).
3. $u_0 = a$; $u_n = ru_{n-1}$. Dan is $u_n = ar^n$ (meetkundige rij).
4. $u_0 = 1$; $u_n = \sum_{h=0}^{n-1} u_h$. Hierbij is het bovengenoemde getal k niet vast. Men heeft $u_n = 2^{n-1}$ voor $n > 0$.
5. $u_0 = 2$; $u_n = u_{n-1}^2$. Bij deze rij is $u_n = 2^{2^n}$.
6. $u_0 = 1$; $u_n = nu_{n-1}$. Hier is $u_n = n!$
7. $u_0 = 0$, $u_1 = 1$; $u_n = au_{n-1} + bu_{n-2}$. Hierbij is het getal $k = 2$. Men heeft $u_2 = a$; $u_3 = a^2 + b$, $u_4 = a^3 + 2ab$, ... Een algemene voorstelling van u_n als functie van n geven wij later.
8. $u_0 = 2$; $u_n = u_{n-1}^2 - 2$. Hierbij is $u_n = 2$ voor alle n.
9. $u_0 = 2$; $u_n = u_{n-1}^{u_{n-1}}$. De rij luidt $2, 4, 256, 2^{2048}, \ldots$
10. $u_0 = 2$; $u_n = 2^{u_{n-1}} - 1$. De rij luidt $2, 3, 7, 127, 2^{127}-1, \ldots$

Bij een aantal der opgesomde rijen is $\lim_{n\to\infty} u_n = \infty$. Wij hebben in het vervolg speciale belangstelling voor het karakter der rijen mod m, waarbij m een vast gegeven natuurlijk getal voorstelt. Hieronder verstaan

wij de kleinste niet negatieve rest, die ontstaat bij deling der elementen der rij door m. Men zegt ook wel, dat de oorspronkelijke rij gereduceerd is tot mod m. Aangezien een mod m gereduceerde rij van natuurlijke getallen slechts uit de getallen $0,1,\ldots,m-1$ kan bestaan, moet ten minste een dezer m getallen oneindig vaak in de gereduceerde rij optreden. Dat niet elk der elementen $0,1,\ldots,m-1$ oneindig vaak optreedt, blijkt o.a. bij de 8^e rij, waarbij voor iedere natuurlijke $m > 2$ de gereduceerde rij slechts uit elementen 2 bestaat. Voor $m = 2^h$ (h vast) is van zekere door h bepaalde n iets dergelijks het geval bij de 10^e rij. Bij reductie mod 7 levert de 5^e rij de oscillerende rij $2,4,2,4,\ldots$ op.

Wij merken op dat als k vast is en elk element u_n der rij alleen door $u_{n-1},\ldots,u_{n-k}$ bepaald wordt, maar verder niet van n afhangt en als een rij van k opeenvolgende elementen zich in een recurrente rij herhaalt, dit ook het geval is met alle elementen die op de eerstgenoemde k elementen volgen; preciéser geformuleerd, als $a_{h+c} = a_h$ voor $h = 0,1,\ldots,k-1$, dan is $a_{h+c} = a_h$ voor alle natuurlijke h. De bewering volgt door volledige inductie naar h onmiddellijk uit de definitie volgens

$$u_n = f(u_{n-1},\ldots,u_{n-k}) = f(u_{n+c-1},\ldots,u_{n+c-k}) = u_{n+c}.$$

§ 2. Enkele opmerkingen over bepaalde rijen.

In dit colloquium beperken wij ons bijna steeds tot zeer speciale rijen en wel zulke waarbij u_n homogeen lineair en met constante coëfficiënten afhangt van $u_{n-1},\ldots,u_{n-k}$, dus

$$u_n = \sum_{h=1}^{k} a_h u_{n-h}.$$

Speciaal zal worden onderzocht hetgeen bij $k = 1$ en bij $k = 2$ optreedt.

Bij $k = 1$ krijgen wij een rij van het type 3 uit het hierboven gegeven lijstje van voorbeelden. Gaat het om deelbaarheid van de elementen der rij door een getal m, dat geen factoren met a gemeen heeft, dan kunne wij zonder de algemeenheid te schaden ons beperken tot het geval dat $a = 1$ is. Is de G.G.D. van a en m, die men met (a,m) pleegt aan te duiden niet gelijk aan 1, dan is dat geval gemakkelijk terug te brengen op het voorafgaande, zoals wij in hoofdstuk III zullen zien.

Wij beschouwen dus de rij $1,r,r^2,\ldots$. Zij m een gegeven al of niet samengesteld getal. Om na te gaan of het getal 1 optreedt in de mod m gereduceerde rij, dus of een getal $C = C(m)$ bestaat met $r^{C(m)} \equiv 1 \pmod m$, gaat men uit van de ondubbelzinnig bepaalde priemontbinding $m = p_1^{s_1}\ldots p_t^{s_t}$ van m en onderzoekt het karakter der rij modulo elk der priemgetallen $p_1,\ldots,p_t$ en modulo de hiervan vereiste machten. Dit geschiedt nader in hoofdstuk III.

Hier zij reeds de (kleine) stelling van Fermat genoemd, die zegt

dat voor een priemgetal dat niet op r deelbaar is, geldt $r^{p-1} \equiv 1 (\mathrm{mod}\ p)$. Zo heeft men bij de rij 3 met a = 1, r = 2, dus bij de rij 1,2,4,8,... $2^{10} \equiv 1 (\mathrm{mod}\ 11)$, zodat de rij zich mod 11 zeker na 10 stappen herhaalt. Inderdaad luidt de gereduceerde rij 1,2,4,8,5,10,9,7,3,6; 1,2,4,8,... . Het kan zijn dat de rij zich eerder herhaalt, zoals b.v. blijkt bij beschouwing mod 7. Weliswaar is $2^6 \equiv 1 (\mathrm{mod}\ 7)$, zodat de rij zich zeker na 6 stappen herhaalt, maar omdat ook $2^3 \equiv 1 (\mathrm{mod}\ 7)$ herhaalt de rij zich al na 3 stappen. De mod 7 gereduceerde rij luidt dan ook 1,2,4; 1,2,4; ... .

Wij geven thans een voorbeeld van een recurrente rij met k = 2, en wel de rij gedefinieerd door

$$u_0 = 0,\ u_1 = 1;\ u_{n+2} = 2u_{n+1} + u_n.$$

De rij luidt

0,1,2,5,12,29,70,169,408,985,2378,... .

Zoals hierboven reeds werd opgemerkt, herhaalt deze rij zich mod m zeker zodra het paar 0,1 weer optreedt, dus als

$$u_C \equiv 0 (\mathrm{mod}\ m);\quad u_{C+1} \equiv 1 (\mathrm{mod}\ m)$$

is. Beschouwt men de rij mod 5, dan is weliswaar $u_3 \equiv 0 (\mathrm{mod}\ 5)$, maar $u_4 \not\equiv 1 (\mathrm{mod}\ 5)$, zodat $C(5) \neq 3$ is.

Definitie. De kleinste index waarvoor $u_c \equiv 0 (\mathrm{mod}\ m)$ is, noemen we de kleine periode c(m) van m. De kleinste index waarvoor zowel $u_C \equiv 0 (\mathrm{mod}\ m)$ als $u_{C+1} \equiv 1 (\mathrm{mod}\ m)$ is, noemen wij de grote periode C(m). Om iets naders over de getallen c(m) en C(m) te weten te komen, blijkt het merkwaardigerwijze van voordeel te zijn, om, hoewel in het bovenstaande slechts gehele getallen optreden, bepaalde irrationale getallen te beschouwen.

Wij voeren in de wortels ω en $\overline{\omega}$ van de bij de betrekking $u_{n+2} = 2u_{n+1} + u_n$ behorende karakteristieke vergelijking $x^2 - 2x - 1 = 0$. Wegens $\omega^2 = 2\omega + 1$ is elk polynoom in ω met rationale coëfficiënten dan op ondubbelzinnige wijze te schrijven in de gedaante $A\omega + B$, waarbij A en B rationaal zijn. Wij maken van deze opmerking slechts gebruik voor de mononomen ω^n en bewijzen dat de genoemde voorstelling hiervan luidt

$$\omega^n = u_n\omega + u_{n-1}.$$

Om deze relatie die voor n = 1 evident is te bewijzen, merken wij op, dat uit de relatie voor n volgt

$$\omega^{n+1} = \omega(u_n\omega + u_{n-1}) = u_n\omega^2 + u_{n-1}\omega = u_n(2\omega+1) + u_{n-1}\omega =$$
$$= (2u_n + u_{n-1})\omega + u_n = u_{n+1}\omega + u_n,$$

waarmee de relatie door volledige inductie bewezen is.

De getallen $A\omega + B$ (A en B geheel) vormen een commutatieve ring zonder nuldelers, waarin bepaalde deelbaarheidseigenschappen gelden, die wij in het vervolg nodig zullen hebben.

Men definieert, dat $A\omega + B \equiv C\omega + D(\text{mod } m)$ dan en slechts dan als $A \equiv C(\text{mod } m)$ en $B \equiv D(\text{mod } m)$; verder $m \mid A\omega + B$ als $A\omega + B \equiv 0(\text{mod } m)$. Als dan $m \mid A\omega + B$, dan $m \mid (A\omega+B)(E\omega+F)$ voor alle gehele E en F. Immers $m \mid A\omega + B$ is aequivalent met $m \mid A$ en $m \mid B$, zodat er gehele A' en B' bestaan met $A = mA'$, $B = mB'$, dus $A\omega + B = m(A'\omega+B')$. Dan is $(A\omega+B)(E\omega+F) = m(A'\omega+B')(E\omega+F)$, waaruit de bewering volgt.

Dat gewone deelbaarheidseigenschappen niet gelden voor de getallen van de gedaante $A\omega + B$ blijkt uit het volgende voorbeeld. In de ring der gehele getallen volgt voor een priemgetal p uit de relaties $p \mid ab$, $p \nmid a$ dat $p \mid b$ is. Dit geldt niet voor het geval a en b van bovengenoemde gedaante zijn, zoals b.v. blijkt uit

$$7 \mid (\omega+2)(\omega+3) = \omega^2 + 5\omega + 6 = 7\omega + 7.$$

Echter $7 \nmid \omega + 2$ en $7 \nmid \omega + 3$. In hoofdstuk VI wordt dit nader onderzocht om in hoofdstuk VII waar nodig te worden toegepast.

Zonder op dit alles hier in te gaan, kunnen wij hier toch reeds gebruik maken van het invoeren van het bovengenoemde getal ω. Men heeft nl. bij gegeven m dat $\omega^c \equiv u_c(\text{mod } m)$; $\omega^C \equiv 1(\text{mod } m)$. Hieruit volgt reeds dat c een deler is van C. Zij nl. $C = qc + r$ met $0 \leqq r \leqq c - 1$, dan heeft men

$$1 \equiv \omega^C = \omega^{vc+r} \equiv (\omega^c)^v \omega^r \equiv u_c^v \omega^r (\text{mod } m),$$

zodat $\omega^r \equiv u_c^{-v}(\text{mod } m)$ en ω^r dus rationaal is (mod m). Daar c de kleinste positieve exponent is waarvoor ω^c rationaal is mod m, volgt dan uit $0 \leqq r \leqq c - 1$ dat $r = 0$, dus $C = vc$.

Over de getallen C(m), c(m) en v(m) worden in hoofdstuk VII belangrijke eigenschappen afgeleid. Voor een bijzonder geval nl. het geval dat de recurrente rij gegeven is door

$$u_0 = 0;\ u_1 = 1;\ u_n = u_{n-1} + u_{n-2} \text{ (rij van Fibonacci)}$$

geschiedt dit reeds in hoofdstuk V.

In de hoofdstukken II en IV wordt datgene uit de getallentheorie behandeld, dat voor de volgende hoofdstukken onontbeerlijk is.

Hoofdstuk II

H.J.A. Duparc.

Elementaire deelbaarheidseigenschappen van natuurlijke getallen.

In dit hoofdstuk houden wij ons, tenzij anders vermeld wordt, steeds met natuurlijke getallen bezig.

Een priemgetal is een getal, dat geen andere delers bezit, dan het getal 1 en zichzelf. Men is echter gewoon het getal 1 niet onder de priemgetallen te rekenen.

Ieder natuurlijk getal m is in priemfactoren te ontbinden. Men ziet dit het eenvoudigste in door achtereenvolgens te onderzoeken of de getal-

len 2,3,5,... deelbaar zijn op m. Gaat de deling op dan behoeft het onderzoek slecht voor een getal $\prec$ m te geschieden, waarvan bij inductie de mogelijkheid van priemontbinding bekend mag worden ondersteld. Gaat de deling voor geen enkel getal $\prec$ m op, dan bestaat de ontbinding uit de ene factor m zelf. In de praktijk beschikt men nauwelijks over andere methoden om de ontbinding of het priem zijn van een getal te onderzoeken.

Dat een getal slechts op één manier in priemfactoren te ontbinden is, volgt uit de volgende

Hulpstelling 1. Als voor een priemgetal p geldt $p \mid ab$, $p \nmid a$, dan is $p \mid b$. Stel nu dat een getal m twee verschillende priemontbindingen

$$m = p_1^{s_1} \dots p_t^{s_t} = q_1^{r_1} \dots q_u^{r_u}$$

bezat, dan was $q_u \mid m$, dus herhaalde toepassing der hulpstelling leert dat q_u met één der priemgetallen $p_1,\dots,p_t$ moet samenvallen. Als m dus twee verschillende priemontbindingen bezat, was dit ook het geval met een getal $m_1 = \frac{m}{q_u}$, dat $\prec$m is. Zo doorgaande komt men tot een contradictie.

Wij schetsen nu het bewijs der hulpstelling 1.

Allereerst is het duidelijk, dat ieder natuurlijk getal slechts eindig veel delers bezit, dus dat twee natuurlijke getallen slechts eindig veel gemeenschappelijke delers bezitten en dus juist één grootste gemeenschappelijke deler. Is deze = 1, dan noemt men die twee getallen onderling ondeelbaar. Voor het bewijs van hulst. 1 behandelen wij eerst de volgende

Hulpstelling 2. De G.G.D. d van twee natuurlijke getallen m en n is te schrijven als een lineair compositum dier getallen, d.w.z. dat er gehele x en y bestaan met d = mx + ny. Wij bewijzen de stelling door volledige inductie. Voor m = 1, n = 1 is d = 1 en de stelling dus juist. Onderstel nu dat m en n willekeurig gegeven zijn. Zonder de algemeenheid te schaden, mogen wij aannemen $m \geqslant n$. Iedere gemeenschappelijke deler van m en n is ook een gemeenschappelijke deler van m-n en n, en omgekeerd zodat de grootste gemeenschappelijke deler van m en n dezelfde is als die van m-n en n. Dus d = (m-n, n). Bij inductie mag men aannemen, dat er gehele x' en y' bestaan met d = (m-n)x' + ny'. Dus d = mx' + n(y'-x'), waarmee de hulpstelling 2 bewezen is.

Dit resultaat nu geeft ons onmiddellijk het gewenste bewijs van hulpstelling 1. Immers zij d de G.G.D. van p en a. Daar p priem is, is d = 1 of d = p. Daar $p \nmid a$, is d = 1. Volgens hulpstelling 1 bestaan er gehele x en y met 1 = px + ay, dus b = pbx + aby. Wegens $p \mid ab$, is het rechterlid der laatste betrekking deelbaar door p, dus $p \mid b$, waarmee de 1^e hulpstelling bewezen is en dus de ondubbelzinnigheid van priemontbindingen van natuurlijke getallen vast staat.

Wij sommen nu nog een aantal eigenschappen op van congruenties. Bij definitie betekent

$$a \equiv b \pmod{d}$$

dat $d \mid a - b$.

Men ziet onmiddellijk in dat dan voor natuurlijke n geldt $a^n \equiv b^n \pmod{d}$. Verder volgt uit $a \equiv b \pmod{d}$ en $e \equiv f \pmod{d}$ dat $a + e \equiv b + f \pmod{d}$, $a - e \equiv b - f \pmod{d}$, $ae \equiv bf \pmod{d}$. Uit $ac \equiv bc \pmod{d}$ volgt $a \equiv b \pmod{d'}$ met $d' = d = (c,d)$. Gevolg: als $(c,d) = 1$, dan is zelfs $a \equiv b \pmod{d}$.

Hulpstelling 3. Als $(a,b) = 1$, dan bestaat er 1 natuurlijk getal c met $0 < c \leq b - 1$ waarvoor geldt $ca \equiv 1 \pmod{b}$.

Bewijs: Dat er niet meer zulke getallen c zijn, is duidelijk, want had men twee verschillende dergelijke getallen c en c', dan was $c'a \equiv 1 \equiv ca \pmod{b}$. Wegens $(a,b) = 1$ volgt dan uit bovenstaande opmerking dat $c' = c \pmod{b}$, wat echter onmogelijk is wegens $0 < c < b-1$ en $0 < c' < b-1$.

Dat er inderdaad één oplossing te vinden is, blijkt als volgt. Uit $(a,b) = 1$ volgt wegens hulpstelling 2, dat er gehele x en y bestaan met $1 = ax + by$, dus $ax \equiv 1 \pmod{b}$. De rest c bij deling van x door b voldoet dan aan de gewenste relatie.

Men schrijft wel $c \equiv a^{-1} \pmod{b}$ en bedoelt dan met $a^{-n} \pmod{b}$ het getal c^n.

Uit $e \equiv f \pmod{b}$ en $(e,b) = (f,b) = 1$ volgt dan $e^{-1} \equiv f^{-1} \pmod{b}$, dus $e^{-n} \equiv f^{-n} \pmod{b}$.

Hoofdstuk III

H.J.A. Duparc.

§ 1. De rij $u_n = ru_{n-1}$.

Wij beschouwen thans de rij $u_n = ru_{n-1}$. Laat m een willekeurig vast gegeven natuurlijk getal zijn. Wij onderstellen twee gevallen:

1^o: $(u_o,m) = 1$. In dit geval is $u_n \equiv u_o \pmod{m}$ als $r^n \equiv 1 \pmod{m}$, zodat in plaats van de oorspronkelijke rij even goed de rij $1, r, r^2, \ldots$ kan worden beschouwd.

2^o: $(u_o,m) \neq 1$. Zij $(u_o,m) = d$ en $u_o = du_o'$; $m = dm'$. Dan is $(u_o',m') = 1$. Elk element u_n der gegeven rij is dan deelbaar door d, zodat slechts het karakter van de rij $\frac{u_o}{d}, \frac{u_1}{d}, \ldots$ dus van de rij $u_o', ru_o', \ldots$ mod m' dient te worden onderzocht. Wegens $(u_o',m') = 1$ leidt dit tot het onderzoek van een rij van het type 1^o, zodat wij ons in het vervolg daartoe kunnen beperken.

Wij bewijzen nu allereerst de stelling van Fermat, die zegt dat voor ieder getal r dat niet door een priemgetal p deelbaar is, geldt $r^{p-1} \equiv 1 \pmod{p}$.

Wij bewijzen $r^p \equiv r \pmod{p}$ een relatie waaruit het genoemde resultaat

volgt en die voor elke natuurlijke r geldt.

Voor r = 1 is die bewering juist en als zij geldt voor r = n, dan heeft men wegens de binomiaalformule van Newton $(n+1)^p \equiv n^p+1 \equiv n+1 \pmod p$ wegens inductieonderstelling, waarmee de bewering bewezen is.

Stelling. Als $r^u \equiv 1 \pmod p$ en $r^v \equiv 1 \pmod p$, dan is $r^{(u,v)} \equiv 1 \pmod p$. Immers volgens hulpstelling 2 bestaan er gehele x en y met $(u,v) = ux + vy$, dus $r^{(u,v)} = r^{ux+vy} = (r^u)^x (r^v)^y \equiv 1 \pmod p$.

Definitie. Zij $(r,p) = 1$. Dan noemt men de exponent van r mod p het kleinste natuurlijke getal c waarvoor $r^c \equiv 1 \pmod p$.

Als verder $r^e \equiv 1 \pmod p$, dan is $c \mid e$. Immers zij $e = qc + t$ met $0 \leqq t \leqq c-1$, dan is $1 \equiv r^e = (r^c)^q r^t \equiv r^t \pmod p$, dus in verband met de definitie van c is $t = 0$, derhalve $e = qc$.

Gevolg. In verband met $r^{p-1} \equiv 1 \pmod p$ heeft men $c \mid p-1$.

Definitie. r heet primitieve wortel van p als $c = p-1$.

Toepassing. Om $2^{11}-1$ in factoren te ontbinden, merken wij op, dat als $p \mid 2^{11}-1$, dus $2^{11} \equiv 1 \pmod p$, het getal 11 de exponent van 2 mod p is. Uit $2^{p-1} \equiv 1 \pmod p$ volgt dan $11 \mid p-1$.

Men behoeft dus slechts priemgetallen p te proberen die een 22-voud + 1 zijn. Inderdaad voldoet p = 23 en heeft men $2^{11}-1 = 23.89$.

Is eenmaal de exponent $c = c(p)$ van het getal r mod p bepaald, dan kan het gebeuren dat r^c-1 deelbaar is door p^2 (b.v. r = 7, p = 5).

Zij n de grootste exponent met $p^n \mid r^c-1$. Dan is $c(p^h) = c(p)$ voor $h \leqq n$. Om $c(p^h)$ voor $h > n$ te bepalen, bewijzen wij de volgende

Hulpstelling 1. Als p een oneven priemgetal is en als $p^k \mid r^c-1$, maar $p^{k+1} \nmid r^c-1$, dan geldt $p^{k+1} \mid r^{pc}-1$ en $p^{k+2} \nmid r^{pc}-1$.

Bewijs. Uit het gegeven volgt $r^c = 1 + p^k w$ met $p \nmid w$. Dus $r^{pc} = (1+p^k w)^p \equiv 1 + p^{k+1} w \pmod{p^{k+2}}$, waaruit wegens $p \nmid w$ volgt, dat $p^{k+1} \mid r^{pc}-1$ en $p^{k+2} \nmid r^{pc}-1$.

Hieruit volgt nu onmiddellijk voor $h \geqq n$, dat $c(p^h) = p^{h-n} c(p^n) = p^{h-n} c$ voor elk oneven priemgetal p.

Om ook voor het geval p = 2 een dergelijk resultaat te verkrijgen, merken wij op, dat de hulpstelling 1 ook geldt voor p = 2 mits $k \geqq 2$ zij.

Voor p = 2 vinden wij dan het volgende:
Zij c(4) de exponent van r mod 4. Zij n de grootste exponent met $2^n \mid r^c-1$. Dan is $c(2^h) = c(4)$ voor $1 < h \leqq n$ en $c(2^h) = 2^{h-n} c(4)$ voor $h > n$.

Uiteraard is de waarde van c(4) onmiddellijk uit het karakter van r te bepalen. Is nl. $r \equiv 1 \pmod 4$, dan is $c(4) = 1$; is echter $r \equiv 3 \pmod 4$, dan is $c(4) = 2$.

Nu de exponent van samengestelde getallen van het type p^h bepaald is, kunnen wij ook gemakkelijk die van een willekeurig getal m bepalen.

Zij $m = p_1^{s_1}\ldots p_u^{s_u}$. Als e de exponent e(m) is, is $p_i^{s_i} \mid r^e-1$, dus $c(p_i^{s_i}) \mid e$. Kennelijk is dus e het K.G.V. $\{c(p_1^{s_1}),\ldots,c(p_u^{s_u})\}$ der getallen $c(p_1^{s_1}),\ldots,c(p_u^{s_u})$. Een echte deler d van e voldoet nl. niet omdat daarbij een getal j te vinden is met $c(p_j^{s_j}) \nmid d$, dus $p_j^{s_i} \nmid r^d-1$, dus $m \nmid r^d-1$.

Keren wij thans ter g tot de rij

$$u_0 = 1,\ u_{n+1} = ru_n.$$

Het is duidelijk dat voor een m met (r,m) = 1 uit $u_i \equiv u_j \pmod m$ volgt $u_{i+1} \equiv u_{j+1} \pmod m$ en omgekeerd.

