STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1950-008

Theorie van de cirkelverdeling

"Elementaire onderwerpen van hoger standpunt belicht"

Prof.dr. S.C. v. Veen

1950

Mathematisch Centrum,
2de Boerhaavestr. 49,
A m s t e r d a m/ O.

Rapport Z.W., 1950-008
26 April 1950.

Voordracht van Prof. Dr S.C. v. Veen

THEORIE VAN DE CIRKELVERDELING

in de serie Elementaire Onderwerpen van Hoger Standpunt uit.

Tot de oudste problemen uit de elementaire vlakke meetkunde mag wel worden gerekend het probleem van de cirkelverdeling, d.w.z. het verdelen van de omtrek van een cirkel in een geheel aantal gelijke delen, uitsluitend met behulp van passer en lineaal. De verbindingslijnen der deelpunten bepalen regelmatige veelhoeken, zodat het gestelde probleem gelijkwaardig is met het vraagstuk van de constructie van regelmatige veelhoeken. Noemen wij het aantal gelijke delen = n, dan is het gestelde probleem reeds door de oude Griekse wiskundigen voor

$$n = 2^m,\ 3.2^m,\ 5.2^m \text{ en } 3.5.2^m \text{ (m is een natuurlijk getal).}$$

Men vindt de grondslagen behandeld in het vierde boek van de Elementen van Euklides.
Nadat er gedurende een tijdsverloop van 2000 jaren geen principiele vooruitgang te bespeuren was, is het bovengenoemde probleem in alle volledigheid opgelost door Gauss ($\pm$ 1800).
De jeugdige Gauss heeft op 30 Maart 1796 een klasse van met passer en lineaal construeerbare regelmatige veelhoeken ontdekt, welke de bovengenoemde omvat, maar welke bovendien nog tal van anderen bevat (wellicht nog oneindig vele andere). Eerst later, in 1801 heeft hij gevonden, dat het gestelde probleem door zijn oplossing van 1796 afgesloten was; er zijn geen andere regelmatige veelhoeken te construeren met passer en lineaal, dan de in 1796 gevondene.
Het resultaat van Gauss kan in de volgende uitkomst worden samengevat:
Noodzakelijke en voldoende voorwaarde voor de construeerbaarheid van een regelmatige veelhoek met passer en lineaal is, dat het aantal zijden wordt gegeven door

$$n = 2^m \prod p_k. \qquad (1)$$

m geheel ≥ 0; het product wordt uitgestrekt over een willekeurig aantal verschillende priemgetallen van de gedaante

$$2^s + 1 \qquad (s \text{ geheel} \geq 0)$$

Het is evident, dat de exponent s zelf van de gedaante 2^t (of 0) moet zijn. Voorbeelden: $p_k = 3, 5, 17, 257, \ldots\ldots$
Wij zullen eerst ons bezighouden met de afleiding van het resultaat, dat de gestelde voorwaarde voldoende is. Daarbij zullen wij

ons voorlopig beperken tot het geval m = 0, terwijl het product slechts 1 factor bevat, dus

$$n = p \quad (p \text{ priem, van de gedaante } 2^{2^t} + 1)$$

De uitbreiding op de meer algemene vorm (1) is triviaal

Het is in deze vorm, dat het probleem in 1796 door Gauss is opgelost, i.h.b. voor p = 17.
Gauss werd tot dit onderzoek gevoerd door zijn werk op algebraïsch gebied. Hij hield zich toen bezig met het onderzoek naar de algebraische oplosbaarheid van de binomische vergelijking:

$$x^p - 1 = 0.$$

In analytische vorm kunnen de p verschillende wortels van deze vergelijking (eenheidswortels) onmiddelijk worden neergeschreven in de gedaante

$$x_k = e^{\frac{2\pi ik}{p}} \qquad (k = 0, 1, 2, \ldots\ldots, p-1)$$

Het is duidelijk, dat met deze oplossing ook het probleem der cirkelverdeling zou zijn opgelost.
Alleen x_o is reëel = 1. De p-1 complexe wortels voldoen aan