Zij nu e het kleinste natuurlijke getal waarvoor $u_e \equiv 1 \pmod m$. Het getal e is dan het kleinste getal met $r^e \equiv 1 \pmod m$, dus e = c(m) in de zoëven gebruikte notatie. Het is verder duidelijk, dat $u_i \equiv u_j \pmod m$ dan en slechts dan als $i \equiv j \pmod{c(m)}$. De rij heeft dus de periode c(m).

Het geval dat $(r,m) \neq 1$ is, brengen wij op het voorafgaande terug. Stel (r,m) = d, r = dr', m = dm'; dan is (r',m') = 1. Alle elementen $u_1,u_2,\ldots$ zijn dan deelbaar door d. Het gaat dus slechts om het gedrag der rij $\frac{u_1}{d}, \frac{u_2}{d}, \frac{u_3}{d}, \ldots$ dus van de rij r', rr', r^2r', ... mod m'. Wegens m' < m mogen wij bij inductie dit bedrag bekend onderstellen en bepalen dan daaruit het gedrag der oorspronkelijke rij mod m.

Wij kunnen het gevondene ook anders verkrijgen. Zij weer d = (r,m). Laat d slechts door de priemfactoren $p_1,p_2,\ldots,p_u$ deelbaar zijn. Stel $r = p_1^{s_1}\ldots p_u^{s_u}r''$ met (d,r") = 1; $m = p_1^{t_1}\ldots p_u^{t_u}m''$ met (d,m") = 1. Zij f het kleinste natuurlijke getal $\geqslant \frac{t_1}{s_1},\ldots,\frac{t_u}{s_u}$. Het is dan duidelijk dat voor $n \geqslant f$ de elementen $u_n = r^n$ der oorspronkelijke rij deelbaar zijn door $p_1^{t_1}\ldots p_u^{t_u}$. Rest dus te onderzoeken hoe de rij $u_f,u_{f+1},\ldots$ zich gedraagt mod m"; wegens (m",r) = 1 is dit gedrag direct uit de stelling van Fermat en de daaruit getrokken conclusies af te leiden.

Tenslotte beschouwen we een recurrente rij van het type

$$u_0 = a;\ u_{n+1} = ru_n + s.$$

Zij m een willekeurig gegeven natuurlijk getal van de gedaante p^t, waarbij p priem is. Zij (r-1,m) = 1. Zij $q \equiv s(r-1)^{-1} \pmod m$. Stel $v_n = u_n+q$ (n = 0,1,...). Dan is

$$v_{n+1} = u_{n+1} + q \equiv ru_n + s + s(r-1)^{-1} = ru_n + sr(r-1)^{-1} =$$
$$= r(u_n+s(r-1)^{-1}) \equiv rv_n \pmod m,$$

zodat het gedrag der u-rij op dat van een v-rij van een reeds eerder beschouwd type is teruggebracht.

Is echter $r \equiv 1 \pmod p$, dan heeft men $u_{n+1} \equiv u_n + s \pmod m$, dus $u_n \equiv u_o + ns \pmod m$. Het getal n is minimaal met $u_n \equiv u_o \pmod m$ als ns

het K.G.V. is van s en m, dus $ns = \frac{sm}{(s,m)}$, dus $n = \frac{m}{(s,m)}$. In dit geval gaat de oorspronkelijke rij over in een mod m rekenkundige rij.

In het geval dat $m = p_1^{t_1} \ldots p_u^{t_u}$, vindt men de periode van de rij mod m als K.G.V. der hierboven afgeleide perioden mod $p_1^{p_t}, \ldots, p_u^{t_u}$.

Voorbeelden.

1°. $u_o = 1$; $u_{n+1} = 10u_n$; $m = 27$. Men heeft $c(3) = 1$ en $3^2 \mid 10^{c(3)}-1$. Dus $c(27) = c(3^3) = 3^{3-2}c(3) = 3$.

2°. $u_o = 3$; $u_{n+1} = 10\,u_n$; $m = 168 = 2^3.3.7$. Voor alle n is $3 \mid u_n$; voor $n \geqq 3$ is $8 \mid u_n$, dus voor $n \geqq 3$ is $24 \mid u_n$. Verder is $c(7) = 6$. Dus $c(168) = 6$ en $u_{n+6} \equiv u_n \pmod{168}$ voor alle $n \geqq 3$.

3°. $u_o = 2$; $u_{n+1} = 6u_n+1$; $m = 10$. Voor de factor 2 van m beschouwe men de rij $v_{n+1}=6v_n$ met $v_o = u_o + 1 = 3$. Dus voor $n \geqq 1$ is $u_{n+1} \equiv u_n \pmod 2$. Verder heeft men voor de periode $c(5)$ wegens $(5,10) \neq 1$ dat $c(5) = \frac{5}{(1,5)} = 5$. Bijgevolg is voor $n \geqq 1$ steeds $u_{n+5} \equiv u_n \pmod{10}$.

4°. $u_o = 3$; $u_{n+1} = 7u_n$. Men heeft $c(5) \mid 4$; inderdaad is $c(5) = 4$ en ook $c(25) = 4$. Echter is $c(125) = 20$ en in het algemeen $c(5^k) = 4.5^{k-2}$ voor $k \geqq 2$.

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

Colloquium Recurrente Rijen

Hoofdstuk IV

C.G. Lekkerkerker.

Kwadraat-resten

Zij m een natuurlijk getal. Een geheel getal a is op één manier te schrijven als $a = qm+s$, waarbij $0 \leqq s \leqq m-1$. De getallen, die congruent zijn met a modulo m, zijn ook de getallen, die bij deling door m dezelfde rest s laten. We zeggen dat ze een restklasse vormen; er zijn m van zulke klassen.

Een getal a heet (kwadraat-)rest modulo m indien geldt:

1°. $(a,m) = 1$.

2°. de vergelijking $x^2 \equiv a \pmod m$ bezit een oplossing, d.w.z. de restklasse waarin a voorkomt, bevat een kwadraat. Is $(a,m) = 1$, maar niet voldaan aan 2°, dan noemen we a een (kwadraat-)nietrest.

In het vervolg onderstellen we steeds, dat m een priemgetal, zeg p, is. Legendre voerde het symbool $(\frac{a}{p})$ in, vastgelegd als volgt:

$$(4.1) \quad \begin{cases} (\frac{a}{p}) = 1 \text{ als a kwadraat-rest modulo p is.} \\ (\frac{a}{p}) = -1 \text{ als a kwadraat-nietrest modulo p is.} \end{cases}$$

Voorbeelden. $(\frac{5}{7}) = 1$ wegens $5 \equiv 8^2 \pmod 7$, $(\frac{-1}{13}) = 1$ wegens $-1 \equiv 8^2 \pmod{13}$.

Stelling 1. Is a kwadraat-rest modulo p, en is $b \equiv a \pmod p$, dan is ook b kwadraat-rest modulo p. En omgekeerd. Is a nietrest, dan ook b.

Bewijs. Allereerst is $(b,p) = (a,p) = 1$. Verder voldoet het getal x, waarvoor geldt $x^2 \equiv a \pmod p$, ook aan $x^2 \equiv b \pmod p$. Hiermee is het eerste deel der stelling bewezen. Het laatste deel volgt onmiddellijk.

Conclusie. Voor het onderzoek, welke getallen rest en welke nietrest zijn, kunnen we ons beperken tot de beschouwing van de getallen $1,2,\ldots,p-1$.

Stelling 2. Is $p > 2$, dan komen onder de getallen $1,2,\ldots,p-1$ evenveel resten als nietresten modulo p voor, nl. $\frac{1}{2}(p-1)$.

Bewijs. Wegens $(x+vp)^2 \equiv x^2 \pmod p$ is elke rest congruent met een der kwadraten $1^2, 2^2, \ldots, (p-1)^2$. Ook is elk van die kwadraten een rest. We laten nu zien, dat die kwadraten juist $\frac{1}{2}(p-1)$ onderling incongruente getallen voorstellen. Ten eerste geldt:

$$(p-i)^2 \equiv i^2 \pmod p.$$

Ten tweede geldt:

$$i^2 \not\equiv j^2 \pmod p, \text{ indien } 1 \leqq i < j \leqq \frac{p-1}{2}.$$

Want uit $i^2 \equiv j^2 \pmod p$ volgt $j^2 - i^2 = (j-i)(j+i) \equiv 0 \pmod p$, dus $p / j-1$ of $p / j+1$ (wegens hulpstelling 1, pag. 5), wat onmogelijk is wegens $0 < j-i,\ j+i < p$.

Als toepassing nemen we $p = 11$. Dan geven $1^2, 2^2, 3^2, 4^2, 5^2$ aanleiding tot de verschillende mogelijke resten. Dus 1,3,4,5,9 zijn resten en 2,6, 7,8,10 zijn nietresten mod 11.

Stelling 3. Het symbool van Legendre is multiplicatief t.a.v. de teller, d.w.z. er geldt $(\frac{ab}{p}) = (\frac{a}{p}).(\frac{b}{p})$

Bewijs. We mogen $p > 2$ onderstellen. We moeten verschillende gevallen onderscheiden, al naar gelang a en b rest of nietrest zijn.

1^o. a en b zijn beide rest. Dan bestaan er dus x en y, zodat $x^2 \equiv a \pmod p$, $y^2 \equiv b \pmod p$. Daaruit volgt $(xy)^2 \equiv ab \pmod p$, zodat ook ab rest is. Dus in dit geval $(\frac{a}{p})(\frac{b}{p}) = 1$. $1 = 1$ en $(\frac{ab}{p}) = 1$.

2^o. a is rest en b is nietrest. Er is een x, zodat $x^2 \equiv a \pmod p$; daarbij is $(a,p) = 1$, dus ook $(x,p) = 1$. We kunnen dus de inversen a^{-1}, x^{-1} beschouwen; wegens $(x^{-1})^2 \equiv a^{-1} \pmod p$ is a^{-1} rest. Was nu ab rest, dan wegens 1^o ook $b = a^{-1}(ab)$. Dus is ab nietrest en

$$(\frac{a}{p})(\frac{b}{p}) = -1, \quad (\frac{ab}{p}) = -1.$$

3^o. a en b zijn beide nietrest. Bij vermenigvuldiging van a met de $\frac{p-1}{2}$ resten ontstaan wegens 2^o juist de $\frac{p-1}{2}$ nietresten. Dus is ab een rest. Dus

$$(\frac{a}{p})(\frac{b}{p}) = -1.\ -1 = 1, \quad (\frac{ab}{p}) = 1.$$

Criterium van Euler. Het symbool van Legendre voldoet voor $p > 2$ aan de volgende congruentie:

$$(4.2) \qquad (\frac{a}{p}) \equiv a^{\frac{1}{2}(p-1)} \pmod p.$$

Bewijs. We merken op, dat wegens Fermat en $(a,p) = 1$ geldt:

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

dus

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

dus (hulpstelling 1)

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

Is $(\frac{a}{p}) = 1$, dan is er een getal x zodat $a \equiv x^2 \pmod p$, dus $a^{\frac{1}{2}(p-1)} \equiv x^{p-1} \equiv 1$; voor dit geval is dus (4.2) bewezen. Tevens kennen we $\frac{1}{2}(p-1)$ onderling incongruente getallen a, zodat $a^{\frac{1}{2}(p-1)} \equiv 1 \pmod p$. Evenals een k^{de} graadsvergelijking niet meer dan k wortels bezit, geldt ook dat aan de laatste congruentie niet meer dan $\frac{1}{2}(p-1)$ onderling incongruente getallen voldoen; bij het, niet nader uitgevoerde, bewijs maakt men uitvoerig gebruik van hulpstelling 1. Is dus $(\frac{a}{p}) = -1$, dan is noodzakelijk $a^{\frac{1}{2}(p-1)} \equiv -1 \pmod p$. Zodat (4.2) ook in dit geval geldt.

We zouden graag een methode bezitten om in elk concreet geval zo snel mogelijk het symbool van Legendre te berekenen. Daartoe leiden we eerst m.b.v. het criterium van Euler, het zg. Lemma van Gauss af. Dit luidt als volgt:

Zij p een oneven priemgetal, $(a,p) = 1$ en r_h de rest bij deling van ha door p ($h = 1,2,\ldots,\frac{1}{2}(p-1)$). Zij μ het aantal getallen r_h, waarvoor $\frac{1}{2}p < r_h < p$ is. Dan is

$$(4.3) \qquad \left(\frac{a}{p}\right) = (-1)^{\mu}.$$

Bewijs. Is $h \neq k$ en $1 \leq h,k \leq \frac{1}{2}(p-1)$, dan is $r_h \not\equiv r_k \pmod p$ en ook $r_h \not\equiv p - r_k \pmod p$. Anders was nl. $(h-k)a \equiv 0 \pmod p$ resp. $(h+k)a \equiv 0 \pmod p$, wat een tegenspraak oplevert. Noemen we nu die getallen r_h, waarbij $0 < r_h < \frac{1}{2}p$ is, $\rho_1,\ldots,\rho_\lambda$ en die getallen r_h, waarbij $\frac{1}{2}p < r_h < p$ is, $\sigma_1,\ldots,\sigma_\mu$ (N.B. 0 en $\frac{1}{2}p$ komen niet voor als rest). Dan is $\lambda + \mu = \frac{1}{2}(p-1)$. De getallen ρ_i ($i = 1,\ldots,\lambda$) en de getallen $p - \sigma_k$ ($k = 1,\ldots,\mu$) zijn onderling incongruent, dus blijkbaar in een of andere volgorde de getallen $1,2,\ldots,\frac{1}{2}(p-1)$. Door vermenigvuldiging ontstaat dan

$$\rho_1 \rho_2 \cdots \rho_\lambda (p-\sigma_1)(p-\sigma_2) \cdots (p-\sigma_\mu) = (\tfrac{1}{2}(p-1))!$$

Dus ook

$$(-1)^{\mu} r_1 r_2 \cdots r_{\frac{1}{2}(p-1)} = (\tfrac{1}{2}(p-1))!$$

Wegens

$$r_1 r_2 \cdots r_{\frac{1}{2}(p-1)} = (\tfrac{1}{2}(p-1))!\ a^{\frac{1}{2}(p-1)}$$

krijgen we

$$(\tfrac{1}{2}(p-1))!\ a^{\frac{1}{2}(p-1)} \equiv (\tfrac{1}{2}(p-1))!\ (-1)^{\mu} = (\tfrac{1}{2}(p-1))!\ (-1)^{\mu}.$$

Nu is $\frac{1}{2}(p-1)!$ onderling ondeelbaar met p, zodat i.v.m. hulpstelling 1 volgt: $a^{\frac{1}{2}(p-1)} \equiv (-1)^{\mu} \pmod p$. Door toepassing van het criterium van Euler ontstaat hieruit $\left(\frac{a}{p}\right) \equiv (-1)^{\mu} \pmod p$. Deze congruentie is zeker een gelijkheid, daar $p > 2$ is en beide leden +1 of -1 zijn, dus minder dan p verschillen.

Als toepassing volgt meteen de berekening van $\left(\frac{2}{p}\right)$ en $\left(\frac{-1}{p}\right)$.

Berekening van $\left(\frac{2}{p}\right)$. We moeten dus nu beschouwen de getallen $2,\ 2.2,2.3,\ldots$ $\ldots,p-1$; het zijn tevens de resten modulo p. Het aantal μ hiervan, dat tussen $\frac{1}{2}p$ en p in ligt, is gelijk aan $\left[\frac{1}{2}p\right] - \left[\frac{1}{4}p\right]$. Nu komt het alleen op de pariteit van μ aan. We maken even een lijstje om te zien wanneer $\left[\frac{1}{2}p\right] - \left[\frac{1}{4}p\right]$ even is, en wanneer oneven.

p	$\left[\frac{1}{2}p\right]$	$\left[\frac{1}{4}p\right]$	$\mu = \left[\frac{1}{2}p\right] - \left[\frac{1}{4}p\right]$
$\equiv 1 \pmod 8$	even	even	even
$\equiv 3 \pmod 8$	oneven	even	oneven
$\equiv 5 \pmod 8$	even	oneven	oneven
$\equiv 7 \pmod 8$	oneven	oneven	even

Het getal $p^2-1 = (p-1)(p+1)$ is als product van twee opeenvolgende even getallen zeker door 8 deelbaar, en wel is $\frac{1}{8}(p^2-1)$ onder dezelfde omstandigheden even en oneven als μ. Hiermee is bewezen:

$$(4.4) \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}.$$

We kunnen het resultaat ook aldus aangeven:

$$\left(\frac{2}{p}\right) = \begin{cases} +1 \text{ als } p \equiv \pm 1 \pmod 8 \\ -1 \text{ als } p \equiv \pm 3 \pmod 8. \end{cases}$$

Berekening van $\left(\frac{-1}{p}\right)$. Nu is μ kennelijk gelijk aan $\frac{1}{2}(p-1)$. Dus hebben we

$$(4.5) \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}.$$

Anders gezegd:

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 \text{ als } p \equiv 1 \pmod 4 \\ -1 \text{ als } p \equiv 3 \pmod 4 \end{cases} \equiv -1 \pmod 4.$$

De kwadratische reciprociteitsstelling. Deze luidt als volgt: Zij p en q twee verschillende oneven priemgetallen, dan is $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1).\frac{1}{2}(q-1)}$.

Bewijs. We voeren de beide volgende sommen in

$$S_1 = \sum_{k=1}^{\frac{1}{2}(p-1)} \left[\frac{kq}{p}\right], \quad S_2 = \sum_{l=1}^{\frac{1}{2}(q-1)} \left[\frac{lp}{q}\right].$$

Zetten we $kq = p\left[\frac{kq}{p}\right] + r_k$ $(k = 1,2,\ldots,\frac{1}{2}(p-1))$,

$$A = \rho_1 + \rho_2 + \ldots + \rho_\lambda, \quad B = \sigma_1 + \sigma_2 + \ldots + \sigma_\mu,$$

waarbij $\rho_1, \rho_2, \ldots, \rho_\lambda$ diegene onder de getallen r_k $(k = 1,2,\ldots,\frac{1}{2}(p-1))$ zijn, die inliggen tussen 0 en $\frac{1}{2}p$, en $\sigma_1, \sigma_2, \ldots, \sigma_\mu$ diegene, die inliggen tussen $\frac{1}{2}p$ en p. Dan volgt:

$$\sum_{k=1}^{\frac{1}{2}(p-1)} kq = \frac{1}{8}(p^2-1)q = pS_1 + A + B.$$

In verband met $\rho_1 + \rho_2 + \ldots + \rho_\lambda + (p-\sigma_1) + (p-\sigma_2) + \ldots + (p-\sigma_\mu) =$

$= 1 + 2 + \ldots + \frac{1}{2}(p-1) = \frac{1}{8}(p^2-1)$ hebben we ook $A + \mu p - B = \frac{1}{8}(p^2-1)$, dus

$\frac{1}{8}(p^2-1)q = pS_1 + 2A + \mu p - \frac{1}{8}(p^2-1)$. Dus

$$(\mu + S_1)p = \frac{1}{8}(p^2-1)(q+1) - 2A \equiv 0 \pmod 2,$$

en wegens $p \equiv 1 \pmod 2$ dus ook $\mu \equiv S_1 \pmod 2$. Hierbij is μ het aantal getallen kq met $k = 1,2,\ldots,\frac{1}{2}(p-1)$, dat bij deling door p een rest $> \frac{1}{2}p$ heeft. Evenzo geldt, als ν het aantal getallen lp is $(l = 1,2,\ldots,\frac{1}{2}(q-1))$, dat bij deling door q een rest $> \frac{1}{2}q$ heeft, $\nu \equiv S_2 \pmod 2$.

Toepassing van het lemma van Gauss levert

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu}(-1)^{\nu} = (-1)^{S_1+S_2}.$$

Het gaat er nu nog om te laten zien, dat S_1+S_2 en $\frac{1}{2}(p-1).\frac{1}{2}(q-1)$ dezelfde pariteit bezitten. We zullen zelfs aantonen: $S_1+S_2 = \frac{1}{2}(p-1).\frac{1}{2}(q-1)$. Daartoe beschouwen we in een (x,y)-vlak de rechthoek R met zijden $x=0$, $x=\frac{1}{2}p$,

$y=0$, $y=\frac{1}{2}q$ en tellen op twee manieren het aantal roosterpunten, d.i. punten met gehele coördinaten, dat binnen R gelegen is.

Ten eerste kunnen we zeggen, dat er $\frac{1}{2}(q-1)$ horizontale rijen, ieder van $\frac{1}{2}(p-1)$ roosterpunten, binnen R zijn. Het genoemde aantal is dus $\frac{1}{2}(p-1).\frac{1}{2}(q-1)$.

Ten tweede verdelen we R in twee driehoeken door de diagonaal van $(0,0)$ naar $(\frac{1}{2}p, \frac{1}{2}q)$ te trekken. Op deze diagonaal liggen geen roosterpunten, behalve $(0,0)$. Want uit $0 < x < \frac{1}{2}p$, $\frac{x}{y} = \frac{\frac{1}{2}p}{\frac{1}{2}q}$ volgt $xq = py$, dus p/x, dus $x = 0$. In de onderste driehoek tellen we de roosterpunten op de verticale rechten $x=1$, $x=2$, ..., $x=\frac{1}{2}(p-1)$; op $x = k$ liggen blijkbaar $\left[\frac{kq}{p}\right]$ roosterpunten, in de hele driehoek dus juist S_1. In de bovenste driehoek tellen we de roosterpunten op de horizontale rechten $y=1$, $y=2$, ..., $y=\frac{1}{2}(q-1)$; op $y = 1$ liggen blijkbaar $\left[\frac{1p}{q}\right]$ roosterpunten, in de hele driehoek dus S_2. In R liggen dus S_1+S_2 roosterpunten. In verband met het bovenstaande volgt hieruit de stelling.

Met behulp van de laatste stelling kan men snel een willekeurig restsymbool uitrekenen.

Voorbeelden.

$$\left(\frac{23}{67}\right) = (-1)^{33.11}.\left(\frac{67}{23}\right) = -\left(\frac{-2}{23}\right) = -\left(\frac{-1}{23}\right).\left(\frac{2}{23}\right) = (-1).(-1).(+1) = 1.$$

$$\left(\frac{20}{79}\right) = \left(\frac{4}{79}\right).\left(\frac{5}{79}\right) = \left(\frac{5}{79}\right) = (-1)^{2.39}.\left(\frac{79}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

We beschouwen nog enige speciale gevallen.

Voor $\left(\frac{3}{p}\right)$ vinden we $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{1}{2}(p-1)}$, dus $\left(\frac{3}{p}\right) = (-1)^{\frac{1}{2}(p-1)}\left(\frac{p}{3}\right)$. In het rechterlid is de eerste factor $+1$ of -1 voor $p \equiv 1$ resp. $\equiv -1 \pmod 4$ en de tweede factor $+1$ en -1 voor $p \equiv 1$ resp. $\equiv -1 \pmod 3$. Om de waarde van het product te kennen, moeten we p modulo 12 bekijken. En wel komt er $+1$ uit voor $p \equiv \pm 1 \pmod{12}$ en -1 voor $p \equiv \pm 5 \pmod{12}$; andere mogelijkheden voor p hoeven niet bekeken te worden omdat p een priemgetal $\neq 2,3$ is.

Evenzo $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, dus $+1$ als $p \equiv \pm 1 \pmod 5$ is en -1 als $p \equiv \pm 2 \pmod 5$ is.

Door combinatie van de uitkomsten voor $\left(\frac{-1}{p}\right)$ en $\left(\frac{3}{p}\right)$ kunnen we $\left(\frac{-3}{p}\right)$ algemeen berekenen. Voor $p \equiv 1,-1,5,-5 \pmod{12}$ is opvolgend $\left(\frac{-3}{p}\right) =$ $= 1,-1,-1,1$. Dus 1 voor $p \equiv 1 \pmod 6$ en -1 voor $p \equiv -1 \pmod 6$. We vatten de verkregen resultaten in het volgende schema samen; in de tweede kolom staan de gevallen opgesomd, waarin het betreffende restsymbool gelijk is aan $+1$ en in de derde die waarin het -1 is.

(4.6)

	$\left(\frac{-1}{p}\right)$	$\left(\frac{2}{p}\right)$	$\left(\frac{3}{p}\right)$	$\left(\frac{-3}{p}\right)$	$\left(\frac{5}{p}\right)$
$+1$	$p \equiv 1 \pmod 4$	$\equiv \pm 1 \pmod 8$	$\equiv \pm 1 \pmod{12}$	$\equiv +1 \pmod 6$	$\equiv \pm 1 \pmod 5$
-1	$p \equiv -1 \pmod 4$	$\equiv \pm 3 \pmod 8$	$\equiv \pm 5 \pmod{12}$	$\equiv -1 \pmod 6$	$\equiv \pm 2 \pmod 5$

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

Colloquium Recurrente Rijen

Hoofdstuk V

§1. De rij van Fibonacci

W.Peremans

We gaan uit van de vergelijking $x^2-x-1=0$ met de wortels $\omega = \frac{1}{2}(1+\sqrt{5})$ en $\bar{\omega} = \frac{1}{2}(1-\sqrt{5})$. Omdat $\omega^2 = \omega+1$ en $\frac{1}{\omega} = \omega-1$ is, voor ieder geheel getal n, ω^n te schrijven in de vorm $\omega^n = u_n\omega+w_n$ met gehele rationale u_n en w_n. Nu is $u_{n+1}\omega+w_{n+1} = \omega^{n+1} = \omega\omega^n = u_n\omega^2 + w_n\omega = u_n(\omega+1)+ w_n\omega = (u_n+w_n)\omega + u_n$. Als echter $a\omega+b = c\omega+d$ met rationale a, b, c, d, dan geldt a = c en b = d. Was n.l. $a \neq c$, dan was $\omega = \frac{d-b}{c-a}$ rationaal, hetgeen niet het geval is, dus is a = c en dan ook b = d. Past men dit toe op $u_{n+1}\omega + w_{n+1} = (u_n+w_n)\omega+u_n$, dan volgt hieruit dat $w_{n+1} = u_n$ voor alle n en $u_{n+1}=u_n+u_{n-1}$ voor alle n. Verder is $\omega = u_1\omega+u_0$, dus $u_0 = 0$, $u_1 = 1$.

We noemen de rij u_n, bepaald door $u_0 = 0$, $u_1 = 1$ en $u_n = u_{n-1}+u_{n-2}$ de rij van Fibonacci. Voor deze rij geldt dan $\omega^n = u_n\omega + u_{n-1}$ en evenzo $\bar{\omega}^n = u_n\bar{\omega} + u_{n-1}$. Hieruit volgt direct

$$(5.1.1) \qquad u_n = \frac{\omega^n-\bar{\omega}^n}{\omega-\bar{\omega}} = \frac{\omega^n-\bar{\omega}^n}{\sqrt{5}} .$$

Dit geldt zowel voor positieve als voor negatieve n, maar daar $u_{-n} = \frac{\omega^{-n}-\bar{\omega}^{-n}}{\sqrt{5}} = \frac{\bar{\omega}^n-\omega^n}{(\omega\bar{\omega})^n\sqrt{5}} = (-)^{n-1}\frac{\omega^n-\bar{\omega}^n}{\sqrt{5}} = (-)^{n-1}u_n$ (immers $\omega\bar{\omega} = -1$) zijn de elementen van de rij met negatieve indices niet interessant.

Verder is voor natuurlijke k en n $u_{kn}\omega + u_{kn-1} = \omega^{kn} = (u_n\omega+u_{n-1})^k = \sum_{j=0}^{k}\binom{k}{j} u_{n-1}^{k-j}u_n^j\omega^j = (\sum_{j=0}^{k}\binom{k}{j}u_{n-1}^{k-j}u_n^j u_j)\omega + \sum_{j=0}^{k}\binom{k}{j}u_{n-1}^{k-j}u_n^j u_{j-1}$. Omdat $u_0 = 0$ is, volgt hieruit

$$(5.1.2) \qquad u_{kn} = \sum_{j=1}^{k}\binom{k}{j}u_{n-1}^{k-j}u_n^j u_j,$$

$$(5.1.3) \qquad u_{kn-1} = \sum_{j=0}^{k}\binom{k}{j}u_{n-1}^{k-j}u_n^j u_{j-1}.$$

Uit (5.1.2) volgt dat $u_n \mid u_{kn}$, of anders uitgedrukt:

(5.1.4) Uit $n \mid m$ volgt $u_n \mid u_m$.

Nemen we in (5.1.2) en (5.1.3) k = 2 dan vinden we $u_{2n}=2u_{n-1}u_n+u_n^2$ en $u_{2n-1} = u_{n-1}^2 + u_n^2$, dus

$$(5.1.5) \qquad u_{2n} = u_n(u_{n-1} + u_{n+1}); \quad u_{2n-1} = u_{n-1}^2 + u_n^2.$$

We beschouwen nu de elementen van de rij van Fibonacci, gereduceerd modulo een of ander priemgetal p. Daar er slechts eindig veel restklassen mod p zijn moeten

er verschillende natuurlijke getallen m en n zijn zodat $u_m \equiv u_n \pmod p$ en $u_{m+1} \equiv u_{n+1} \pmod p$. Dan geldt blijkbaar voor iedere k, dat $u_{m+k} \equiv u_{n+k} \pmod p$. Stel $m > n$; dan is $u_{m-n} \equiv 0 \pmod p$ en $u_{m-n+1} \equiv 1 \pmod p$. Er is dus een natuurlijk getal k, zodat $u_k \equiv 0 \pmod p$ en $u_{k+1} \equiv 1 \pmod p$. Noem C(p) het kleinste natuurlijke getal met deze eigenschap; we noemen C(p) de (grote) periode modulo p van de rij van Fibonacci. Als we met een vaste p werken schrijven we ook kortweg C. Naast de grote periode beschouwen we ook de kleine periode modulo p dat is het kleinste getal c(p) (of kortweg c) waarvoor geldt $u_c \equiv 0 \pmod p$.

We beschouwen nu de verzameling R der getallen $a\omega+b$, waarin a en b alle gehele (rationale) getallen doorlopen. Som, verschil en product van twee getallen uit R liggen ook in R (we zeggen daarom dat R een ring is). We zeggen, dat het getal α in R deelbaar is op het getal β in R (geschreven $\alpha \mid \beta$), als er een getal ξ in R is, zodat $\alpha\xi = \beta$. Als α een gewoon geheel getal m is en $\beta = a\omega+b$, dan is er een $\xi = x\omega+y$, zodat $a\omega+b = m(x\omega+y) = mx\omega + my$, dus $a = mx$ en $b = my$, dus $m \mid a$ en $m \mid b$.

(5.1.6) Als $\alpha, \beta, \delta, \lambda$ en μ in R liggen, $\delta \mid \alpha$ en $\delta \mid \beta$, dan geldt $\delta \mid \lambda\alpha + \mu\beta$.

Immers $\alpha = \xi\delta$, $\beta = \eta\delta$, dus $\lambda\alpha + \mu\beta = (\lambda\xi + \mu\eta)\delta$.

Als α, β en δ in R liggen heet α congruent met β modulo δ (geschreven $\alpha \equiv \beta \pmod\delta$), als $\delta \mid \alpha - \beta$. Dan geldt blijkbaar

(5.1.7) $\alpha \equiv \alpha \pmod\delta$.

(5.1.8) Uit $\alpha \equiv \beta \pmod\delta$ volgt $\beta \equiv \alpha \pmod\delta$.

(5.1.9) Uit $\alpha \equiv \beta \pmod\delta$ en $\beta \equiv \gamma \pmod\delta$ volgt $\alpha \equiv \gamma \pmod\delta$.

Verder kan men met congruenties rekenen op grond van de volgende stellingen.

(5.1.10) Uit $\alpha_1 \equiv \beta_1 \pmod\delta$ en $\alpha_2 \equiv \beta_2 \pmod\delta$ volgt $\alpha_1+\alpha_2 \equiv \beta_1+\beta_2 \pmod\delta$.

(5.1.11) Uit $\alpha_1 \equiv \beta_1 \pmod\delta$ en $\alpha_2 \equiv \beta_2 \pmod\delta$ volgt $\alpha_1-\alpha_2 \equiv \beta_1-\beta_2 \pmod\delta$.

(5.1.12) Uit $\alpha_1 \equiv \beta_1 \pmod\delta$ en $\alpha_2 \equiv \beta_2 \pmod\delta$ volgt $\alpha_1\alpha_2 \equiv \beta_1\beta_2 \pmod\delta$.

De laatste stelling wordt als volgt bewezen: uit $\delta \mid \alpha_1-\beta_1$ en $\delta \mid \alpha_2-\beta_2$ volgt $\delta \mid \alpha_2(\alpha_1-\beta_1)+\beta_1(\alpha_2-\beta_2) = \alpha_1\alpha_2-\beta_1\beta_2$.

De vraag onder welke omstandigheden uit $\gamma\alpha \equiv \gamma\beta \pmod\delta$ volgt $\alpha \equiv \beta \pmod\delta$ is hier moeilijker te beantwoorden dan in het geval van de gehele getallen, omdat we hier nog niet over een stelling over eenduidige ontbindbaarheid in priemfactoren beschikken. In hoofdstuk VI zal hier dieper op in worden gegaan. Voorlopig volstaan we met de opmerking, dat een gewoon priemgetal ontbindbaar kan zijn in R. Zo is b.v.

$11 = (2\omega+3)(-2\omega+5)$.

(5.1.13) Als m een geheel getal is, geldt $a_1\omega + b_1 \equiv a_2\omega+b_2 \pmod m$ dan en slechts dan als $a_1 \equiv a_2 \pmod m$ en $b_1 \equiv b_2 \pmod m$.

Omdat $u_c \equiv 0 \pmod p$, geldt $\omega^c \equiv u_{c-1} \pmod p$, d.w.z. ω^c is congruent met een rationaal getal modulo p. Als omgekeerd ω^k congruent is met een rationaal getal r modulo p dan is $u_k\omega + u_{k-1} \equiv r \pmod p$, dus $u_k \equiv 0 \pmod p$. Het getal c kan dus ook gedefinieerd worden als het kleinste natuurlijke getal waarvoor ω^c congruent is met een rationaal getal modulo p.

(5.1.14) Als a en b gehele getallen zijn en $b \neq 0$, bestaan er gehele getallen q en r zodat $a = qb+r$ en $0 \leqslant r < |b|$ (deling met rest).

Om dit te bewijzen beschouwen we de verzameling der getallen a-nb, waarin n alle gehele getallen doorloopt. Deze verzameling bevat zeker een niet-negatief getal (kies $n = |a|$ als $b < 0$ en $n = -|a|$ als $b > 0$). Noem het kleinste niet-negatieve getal in deze verzameling r ($r = a-qb$). Als dan $r \geqslant |b|$ was, zou voor $b > 0$ gelden $0 = |b| - b \leqslant r - b < r$ en $r - b = a-(q+1)b$ en voor $b < 0$ gelden $0 = |b| + b \leqslant r + b < r$ en $r + b = a-(q-1)b$. Dit is in strijd met de minimaliteit van r, dus $r < |b|$.

Als $u_k \equiv 0 \pmod p$, schrijven we $k = qc + r$ met gehele q en r en $0 \leqslant r < c$ (deling met rest), dan is $u_{k-1} \equiv \omega^k = (\omega^c)^q\omega^r \equiv u_{c-1}^q\omega^r$. Nu is $u_{c-1} \not\equiv 0 \pmod p$; was n.l. $u_{c-1} \equiv 0 \pmod p$, dan volgde uit het feit dat ook $u_c \equiv 0 \pmod p$ en uit de recursieve betrekking die de rij van Fibonacci bepaalt direct, dat alle getallen uit de rij door p deelbaar zouden zijn, hetgeen voor $u_1 = 1$ niet het geval is. Er is dus een geheel rationaal getal $u_{c-1}^{-1} \pmod p$ zodat $u_{c-1}^{-1}\, u_c \equiv 1 \pmod p$, dus $u_{c-1}^{-q}\, u_{k-1} \equiv \omega^r \pmod p$, dus ω^r congruent met een rationaal getal modulo p. Daar c het kleinste natuurlijke getal met deze eigenschap is, geldt $r = 0$, dus $c|k$. Als omgekeerd $c|k$, dus $k = qc$ is, geldt $\omega^k = (\omega^c)^k \equiv u_{c-1}^k$ dus $u_k \equiv 0 \pmod p$.

(5.1.15) $u_k \equiv 0 \pmod p$ geldt dan en slechts dan als $c|k$.

Hieruit volgt dus ook direct:

(5.1.16) $c|C$.

We schrijven $C = vc$.

Uit de definitie van C volgt direct, dat C ook gedefinieerd kan worden als het kleinste natuurlijke getal, waarvoor $\omega^C \equiv 1 \pmod p$. Als $\omega^k \equiv 1 \pmod p$, stellen we $k = qC+r$ met gehele q en r en $0 \leqslant r < C$, dan is $1 \equiv \omega^k = (\omega^C)^q\omega^r \equiv \omega^r$. Omdat C het kleinste natuurlijke getal is waarvoor $\omega^C \equiv 1 \pmod p$ is $r = 0$, dus $C|k$. Als omgekeerd $C|k$, dus $k = qC$, geldt $\omega^k = (\omega^C)^q \equiv 1 \pmod p$. We hebben dus gevonden:

(5.1.17) $\omega^k \equiv 1 \pmod p$ geldt dan en slechts dan als $C|k$.

Verder volgt uit $C = vc$ dat $1 \equiv \omega^C = (\omega^c)^v \equiv u_{c-1}^v$, dus $u_{c-1}^v \equiv 1 \pmod p$. Als omgekeerd $u_{c-1}^w \equiv 1$, geldt $1 \equiv u_{c-1}^w \equiv (\omega^c)^w = \omega^{cw}$, dus, volgens (5.1.17), $C|cw$. We kunnen dus v ook definiëren als het kleinste natuurlijke getal waarvoor $u_{c-1}^v \equiv 1 \pmod p$; anders uitgedrukt v is de

exponent van u_{c-1} modulo p. Hieruit volgt $v \mid p-1$ (zie blz. 7). We zullen straks evenwel veel meer over v bewijzen.

We onderstellen nu $p \equiv \pm 1 \pmod{10}$. Dan is (zie blz. 14) $(\frac{5}{p}) = 1$, dus volgens het criterium van Euler (zie blz. 11) $5^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, dus, wegens $5 = (2\omega-1)^2$, $(2\omega-1)^{p-1} \equiv 1 \pmod{p}$, dus $(2\omega-1)^p \equiv 2\omega-1 \pmod{p}$. Ontwikkelen we $(2\omega-1)^p$ volgens de binomiaalformule van Newton dan zijn alle termen behalve de eerste en de laatste deelbaar door p, dus $2^p\omega^p + (-1)^p \equiv 2\omega-1 \pmod{p}$. Verder is $2^p \equiv 2 \pmod{p}$, dus $2\omega^p - 1 \equiv 2\omega-1 \pmod{p}$, dus $2\omega(\omega^{p-1}-1) \equiv 0 \pmod{p}$. Laat $\omega^{p-1}-1 = a\omega+b$ zijn, dan is $p \mid 2\omega(a\omega+b) = 2(a+b)\omega+2a$, dus omdat p oneven is, $p \mid a$ en $p \mid a+b$, dus $p \mid a$ en $p \mid b$. Dus $\omega^{p-1} \equiv 1 \pmod{p}$. Dus $C \mid p-1$.

We onderstellen nu $p \equiv \pm 3 \pmod{10}$. Dan is $(\frac{5}{p}) = -1$, dus $5^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, dus $(2\omega-1)^{p-1} \equiv -1 \pmod{p}$, dus $(2\omega-1)^p \equiv 1-2\omega \pmod{p}$, dus $2\omega^p - 1 = 1-2\omega \pmod{p}$, dus $2\omega^p \equiv 2(1-\omega) \pmod{p}$, dus $2\omega^{p+1} \equiv -2 \pmod{p}$, dus $\omega^{p+1} \equiv -1 \pmod{p}$, dus $\omega^{2(p+1)} \equiv 1 \pmod{p}$, dus $C \mid 2(p+1)$, $C \nmid p+1$, $c \mid p+1$.

(5.1.18) Uit $p \equiv \pm 1 \pmod{10}$ volgt $c \mid C \mid p-1$; uit $p \equiv \pm 3 \pmod{10}$ volgt $c \mid p+1$, $C \mid 2(p+1)$, $C \nmid p+1$.

Er resten nog de gevallen $p = 2$ en $p = 5$. Nu is $c(2) = C(2) = 3$ en $c(5) = 5$, $C(5) = 20$.

Om het verband tussen c, C en v nader te onderzoeken, maken we gebruik van het feit, dat we onze afleiding evenzo met $\bar{\omega}$ in plaats van ω hadden kunnen uitvoeren. Zo is ook $\bar{\omega}^c \equiv u_{c-1} \pmod{p}$, dus $u_{c-1}^2 \equiv (\omega\bar{\omega})^c = (-)^c \pmod{p}$, dus $u_{c-1}^4 \equiv 1 \pmod{p}$, dus $v \mid 4$, m.a.w. $v = 1$, $v = 2$ of $v = 4$. We onderscheiden drie gevallen.

1°. c oneven; dan is $u_{c-1}^2 \equiv -1 \pmod{p}$, dus $v = 4$.

2°. $c = 2d$, d oneven. Dan is $u_{c-1}^2 \equiv 1 \pmod{p}$, dus $u_{c-1} \equiv \pm 1 \pmod{p}$. Als $u_{c-1} \equiv -1 \pmod{p}$ is, is $\omega^{2d} = \omega^c \equiv u_{c-1} \equiv -1 = (-)^d \pmod{p}$, dus $\omega^d = (-\bar{\omega})^d\omega^{2d} \equiv (-\bar{\omega})^d(-)^d = \bar{\omega}^d \pmod{p}$, dus $0 \equiv u_d(\omega-\bar{\omega}) = 2u_d\omega - u_d \pmod{p}$, dus $u_d \equiv 0 \pmod{p}$, hetgeen in strijd is met het feit dat c het kleinste natuurlijke getal is, waarvoor $u_c \equiv 0 \pmod{p}$. Dus $u_{c-1} \not\equiv 1 \pmod{p}$, dus $v = 1$.

3°. $c = 2d$, d even. Dan is $u_{c-1}^2 \equiv 1 \pmod{p}$, dus $u_{c-1} \equiv \pm 1 \pmod{p}$. Als $u_{c-1} \equiv 1 \pmod{p}$, is $\omega^{2d} = \omega^c \equiv u_{c-1} \equiv 1 = (-)^d \pmod{p}$, dus $\omega^d \equiv \bar{\omega}^d \pmod{p}$, dus $u_d \equiv 0 \pmod{p}$, hetgeen in strijd is met het feit dat c het kleinste natuurlijke getal is, waarvoor $u_c \equiv 0 \pmod{p}$. Dus $u_{c-1} \equiv -1 \pmod{p}$, dus $v = 2$.

Dit geeft ons het volgende:

(5.1.19)

c(mod 4)	v	C(mod 8)
± 1	4	4
0	2	0
2	1	± 2

Stel $p \equiv 11$ of 19 (mod 20), dan geldt $C \mid p-1$ en $4 \mid p-1$, dus $4 \mid C$, dus $v = 1$. Stel $p \equiv 3$ of 7 (mod 20), dan geldt $C \mid 2(p+1)$ en $C \nmid p+1$, dus C bevat meer factoren 2 dan p+1, dat er ten minste twee bevat, dus $8 \mid C$, dus $v = 2$. Stel $p \equiv 13$ of 17 (mod 20), dan bevat C eveneens meer factoren 2 dan p+1, dat er nu één en slechts één bevat, dus $4 \mid C$, $8 \nmid C$, dus $v = 4$. Als $p \equiv 1$ of 9 (mod 20), kan $v = 1$, 2 of 4 zijn. Als $v = 2$ is, is $8 \mid C \mid p-1$, dus $p \equiv 1$ (mod 8), dus $p \equiv 1$ of 9 (mod 40).

Dit geeft ons het volgende:

p (mod 20)	v	c(mod 4)	C(mod 8)	opmerkingen
1	1,2,4	0,± 1,2	0,± 2,4	v=2 slechts bij $p \equiv 1$ (mod 40)
3	2	0	0	
7	2	0	0	
(5.1.20) 9	1,2,4	0,± 1,2	0,± 2,4	v=2 slechts bij $p \equiv 9$ (mod 40)
11	1	2	± 2	
13	4	± 1	4	
17	4	± 1	4	
19	1	2	± 2	

We hebben nu de periodiciteit van de rij van Fibonacci modulo een priemgetal onderzocht. Hieruit is nu echter het gedrag modulo een samengesteld getal af te leiden op een wijze die geheel analoog is met die bij de rij $u_n = ru_{n-1}$ (zie blz. 7 en 8). Zoals toen voor de periode modulo m gold, dat het het kleinste natuurlijke getal C was, waarvoor $r^C \equiv 1$ (mod m), is het nu het kleinste natuurlijke getal C waarvoor $\omega^C \equiv 1$ (mod m).

We vinden nu evenals vroeger voor oneven p, dat als $\omega^{C(p)} \equiv 1 \pmod{p^n}$ en $\omega^{C(p)} \not\equiv 1 \pmod{p^{n+1}}$, geldt $C(p^h) = C(p)$ voor $h \leqslant n$ en $C(p^h) = p^{h-n}C(p)$ voor $h > n$. Er is ons geen priemgetal bekend, waarvoor $n > 1$ is. Verder is $C(4) = 6$ en $\omega^6 = 8\omega+13 \equiv 1 \pmod{2^2}$ en $\omega^6 \not\equiv 1 \pmod{2^3}$. We vinden dan evenals vroeger, dat $C(2^h) = 2^{h-2}.6 = 2^{h-1}.3$ voor $h \geqslant 2$. Voor $h = 1$ blijkt het ook te gelden.

Als $m = p_1^{s_1} \ldots p_u^{s_u}$, geldt evenals vroeger $C(m) = \left\{C(p_1^{s_1}), \ldots, C(p_u^{s_u})\right\}$.

Het hierboven gevondene levert ons ook hulpmiddelen om de ontbinding in factoren van de getallen van Fibonacci snel uit te voeren. Omdat voor $d \mid n$ geldt $u_d \mid u_n$, delen we eerst de priemfactoren van u_d (d doorloopt de delers van n) uit u_n (we behoeven ons daarbij uiteraard slechts te beperken tot de delers $d_i = \frac{n}{p_i}$ van $n = p_1^{s_1} \ldots p_u^{s_u}$). Voor de priemfactoren p van u_n, die dan nog overblijven geldt dan $c(p) = n$. Als dan

$p \equiv 1$ (mod 10), dan is p-1 een n-voud en $p-1 \equiv 0$ (mod 10),
$p \equiv 3$ (mod 10), dan is p+1 een n-voud en $p+1 \equiv 4$ (mod 10),
$p \equiv -3$ (mod 10), dan is p+1 een n-voud en $p+1 \equiv 8$ (mod 10),
$p \equiv -1$ (mod 10), dan is p-1 een n-voud en $p-1 \equiv 8$ (mod 10).

We behoeven dus alleen priemgetallen te beschouwen, die n-vouden $\pm$ 1 zijn en daarbij alleen n-vouden, die op een 0,4 of 8 eindigen; bij 0 en 8 zijn de n-vouden +1 en bij 4 en 8 de n-vouden -1 te beschouwen.

Willen we b.v. $u_{27} = 196418$ ontbinden, dan beschouwen we eerst $u_9 = 34 = 2.17$. Nu is $196418:34 = 5777$. We proberen eerst $2.27-1 = 53$ en dit blijkt daarop inderdaad deelbaar met quotiënt 109 hetgeen $4.27+1$ is. Dus $u_{27} = 2.17.53.109$.

Nemen we $u_{23} = 28657$, dan is 138 het kleinste veelvoud van 23 dat op 0,4 of 8 eindigt, maar 137 en 139 blijken niet deelbaar te zijn op 28657. Het volgende bruikbare veelvoud van 23 is 184 maar 183 is niet priem. Het volgende bruikbare veelvoud van 23 is 230, maar dit is groter dan $\sqrt{28657}$. (Bij het zoeken naar de priemfactoren van een getal hoeven we nooit verder te gaan dan tot de vierkantswortel van dat getal, want als een factor groter is dan die vierkantswortel, is het quotiënt kleiner.) Dus is 28657 priem.