$$\frac{x^p - 1}{x - 1} = 0$$

of

$$x^{p-1} + x^{p-2} + \ldots\ldots\ldots + 1 = 0 \qquad (2)$$

Dit is de vergelijking van de cirkelverdeling. Stellen wij

$$x_1 = e^{\frac{2\pi i}{p}} = r ,$$

dan is

$$x_k = r^k,$$

zodat alle complexe wortels kunnen worden voorgesteld door

$$r, r^2, r^3, \ldots\ldots, r^{p-1} \qquad (3)$$

Iedere wortel is dan een eenvoudige rationale functie (gehele macht) van de eerste uit de rij. Gauss gaat nog een stap verder, door te laten zien, dat bij bepaalde rangschikking van de rij (3) iedere wortel dezelfde gehele (g-de) macht van zijn voorganger is, waardoor de rij (3) de volgende gedaante verkrijgt:

$$r, r^g, r^{g^2}, \ldots\ldots\ldots, r^{g^{p-2}} \qquad (3')$$

Dit wordt bereikt, door voor g een zodanig geheel getal te kiezen, dat de p-1 getallen g^k(k = 0,1,2,.....,p-2) een gereduceerd restsysteem (mod.p) vormen, dus op de volgorde na congruent met de getallen 1,2,3,.....,p-1 zijn. g moet dan een primitieve wortel (mod p) zijn. Men kan bewijzen, dat voor ieder priemgetal van de gedaante $2^s + 1$ o.a. het getal 3 aan de gestelde eisen voldoet.
Juist in de bijzondere rangschikking (3') schuilt de kern van de

$$z_{17} = \frac{R}{4}\sqrt{34-2\sqrt{17}} - 2\sqrt{34-2\sqrt{17}} - 4\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34-}}$$

oplossingsmethode van Gauss. Daartoe wordt de rij (3') voor $p = 2^s + 1$ in twee rijen van 2^{s-1} termen gesplitst als volgt:

$$r,\ r^g,\ r^{g^2},\ r^{g^3},\ \ldots\ldots,\ r^{g^{p-3}},\ r^{g^{p-2}},$$

en men stelt

$$\eta_1 = r + r^{g^2} + r^{g^4} + r^{g^6} + \ldots\ldots + r^{g^{2^s-2}},$$

$$\eta_2 = r^g + r^{g^3} + r^{g^5} + r^{g^7} + \ldots\ldots + r^{g^{2^s-1}}. \qquad (4)$$

Het is duidelijk, dat:

$$\eta_1 + \eta_2 = \sum_{k=1}^{p-1} r^k = -1$$

terwijl het gemakkelijk in te zien is, dat:

$$\eta_1\eta_2 = \sum_{k=0}^{2^{s-1}-1} r^{(1+g)g^{2k}} + \sum_{k=0}^{2^{s-1}-1} r^{(1+g^3)g^{2k}} + \ldots\ldots + \sum_{k=0}^{2^{s-1}-1} r^{(1+g^{2^s-1})g^{2k}}$$

waarin iedere som van het rechterlid gelijk is aan η_1 of η_2 of 2^{s-1}.
Dus

$$\eta_1\eta_2 = A_0 + A_1\eta_1 + A_2\eta_2 \qquad (A_k \text{ geheel}) \qquad (5)$$

Uit (4) blijkt, dat bij vervanging van r door r^g η_1 in η_2 overgaat, en omgekeerd dus

$$\eta_1\eta_2 = A_0 + A_1\eta_2 + A_2\eta_1 \qquad (6)$$

Uit (5) en (6) volgt door optelling

$$\eta_1\eta_2 = A_0 + \frac{A_1+A_2}{2}(\eta_1+\eta_2) = A_0 - \frac{A_1+A_2}{2}$$

dus rationaal. (Men kan bewijzen, dat $A_1 = A_2$, dus $\eta_1\eta_2 = A_0 - A_1$, dus geheel, maar dat is voor ons doel van minder belang).

η_1 en η_2 zijn dus de wortels van de vierkantsvergelijking met rationale (zelfs gehele) coefficienten;

$$x^2 + x + A_0 - \frac{A_1+A_2}{2} = 0.$$

Ze zijn dus door worteltrekking te bepalen.
Op dezelfde wijze worden η_1 en η_2 verder gesplitst in:

$$\eta_{11} = r + r^{g^4} + r^{g^8} + \ldots + r^{g^{2^s-4}}$$
$$\eta_{12} = r^{g^2} + r^{g^6} + r^{g^{10}} + \ldots + r^{g^{2^s-2}}$$
$$\eta_{21} = r^g + r^{g^5} + r^{g^9} + \ldots + r^{g^{2^s-3}}$$
$$\eta_{22} = r^{g^3} + r^{g^7} + r^{g^{11}} + \ldots + r^{g^{2^s-1}}$$

$$\eta_{11} + \eta_{12} = \eta_1 \;;\; \eta_{21} + \eta_{22} = \eta_2$$
$$\eta_{11}\eta_{12} = B_0 + B_1\eta_{11} + B_2\eta_{12} + B_3\eta_{21} + B_4\eta_{22}$$
$$\eta_{21}\eta_{22} = C_0 + C_1\eta_{11} + C_2\eta_{12} + C_3\eta_{21} + C_4\eta_{22}$$