Het is niet zo dat als de index priem is, het getal van Fibonacci ook priem is. Neem b.v. $u_{37} = 24157817$. Eerst proberen we $2.37-1 = 73$ en dit blijkt deelbaar te zijn op u_{37}. Quotiënt 330929. Dit is niet deelbaar door 73. Daarna proberen we $4.37 + 1 = 149$ (147 is niet priem) en dit blijkt deelbaar te zijn op 330929. Quotiënt 2221. Nu zijn we klaar want $\sqrt{2221} < 50$. Dus $u_{37} = 73.149.2221$.

Het kleinste priemgetal waarvoor geldt dat het bijbehorende getal van Fibonacci niet priem is, is 19; $u_{19} = 4181 = 37.113$.

In de nu volgende paragraaf wordt nog een belangrijke getallentheoretische toepassing van de getallen van Fibonacci gegeven.

§ 2 Getallen van Mersenne

H.J.A.Duparc

Als toepassing van het in de vorige paragraaf behandelde laten wij zien hoe daarmede onderzocht kan worden of een bepaald getal van Mersenne priem is of niet.

Onder een getal van Mersenne verstaat men een getal van de gedaante 2^p-1, waarbij p een priemgetal is. Het is duidelijk dat 2^m-1 voor samengestelde m niet priem is, immers $2^{ab}-1$ is deelbaar door 2^a-1. Bijgevolg kan een getal 2^m-1 slechts priem zijn als m priem is, dus als 2^m-1 een getal van Mersenne is. Niet elk getal van Mersenne is echter priem zoals blijkt uit $2^{11}-1 = 23.89$.

In 1644 beweerde o.a. Mersenne dat 2^p-1 priem is voor p = 2,3,5,7,13, 17,19,31,67,127,257. Later bleek dat dit niet geheel juist was en dat o.a. $2^{67}-1$ samengesteld is.

Een eerste uitspraak over de getallen 2^p-1 is gedaan door Euler.

Euler merkte op dat 2^p-1 samengesteld is als $p \equiv 3 \pmod 4$ en als $q=2p+1$ priem is. Immers dan is $q \equiv 7 \pmod 8$ dus (vgl. hoofdstuk IV blz. 13) dan is het getal 2 kwadraatrest mod q, zodat het criterium van Euler (zie hoofdstuk IV blz. 11) ons dan leert $2^{\frac{1}{2}(q-1)} \equiv 1 \pmod q$, dus $q \mid 2^p-1$. Wij merken op dat Eulers opmerking slechts van toepassing kan zijn als p en 2p+1 priem zijn, dus 2p en 2p+1 niet door 3 deelbaar zijn, dus als $3 \mid 2p-1$ is, d.w.z. $p \equiv 2 \pmod 3$. Eulers opmerking is dus slechts van toepassing als $p \equiv 11 \pmod{12}$ en als 2p+1 priem is. Dan is dus $2p+1 \mid 2^p-1$. Voor p = 11 vonden wij dit resultaat reeds eerder. De eerstvolgende waarde van p waarop het behandelde van toepassing is, is p = 23, dus $47 \mid 2^{23}-1$.

De mathematicus Lucas heeft een methode aangegeven, waarmede men voor een willekeurige ondeelbare p kan uitmaken of 2^p-1 priem is. Wij zullen een speciaal geval behandelen, waarbij $p \equiv 3 \pmod 4$ is. Voor $p \equiv 1 \pmod 4$ verloopt het onderzoek op een analoge wijze.

Alvorens Lucas' criterium te formuleren, beschouwen wij nog de in §1 van dit hoofdstuk behandelde rij $u_0, u_1, \ldots$ van Fibonacci. Wij stellen $v_n = \omega^n + \bar{\omega}^n = u_{2n} : u_n$. Dan heeft men zoals bij narekenen onmiddellijk blijkt $v_n = v_{n-1} + v_{n-2}$; $v_0 = 2$, $v_1 = 1$; $v_{2n} = v_n^2 - 2$ $(n \geq 2)$.

Het criterium van Lucas luidt nu als volgt:
Zij $p \equiv 3 \pmod 4$, dan is $2^p-1 \mid v_{2^{p-1}}$, als 2^p-1 priem is en omgekeerd.

Bewijs:
1°. Onderstel $p \equiv 3 \pmod 4$ en $q = 2^p-1$ priem. Dus $q \equiv 2^3-1 \equiv 2 \pmod 5$, dus $C(q) \nmid q+1 = 2^p$; $C(q) \mid 2(q+1) = 2^{p+1}$. Bijgevolg is dan $C(q) = 2^{p+1}$, dus $\omega^{\frac{1}{2}C(q)} \equiv -1 \pmod q$, dus

$$q \mid \omega^{2^p} + 1 \mid \bar{\omega}^{2^{p-1}}(\omega^{2^p} + 1) = \omega^{2^{p-1}} + \bar{\omega}^{2^{p-1}} = v_{2^{p-1}}.$$

Omgekeerd zij $p \equiv 3 \pmod 4$ en $q \mid v_{2^{p-1}}$, dus

$$q \mid \omega^{2^{p-1}} + \bar{\omega}^{2^{p-1}} \mid \omega^{2^{p-1}}(\omega^{2^{p-1}} + \bar{\omega}^{2^{p-1}}) = \omega^{2^p} + 1,$$

dus

$$\omega^{2^p} \equiv -1 \pmod q.$$

Onderstel nu dat $q = a_1 a_2 \ldots a_h \cdot b_1 b_2 \ldots b_k$, waarbij voor $i=1,\ldots,h$ en $j=1,\ldots,k$ de getallen a_i en b_j priem zijn en verder geldt $a_i \equiv \pm 1 \pmod{10}$, $b_j \equiv \pm 3 \pmod{10}$.

Men heeft dan voor elk der bovengenoemde getallen i en j

$$\omega^{2^p} \equiv -1 (a_i); \quad \omega^{2^p} \equiv -1 (b_j),$$

dus

$$\omega^{2^{p+1}} \equiv 1 (a_i); \quad \omega^{2^{p+1}} \equiv 1 (b_j),$$

dus

$$C(a_i) = 2^{p+1}; \quad C(b_j) = 2^{p+1}.$$

Omdat $a_i \equiv \pm 1 \pmod{10}$, is $C(a_i) \mid a_i - 1$. Wegens (5.1.18), dus $a_i = s_i . 2^{p+1} + 1$, waarbij s_i een natuurlijk getal is. Omdat $b_j \equiv \pm 3 \pmod{10}$, is $C(b_j) \mid 2(b_j + 1)$ wegens (5.1.18), dus $b_j = t_j 2^p - 1$, waarbij t_j een natuurlijk getal is.
Dus

$$2^p - 1 = q = \prod_i a_i \prod_j b_j = \prod_i (s_i . 2^{p+1} + 1) \prod_j (t_j . 2^p - 1),$$

waaruit direct volgt dat h = 0, k = 1, zodat $2^p - 1$ slechts één priemfactor b_1 bezit en dus priem is. Hiermede is het criterium van Lucas bewezen.
Als voorbeeld nemen wij p = 7 en hebben dan $q = 2^7 - 1 = 127$.
Wij onderzoeken nu of $127 \mid v_{64}$.
Nu is $v_2 = 3$, $v_4 = v_2^2 - 2 = 7$, $v_8 = 7^2 - 2 = 47$, dus

$$v_{16} = 47^2 - 2 \equiv 48 \pmod{127}, \quad v_{32} \equiv 48^2 - 2 \equiv 16 \pmod{127},$$

$$v_{64} \equiv 16^2 - 2 \equiv 0 \pmod{127}.$$

Het getal 127 is dus priem.
Door gebruik te maken van moderne rekenmachines is het criterium van Lucas ook te gebruiken bij grotere waarden van p.
Ook voor getallen van de gedaante $2^p - 1$, waarbij p een priemgetal is met $p \equiv 1 \pmod{4}$, geldt een criterium als het bovenstaande, maar daarbij moet men uitgaan van een andere recurrente rij van de tweede orde dan de rij van Fibonacci. Dergelijke rijen worden in hoofdstuk VI behandeld. Het criterium is ten slotte ook van toepassing op getallen van de gedaante $a.2^n - 1$ voor zekere waarden van a en n. Ook in die gevallen maakt men gebruik van een bepaalde recurrente rij van de tweede orde. Met de behandelde methode is het getal $2^{127} - 1$ gevonden, dat tientallen jaren het grootste bekende priemgetal was. De Mersennegetallen $2^p - 1$ zijn priem gebleken voor p = 2,3,5,7,13,17,19,31,61,89,107,127. In dit jaar is men, gebruik makende van de methode van Lucas, met behulp van moderne rekenmachines in staat geweest om aan deze rij nog toe te voegen de getallen p = 521, 607 en 1279, zodat het grootste ons thans bekende priemgetal $2^{1279} - 1$ is.

Een vermoeden van Van Wijngaarden luidt, dat als $P = 2^p - 1$ een priemgetal is van Mersenne, dit ook het geval is met het getal $2^P - 1$. Het eerstvolgende nieuwe priemgetal dat op deze wijze te vinden is vindt men dan door p = 13 te nemen; het zou dan het getal $2^{8191} - 1$ zijn. Mocht het vermoeden juist blijken dan is hiermede het bepalen van willekeurig grote priemgetallen geen probleem meer. Men neme slechts de in hoofdstuk I, § 1 behandelde recurrente rij 10, die ons willekeurig veel willekeurig grote priemgetallen oplevert.

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

Colloquium Recurrente Rijen

Hoofdstuk VI

Ontbindingen in priemfactoren van gehele algebraïsche getallen

J.Verhoeff

§1. Idealen en ringen

Onder een binaire operatie op een verzameling V verstaat men een functie die aan elk geordend tweetal elementen uit V éénduidig een derde element uit V toevoegt; men schrijft dit als $\mathcal{O}(a,b) = c$ of $a+b = c$ of $ab = c$ (algemene, additieve en multiplicatieve schrijfwijze). Een binaire operatie heet associatief als voor elk drietal elementen a, b en c uit V (afgekort $a,b,c \in V$) geldt $\mathcal{O}(a, \mathcal{O}(b,c)) = \mathcal{O}(\mathcal{O}(a,b),c)$. Een binop heeft een rechts (resp. links) inverse als voor alle $a,b \in V$ er een x (resp. y) bestaat, zodat $\mathcal{O}(a,x) = b$ (resp. $\mathcal{O}(y,a) = b$). x en y heten de oplossingen van $\mathcal{O}(a,x) = b$ en $\mathcal{O}(y,a) = b$. Een verzameling met een associatieve binop die een links en een rechts inverse heeft heet een groep. Hiervoor geldt het volgende: de oplossing van $\mathcal{O}(a,x) = a$; zij o dan is $\mathcal{O}(b,o)=b$. Bewijs: y zij de oplossing van $\mathcal{O}(y,a) = b$ dan is $\mathcal{O}(b,o) = \mathcal{O}(\mathcal{O}(y,a),o) = \mathcal{O}(y,\mathcal{O}(a,o)) = \mathcal{O}(y,a) = b$ voor alle b. Ook is $\mathcal{O}(o,b) = b$ voor alle b; zij nl. $b = \mathcal{O}(o,x)$ dan is $\mathcal{O}(o,b) = \mathcal{O}(o, \mathcal{O}(o,x)) = \mathcal{O}(\mathcal{O}(o,o),x) = \mathcal{O}(o,x) = b$. Is nu σ_b de oplossing van $\mathcal{O}(b,x) = b$ dan heeft men voor o_b dezelfde eigenschappen dus $\mathcal{O}(o,o_b) = o = o_b$. Is verder $\mathcal{O}(a,x) = \mathcal{O}(a,y)$ dan is $x = y$ immers als $\bar{a}$ de oplossing is van $o = \mathcal{O}(x,a)$ dan is $\mathcal{O}(\bar{a}, \mathcal{O}(a,y)) = \mathcal{O}(\bar{a}\mathcal{O}(a,x)) = \mathcal{O}(\mathcal{O}(\bar{a},a),x) = \mathcal{O}(o,x) = x = y$.

Een groep heet Abels als zijn operatie commutatief is, d.i. $\mathcal{O}(a,b) = \mathcal{O}(b,a)$. Heeft men op een Abelse groep G een tweede associatieve binop $P(a,b)$, die links en rechts distributief is t.o.v. de groepsoperatie, d.w.z. $P(a, \mathcal{O}(b,c)) = \mathcal{O}(P(a,b)P(a,c))$ en $P(\mathcal{O}(a,b),c) = \mathcal{O}(P(a,c),P(b,c))$, dan heet de groep een ring. Meestal schrijft men voor $\mathcal{O}(a,b)$ $a+b$ en voor $P(a,b)$ ab. Uit de distributiviteit volgt $a0=0$ immers $ab + 0 = ab = a(b+0) = ab+a0$. Op dezelfde wijze bewijst men $0a=0$ uit de rechts distributiviteit van de vermenigvuldiging. Als $b \neq 0$ dan is er geen x zodat $0x=b$ of $x0=b$. De ring heet een scheef lichaam als de vermenigvuldiging een links en rechts inverse heeft, waarbij in bovenstaande definitie voor inverse $a \neq 0$ moet zijn. In geval van een commutatieve vermenigvuldiging heet het een lichaam zonder meer.

Een bekend voorbeeld van een ring vormen de gehele getallen met de gewone optelling en vermenigvuldiging als operaties. Ook de restklassen mod m vormen een ring; deze ring kan echter nuldelers bezitten (in een ring heet een element $a \neq 0$ een nuldeler als er een element $x \neq 0$ bestaat zodat ax of xa nul is). Dit kan optreden als m niet priem is, bijv. als

m = ab; dan zijn de restklassen van a en b nuldelers. Een commutatieve ring zonder nuldelers noemen we een integriteitsgebied; bijvoorbeeld de ring der even getallen.

Een ring kan een element e bezitten (één genaamd), zodanig dat ea = = ae = a. De ring der gehele getallen heeft een één terwijl de ring der even getallen die niet bezit.

Een deelverzameling van een ring R, die met a en b ook hun verschil bevat evenals het product ar (resp. ra) met een willekeurig element r uit de ring, heet een rechtsideaal (resp. linksideaal). Bevat de verzameling beide producten dan heet ze een tweezijdig ideaal. In een commutatieve ring vallen deze drie begrippen samen; men spreekt dan van een ideaal. Bevat een ideaal A twee elementen a en b dan ook a-a = 0 en 0-b = -b en a-(-b) = a+b.

Een ideaal dat a bevat zal dus ook 2a, 3a enz. bevatten evenals de producten sa met s in R en de sommen van sa+na. De verzameling van alle elementen van de vorm sa+na is een ideaal; dit heet het ideaal voortgebracht door a; notatie (a). Een dergelijk ideaal heet hoofdideaal. Als de ring een één heeft dan kan men voor sa+na schrijven sa+n(ea) = (s+ne)a = = s'a; het ideaal bestaat dan uit de veelvouden van a. Een ideaal voortgebracht door twee elementen a en b bestaat dan uit alle sommen sa + rb (s en r in de ring); notatie (a,b). Een integriteitsgebied met een één waarin elk ideaal een hoofdideaal is heet hoofdideaalring. De gehele getallen vormen een voorbeeld; het bewijs hiervan berust op de deling met rest (RR 17). Bestaat een ideaal A niet alleen uit nul (anders waren we al klaar) dan bevat het een getal $a \neq 0$ dus ook -a en één van beide is positief. Neem het kleinste positieve getal uit het ideaal, noem het d en zij b een willekeurig getal uit het ideaal. Dan zijn er gehele getallen q en r te vinden, zodat $b = dq + r$ met $0 \leq r < d$.
In geval $r > 0$ hebben we wegens $r = dq - b \in A$ ($dq \in A$ en $b \in A$) een tegenspraak met de minimaliteit van d, dus $r = 0$ en $b = qd$. Dit laat zich als volgt generaliseren. Een commutatieve ring R heet Euclidisch als aan ieder element $a \neq 0$ een niet negatief geheel getal g(a) toegevoegd met de volgende eigenschappen.
1^o Voor $a \neq 0$ en $b \neq 0$ is $ab \neq 0$ en $g(ab) \geq g(a)$.
2^o Voor iedere twee elementen a en b met $a \neq 0$ bestaat er een voorstelling $b = qa + r$ met $r = 0$ of $g(r) < g(a)$. Hieraan voldoet bijv. de ring der gehele getallen met g(a) = |a| en de ring P[x] van de polynomen in x met rationale coëfficiënten, d.w.z. $f \in P[x]$ als $f = \sum_{i=0}^{n} a_i x^i$ met a_i rationaal. Hier kan men voor g(f) de graad n nemen. 1^o is triviaal en 2^o als $a = \sum_{i=0}^{n} a_i x^i$ en $b = \sum_{i=0}^{m} b_i x^i$ als $n > m$ of als $b = 0$, dan voldoet $q = 0$ en $r = b$ en als

$n \leq m$ dan veronderstellen we bij vaste a de stelling bewezen voor polynomen met graad $< m$. Het polynoom $c = b - \frac{b_m}{a_n} x^{m-n} a$ is identiek nul of heeft een graad $< m$. In het eerste geval is $r = 0$ en $q = \frac{b_m}{a_n} x^{m-n}$ en in het tweede geval hebben we $c = q_1 a + r_1$; dan voldoen $q = q_1 + \frac{b_m}{a_n} x^{n-m}$ en $r = r_i$.
In een Euclidische ring is elk ideaal een hoofdideaal (a), waarvan ieder element een veelvoud van a is. Het bewijs hiervan is analoog aan dat hierboven gegeven voor de gehele getallen. In het bijzonder heeft een Euclidische ring een één. De gehele ring is nl. een ideaal, dus een hoofdideaal (a), en elk element is een veelvoud van a. In het bijzonder $a = ea$ en $b = qa = qea = be$ dus e is een één. In een integriteitsgebied R met een één e noemt men een element a deelbaar op b, $(a|b)$, als er een x bestaat zodat $ax = b$. Een element deelbaar op e heet een eenheid; deze eenheden vormen een ~~lichaam~~ multiplicatieve groep. Elementen die op elkaar deelbaar zijn heten geassocieerd; hun quotient is een eenheid, immers $ax = b$ en $by = a$, dus $b = bxy$ $xy = e$. Verder zal een element p priem heten als het geen eenheid is en alleen deelbaar is door eenheden en door met p geassocieerde elementen.

Wil men nu een willekeurig element schrijven als product van priemelementen dan zal dit slechts éénduidig kunnen zijn op de volgorde van de factoren en op eenheidsfactoren na. In een hoofdideaalring geldt de stelling van de „eenduidige" priemfactorontbinding: In een hoofdideaalring H is ieder element a dat geen eenheid is een product van priemfactoren $a = p_1 \ldots p_s$ en als $a = q_1 \ldots q_t$ een tweede ontbinding van a in priemfactoren is dan is $s = t$ en dan is er een permutatie $(i_1 \ldots i_s)$ van de getallen $(1 \ldots s)$ zodanig dat p_j geassocieerd is met q_{i_j}.

Bew.: Stel dat a niet het product is van eindig veel priemelementen, dan is a niet priem en dus te schrijven als $a_1 b_1$ met a_1 en b_1 niet geassocieerd met a. Nu moet voor a_1 of b_1 eveneens gelden dat het niet het product is van eindig veel priemelementen; laat dit voor b_1 zo zijn. Dan is $b_1 = a_2 b_2$ enz. en $b_n = a_{n+1} b_{n+1}$ waarbij voor alle n de factor b_n niet als product van eindig veel priemfactoren is te schrijven, a_n geen eenheid is en $a = a_1 a_2 \ldots a_n b_n$.

Beschouw nu de verzameling $\{rb_j\} = B$ van alle producten van een of ander element $r \in H$ en een b_j. Deze verzameling B is een ideaal, want $rb_j - sb_j = (r-s)b_j \in B$ en als $k < j$ dan is $rb_j - sb_k = rb_j - sa_{k+1} \ldots a_j b_j = (r - sa_{k+1} \ldots a_j) b_j \in B$. B is een hoofdideaal dus $B = (ub_m)$ met $u \in H$. Daar $b_m \in B$ is $b_m = vub_m$ en $(b_m) = (ub_m) = B$. Voor b_{m+1} hebben we dan $b_{m+1} = tb_m$, maar $b_m = a_{m+1} b_{m+1}$ dus $b_{m+1} = ta_{m+1} b_{m+1}$ en $e = ta_{m+1}$. Hieruit volgt dat a_{m+1} een eenheid is, in tegenspraak met de veronderstelling.
Voor de eenduidigheid gebruiken we als de klassieken de stelling: als p

een priemelement is waarvoor geldt $p \mid ab$ en $p \nmid a$ dan geldt $p \mid b$. Om dit te bewijzen beschouwen we het ideaal voortgebracht door a en p. Dit is een hoofdideaal, dus geldt $(a,p) = (d)$. We hebben dus $d = ax + py$, $a = sd$ en $p = td$. Daar p priem is, is dus of d of t een eenheid. Als t een eenheid is dan $p \mid d$, dus $p \mid sd = a$ in tegenspraak met het gegeven. Dus d is een eenheid; dus is wegens $bd = abx + pby$ en $p \mid ab$, $p \mid bd$ en $p \mid b$. Het bewijs is nu verder simpel.

Stel $a = \prod_{i=1}^{n} p_i = \prod_{i=1}^{m} q_i$ met p_i en q_i priem. p_1 deelbaar op $\prod q_i$ dus deelbaar op een q_j, dus geassocieerd aan q_j. Deel p_1 en q_j weg dan is er aan weerszijden één factor minder.

Door dit proces herhaaldelijk toe te passen volgt het laatste deel van de stelling.

§ 2. Algebraïsche getallen.

In de vorige paragraaf beschouwden we verzamelingen met willekeurige elementen; thans echter zullen we uitsluitend verzamelingen V van complexe getallen beschouwen. Als operaties nemen we de optelling en de vermenigvuldiging; of dit inderdaad operaties op V zijn hangt van V af, immers de som en het product van twee getallen uit V behoeven niet tot V te behoren. Is hieraan wel voldaan en behoort bovendien hun verschil ook tot V dan is de verzameling een ring, daar aan de andere eisen automatisch voldaan is. De verzameling is een lichaam als ze met twee getallen hun som, product, verschil en quotient (zo dat bestaat) bevat. We spreken dan van een getallenlichaam, waarbij we het geval dat nul het enige element is uitsluiten. Elk getallenlichaam K bevat het lichaam P der rationale getallen, zodat dit het kleinste getallenlichaam is. Immers K bevat een getal $a \neq 0$, dus ook $a/a = 1$ en $1+1$ enz., dus de gehele getallen, die we voortaan de gehele rationale getallen zullen noemen. Het quotient van twee gehele getallen moet dan ook tot K behoren en dus $P \subseteq K$. De verzameling van alle complexe getallen is kennelijk ook een getallenlichaam en uiteraard het grootste. Andere voorbeelden zijn:

1° Alle getallen van de vorm $a + b\sqrt{37}$ met $a,b \in P$;

2° Als 1° maar $a,b \in K$ met K een willekeurig getallenlichaam;

3° Alle getallen van de vorm $a+bi$ met $ab \in P$;*)

4° Als 3° met $a,b \in K$ (K een willekeurig getallenlichaam);

5° Alle getallen van de vorm $\frac{f(t)}{g(t)}$ waarbij $f(x)$ en $g(x)$ willekeurige veeltermen zijn met coëfficiënten uit P en $g(t) \neq 0$;

6° Als 5° maar $f(x)$ en $g(x)$ met coëfficiënten uit een willekeurig getallenlichaam K;

7° Als 5° maar met e i.p.v. t. Hier is aan $g(e) \neq 0$ altijd voldaan als $g(x) \not\equiv 0$, wat we echter hier niet zullen bewijzen. Men ziet gemakkelijk in dat in deze voorbeelden aan alle eisen is voldaan.

*) Dit zijn de zgn. getallen van Gausz.

8^{o} Als 6^{o} maar met e i.p.v. t.

In voorbeeld 1 hebben we een minimaal getallenlichaam dat $\sqrt{37}$ bevat en in voorbeeld 7 één dat e bevat. Een getal ϑ heet algebraïsch over een lichaam K als ϑ nulpunt is van één of ander polynoom met coëfficiënten uit K, dat niet identiek nul is. Bestaat een dergelijk polynoom niet, dan heet ϑ transcendent over K. In geval K = P spreekt men van algebraïsch resp. transcendent zonder nadere toevoeging. Zo is bijvoorbeeld $\sqrt{e}$ transcendent, maar algebraïsch over elk lichaam dat e bevat (nulpunt van $x^2 - e = 0$).

De polynomen over een lichaam K vormen een Euclidische ring K[x] (VI §1). De van nul verschillende getallen uit K zijn hierin de eenheden. Immers $C.C^{-1} = 1$ (1 is ook de één van K[x]!) en uit $F(x)G(x) = 1$ volgt $F(x) = a$ en $G(x) = a^{-1}$. De priemelementen, dat zijn dan de polynomen F(x) die niet te schrijven zijn als $F(x) = P(x)Q(x)$ (waarin P(x) en Q(x) geen eenheden zijn, dus een graad > 0 hebben) heten irreducibel (over K).

Bij een getal ϑ dat algebraïsch is over K bestaat er dus een polynoom $\varphi(x)$, zodat $\varphi(\vartheta) = 0$; er is dan ook een polynoom f(x) met minimale graad n en hoogste coëfficiënt (dat is de coëfficiënt van x^n) gelijk aan 1. We noemen ϑ algebraïsch van de graad n.

Stelling. Het boven beschouwde polynoom f(x) is irreducibel over K en is éénduidig bepaald. Het heet het canonieke polynoom van ϑ.

Bewijs. Stel $f(x)=f_1(x)f_2(x)$ met graad $f_i(x)=n_i > 0$ dan is $f(\vartheta)=f_1(\vartheta)f_2(\vartheta)=0$ dus $f_i(\vartheta) = 0$ (i = 1 of 2). Daar $n_1+n_2 = n$ geldt $n_i < n$, maar dan is ϑ nulpunt van een polynoom met lagere graad dan f(x) wat een tegenspraak geeft; derhalve is f(x) irreducibel over K. Stel er zijn twee dergelijke polynomen f(x) en $f^*(x)$ beschouw dan $g(x) = f(x) - f^*(x)$. g(x) heeft een graad kleiner dan n (x^n valt zéker weg) of is identiek nul. Het eerste geval kan niet daar $g(\vartheta) = 0$, dus $f(x) = f^*(x)$. Elk getal $a \in K$ is algebraïsch van de graad 1 over K met x-a als canoniek polynoom.

Het minimale lichaam dat K en ϑ bevat (het bestaat als doorsnede van alle lichamen met die eigenschap) heet het lichaam $K(\vartheta)$ ontstaan door adjunctie van ϑ aan K. Voorbeeld 6 is het lichaam K(t).

Op dezelfde wijze kan men de adjunctie van meer getallen aan een getallenlichaam definiëren. Notatie $K(\vartheta_1, \vartheta_2)$ enz. De stelling dat de adjunctie van meer (eindig veel) algebraïsche getallen altijd gelijkwaardig is met de adjunctie van één geschikt gekozen algebraïsch getal zullen we hier niet bewijzen. Een lichaam ontstaan uit K door adjunctie van een algebraïsch getal ϑ heet een algebraïsch getallenlichaam over K. De toevoeging over K wordt weer weggelaten als K = P.

Stelling. Als ϑ algebraïsch is over K van de graad n, dan is elk getal ξ uit $K(\vartheta)$ éénduidig te schrijven als $\xi = \sum_{i=0}^{n-1} a_i \vartheta^i$ waarbij $a_i \in K$.

Daar $\xi \in K(\vartheta)$ geldt $\xi = \frac{P(\vartheta)}{Q(\vartheta)}$ met $P(x)$ en $Q(x) \in K[x]$ en $Q(\vartheta) \neq 0$. Stel $f(x)$ het canonieke polynoom van ϑ, dan geldt $f(x) \nmid Q(x)$ (anders $Q(\vartheta) = 0$) en $f(x)$ priem dus is er, daar $K[x]$ Euclidisch is, een voorstelling $d = f(x)p(x) + Q(x)q(x)$ waarin d een eenheid is (dus $d \in K$) (zie RR 26). Derhalve $d = Q(\vartheta)q(\vartheta)$ en $\xi = \frac{P(\vartheta)}{Q(\vartheta)} = d^{-1}\, q(\vartheta).P(\vartheta) = g(\vartheta)$ als $g(x) = d^{-1}\, q(x).P(x)$. Wederom volgens Euclides is $g(x) = f(x)\, t(x) + r(x)$ met $r(x) = 0$ of graad $r(x)$ kleiner dan n, dus $\xi = g(\vartheta) = r(\vartheta) = \sum_{i=0}^{n-1} a_i \vartheta^i$. De éénduidigheid is eenvoudig; zij nl. $\xi = r(\vartheta) = r^*(\vartheta)$ en $r(x) \neq r^*(x)$ dan is $p(x) = r(x) - r^*(x)$ een polynoom van een lagere graad dan n met $f(\vartheta) = 0$. $\sum_{i=0}^{n-1} a_i \vartheta^i$ heet de canonieke voorstelling van ξ. $\sqrt{37}$ is algebraïsch van de graad 2, daarom bestaat $P(\sqrt{37})$ uit getallen van de vorm $a + b\sqrt{37}$ met $a,b \in P$.

Een algebraïsch getal π zal geheel heten als het nulpunt is van een polynoom met gehele rationale coëfficiënten en hoogste coëfficiënt 1. We zullen laten zien dat ook het bij π behorende canonieke polynoom gehele rationale coëfficiënten heeft.

Een polynoom met gehele rationale coëfficiënten heet primitief als de g.g.d. van zijn coëfficiënten 1 is. Elk polynoom $F(x) = \sum_{i=0}^{m} a_i x^i$ uit $P[x]$ is éénduidig te schrijven als $c.F^*(x)$ waarbij $F^*(x)$ primitief is en een positieve hoogste coëfficiënt heeft. Stel $a_i = \frac{p_i}{q_i}$ met p_i, q_i geheel rationaal, $(p_i,q_i) = 1$ $i = 0,\ldots,m$ dan voldoet $c = \frac{(p_1,\ldots,p_m)}{\{q_1,\ldots,q_m\}}\,(\operatorname{sgn} a_m)$.

Waren er twee van zulke voorstellingen $F(x) = c_1F^*(x) = c_2F^{**}(x)$ $c_j = \frac{s_j}{t_j}$ $(j = 1,2)$ dan was $s_1t_2F^*(x) = s_2t_1F^{**}(x)$. Elke factor van s_1t_2 deelt dan s_2t_1 wegens de primitiviteit van $F^{**}(x)$ en omgekeerd en daar de hoogste coëfficiënten van F^* en F^{**} positief zijn is dan $s_2t_1 = s_1t_2$ en dus ook $F^* = F^{**}$. Heeft $F(x)$ gehele rationale coëfficiënten dan is c geheel rationaal.

<u>Stelling van Gausz</u>. Het product van twee primitieve polynomen $A(x) = \sum_{i=0}^{n} a_i x^i$ en $B(x) = \sum_{i=0}^{m} b_i x^i$ is primitief.

<u>Bewijs</u>. Stel $A(x)B(x) = C(x) = \sum_{j=0}^{m+n} c_j x^j$ waarbij dus $c_j = \sum_{i=0}^{j} a_i b_{j-i}$, dus c_j geheel. Stel $C(x)$ niet primitief dan is er een priemgetal p zodat $p \mid c_j$ voor alle j. Laat nu a_K en b_l de eerste coëfficiënten van $A(x)$ resp. $B(x)$ zijn, niet deelbaar door p, dus $p \mid a_j$ $j < K$ $p \nmid a_K$ en $p \mid b_j$ als $j < l$ $p \nmid b_l$. Daar $p \mid c_{K+l} = a_0b_{K+l} + a_1b_{K+l-1} + \ldots + a_{K-1}b_{l+1} + a_Kb_l + a_{K+1}b_{l-1} + \ldots + a_{K+l}b_0$, geldt dan $p \mid a_Kb_l$ maar dat geeft een tegenspraak dus $C(x)$ is primitief.

Laat π een geheel algebraïsch getal zijn. Er is dan een polynoom $g(x)$ met

gehele rationale coëfficiënten en hoogste coëfficiënt 1 (g(x) is dus primitief) zodat $g(\pi) = 0$. Noem het canonieke polynoom van π weer f(x). Nu is $g(x) = f(x)q(x)+r(x)$; hier moet $r(x) = 0$ gelden daar $r(\pi) = 0$ en graad r(x) < graad f(x) is. Maar $f(x) = c_1 f^*(x)$ en $q(x) = c_2 q^*(x)$ met $f^*(x)$ en $g^*(x)$ primitief en dus volgens de vorige stelling is $f^*(x)q^*(x)$ primitief. Dus $g(x) = c_1 c_2 (f^*(x).q^*(x))$, maar dan moet $c_1 c_2 = 1$ zijn. Vergelijking van de hoogste coëfficiënt links en rechts geeft $c_1 = 1$ dus $f(x) = f^*(x)$ en f(x) heeft dus gehele rationale coëfficiënten.
Een geheel, rationaal getal is een geheel rationaal getal. Immers het canonieke polynoom van een rationaal getal a is x-a; de coëfficiënten hiervan moeten geheel rationaal zijn als a geheel is, maar dan is a ook geheel rationaal.
Stelling. Bij elk algebraïsch getal ϑ is er een natuurlijk getal n te vinden zodat $n\vartheta$ geheel (algebraïsch) is.
Bewijs. Er bestaat een polynoom $g(x) = \sum_{i=0}^{m} a_i x^i$ zodat $g(\vartheta) = 0$. We mogen de a_i's geheel rationaal nemen en $a_m > 0$ veronderstellen.
Dan voldoet $n = a_m$ daar $a_m\vartheta$ nulpunt is van $a_m^{m-1}\, g(\frac{x}{a_m}) = x^m + a_{m-1}x^{m-1} + + a_{m-2}a_m x^{m-2} + \ldots + a_m^{m-1}a_0$.

We zullen nu aantonen:
A) dat de getallen van een algebraïsch getallenlichaam algebraïsche getallen zijn, en
B) dat de gehele algebraïsche getallen een ring vormen (zoals we van gehele getallen gewend zijn).
Hiertoe gebruiken we een hulpstelling: Een complex getal α is algebraïsch over een getallenlichaam K, resp. geheel algebraïsch als er k complexe getallen ξ_i $(i = 1,\ldots,k)$ bestaan, waarvoor geldt: 1° niet alle ξ_i's zijn nul en 2° $\alpha \xi_j = \sum_{i=1}^{k} a_{ij}\xi_i$ voor $j = 1,\ldots,k$ en $a_{ij} \in K$ resp. a_{ij} geheel rationaal.
Bewijs. De k homogene lineaire vergelijkingen $\sum_{i=1}^{k} (\delta_{ij}\alpha - a_{ij})x_i = 0$ voor $j = 1,\ldots,k$ en $\delta_{ij} = \begin{cases} 0 \text{ als } i \neq j \\ 1 \text{ als } i = j \end{cases}$ hebben een oplossing $(\xi_1,\ldots,\xi_k)$ ongelijk aan de nuloplossing dus geldt $|\delta_{ij}\alpha - a_{ij}| = 0$.

Dus is α nulpunt van het polynoom $|\delta_{ij}x - a_{ij}| = x^k + \gamma_1 x^{k-1} + \ldots$ $\ldots + \gamma_k$ dat hoogste coëfficiënt 1 heeft en overigens coëfficiënten uit K resp. gehele rationale coëfficiënten heeft, zodat het gestelde volgt.
Bewijs van A. $\alpha \in K(\vartheta)$. ϑ algebraïsch van de graad n over K. f(x) zij het canonieke polynoom van ϑ. Stel $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_n = 1$. We passen de hulpstelling toe met k = n en $\xi_i = \vartheta^{i-1}$. De canonieke voorstelling van $\alpha\vartheta^j$ zij: $\alpha\vartheta^j = \sum_{i=0}^{n-1} a_{ij}\vartheta^i$, waarbij $a_{ij} \in K$, zodat aan alle eisen is voldaan.

De determinant $|a_{ij}|$ heet de norm van α in $K(\vartheta)$ ten opzichte van K. Notatie $|a_{ij}| = N(\alpha)$. De norm van een element a uit K is a^n. Immers $a_{ij} = a\delta_{ij}$ en $|a\delta_{ij}| = a^n$.

Stelling. $N(\alpha\beta) = N(\alpha).N(\beta)$. $\alpha, \beta \in K$.

Bewijs. Stel $\alpha\vartheta^j = \sum_{i=0}^{n-1} a_{ij}\vartheta^i$ en $\beta\vartheta^j = \sum_{i=0}^{n-1} b_{ij}\vartheta^i$ dan is $\alpha\beta\vartheta^j =$

$$= \alpha \sum_{i=0}^{n-1} b_{ij}\vartheta^i = \sum_{i=0}^{n-1} b_{ij} \sum_{K=0}^{n-1} a_{Ki}\vartheta^K = \sum_{K=0}^{n-1} \left(\sum_{i=0}^{n-1} a_{Ki}b_{ij}\right)\vartheta^K = \sum_{K=0}^{n-1} c_{Kj}\vartheta^K$$

Dus $N(\alpha\beta) = |c_{Kj}| = |a_{Ki}| \cdot |b_{ij}|$ volgens de productregel van determinanten.

Stelling B. Zijn α en β algebraïsche getallen over K resp. gehele getallen, dan zijn $\alpha \pm \beta$ en $\alpha\beta$ ook algebraïsch over K resp. geheel.

Bewijs. Er bestaan polynomen p(x) en q(x) met hoogste coëfficiënt 1 waarvan de coëfficiënten getallen uit K resp. geheel rationaal zijn zodat $p(\alpha) = 0$ en $q(\beta) = 0$. Stel $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ en $q(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_0$. We passen weer de hulpstelling toe en wel met $k = nm$ en

$$\xi_j = \alpha^N\beta^M \qquad 0 \leqslant N < n \text{ en } 0 \leqslant M < m$$

in een of andere nummering van de getallen $\alpha^N\beta^M$.

Dan is $\alpha\xi_j = \alpha^{N+1}\beta^M =$ een andere ξ_j of, nl. als $N+1 = n$,

$$\alpha\xi_j = -\sum_{K=0}^{n-1} a_K\alpha^K\beta^M.$$

Dus in elk geval $\alpha\xi_j = \sum_{K=1}^{nm} a_{Kj}\xi_K$ $\qquad a_{Kj} \in K$ resp. geheel rationaal

evenzo $\beta\xi_j = \sum_{K=1}^{nm} b_{Kj}\xi_K$ $\qquad b_{Kj} \in K$ resp. geheel rationaal,

zodat $(\alpha \pm \beta)\xi_j = \sum_{K=1}^{nm} (a_{Kj} + b_{Kj})\xi_K$

en $\alpha\beta\xi_j = \sum_{K=1}^{nm} c_{Kj}\xi_K$ met $c_{Kj} = \sum_{i=1}^{nm} a_{Ki}b_{ij}$,

waardoor het gestelde volgt.

De gehele getallen vormen dus een ring evenals de gehele getallen van een algebraïsch getallenlichaam.

De algebraïsche getallen vormen een lichaam, daar als $\alpha \neq 0$ algebraïsch is α^{-1} dat ook is (als α nulpunt is van $\sum_{i=0}^{n} a_i x^i$ dan is α^{-1} het van $\sum_{i=0}^{n} a_i x^{n-i}$). Het is echter geen algebraïsch getallenlichaam (bewijzen we hier niet).

Eenheden zijn die gehele getallen ε waarvoor ε^{-1} ook geheel is.

In de ring der gehele algebraïsche getallen kan men niet van priemgetallen spreken. Immers als π geheel is, dan is $\sqrt{\pi}$ dat ook en $\pi = \sqrt{\pi}.\sqrt{\pi}$ geeft een ontbinding ($\sqrt{\pi}$ geen eenheid als π dat niet is).

Dit heeft wel zin in de ring der gehele getallen van een algebraïsch getallenlichaam $P(\vartheta)$.

Alvorens hier verder op in te gaan bewijzen we twee stellingen.
1^o. De norm van een geheel getal is geheel rationaal en
2^o. Als van een geheel getal de norm ± 1 is dan is het een eenheid en omgekeerd.

Stel $\alpha \in P(\vartheta)$ (ϑ algebraïsch van de graad n). We hadden (RR 29 onderaan) $\alpha \vartheta^j = \sum_{i=0}^{n-1} a_{ij} \vartheta^i$ waarbij de a_{ij}'s éénduidig bepaald (zie RR 26) en hier rationaal zijn. Bovendien (zie hulpstelling RR 29) is α nulpunt van $g(x) = \det(\delta_{ij}x - a_{ij}) = \sum_{i=0}^{n} \gamma_i x^i$ met $N(\alpha) = \pm \gamma_0$ en $\gamma_n = 1$.

Nu geldt de volgende <u>hulpstelling</u>:
Als $f(x) = \sum_{i=0}^{m} a_i x^i$ het kanonieke polynoom van α is dan is $g(x)$ een macht van $f(x)$.

<u>Bewijs</u>. Aan elk getal $\alpha \in P(\vartheta)$ kunnen we als boven een matrix $M_\alpha = (a_{ij})$ toevoegen. Deze matrices vormen een ring met $(a_{ij})+(b_{ij}) = (a_{ij}+b_{ij})$; $(a_{ij})(b_{ij}) = (\sum_{k=0}^{n} a_{ik}b_{kj})$ en $a(a_{ij}) = (a_{ij})a = (aa_{ij})$ en met $(\delta_{ij}) = \mathcal{J}$ als eenheid. Blijkbaar is $M_{\sigma+\tau} = M_\sigma + M_\tau$ terwijl tevens $M_{\sigma\tau} = M_\sigma M_\tau$ (zie bewijs van normproducteigenschap) en als $a \in P$ geldt $M_a = a\mathcal{J}$.
Daar $f(\alpha) = 0$, geldt dus ook $\sum_{i=0}^{m} a_i \mathcal{J} A^i = M_0 = 0$, waarin $A = M_\alpha$.
We definiëren recurrent m matrices C_i als volgt $C_{m-1} = a_m \mathcal{J}$ en $C_{k-1} = a_k \mathcal{J} + C_k A$ $(k = m-1, \ldots, 1)$ of anders geschreven $a_m \mathcal{J} = C_{m-1}$ en $a_k \mathcal{J} = C_{k-1} - C_k A$.
Stel $C(x) = \sum_{i=0}^{m-1} C_i x^i$, dan is $C(x)(\mathcal{J}x - a) = \sum_{i=0}^{m-1} C_i x^{i+1} - \sum_{i=0}^{m-1} C_i A x^i =$
$= C_m x^m + \sum_{i=1}^{m-1} (C_{i-1} - C_i A)x^i - C_0 A = \sum_{i=0}^{m} a_i \mathcal{J} x^i - a_0 \mathcal{J} - C_0 A =$
$= f(x)\mathcal{J} - a_0 \mathcal{J} - c_0 A$.
Voor x substitueren we nu A; dan krijgen we $C(A).(\mathcal{J}A - A) = 0 = \sum_{i=0}^{m} a_i \mathcal{J} A^i +$
$- a_0 \mathcal{J} - C_0 A = - a_0 \mathcal{J} - C_0 A$.
Dus $C(x)(\mathcal{J}x - A) = f(x)\mathcal{J}$ dus ook $\det C(x).\det(\mathcal{J}x - A) = \det(f(x)\mathcal{J})$ of wel $g(x) \det(C(x)) = \{f(x)\}^n$ en dus $g(x) \mid f(x)^n$.
Daar $f(x)$ irreducibel is geldt $g(x) = c\{f(x)\}^k$ met $k \leqslant n$.
Vergelijking van de hoogste coëfficiënt geeft $c = 1$.

<u>Bewijs 1^o</u>. Is nu α geheel dan heeft $f(x)$ gehele rationale coëfficiënten en dus $g(x) = \{f(x)\}^k$ ook en $N(\alpha) = \pm \gamma_0$ is dus geheel rationaal.

<u>Bewijs 2^o</u>. Is α geheel en is bovendien $N(\alpha) = \pm 1$ dan heeft het polynoom $x^n \gamma_0 g(x^{-1}) = \gamma_0 \sum_{i=0}^{n} \gamma_i x^{n-i}$ gehele rationale coëfficiënten en hoogste coëfficiënt $1 (= \gamma_0^2 = (\pm N(\alpha))^2)$ en α^{-1} is een nulpunt. Dus is met α ook α^{-1} geheel en α is een eenheid. Het omgekeerde volgt uit $N(\alpha).N(\alpha^{-1}) = N(1) = 1$. Nu zijn $N(\alpha)$ en $N(\alpha^{-1})$ geheel rationaal, dus $N(\alpha) = \pm 1$.

Stelling. Is voor een geheel getal $\pi \in P(\vartheta)$ de norm priem, dan is π priem in de ring der gehele getallen van $P(\vartheta)$.

Bewijs. Stel $\pi = \sigma\tau$ met gehele σ en τ uit $P(\vartheta)$.

Dan is $N(\pi) = N(\sigma).N(\tau)$ dus, daar $N(\pi)$ priem is, $N(\sigma) = \pm 1$ of $N(\tau) = \pm 1$. Dus of σ of τ een eenheid.

We zullen nu de gehele getallen van een quadratisch getallenlichaam nader onderzoeken. Wij kunnen ons beperken tot getallenlichamen $P(\sqrt{D})$ met D geheel rationaal, quadraatvrij en ongelijk 0 of 1. Immers als $f(x)=x^2+ax+b$ het canonieke polynoom van ϑ is, dan is $\vartheta = -\frac{1}{2}a \pm \frac{1}{2}\sqrt{a^2-b} = c_1+c_2\sqrt{D}$ waarbij D aan de boven-vermelde eisen voldoet en $c_2 \neq 0$ (anders is f(x) reducibel). Het is eenvoudig in te zien dat $P(c_1+c_2\sqrt{D}) = P(\sqrt{D})$ als $c_2 \neq 0$.

Stel $\alpha \in P(\sqrt{D})$ we kunnen dan schrijven $\alpha = \frac{m+n\sqrt{D}}{l}$ met geheel rationale m, n en l en $((m,n),l) = (m,n,l) = 1$.

Dan is $\alpha\sqrt{D} = \frac{nD+m\sqrt{D}}{l}$ en α is dus nulpunt van (zie RR 31)

$$g(x)=\begin{vmatrix} (x - \frac{m}{l}) & -\frac{n}{l} \\ -\frac{nD}{l} & (x - \frac{m}{l}) \end{vmatrix} = x^2 - \frac{2m}{l}x + \frac{m^2-n^2D}{l^2}.$$ Nu zijn de coëfficiënten

$\frac{m^2-n^2D}{l^2} = N(\alpha)$ en $\frac{-2m}{l}$ geheel rationaal als α geheel is en omgekeerd.

Stel dus $\frac{m^2-n^2D}{l^2}$ en $\frac{2m}{l}$ geheel. Stel verder $d = (m,l)$, dan hebben we $d^2 \mid l^2 \mid m^2 - n^2D$, dus $d^2 \mid n^2D$, maar D quadraatvrij dus $d \mid n^2$. Hieruit volgt in verband met $(m,n,l) = 1$ dat $d = 1$.

Uit $l \mid 2m$ volgt dan $l \mid 2$. Als $l = \pm 1$ is alles in orde, dus alle getallen van de vorm $m+n\sqrt{D}$, met m en n geheel rationaal, zijn geheel. Stel $l = \pm 2$, dan moet $m^2 \equiv n^2D \pmod 4$ gelden. Echter daar $(m,l) = 1$, geldt $m^2 \equiv 1 \pmod 4$. We kunnen dus alleen aan de eisen voldoen als $D \equiv 1 \pmod 4$ en n oneven is.

Samenvattend: De gehele getallen in $P(\sqrt{D})$ zijn $m+n\sqrt{D}$, met m en n geheel rationaal, als $D \not\equiv 1 \pmod 4$ en $\frac{m+n\sqrt{D}}{2}$ met m en n beide even of beide oneven als $D \equiv 1 \pmod 4$.

We zullen nu een paar voorbeelden geven van priemgetallen.

In $P(\sqrt{-5})$ zijn de getallen 2, 3 en $(1\pm\sqrt{-5})$ priem.

Bewijs. $N(2) = 4$, $N(3) = 9$ en $N(1\pm\sqrt{-5}) = 6$. Een ontbinding in gehele getallen moet van de vorm $(a+b\sqrt{-5})(c+d\sqrt{-5})$ zijn, met a, b, c en d geheel rationaal (daar $-5 \not\equiv 1 \pmod 4$). $N(a+b\sqrt{-5}).N(c+d\sqrt{-5})$ moet dan 4 of 9 of 6 zijn. In elk geval dus $N(a+b\sqrt{-5}) = a^2+5b^2 = \pm 2$ of ± 3 wat kennelijk niet kan.

In $P(\sqrt{10})$ zijn 2, 3 en $(4\pm\sqrt{10})$ priem.
Bewijs. Weer geldt $N(2) = 4$, $N(3) = 9$ en $N(4\pm\sqrt{10}) = 6$. Ook hier is, daar $10 \not\equiv 1 \pmod 4$ een factor van de vorm $a+b\sqrt{10}$ met a en b geheel rationaal. Maar $N(a+b\sqrt{10}) = a^2-10b^2 = \pm 2$ of ± 3 is niet mogelijk daar ± 2 en ± 3 geen quadraatresten mod 10 zijn.
Stelling. Als $D < 0$ zijn er in $P(\sqrt{D})$ geen eenheden behalve eenheidswortels.
Bewijs. 1^o $D \not\equiv 1 \pmod 4$. Dan is $\varepsilon = m+n\sqrt{D}$ geheel als m en n geheel rationaal zijn en ε is een eenheid als $m^2-n^2D = +1$ (-1 kan niet als $D < 0$). Deze vergelijking heeft de oplossingen $m = \pm 1$ en $n = 0$. Dit zijn de enige als $D < -1$. Is $D = -1$ dan zijn bovendien $m = 0$ en $n = \pm 1$ oplossingen.
2^o $D \equiv 1 \pmod 4$. In dit geval hebben we $m^2-n^2D = +4$ met m en n beide even of beide oneven. Nu geven $m = \pm 2$ en $n = 0$ weer de eenheden ± 1. Dit zijn als $D < -4$ de enige en ingeval $D = -3 \equiv 1 \pmod 4$ zijn ook $m = \pm 1$, $n = \pm 1$ oplossingen.
Als eenheden treden dan alleen op ± 1 en als $D = -1$ bovendien $\pm i$ en in geval $D = -3$ ook $\pm\frac{1}{2}\pm i\sqrt{3}$, en dit zijn eenheidswortels.
In het reëel quadratische geval ($D > 0$) is de situatie gecompliceerder. Als voorbeeld nemen wij $D = 5$.
Hulpstelling. Er is in $P(\sqrt{5})$ geen eenheid tussen 1 en ω.
Bewijs. Stel ε zo'n eenheid. Daar $5 \equiv 1 \pmod 4$ mogen we voor ε schrijven $\frac{x+y\sqrt{5}}{2}$, waarin x en y gelijke pariteit hebben en $N(\varepsilon) = \frac{x^2-5y^2}{4} = \pm 1$.

Nu is $\frac{x-y\sqrt{5}}{2} = \frac{2N(\varepsilon)}{x+y\sqrt{5}} = \frac{\pm 1}{\varepsilon}$ dus, daar $\varepsilon > 1$, hebben we $-1 < \frac{x-y\sqrt{5}}{2} < 1$.
Dit geeft met $1 < \frac{x+y\sqrt{5}}{2} < \frac{1}{2} + \frac{1}{2}\sqrt{5}$ door optelling $0 < x < 1+\frac{1}{2}+\frac{1}{2}\sqrt{5} < 2{,}7$.
Dus x gelijk aan 1 of 2. Beide gevallen geven een tegenspraak; n.l.
$x = 1$ geeft $1 < y\sqrt{5} < \sqrt{5}$ en $x = 2$ geeft $0 < y\sqrt{5} < \sqrt{5} - 1 < 0{,}8$.
Stelling. In $P(\sqrt{5}) = P(\omega)$ zijn er oneindig veel eenheden en dit zijn de getallen $\pm\omega^n$ voor $n = 0, \pm 1, \pm 2$. We noemen ω daarom de fundamentale eenheid van $P(\sqrt{5})$.
Bewijs. Daar $N(\omega^n) = (-1)^n = \pm 1$ zijn al deze getallen eenheden.
Stel nu ε een eenheid, dan is ook $-\varepsilon$ het; een van beide is positief.
Stel $\varepsilon > 0$. Daar $\omega > 1$ is er een gehele rationale n zodat $\omega^n \leqslant \varepsilon < \omega^{n+1}$.
Uit $\omega^n < \varepsilon < \omega^{n+1}$ zou volgen dat er een eenheid $\varepsilon' = \varepsilon/\omega^n$ is zodat $1 < \varepsilon' < \omega$, dus $\varepsilon = \omega^n$.
In $P(\sqrt{2})$ is $1 + \sqrt{2}$ de fundamentale eenheid en in $P(\sqrt{3})$ is $2 + \sqrt{3}$ het (kan op analoge wijze bewezen worden).
Dat er in elk reëel quadratisch getallenlichaam een fundamentale eenheid is bewijzen wij hier niet. Het is een bijzonder geval van de eenheden-

stelling van Dirichlet.

We zagen reeds dat elk geheel getal uit een algebraïsch getallenlichaam in eindig veel priemfactoren is te ontbinden. De eenduidigheid van de ontbinding is niet altijd verzekerd. Bij voorbeeld in $P(\sqrt{-5})$ is $6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$ zodat 6 twee essentieel verschillende ontbindingen in priemfactoren heeft.

Een voorbeeld van een reëel quadratisch lichaam waarin de eenduidigheid niet geldt is $P(\sqrt{10})$ waarin 2.3 en $(4+\sqrt{10})(4-\sqrt{10})$ twee verschillende priemfactorontbindingen van 6 zijn. In $P(\sqrt{5}) = P(\omega)$ gaat het wel goed. We bewijzen n.l. dat de gehele getallen in $P(\omega)$ een Euclidische ring vormen. Dit is voldoende voor de eenduidigheid (zie RR 25). Voor de graad van een geheel getal $\pi \neq 0$ nemen we het natuurlijke getal $|N(\pi)|$. Hier is $N(p+q\omega) = p^2+pq-q^2$.

Aan de eerste eis $gr(ab) \geqslant gr(a)$ is trivialerwijze voldaan, daar $|N(ab)| = |N(a)|\,|N(b)|$.

Stel nu π en ρ geheel en $\rho \neq 0$ $(\pi, \rho \in P(\omega))$, dan is $\frac{\pi}{\rho} = \alpha = a_1+a_2\omega$ met $a_1, a_2 \in P$. Er zijn dan gehele rationale getallen b_1 en b_2 zodat $|a_i-b_i| \leqslant \frac{1}{2}$. Stel $\beta = b_1+b_2\omega$ en $\gamma = a_1-b_1+(a_2-b_2)\omega$. Dan is $\pi = \rho\alpha = \rho\beta+\rho\gamma$.

Nu is $\beta = \dfrac{(2b_1+b_2)+b_2\sqrt{5}}{2}$ geheel daar $5 \equiv 1 \pmod 4$, zodat $\rho\gamma = \pi - \rho\beta$ ook geheel is.

We zullen nu laten zien dat als $\gamma \neq 0$ geldt $0 < |N(\rho\gamma)| < |N(\rho)|$. Dit is zo daar $|N(\gamma)| = |(a_1-b_1)^2+(a_2-b_1)(a_2-b_2)-(a_2-b_2)^2| \leqslant \frac{3}{4} < 1$. Waarmee het gestelde bewezen is.

Voor D gelijk aan -11, -7, -3, -2, -1 vormen de gehele getallen uit $P(\sqrt{D})$ op dezelfde wijze een Euclidische ring.

Voor D gelijk aan -19, -43, -67, -163 geldt dit weliswaar niet, maar hier is de eenduidigheid nog wel in orde. Heilbronn en Linfoot hebben bewezen dat er hoogstens 10 imaginaire quadratische getallenlichamen zijn waarvoor de eenduidigheid geldt. Voor het eventueel ontbrekende geval heeft Lehmer bewezen dat $D < -5.10^9$ moet zijn.

De enige reële quadratische getallenlichamen waarin de gehele getallen op de bovenbeschreven wijze een Euclidische ring vormen zijn die met D = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57 en 73. Hoewel $P(\sqrt{23})$ niet hieronder valt geldt hierin wel de eenduidigheid van de ontbinding.

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

Colloquium Recurrente Rijen

Hoofdstuk VII

De rij $u_n = au_{n-1} + bu_{n-2}$.

W.Peremans.

We gaan uit van de vierkantsvergelijking $x^2-ax-b=0$ met gehele rationale coëfficiënten a en b en met $b \neq 0$. Verder veronderstellen we, dat de discriminant $D = a^2+4b \neq 0$, d.w.z. dat de vergelijking twee verschillende wortels heeft, die we ω en $\bar{\omega}$ zullen noemen. Deze wortels mogen rationaal of irrationaal (reëel of complex) zijn. Ze zijn in ieder geval geheel algebraisch. Voor de wortels geldt:

(7.1) $\omega + \bar{\omega} = a$, $\omega\bar{\omega} = -b$, $(\omega - \bar{\omega})^2 = D$.

Omdat $\omega^2 = a\omega+b$ en $\bar{\omega}^2 = a\bar{\omega}+ b$, geldt ook $\omega^n = u_n\omega + v_n$ en $\bar{\omega}^n = u_n\bar{\omega} + v_n$ voor natuurlijke n met gehele rationale u_n en v_n. Als ω en $\bar{\omega}$ rationaal zijn, zijn door één van beide betrekkingen u_n en v_n niet bepaald, maar door beide samen, wegens $\omega \neq \bar{\omega}$, wel. Nu is $\omega^{n+1} = u_n\omega^2 + v_n\omega = (au_n + v_n)\omega + bu_n$ en anderzijds is $\omega^{n+1} = u_{n+1}\omega + v_{n+1}$. Hetzelfde geldt, als men ω door $\bar{\omega}$ vervangt; dus er geldt $v_{n+1} = bu_n$ en $u_{n+1} = au_n + bu_{n-1}$. De rij u_n voldoet dus aan de recurrente betrekking $u_n = au_{n-1} + bu_{n-2}$. Verder is $\omega^n = u_n\omega + bu_{n-1}$ en $\bar{\omega}^n = u_n\bar{\omega} + bu_{n-1}$. Omdat $\omega = u_1\omega + bu_0$ en $\bar{\omega} = u_1\bar{\omega} + bu_0$, geldt $u_1 = 1$ en (wegens $b \neq 0$) $u_0 = 0$. Het is dus niet de meest algemene rij, die aan de gegeven recurrente betrekking voldoet; we zullen ons evenwel voorlopig tot de beschouwing van deze rij beperken.

Uit het voorgaande volgt

$$(7.2) \qquad u_n = \frac{\omega^n - \bar{\omega}^n}{\omega - \bar{\omega}} = \frac{\omega^n - \bar{\omega}^n}{\sqrt{D}} .$$

Nu is $\frac{u_{kn}}{u_n} = \frac{\omega^{kn} - \bar{\omega}^{kn}}{\omega^n - \bar{\omega}^n} = \sum_{j=0}^{k-1} \omega^{n(k-1-j)}\bar{\omega}^{nj}$. Het rechterlid is geheel algebraisch, omdat ω en $\bar{\omega}$ geheel algebraisch zijn, het linkerlid is rationaal; beide leden zijn dus geheel rationaal. Dit geeft ons:

(7.3) Uit $n \mid m$ volgt $u_n \mid u_m$.

Evenals bij de vroeger beschouwde rijen gaan we nu de elementen van de rij modulo een natuurlijk getal m reduceren. Omdat er slechts eindig veel restklassen mod m zijn, zijn er twee natuurlijke getallen k en l te vinden, zodat $u_k \equiv u_l \pmod m$ en $u_{k+1} \equiv u_{l+1} \pmod m$. Hieruit volgt direct voor iedere natuurlijke n, dat $u_{k+n} \equiv u_{l+n} \pmod m$. Anders dan bij de rij van Fibonacci, kunnen we de indices in de congruentie niet zonder meer verlagen. Immers $bu_{k-1} = u_{k+1} - au_k \equiv u_{l+1} - au_l = bu_{l-1}$ en

hieruit kunnen we pas tot $u_{k-1} \equiv u_{l-1}$ concluderen, als we weten, dat $(b,m) = 1$. Veronderstellen we dit echter, dan vinden we, als we $k > 1$ veronderstellen, $u_{k-1} \equiv 0 \pmod m$ en $u_{k-1+1} \equiv 1 \pmod m$: de rij is periodiek mod m. Is echter $(b,m) \neq 1$, dan vinden we slechts, dat de rij op den duur periodiek is mod m, met eventueel een beginstuk dat niet aan de periodiciteit meedoet.

We noemen het kleinste natuurlijke getal $C = C(m)$, waarvoor geldt dat er een natuurlijk getal k bestaat, zodat $u_k \equiv u_{k+C} \pmod m$ en $u_{k+1} \equiv u_{k+C+1} \pmod m$ de (grote) periode van de rij modulo m. Als $(b,m)=1$ kunnen we $C(m)$ ook definiëren als het kleinste natuurlijke getal, waarvoor $u_{C(m)} \equiv 0 \pmod m$ en $u_{C+1} \equiv 1 \pmod m$. Als $(b,m)=1$, noemen we het kleinste natuurlijke getal $c=c(m)$, waarvoor geldt $u_c \equiv 0 \pmod m$ de kleine periode van de rij modulo m.

Als P het lichaam van de rationale getallen is, beschouwen we het kleinste getallenlichaam dat ω bevat, dat is, als ω rationaal is, P zelf en, als ω irrationaal is, het lichaam $P(\omega)$ bestaande uit de getallen $x\omega + y$ met rationale x en y. In dit lichaam beschouwen we de ring R der gehele getallen; deze bestaat, als ω rationaal is, uit de gehele rationale getallen en, als ω irrationaal is, uit de gehele getallen van $P(\omega)$. In hoofdstuk VI zijn de deelbaarheidseigenschappen van deze getallen uitvoerig nagegaan. In ieder geval is ieder element van de ring te schrijven als een product van priemelementen; deze schrijfwijze behoeft echter niet eenduidig te zijn.

Op grond van het deelbaarheidsbegrip kunnen in R congruenties worden ingevoerd op geheel analoge wijze als we dat op RR 16 gedaan hebben.

Omdat $\omega^n = u_n\omega + bu_{n-1}$ en $\bar\omega^n = u_n\bar\omega + bu_{n-1}$, volgt uit $u_n \equiv 0 \pmod m$ dat $\omega^n \equiv \bar\omega^n \pmod m$. Stel nu dat voor het natuurlijke getal m geldt $(m,D) = 1$. Dan volgt uit $\omega^n \equiv \bar\omega^n \pmod m$, dat $u_n(\omega-\bar\omega) \equiv 0 \pmod m$, dus $0 \equiv u_n(\omega-\bar\omega)^2 = u_nD$, dus $u_n \equiv 0 \pmod m$.

(7.3) Als $(m,D) = 1$, is $u_n \equiv 0 \pmod m$ dan en slechts dan als $\omega^n \equiv \bar\omega^n \pmod m$.

(7.4) Als $(m,b) = (m,D) = 1$, is $c(m)$ het kleinste natuurlijke getal n waarvoor $\omega^n \equiv \bar\omega^n \pmod m$.

Als we met een vaste modulus werken schrijven we c resp. C voor $c(m)$, resp. $C(m)$.

Als nu $u_d \equiv 0 \pmod m$, dan is $\omega^d \equiv \bar\omega^d \pmod m$. Delen we nu d door c met rest: $d = cq+r$, dan vinden we $(\omega^c)^q\omega^r \equiv (\bar\omega^c)^q\bar\omega^r$, dus $\omega^{cq}(\omega^r-\bar\omega^r) \equiv 0 \pmod m$; door vermenigvuldiging met $\bar\omega^{cq}(\omega-\bar\omega)$ vinden we $(-b)^{cq}u_rD \equiv 0 \pmod m$, dus, als $(m,D) = (m,b) = 1$, $u_r \equiv 0 \pmod m$, dus, wegens de minimaliteit van c, $r = 0$, dus $c \mid d$. Dat omgekeerd uit $c \mid d$ volgt $u_d \equiv 0 \pmod m$, is een gevolg van (7.3).

(7.5) Als $(m,D) = (m,b) = 1$ geldt, is $u_d \equiv 0 \pmod m$ dan en slechts dan als $c(m) \mid d$.

Uit (7.5) volgt direct:

(7.6) Als $(m,D) = (m,b) = 1$ geldt, is $c(m) \mid C(m)$.

We schrijven dan $C(m) = v(m)c(m)$.

Uit $u_n \equiv 0 \pmod m$ en $u_{n+1} \equiv 1 \pmod m$, volgt dat $bu_{n-1} \equiv 1 \pmod m$, dus $\omega^n \equiv \bar\omega^n \equiv 1 \pmod m$. Als omgekeerd $\omega^n \equiv \bar\omega^n \equiv 1 \pmod m$ en $(m,D)=1$, dan volgt uit (7.3) dat $u_n \equiv 0 \pmod m$ en vervolgens uit $\omega^n \equiv 1 \pmod m$, dat $bu_{n-1} \equiv 1$, dus $u_{n+1} \equiv 1 \pmod m$.

(7.7) Als $(m,D) = 1$, is $u_n \equiv 0 \pmod m$ en $u_{n+1} \equiv 1 \pmod m$ dan en slechts dan als $\omega^n \equiv \bar\omega^n \equiv 1 \pmod m$.

(7.8) Als $(m,b) = (m,D) = 1$, is $C(m)$ het kleinste natuurlijke getal n, waarvoor $\omega^n \equiv \bar\omega^n \equiv 1 \pmod m$.

Uit $\omega^c \equiv \bar\omega^c \equiv bu_{c-1} \equiv u_{c+1}$ volgt, dat $\omega^{kc} \equiv \bar\omega^{kc} \equiv u_{c+1}^k$. Hieruit volgt:

(7.9) Als $(m,b) = (m,D) = 1$, is $v(m)$ het kleinste natuurlijke getal k, waarvoor geldt $u_{c(m)+1}^k \equiv 1 \pmod m$ (d.w.z. de exponent van $u_{c(m)+1}$ modulo m).

We beschouwen nu eerst als modulus een priemgetal p dat $\neq 2$, niet deelbaar op D en niet deelbaar op b is. We onderscheiden dan twee gevallen, al naar gelang D wel of niet een kwadraatrest modulo p is

I D is kwadraatrest mod p. Nu is $D = (\omega - \bar\omega)^2 = (2\omega - a)^2 = (2\bar\omega - a)^2$. Dus $1 \equiv D^{\frac{1}{2}(p-1)} = (2\omega - a)^{p-1}$, dus $(2\omega - a)^p \equiv 2\omega - a$, dus $2^p\omega^p - a^p \equiv 2\omega - a$, dus $2\omega^p - a \equiv 2\omega - a$, dus $\omega(\omega^{p-1} - 1) \equiv 0$, dus $-b(\omega^{p-1} - 1) = \bar\omega\omega(\omega^{p-1} - 1) \equiv 0$ en evenzo $-b(\bar\omega^{p-1} - 1) \equiv 0$. Omdat $p \nmid b$, geldt $\omega^{p-1} \equiv 1$ en $\bar\omega^{p-1} \equiv 1$, dus $C \mid p-1$.

II D is niet rest mod p. Dan is $-1 \equiv D^{\frac{1}{2}(p-1)} = (2\omega - a)^{p-1}$, dus $(2\omega - a)^p \equiv a - 2\omega$, dus $2^p\omega^p - a^p \equiv a - 2\omega$, dus $2\omega^p - a \equiv a - 2\omega$, dus $2\omega^p \equiv 2(a - \omega)$, dus $2\omega^{p+1} \equiv 2(a\omega - \omega^2) = -2b$, dus $2(\omega^{p+1} + b) \equiv 0$ en evenzo $2(\bar\omega^{p+1} + b) \equiv 0$, dus $\omega^{p+1} \equiv -b$ en $\bar\omega^{p+1} \equiv -b$, dus $c \mid p+1$. Noem e de exponent van $-b$ modulo p, dan is $\omega^{(p+1)e} \equiv \bar\omega^{(p+1)e} \equiv 1$, dus $C \mid e(p+1)$.

III Als $p \mid D, p \neq 2$, $p \nmid b$, dan moeten we de gevallen dat ω en $\bar\omega$ rationaal zijn of niet onderscheiden. Als ω en $\bar\omega$ rationaal zijn, volgt uit $p \mid D = (\omega - \bar\omega)^2$, dat $\omega \equiv \bar\omega \pmod p$, dus $u_p = \dfrac{\omega^p - \bar\omega^p}{\omega - \bar\omega} = \sum_{j=0}^{p-1} \omega^j \bar\omega^{p-1-j} \equiv p\omega^{p-1}$, dus $c \mid p$, dus $c = p$, daar $c = 1$ kennelijk uitgesloten is wegens $u_1 = 1$. Als ω en $\bar\omega$ irrationaal zijn, hebben we $(2\omega - a)^2 = D \equiv 0$, dus $0 \equiv (2\omega - a)^p \equiv 2^p\omega^p - a^p \equiv 2\omega^p - a$, waaruit ook weer $c \mid p$, dus $c = p$ volgt.

IV Als $p = 2$ en b oneven is, dan heeft men voor a even, dat $u_n \equiv u_{n-2}$ dus $c = C = 2$. Voor a oneven heeft men $u_n \equiv u_{n-1} + u_{n-2} \equiv u_{n-3}$, dus $c = C = 3$. We willen ook de periode van 4 bepalen. Als $a \equiv 2 \pmod 4$, dan is $u_2 = a \not\equiv 0$, en $u_4 = a^3 + 2ab \equiv 0$ en $a_5 = a^4 + 3a^2b + b^2 \equiv 1$, dus $c = C = 4$. Verder is $u_4 \not\equiv 0 \pmod 8$. Als $a \not\equiv 0 \pmod 4$, dan is $u_2 = a \equiv 0$ en $u_3 = a^2 + b \equiv \pm 1$ naar gelang $b \not\equiv \pm 1$ is. Verder is $u_5 \equiv 1$, dus als $b \equiv 1$, dan is $c = C = 2$ en als $b \equiv -1$ dan is $c = 2$, $C = 4$. In het laatste

geval is ook $C(8) = 4$. Als $a \equiv \pm 1$ en $b \equiv 1$, dan is $u_3 \not\equiv 0$, maar $u_6 = a^5 + 4a^3b + 3ab^2 \equiv 0$ en $u_7 = a^6 + 5a^4b + 6a^2b^2 + b^3 \equiv 1$, dus $c = C = 6$. Als $a \equiv 1$, $b \equiv -1$, dan is $u_3 \equiv 0$, $u_4 \equiv -1$, $u_7 \equiv 1$ dus $c = 3$ $C = 6$. Als $a \equiv -1$, $b \equiv -1$, dan is $u_3 \equiv 0$, $u_4 \equiv 1$, dus $c = C = 3$. Dit geeft dus het volgende staatje:

a	b	c(4)	C(4)
0	1	2	2
0	- 1	2	4
1	1	6	6
1	- 1	3	6
2	± 1	4	4
- 1	1	6	6
- 1	- 1	3	3

V Als $p \mid b$, dan is $u_n \equiv au_{n-1}$. Als $p \nmid a$ en d de exponent van a mod p is dan is blijkbaar $C(p) = d$. Als $p \mid a$ en $p \mid b$, dan is $C(p) = 1$.

Als $p \nmid b$ en $p \nmid D$, dan geldt in ieder geval $\omega^c \equiv u_{c+1}$ en $\bar{\omega}^c \equiv u_{c+1}$, dus $(-b)^c \equiv u_{c+1}^2$. We willen nu iets over v afleiden. We noemen weer e de exponent van -b modulo p. Dan is $u_{c+1}^{\frac{2e}{(c,e)}} \equiv (-b)^{\frac{ce}{(c,e)}} \equiv 1$, dus $v \mid \frac{2e}{(c,e)}$. Verder geldt $(-b)^{cv} \equiv u_{c+1}^{2v} \equiv 1$, dus $e \mid cv$, en verder $c \mid cv$, dus $\frac{ec}{(e,c)} \mid cv$, dus $\frac{e}{(e,c)} \mid v$. Dus $v = \frac{e}{(c,e)}$ of $v = \frac{2e}{(c,e)}$. Het eerste is dan en slechts dan het geval als $u_{c+1}^{\frac{e}{(c,e)}} \equiv 1$, het tweede dan en slechts dan als $u_{c+1}^{\frac{e}{(c,e)}} \equiv -1$. We onderscheiden nu gevallen betreffende het aantal factoren 2 in e en in c.

1° e bevat meer factoren 2 dan c; dit is dan en slechts dan het geval als $\frac{e}{(c,e)}$ even is. Dan is $u_{c+1}^{\frac{e}{(c,e)}} = (u_{c+1}^2)^{\frac{e}{2(c,e)}} \equiv (-b)^{\frac{ce}{2(c,e)}}$. Als $v = \frac{e}{(c,e)}$, dan is $1 \equiv (-b)^{\frac{ce}{2(c,e)}}$, dus $\frac{c}{(c,e)}$ is even, wat niet het geval is. Dus is $v = \frac{2e}{(c,e)}$. Wegens $4 \mid v \mid p-1$ is dan $p \equiv 1 \pmod 4$.

2° c bevat meer factoren 2 dan e; dan is c even, $c = 2d$. Uit $u_{c+1}^2 \equiv (-b)^c$ volgt dan $u_{c+1} \equiv \pm (-b)^d$, dus $\omega^c \equiv \pm(-b)^d$, dus $(-b)^d\omega^d \equiv \bar{\omega}^d\omega^c \equiv \pm(-b)^d\bar{\omega}^d$, dus $\omega^d \equiv \pm \bar{\omega}^d$. Het plusteken is uitgesloten wegens de minimaliteit van c, dus $u_{c+1} \equiv -(-b)^d$. Dus $u_{c+1}^{\frac{e}{(c,e)}} \equiv (-1)^{\frac{e}{(c,e)}} (-b)^{\frac{de}{(c,e)}} \equiv -1$ omdat $\frac{e}{(c,e)}$ oneven en $\frac{d}{(c,e)}$ (wegens $\frac{c}{(c,e)}$ even) geheel is. Dus ook nu is $v = \frac{2e}{(c,e)}$.

3° c en e bevatten evenveel factoren 2 en zijn beide even. Dan zijn $\frac{c}{(c,e)}$ en $\frac{e}{(c,e)}$ beide oneven. Evenals in geval 2° is $u_{c+1} \equiv -(-b)^d$. Verder is $e = 2f$ en $(-b)^f \equiv -1$. Dan is $u_{c+1}^{\frac{e}{(c,e)}} \equiv (-1)^{\frac{e}{(c,e)}} (-b)^{\frac{de}{(c,e)}} \equiv$

$\equiv -(-b)^{\frac{fc}{(c,e)}} \equiv 1$ omdat $\frac{c}{(c,e)}$ oneven is. Nu is dus $v = \frac{e}{(c,e)}$.

4^o c en e zijn beide oneven. Dan kan $v = \frac{e}{(c,e)}$ en $v = \frac{2e}{(c,e)}$ zijn.

Door combinatie van deze gevallen met de vroeger gemaakte gevalonderscheidingen valt nog meer af te leiden. In het vroegere geval II was $c \mid p+1$ en $e \mid p-1$, dus $(c,e) = 1$ of 2. Geval 3^o is dan echter niet mogelijk. In geval 3^o zou n.l. $v = \frac{1}{2}e$ zijn, maar $\omega^{\frac{1}{2}e(p+1)} \equiv (-b)^{\frac{1}{2}e} \equiv -1$, in strijd met $C = vc \mid \frac{1}{2}e(p+1)$. Geval 1^o levert dan de mogelijkheden c oneven, e even, $v = 2e$ en c bevat één en slechts één factor 2, $4 \mid e$, $v = e$. Geval 2^o geeft de mogelijkheden e oneven, c even, $v = 2e$ en e bevat één en slechts één factor 2, $4 \mid c$, $v = e$. Geval 4^o geeft $v = e$ of $2e$.

Om de periode van een samengesteld getal m nader te beschouwen ontbinden we m in priemfactoren: $m = p_1^{s_1} \ldots p_j^{s_j}$. We behandelen eerst een macht p^n van een priemgetal p met $p \nmid D$, $p \nmid b$. We weten dan, dat $\omega^{C(p)} \equiv \bar{\omega}^{C(p)} \equiv 1 \pmod{p}$. Noem k het grootste natuurlijke getal waarvoor $\omega^{C(p)} \equiv \bar{\omega}^{C(p)} \equiv 1 \pmod{p^k}$, dan geldt blijkbaar $C(p^h) = C(p)$ voor $1 \leq h \leq k$. We kunnen dan op een wijze, die geheel analoog is met hulpstelling 1 op blz. RR 7, bewijzen dat voor oneven p geldt dat $C(p^h) = p^{h-k}C(p)$ voor $h \geq k$. Voor $p = 2$ moeten we $C(4)$ bepalen, hetgeen hierboven daarom ook geschied is. Vervolgens bepalen we weer k door $\omega^{C(4)} \equiv \bar{\omega}^{C(4)} \equiv 1 \pmod{2^k}$ dan is $C(2^h) = C(4)$ voor $2 \leq h \leq k$ en $C(2^h) = 2^{h-k}C(4)$ voor $h \geq k$. Ten slotte is, voor $(m,D) = (m,b) = 1$, $C(m)$ het k.g.v. van $C(p_1^{s_1})$, $C(p_2^{s_2}), \ldots, C(p_j^{s_j})$. Dat het inderdaad kan gebeuren dat de k van een oneven priemgetal > 1 is (bij de rij van Fibonacci was ons daarvan geen voorbeeld bekend), blijkt uit de rij met $a = 2$, $b = 1$, dus de rij bepaald door $u_n = 2u_{n-1} + u_{n-2}$, d.i. de rij 0, 1, 2, 5, 12, 29, 70, 169, 408,... Hierin is blijkbaar $c(13) = c(13^2) = 7$. Verder is $u_8 \equiv 70 \pmod{13^2}$ dus, wegens (7.9), is $v(13^2)$ de exponent van 70 modulo 13^2. Nu is $70^2 \equiv -1 \pmod{13^2}$, dus $v(13^2) = 4$. Hieruit volgt, dat $C(13) = C(13^2) = 28$.

In de formules voor de perioden treedt de exponent e van -b op. Deze wordt bijzonder eenvoudig als b = $\pm$ 1. Als b = 1 is e = 2 en (e,c) = 1 of 2 naar gelang c oneven of even is en v = 1, 2 of 4 evenals bij Fibonacci. Als b = -1, is e = 1 en v = 1 of 2.

Een willekeurige rij w_n, die voldoet aan de betrekking $w_n = aw_{n-1} + bw_{n-2}$ met beginwaarden w_0 en w_1 is op te bouwen uit de overeenkomstige rijen u_n en v_n die aan dezelfde recursieve betrekking met $u_0 = 0$, $u_1 = 1$ en $v_0 = 1$, $v_0 = 0$ voldoen. Dan is n.l. $w_n = w_0 v_n + w_1 u_n$. Nu is echter blijkbaar $v_n = bu_{n-1}$ en dus is $w_n = w_1 u_1 + w_0 bu_{n-1}$ of

$$w_n = w_1 \frac{\omega^n - \bar{\omega}^n}{\omega - \bar{\omega}} + bw_0 \frac{\omega^{n-1} - \bar{\omega}^{n-1}}{\omega - \bar{\omega}} .$$

Hieruit volgt direct dat uit $u_n \equiv u_{n+C(m)} \pmod m$ volgt dat $w_n \equiv w_{n+C(m)} \pmod m$. De rij w_n is dus zeker periodiek modulo m met een periode C(m). De "echte" periode, d.w.z. het kleinste natuurlijke getal l, dusdanig dat de rij w_n periodiek is modulo m met een periode l, zou echter kleiner kunnen zijn dan C(m). Dit blijkt het geval te zijn als m een factor met w_1 en bw_0 gemeen heeft.

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

Colloquium Recurrente Rijen

Hoofdstuk VIII

De homogene recurrente rij van willekeurige orde.

H.J.A.Duparc.

§1 Hulpeigenschappen.

Om voor homogene recurrente rijen van willekeurige orde periodiciteitseigenschappen af te kunnen leiden voeren wij een aantal nieuwe begrippen in, die ons in de volgende paragraaf gemakkelijk de gewenste resultaten zullen opleveren.

Definitie. Een veelterm heet geheel als al haar coëfficiënten geheel zijn.

De gehele veeltermen vormen een ring.

In het vervolg zij $f(x)$ een gehele veelterm, waarvan de coëfficiënt der hoogstemachtsterm in x gelijk is aan 1. Zulke veeltermen noemen wij genormeerd. Als $f(x)$ te schrijven is in de gedaante $f_1(x)f_2(x)$ waarbij ook $f_1(x)$ en $f_2(x)$ gehele veeltermen zijn, dan zijn $f_1(x)$ en $f_2(x)$ genormeerd.

Definitie. Onder het residu mod $f(x)$ van een veelterm $g(x)$ verstaat men de ondubbelzinnig bepaalde veelterm $r(x)$, waarvan de graad kleiner is dan die van $f(x)$ (of die gelijk is aan nul) en die voldoet aan

$$g(x) = q(x)f(x)+r(x),$$

waarbij $q(x)$ een gehele veelterm is. Kort gezegd: $r(x)$ is de rest bij deling van $g(x)$ door $f(x)$.

Definitie. Zij m een willekeurig natuurlijk getal. Onder het residu modd $f(x),m$ van een veelterm $g(x)$ verstaat men de ondubbelzinnig bepaalde veelterm $s(x)$, die uit het residu $r(x)$ mod $f(x)$ van $g(x)$ ontstaat door daarin elke coëfficiënt te reduceren mod m.

M.a.w., is $f(x)$ van de graad n, dan is het residu $s(x)$ de ondubbelzinnig bepaalde veelterm van een graad $\leq n-1$, waarvan alle coëfficiënten gehele getallen ≥ 0 en $\leq m-1$ zijn, zodanig dat

$$g(x) = q(x)f(x)+mt(x)+s(x),$$

waarbij $q(x)$ en $m(x)$ gehele veeltermen zijn.

Definitie. Bij gegeven $f(x)$ en m zegt men dat voor twee gehele veeltermen $g(x)$ en $h(x)$ geldt

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

dan en slechts dan als $g(x) - h(x)$ een residu modd $f(x),m$ bezit dat gelijk is aan nul.

Stelling 1. Men heeft $g(x) \equiv h(x)$ (modd $f(x),m$) dan en slechts dan als er gehele veeltermen $q(x)$ en $r(x)$ bestaan, die voldoen aan

$$g(x) = h(x)+q(x)f(x)+mr(x).$$

Bewijs. Stel $g(x) \equiv h(x)$ (modd $f(x),m$). Bij definitie is dan het residu mod $f(x)$ van $g(x) - h(x)$ deelbaar door m; dus er bestaan dan gehele

veeltermen $q(x)$ en $r(x)$ waarvoor

$$g(x) - h(x) = q(x)f(x)+mr(x). \tag{1}$$

Omgekeerd, stel dat er gehele veeltermen $q(x)$ en $r(x)$ bestaan waarvoor (1) geldt. Zij $r_1(x)$ het residu mod $f(x)$ van $r(x)$, d.w.z. er bestaat een gehele veelterm $q_1(x)$ met

$$r(x) = q_1(x)f(x)+r_1(x).$$

Dan is

$$g(x) - h(x) = \left\{ q(x)+mq_1(x) \right\} f(x)+mr_1(x).$$

Omdat de graad van $mr_1(x)$ ten hoogste n-1 is (ofwel $mr_1(x) = 0$ is) en elk der coëfficiënten van $r_1(x)$ deelbaar is door m is het residu van $g(x)-h(x)$ modd $f(x)$,m gelijk aan nul.

De veeltermen die modd $f(x)$,m een residu nul bezitten, vormen dus een ideaal in de ring der gehele polynomen. Dit ideaal wordt voortgebracht door $f(x)$ en m.

Daar dit ideaal ook voort te brengen is door $f_1(x)$ en m, waarbij $f_1(x) = f(x)+mt(x)$ (hierbij is $t(x)$ een willekeurige gehele veelterm) heeft men:

Stelling 2. Als $g(x) \equiv h(x)$ (modd $f(x)$,m), dan is $g(x) \equiv h(x)$ (modd $f_1(x)$,m), waarbij $f_1(x) = f(x)+mt(x)$ met gehele $t(x)$.

Stelling 3. Uit $g(x) \equiv h(x)$ (modd $f(x)$,m) en $g_1(x) \equiv h_1(x)$ (modd $f(x)$,m), volgt

$$g(x) \pm g_1(x) \equiv h(x) \pm h_1(x) \text{ (modd } f(x),m)$$

en

$$g(x)g_1(x) \equiv h(x)h_1(x) \text{ (modd } f(x),m).$$

Bewijs. Op grond van het onderstelde bestaan er gehele polynomen $q(x)$, $q_1(x)$, $r(x)$ en $r_1(x)$ met

$$g(x) = h(x) + q(x)f(x) + mr(x);\ q_1(x) = h_1(x) + q_1(x)f_1(x) + mr_1(x).$$

Optelling resp. aftrekking dezer resultaten geeft op grond van stelling 1 onmiddellijk de eerste twee beweringen terwijl vermenigvuldiging leert dat geldt

$$g(x)g_1(x) = h(x)h_1(x) + q_2(x)f(x) + mr_2(x),$$

waarbij men kan nemen

$$q_2(x) = h(x)q_1(x) + h_1(x)q(x) + f(x)q(x)q_1(x)$$

en

$$r_2(x) = h(x)r_1(x) + h_1(x)r(x) + q(x)f(x)r_1(x) + q_1(x)f(x)r(x) + mr(x)r_1(x).$$

Stelling 4. Als $g(x) \equiv h(x)$ (modd $f(x),m_i$) voor $i = 1,2$, waarbij m_1 en m_2 onderling ondeelbaar zijn, dan is $g(x) \equiv h(x)$ (modd $f(x),m_1m_2$) en omgekeerd.

Bewijs. Zij $g(x) \equiv h(x)$ (modd $f(x),m_i$) voor $i = 1,2$. .

Van het residu $r(x)$ mod $f(x)$ van $g(x) - h(x)$ is iedere term deelbaar zowel door m_1 als door m_2, dus omdat m_1 en m_2 onderling ondeelbaar zijn, ook door $m = m_1 m_2$. Dus $g(x) \equiv h(x)$ (modd $f(x),m$).

Omgekeerd, zij $g(x) \equiv h(x)$ (modd $f(x),m$). Dan is iedere term van het residu mod $f(x)$ van $g(x) - h(x)$ deelbaar door m, dus door m_1 en m_2, waaruit de beweringen volgen.

Gevolg. Het onderzoek of $g(x) \equiv h(x)$ (modd $f(x),m$) is terug te brengen tot het onderzoek of geldt $g(x) \equiv h(x)$ (modd $f(x),p_i^{r_i}$) voor $i = 1,\ldots,s$, waarbij $m = p_1^{r_1} \ldots p_s^{r_s}$ en $p_1,\ldots,p_s$ verschillende priemgetallen zijn.

Alvorens een verder resultaat af te leiden, trekken wij eerst nadere conclusies uit het vroeger behandelde.

Bij willekeurig priemgetal p vormen de restklassen mod p een lichaam. Het enige dat hiertoe na het vroeger behandelde nog opgemerkt dient te worden is dat een natuurlijk getal a dat niet door p deelbaar is, mod p een inverse bezit. Dit volgt direct uit het feit dat de GGD van a en p, die dan gelijk is aan 1, te schrijven is in de gedaante $1 = ax+py$, met gehele x en y (zie hulpstelling 2, RR 5). Men heeft dus $ax \equiv 1$ (mod p), waarmede de bewering bewezen is.

Thans passen wij een eigenschap toe van hoofdstuk VI (RR 24), die zegt dat de polynomen, waarvan de coëfficiënten in een lichaam liggen, een Euclidische ring vormen. Op blz. RR 25 is bewezen dat in een Euclidische ring elk element een ondubbelzinnige ontbinding bezit in priemelementen. Bij gevolg heeft men:

Stelling 5. De mod p gereduceerde gehele veeltermen zijn op ondubbelzinnige wijze te ontbinden in priemelementen. Die priemelementen zijn hier dus mod p irreducibele polynomen.

Definitie. Wij noemen twee polynomen onderling ondeelbaar mod p, als er geen polynoom van een graad $\geqslant 1$ bestaat, dat mod p op beide deelbaar is.

Stelling 6. Als $g(x) \equiv h(x)$ (mod $f_i(x),p$) $(i = 1,2)$ waarbij $f_2(x)$ en $f_1(x)$ geen niet constante gemeenschappelijke factor mod p bezitten, dan is $g(x) \equiv h(x)$ (mod $f(x),p$), waarbij $f(x) = f_1(x)f_2(x)$ en omgekeerd.

Bewijs. Stel $g(x) \equiv h(x)$ (mod $f_i(x),p$) $(i = 1,2)$. Er bestaan gehele veeltermen $q_i(x)$ en $r_i(x)$ $(i = 1,2)$, zodanig dat

$$g(x) - h(x) = q_1(x)f_1(x) + r_1(x)p;$$

$$g(x) - h(x) = q_2(x)f_2(x) + r_2(x)p.$$

Na aftrekking vindt men dan

$$q_1(x)f_1(x) \equiv q_2(x)f_2(x) \text{ (mod } p).$$

Omdat mod p de veelterm $f_1(x)$ relatief priem is met $f_2(x)$, moet op grond der ondubbelzinnige ontbindbaarheid mod p van de veelterm $q_1(x)f_1(x)$ (stelling 5) de veelterm $f_1(x)$ deelbaar zijn op $q_2(x)$, dus $q_2(x)=f(x)q(x)$ met gehele $q(x)$. Hieruit volgt dan

$$g(x) \equiv h(x) + f_1(x)f_2(x)q(x) \pmod{p},$$

dus

$$g(x) \equiv h(x) \quad (\text{modd } f(x),p).$$

Omgekeerd, als $g(x) \equiv h(x)$ (modd $f(x),p$) is direct duidelijk dat $g(x) \equiv h(x)$ (modd $f_i(x),p$) voor iedere $f_i(x)$ die deelbaar is op $f(x)$.

Stelling 7. Voor ieder geheel polynoom $g(x)$ dat niet door p deelbaar is geldt $(g(x))^{p^N-1} \equiv 1$ (modd $f(x),p$), waarbij N de graad van $f(x)$ is en $f(x)$ irreducibel is.

Bewijs. Men beschouwt de p^N-1 van 0 verschillende veeltermen $v_i(x) = a_0+a_1x+\ldots+a_{N-1}x^{N-1}$ $(i = 1,\ldots,p^N-1)$, waarbij elk der coëfficiënten $a_0,a_1,\ldots,a_{N-1}$ elk der waarden $0,1,\ldots,p-1$ kan aannemen. Verder beschouwt men de modd $f(x),p$ gereduceerde polynomen $g(x)v_i(x)$, die wij $w_i(x)$ zullen noemen. Uiteraard heeft men $p \nmid w_i(x)$, dus $w_i(x) \not\equiv 0 \pmod{p}$ en voor $i \neq j$ heeft men $w_i(x) \neq w_j(x)$ dus $w_i(x) - w_j(x) \not\equiv 0 \pmod{p}$. Derhalve vormen de veeltermen $w_i(x)$ $(i = 1,\ldots p^N-1)$ een permutatie van de veeltermen $v_i(x)$ $(i = 1,\ldots,p^N-1)$. Zij $v(x)$ hun product. Dan krijgt men uit $w_i(x) \equiv g(x)v_i(x)$ (modd $f(x),p$) voor $i = 1,\ldots,p^N-1$ na vermenigvuldiging

$$v(x) \equiv (g(x))^{p^N-1} v(x) \quad (\text{modd } f(x),p),$$

dus er bestaat een gehele veelterm $q(x)$ met

$$v(x)((g(x))^{p^N-1} - 1) \equiv q(x)f(x) \pmod{p}.$$

Omdat $f(x)$ irreducibel is en $f(x) \nmid v_i(x)$ $(i = 1,\ldots,p^N-1)$ leert stelling 5 ons dat mod p geldt

$$f(x) \mid (g(x))^{p^N-1} - 1,$$

waarmee de bewering bewezen is.

Opmerking. Voor het onderzoek van zekere recurrente rijen kunnen wij volstaan met het geval dat $g(x) = x$ is. Dan heeft men

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

waaruit wij verdere conclusies zullen trekken.

Definitie. Het kleinste natuurlijke getal C waarvoor bij gegeven $f(x)$ en m geldt $x^C \equiv 1$ (modd $f(x),m$) noemt men de grote periode $C = C(f,m)$ van x modd $f(x),m$.

Stelling 8. Men heeft $x^{hC} \equiv 1$ (modd $f(x),m$) voor natuurlijke h en omgekeerd als $x^n \equiv 1$ (modd $f(x),m$), dan is n een veelvoud van C.

Bewijs. Het eerste deel der bewering volgt uit stelling 3. Om het tweede deel te bewijzen stellen wij $n = qC+s$, waarbij q geheel en $0 \leqslant s \leqslant q-1$. Dan zijn er gehele veeltermen $q_i(x)$ en $r_i(x)$ $(i = 1,2)$ te vinden waarvoor geldt

$$x^n = 1 + q_1(x)f(x) + mr_1(x) \quad (\text{want } x^n \equiv 1 \text{ (modd } f(x),m))$$

$$x^{qC} = 1 + q_2(x)f(x) + mr_2(x) \quad (\text{want uit het eerste deel der stelling volgt}$$

$$x^{qC} \equiv 1 \text{ (modd } f(x),m)),$$

dus

$$1 + q_1(x)f(x) + mr_1(x) = x^n = x^{qC}x^s = x^s + q_2(x)x^s f(x) + mr_2(x)x^s,$$

dus

$$x^s \equiv 1 \text{ (modd } f(x),m),$$

waaruit op grond der minimaaleigenschap van C volgt dat s = 0 is. Dus C | n.

Definitie. Onder het getal c(f,m) verstaat men het kleinste natuurlijke getal c waarbij een geheel getal r te vinden is met $x^c \equiv r$ (modd f(x),m). Uit $x^c \equiv r$ (modd f(x),m) volgt direct voor elke natuurlijke h de bewering $x^{ch} \equiv r^h$ (modd f(x),m).

Stelling 9. Als m relatief priem is met de bekende term b van f(x) en als een getal n de eigenschap bezit dat er een geheel getal s bestaat met $x^n \equiv s$ (modd f(x),m), dan is c | n.

Bewijs. Stel n = qc+u, waarbij q geheel is en $0 \leq u \leq c-1$. Dan is er volgens het voorafgaande een geheel getal t te vinden met

$$x^{qc} \equiv t \text{ (modd } f(x),m), \text{ dus } s \equiv x^n = x^{qc}x^u \equiv tx^u \text{ (modd } f(x),m).$$

Nu volgt uit $x^{qc} \equiv t$ (modd f(x),m), dat er gehele veeltermen g(x) en h(x) bestaan met $x^{qc} = t + g(x)f(x) + mh(x)$. Wij nemen in deze formule achtereenvolgens $x = \omega_1, \omega_2, \ldots, \omega_N$, waarbij $\omega_1, \ldots, \omega_N$ de wortels zijn der vergelijking f(x) = 0. Dan vindt men $\omega_i^{qc} = t + mh(\omega_i)$ (i = 1,...,N), dus na vermenigvuldiging

$$(-)^{Nqc}\, b^{qc} = \prod_{i=1}^{n} (t + mh(\omega_i)) \equiv t^N \text{ (mod } m).$$

Daar b en m geen factor gemeen hebben, hebben ook t en m geen factor gemeen zodat dan de inverse t^{-1} van t mod m bestaat. Uit $tx^u \equiv s$ (modd f(x),m) volgt dan $x^u \equiv st^{-1}$ (modd f(x),m), dus op grond der minimaliteitseigenschap van c krijgt men u = 0, dus c | n.

Gevolg. Stelt men bij (m,b) = 1 het getal $v(f,m) = \frac{C(f,m)}{c(f,m)}$, dan is v(f,m) geheel.

Om nu de exponent C(f,m) te bepalen van de veelterm x onderstellen wij dat $m = p_1^{r_1} \ldots p_s^{r_s}$, waarbij $p_1, \ldots, p_s$ verschillende priemgetallen zijn.

Stelling 10. Het getal C(f,m) is het kleinste gemene veelvoud g der getallen $C(f,p_i^{r_i})$ (i = 1,...,s).

Bewijs. Volgens stelling 4 volgt uit

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

dat

$$x^{C(f,m)} \equiv 1 \text{ (modd } f(x),p_i^{r_i}) \quad (i = 1,\ldots,s),$$

waaruit stelling 8 ons leert dat voor i = 1,...,s geldt $C(f,p_i^{r_i}) \mid C(f,m)$, dus g | C(f,m).

Omgekeerd heeft men

$$x^{C(f,p_i^{r_i})} \equiv 1 \pmod{f(x),p_i^{r_i}} \quad (i = 1,\ldots,s),$$

dus volgens stelling 8 geldt

$$x^g \equiv 1 \pmod{f(x),p_i^{r_i}} \quad (i = 1,\ldots,s),$$

waarna stelling 4 leert dat $x^g \equiv 1 \pmod{f(x),m}$ is, dus volgens stelling 8 heeft men dan $C(f,m) \mid g$. Hiermede is bewezen $g = C(f,m)$.

Op geheel analoge wijze vindt men:

Stelling 11. Als $(m,b) = 1$, is het getal $c(f,m)$ het kleinste gemene veelvoud der getallen $c(f,p_i^{r_i})$ $(i = 1,\ldots s)$.

Stelling 12. $C(f,p) \mid C(f,p^r) \mid p^{r-1}C(f,p^r)$.

Bewijs. Uit $x^{C(f,p^r)} \equiv 1 \pmod{f(x),p^r}$ volgt wegens stelling 4 dat $x^{C(f,p^r)} \equiv 1 \pmod{f(x),p}$, dus wegens stelling 8 dat $C(f,p) \mid C(f,p^r)$.

Verder bestaan er gehele veeltermen $q(x)$ en $r(x)$ met

$$x^{C(f,p)} = 1 + q(x)f(x) + pr(x).$$

Dus

$$x^{p^{r-1}C(f,p)} = (1 + q(x)f(x) + pr(x))^{p^{r-1}} = (1 + pr(x))^{p^{r-1}} +$$

$$+ q_1(x)f(x) \equiv 1 \pmod{f(x),p},$$

waarbij $q_1(x)$ een gehele veelterm is.

Gevolg. $C(f,p^r) = p^sC(f,p)$, waarbij s gelijk is aan een der getallen $0,1,\ldots,r-1$.

Op geheel analoge wijze vindt men

Stelling 13. Als $p \nmid b$ dan geldt $c(f,p) \mid c(f,p^r) \mid p^{r-1}c(f,p^r)$.

Gevolg. $c(f,p^r) = p^sc(f,p)$, waarbij s gelijk is aan een der getallen $0,1,\ldots,r-1$.

Uit deze resultaten volgt onmiddellijk

Stelling 14. $v(f,p^r) = p^sv(f,p)$, waarbij s gelijk is aan een der getallen $0,1,\ldots,r-1$.

Stelling 15. Als $f(x) \equiv (f_1(x))^{t_1} \ldots (f_s(x))^{t_s} \pmod{p}$, waarbij $f_1(x),\ldots,f_s(x)$ verschillende mod p irreducibele polynomen zijn, dan is $C(f,p)$ gelijk aan het kleinste gemene veelvoud g der getallen $C(f_i^{t_i},p)$ $(i = 1,\ldots,s)$.

Bewijs. Uit $x^{C(f,p)} \equiv 1 \pmod{f(x),p}$ volgt met stelling 6 direct $x^{C(f,p)} \equiv 1 \pmod{(f_i(x))^{t_i},p}$, dus wegens stelling 8 geldt $C(f_i^{t_i},p) \mid C(f,p)$ voor $i = 1,\ldots,s$, dus $g \mid C(f,p)$.

Verder volgt uit

$$x^{C(f_i^{t_i},p)} \equiv 1 \pmod{(f_i(x))^{t_i},p} \quad (i = 1,\ldots,s),$$

wegens stelling 8 dat

$$x^g \equiv 1 \ (\text{modd } (f_i(x))^{t_i}, p) \quad (i = 1,\ldots,s),$$

waarna stelling 6 leert dat $x^g \equiv 1$ (modd $f(x),p$), dus wegens stelling 8 geldt $C(f,p) \mid g$. Hieruit volgt $C(f,p) = g$.

Op geheel analoge wijze toont men aan

Stelling 16. Als $p \nmid m$ en als $f(x) \equiv (f_1(x))^{t_1} \ldots (f_s(x))^{t_s} \pmod p$, waarbij $f_1(x),\ldots,f_s(x)$ verschillende mod p irreducibele factoren zijn, dan is $c(f,p)$ gelijk aan het kleinste gemeenschappelijke veelvoud der getallen $c(f_i^{t_i},p)$ $(i = 1,\ldots,s)$.

Stelling 17. $C(f,p) \mid C(f^t,p) \mid p^q C(f,p)$, waarin q het kleinste niet negatieve gehele getal is met $t \leqq p^q$.

Bewijs. Uit $x^{C(f^t,p)} \equiv 1$ (modd f^t,p) volgt direct $x^{C(f^t,p)} \equiv 1$ (modd f,p) dus wegens stelling 8

$$C(f,p) \mid C(f^t,p).$$

Voor $t = 0$ is ook het tweede deel der bewering duidelijk, want dan is $q = 0$. Zij de bewering bewezen voor alle $t \leqq p^q$. Dan bestaan er gehele veeltermen $g(x)$ en $h(x)$ met

$$x^{p^q C(f,p)} = 1 + g(x)(f(x))^t + ph(x)$$

dus

$$x^{p^{q+1} C(f,p)} = \left[1 + g(x)(f(x))^t + ph(x)\right]^p \equiv 1 + (g(x))^p (f(x))^{tp} \pmod p,$$

dus

$$C(f^{t_1},p) \mid p^{q+1} C(f,p) \quad \text{voor} \quad t_1 \leqq tp \leqq p^{q+1}.$$

Hiermede is de bewering bewezen.

Gevolg. $C(f^t,p) = p^s C(f,p)$, waarbij s een der getallen $0,1,\ldots,1 + \left[\frac{\log t}{\log p}\right]$ is.

Op geheel analoge wijze vindt men

Stelling 18. Als $p \nmid b$, dan is

$$c(f,p) \mid c(f^t,p) \mid p^q c(f,p),$$

waarbij q het kleinste niet negatieve gehele getal is met $t \leqq p^q$.

Gevolg. $c(f^t,p) = p^s c(f,p)$, waarbij s een der getallen $0,1,2,\ldots,1 + \left[\frac{\log t}{\log p}\right]$ is.

Uit stelling 7 ten slotte volgt direct de volgende

Stelling 19. Voor mod p irreducibele gehele genormeerde $f(x)$ van de graad N geldt $C(f,p) \mid p^N - 1$.

Gevolg. Ook $c(f,p) \mid p^N - 1$.

Analoge beschouwingen gelden voor de kleine periode $c = c(f,m)$. Wij vermelden nog een eigenschap van het bij stelling 9 ingevoerde getal $v = v(f,m)$.

Uit $x^c \equiv r \pmod{f(x),m}$ volgt voor $x = \omega_i$ (waarbij $\omega_1,\ldots,\omega_N$ de nulpunten zijn der karakteristieke veelterm $f(x) = \sum_{h=0}^{N} a_h x^h$) dat er een gehele veelterm $q(x)$ bestaat met

$$\omega_i^c = r + q(\omega_i)m \qquad (i = 1,\ldots,N),$$

dus na vermenigvuldiging dezer relaties waarbij $(-)^N a_0 = b$ genoemd is

$$b^c \equiv r^N \pmod{m}.$$

Zij e de exponent mod m van b. Dan geldt

$$1 \equiv b^{\frac{ce}{(c,e)}} \equiv r^{\frac{eN}{(c,e)}} \pmod{m}, \text{ dus } x^{\frac{ceN}{(c,e)}} \equiv 1 \pmod{f(x),m},$$

dus

$$C \mid \frac{ceN}{(c,e)}, \text{ dus } v \mid \frac{eN}{(c,e)}.$$

Verder volgt op analoge wijze uit $x^C \equiv 1 \pmod{m}$, dat $b^C \equiv 1 \pmod{m}$, dus $e \mid C$, dus wegens $c \mid C$ ook $\frac{ce}{(e,c)} \mid C$, derhalve $\frac{e}{(e,c)} \mid v$. Bij gevolg krijgen we

Stelling 20. Men heeft $\frac{e}{(e,c)} \mid v \mid \frac{Ne}{(e,c)}$, waarbij e de exponent mod m is van de met $(-)^N$ vermenigvuldigde bekende term van $f(x)$.

Gevolg. In het geval dat $b = 1$ is geldt dus $v \mid N$.

§ 2 Toepassingen der resultaten van § 1 op rijen.

Nadat in de vorige paragraaf is aangegeven hoe de symbolen $C(f,m)$ en $c(f,m)$ voor willekeurige gehele genormeerde polynomen $f(x)$ en natuurlijke m kunnen worden bepaald, passen wij thans het gevondene toe om van enige recurrente rijen de periodiciteitseigenschappen te bepalen.

Allereerst beschouwen wij weer de rij van Fermat

$$u_{n+1} = bu_n; \qquad u_0 = 1 \qquad (n = 0,1,\ldots),$$

waarbij de karakteristieke veelterm luidt $f(x) = x-b$.

Stelling 21. Het residu van x^n mod $f(x)$ is gelijk aan u_n.

Bewijs. Voor $n = 0$ is de bewering triviaal. Geldt zij voor zekere natuurlijke n dan volgt uit $x^n \equiv u_n \pmod{f(x)}$ dat er een gehele veelterm $q(x)$ bestaat met

$$x^n = q(x)f(x) + u_n,$$

dus

$$x^{n+1} = xq(x)f(x) + xu_n = (xq(x) + u_n)f(x) + bu_n \equiv bu_n \equiv$$

$$\equiv u_{n+1} \pmod{f(x)},$$

waarmee de bewering bewezen is.

Wij merken nu op dat men voor een gegeven natuurlijk getal m met $(b,m) = 1$ heeft $u_{n+h} \equiv u_h \pmod{m}$ dan en slechts dan als $u_n \equiv u_0 \pmod{m}$, dus $x^n \equiv 1 \pmod{f(x),m}$, zodat de periode der rij juist het in de vorige paragraaf ingevoerde getal $C(f,m)$ is. Om dit getal te bepalen merken wij op dat voor alle m de veelterm $f(x) = x-b$ irreducibel is, dus $N = 1$.

Wij vinden direct uit stelling 10 dat $C(f,m)$ gelijk is aan het klein-

ste gemene veelvoud der getallen $C(f,p_i^{r_i})$ $(i = 1,\ldots,s)$ als de kanonieke ontbinding van m weer luidt $m = p_1^{r_1} \ldots p_s^{r_s}$.

Verder geldt volgens stelling 12, dat $C(f,p^r) = p^t C(f,p)$, waarbij t een geschikt gekozen geheel getal is met $0 \leqslant t \leqslant r-1$. Ten slotte leert stelling 19 dat $C(f,p) \mid p-1$.

Deze resultaten stemmen geheel overeen met de in hoofdstuk III gevondene.

Thans beschouwen wij de rij

$$u_{n+2} = au_{n+1} + bu_n;\ u_0 = 0;\ u_1 = 1 \quad (n = 0,1,\ldots).$$

Hier luidt de karakteristieke veelterm $f(x) = x^2 - ax - b$.

Stelling 22. Het residu mod f(x) van x^n is gelijk aan $u_n x + bu_{n-1}$.

Bewijs. Wij bewijzen dit weer met volledige inductie. Voor $n = 1$ is de bewering triviaal terwijl als zij voor zekere n geldt uit $x^n \equiv u_n x + bu_{n-1}$ volgt dat er een geheel polynoom q(x) bestaat met $x^n = q(x)f(x) + u_n x + bu_{n-1}$. Dan is

$$x^{n+1} = xq(x)f(x) + u_n x^2 + bu_{n-1}x = (xq(x) + u_n)\, f(x) + au_n x + bu_{n-1}x + bu_n$$

$$= (xq(x) + u_n)\, f(x) + u_{n+1}x + bu_n \equiv u_{n+1}x + bu_n \pmod{f(x)},$$

waarmee de bewering bewezen is.

Zij nu m een natuurlijk getal met $(m,b) = 1$. Dan geldt voor alle natuurlijke h $u_{n+h} \equiv u_h \pmod m$ dan en slechts dan als

$$u_{n+1}x + bu_n \equiv u_1 x + bu_0 \pmod m,$$

dus

$$x^{n+1} \equiv x \ (\mathrm{modd}\ f(x), m),$$

dus

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

De grote periode der rij is dus juist het in de vorige paragraaf ingevoerde getal C(f,m). Wij weten volgens stelling 10, dat bij $m = p_1^{r_1} \ldots p_s^{r_s}$ het getal C(f,m) het kleinste gemene veelvoud is der getallen $C(f,p_i^{r_i})$ $(i = 1,\ldots,s)$ en volgens stelling 12, dat $C(f,p^r) = p^t C(f,p)$ is waarbij t een geschikt gekozen geheel getal is met $0 \leqslant t \leqslant r-1$. Ons rest dus weer het getal C(f,p) te bepalen.

Hiertoe onderscheiden wij drie gevallen.

I. De veelterm f(x) is reducibel mod p en in de gedaante $(x-u)(x-v)$ te brengen met $u \neq v$.

Volgens stelling 15 is dan C(f,p) het kleinste gemene veelvoud der getallen C(x-u,p) en C(x-v,p), die beide op grond van stelling 19 delers zijn van p-1, dus $C(f,p) \mid p-1$ (verg. RR 37, geval I).

II. De functie f(x) is irreducibel mod p. Dan heeft men $N = 2$, waarna stelling 19 leert dat $C(f,p) \mid p^2-1$, in overeenstemming met het resultaat van RR 37, geval II, waar het getal e een deler is van p+1.

III. Het priemgetal p is deelbaar op de discriminant D van f(x). Dit houdt in dat er een getal u bestaat met

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

Op grond van stelling 17 heeft men dan

$$C(f,p) = C((x-u)^2,p) \mid pC(x-u,p),$$

waarmede de factor p van RR 37, geval III is teruggevonden.

De gevallen I en II zijn te onderscheiden door middel van de theorie der quadraatresten. Bij I is p een quadraatrest mod p, bij II een niet-rest. Een dergelijke karakterisering der gevallen I en II treedt helaas niet op bij polynomen f(x) van hogere graad.

Wij onderzoeken nu een derde orde rij

$$u_{n+3} = a_0u_{n+2} + a_1u_{n+1} + bu_n;\ u_0 = u_1 = 0,\ u_2 = 1\ (n = 0,1,\ldots),$$

waarvan de karakteristieke veelterm luidt $f(x) = x^3-a_0x^2-a_1x-b$.

Stelling 23. Analoog aan stelling 20 en 21 heeft men:
Het residu van x^n mod f(x) is gelijk aan $u_nx^2 + (a_1u_{n-1} + u_{n-2})x + bu_{n-1}$.

Bewijs. Dit gaat analoog aan dat van stelling 20 en 21 door volledige inductie.

Gevolg. Men heeft $u_{n+h} \equiv u_h \pmod{m}$ voor h = 0,1,... en voor natuurlijke m met (m,b) = 1 dan en slechts dan als

$$u_{n+2}x^2 + (a_1u_{n+1} + u_n)x + bu_{n+1} \equiv u_2x^2 + (a_1u_1 + u_0)x + bu_1 = x^2 \pmod{m},$$

dus als

$$x^{n+2} \equiv x^2 \text{ (modd } f(x),m),$$

dus

$$x^n \equiv 1 \text{ (modd } f(x),m).$$

De grote periode der rij is dus juist het in de vorige paragraaf ingevoerde getal C(f,m).

Evenals in de vorige gevallen is het getal C(f,m) te vinden uit de getallen C(f,p) waarbij p priem is. Het gedrag van C(f,p) blijkt te verschillen al naar men verkeert in de volgende gevallen:
I. f(x) is mod p reducibel en wel $f(x) \equiv (x-w_1)(x-w_2)(x-w_3) \pmod{p}$, waarbij w_1, w_2 en w_3 mod p verschillend zijn. Volgens stelling 19 geldt $C(x-w_i,p) \mid p-1$ voor i = 1,2,3, dus volgens stelling 15 is dan $C(f,p) \mid p-1$.
II. Men heeft $f(x) \equiv (x-w)g(x) \pmod{p}$, waarbij g(x) irreducibel is mod p. Stelling 19 leert dan $C(x-w,p) \mid p-1$; $C(g,p) \mid p^2-1$, dus leert stelling 15 ons dan daaruit dat $C(f,p) \mid p^2-1$.
III. De veelterm f(x) is irreducibel mod p. Dan is N = 3, dus wegens de meergenoemde stelling 19 krijgt men $C(f,p) \mid p^3-1$.
IV. p is deelbaar op D. Men heeft dan

$$f(x) \equiv (x-w_1)^2(x-w_2) \pmod{p}.$$

Is $w_1 \not\equiv w_2 \pmod{p}$, dan leert stelling 19 dat geldt $C(x-w_i,p) \mid p-1$ (i = 1,2). Stelling 17 leert dan $C((x-w_1)^2,p) \mid p(p-1)$, dus stelling 15

geeft $C(f,p) \mid p(p-1)$.

Is echter $w_1 \equiv w_2 \pmod p$, dus $f(x) \equiv (x-w_1)^3 \pmod p$, dan geldt volgens stelling 17 en 19

$$C(f,p) = C((x-w_1)^3,p) \mid pC(x-w_1,p) \mid p(p-1),$$

behalve voor $p = 2$. Dan leert stelling 17 nl. dat

$$C(f,2) = C((x-w_1)^3,2) \mid 4C(x-w_1,2) = 4.$$

Wij geven een voorbeeld van een cubische rij en nemen de rij

$$u_{n+3} = u_{n+1} + u_n \quad (n = 0,1,\ldots);\ u_0 = u_1 = 0,\ u_2 = 1.$$

De karakteristieke veelterm $f(x) = x^3 - x - 1$ bezit een discriminant $D = 23$, zodat het priemgetal 23 in geval IV verkeert en elk ander priemgetal in een der gevallen I, II of III. Verder is $b = 1$, dus $e = 1$, dus volgens stelling 20 heeft men $v \mid 3$, d.w.z. $v = 1$ of $v = 3$. Men heeft

n	u_n
0	0
1	0
2	1
3	0
4	1
5	1
6	1
7	2
8	2
9	3
10	$4 = 2^2$
11	5
12	7
13	$9 = 3^2$
14	$12 = 2^2.3$
15	$16 = 2^4$
16	$21 = 3.7$
17	$28 = 2^2.7$
18	37
19	$49 = 7^2$
20	$65 = 5.13$
21	$86 = 2.43$
22	$114 = 2.3.19$
23	151
24	$200 = 2^3.5^2$
25	$265 = 5.53$
26	$351 = 3^3.13$
27	$465 = 3.5.31$
28	$616 = 2^3.7.11$
29	$816 = 2^4.3.17$
30	$1081 = 23.47$
31	$1432 = 2^3.179$
32	$1897 = 7.271$
33	$2513 = 7.359$
34	3329
35	$4410 = 2.3^2.5.7^2$
36	$5842 = 2.23.127$
37	$7739 = 71.109$
38	$10252 = 2^2.11.233$
39	$13581 = 3^3.503$
40	$17991 = 3^2.1999$
41	23833
42	$31572 = 2^2.3^2.877$
43	$41824 = 2^5.1307$
44	$55405 = 5.7.1583$
45	$73396 = 2^2.59.311$
46	$97229 = 11.8839$
47	128801
48	$170625 = 3.5^4.7.13$
49	$226030 = 2.5.7.3229$
50	$299426 = 2.149713$
51	$396655 = 5.7^2.1619$
52	$525456 = 2^4.3^2.41.89$
53	$696081 = 3.37.6271$
54	$922111 = 59.15629$
55	$1221537 = 3.407179$
56	$1618192 = 2^4.19.5323$
57	$2143648 = 2^5.13.5153$
58	$2839729 = 59.48131$
59	$3761840 = 2^4.5.59.797$
60	$4983377 = 7.19.89.421$
61	$6601569 = 3.13.19.59.151$
62	$8745217 = 13.107.6287$
63	$11584946 = 2.19.304867$

Men heeft voor deze rij

p	c	C	v	
2	7	$7 \mid 2^3-1$	1	geval I; f(x) irreducibel mod 2
3	13	$13 \mid 3^3-1$	1	geval I; f(x) irreducibel mod 3
5	24	$24 \mid 5^2-1$	1	geval II; $f(x) \equiv (x-2)(x^2+2x+3) \pmod 5$
7	16	$48 \mid 7^2-1$	3	geval II; $f(x) \equiv (x+2)(x^2+2x+3) \pmod 7$
11	120	$120 \mid 11^2-1$	1	geval II; $f(x) \equiv (x+5)(x^2-5x+2) \pmod{11}$
13	61	$183 \mid 13^3-1$	3	geval I; f(x) irreducibel mod 13
17	288	$288 \mid 17^2-1$	1	geval II; $f(x) \equiv (x-5)(x^2+5x+7) \pmod{17}$
19	60	$180 \mid 19^2-1$	3	geval II; $f(x) \equiv (x-6)(x^2+6x-3) \pmod{19}$
23	506	$506 \mid 22.23$	1	geval IV; $f(x) \equiv (x-10)^2(x-3) \pmod{23}$
59	58	$58 \mid 59-1$	1	geval III; $f(x) \equiv (x-4)(x-13)(x+17) \pmod{59}$

Zeer schematisch geven wij aan wat bij een 4e orde rij kan geschieden. Is f(x) hiervan de karakteristieke veelterm en stelt p een priemgetal voor dan heeft men de volgende gevallen, waarbij l_i, q_i en c_i resp. lineaire, quadratische en cubische mod p irreducibele polynomen zijn en $l_i \not\equiv l_j \pmod p$, $q_i \not\equiv q_j \pmod p$ voor $i \neq j$.

I. $f(x) \equiv l_1 l_2 l_3 l_4 \pmod p$. Dan is $C(f,p) \mid p-1$.

II. $f(x) \equiv l_1 l_2 q_1 \pmod p$. Dan is $C(f,p) \mid p^2-1$.

III. $f(x) \equiv l_1 c_1 \pmod p$. Dan is $C(f,p) \mid p^3-1$.

IV. f(x) irreducibel. Dan is $C(f,p) \mid p^4-1$.

De volgende gevallen treden alleen op voor priemgetallen, die deelbaar zijn op de discriminant D van f.

V. $f(x) \equiv l_1^2 l_2 l_3 \pmod p$. Dan is $C(f,p) \mid p(p-1)$.

VI. $f(x) \equiv l_1^2 q_1 \pmod p$. Dan is $C(f,p) \mid p(p^2-1)$.

VII. $f(x) \equiv l_1^2 l_2^2 \pmod p$. Dan is $C(f,p) \mid p(p-1)$.

VIII. $f(x) \equiv q_1^2 \pmod p$. Dan is $C(f,p) \mid p(p^2-1)$.

IX. $f(x) \equiv l_1^3 l_2 \pmod p$. Dan is $C(f,p) \mid p(p-1)$ voor $p \geqslant 3$ en $C(f,p) \mid p^2(p-1)$ voor $p = 2$.

X. $f(x) \equiv l_1^4 \pmod p$. Dan is $C(f,p) \mid p(p-1)$ voor $p \geqslant 5$; $C(f,p) \mid p^2(p-1)$ voor $p = 2$ en 3.