} B en C geheel.

ar bij vervanging van r door r^g $\eta_{11} \rightleftarrows \eta_{12}$, $\eta_{21} \rightleftarrows \eta_{22}$, is:

Dus: $\eta_{11}\eta_{12} = B_0 + B_1\eta_{12} + B_2\eta_{11} + B_3\eta_{22} + B_4\eta_{21}$

$\eta_{11}\eta_{12} = B_0 + \frac{B_1+B_2}{2}\eta_1 + \frac{B_3+B_4}{2}\eta_2$

$\eta_{21}\eta_{22} = C_0 + \frac{C_1+C_2}{2}\eta_1 + \frac{C_3+C_4}{2}\eta_2$

De getallen η_{11}, η_{12} kunnen nu worden bepaald als wortels van de vierkantsvergelijking: $x^2 - \eta_1 x + \left\{B_0 + \frac{B_1+B_2}{2}\eta_1 + \frac{B_3+B_4}{2}\eta_2\right\} = 0$

analoog η_{21}, η_{22}. Zo kan men doorgaan en tenslotte bepaalt men uit een schakel van vierkantsvergelijkingen:

$$r + r^{g^{2k-1}} = r + r^{-1} = 2\cos\frac{2\pi}{p}$$

waarmede het algebraisch gedeelte van het cirkelverdelingsprobleem voltooid is.

Voorbeeld: p = 17, g = 3, $r = e^{\frac{2\pi i}{17}}$

$\eta_1 = r + r^{-8} + r^{-4} + r^{-2} + r^{-1} + r^8 + r^4 + r^2$

$\eta_2 = r^3 + r^{-7} + r^5 + r^{-6} + r^{-3} + r^7 + r^{-5} + r^6$

$\eta_1 + \eta_2 = -1$; $\eta_1\eta_2 = 4\eta_1 + 4\eta_2 = -4$.

Dus:

η_1 en η_2 zijn de wortels van de vergelijking $y^2 + y - 4 = 0$,

$= -\frac{1}{2} \pm \frac{1}{2}\sqrt{17}$.

Nu komt er nog een kleine finesse. Welke van de gevonden wortels is η_1, welke η_2 ? $\eta_1 = 2(\cos\frac{2\pi}{17} + \cos\frac{16\pi}{17} + \cos\frac{8\pi}{17} + \cos\frac{4\pi}{17}) >$

$2(\frac{1}{2} - 1 + 0 + \frac{1}{2}) = 0$

dus $\eta_1 = -\frac{1}{2} + \frac{1}{2}\sqrt{17}$

$\eta_{11} = r + r^{-4} + r^{-1} + r^4$ $\qquad$ $\eta_{11} + \eta_{12} = \eta_1$

$\eta_{12} = r^{-8} + r^{-2} + r^8 + r^2$ $\qquad$ $\eta_{21} + \eta_{22} = \eta_2$

$\eta_{21} = r^3 + r^5 + r^{-3} + r^{-5}$ $\qquad$ $\eta_{11}\eta_{12} = \eta_{11} + \eta_{12} + \eta_{21} + \eta_{22} = -1$

$\eta_{22} = r^{-7} + r^{-6} + r^7 + r^6$

Dus η_{11} en η_{12} zijn de wortels van $z^2 - \eta_1 z - 1 = 0$ (7')

evenzo en " " " $z^2 - \eta_2 z - 1 = 0$ (7'')

De wortels van (7') en (7'') zijn reëel en van tegengesteld teken.

$\eta_{11} = 2(\cos\frac{2\pi}{17} + \cos\frac{8\pi}{17}) > 0$

$\eta_{22} = 2(\cos\frac{14\pi}{17} + \cos\frac{12\pi}{17}) < 0$ dus $\eta_{21} > 0$

Tenslotte is: $\eta_{111} = r + r^{-1} = 2\cos\frac{2\pi}{17}$
$\eta_{112} = r^4 + r^{-4} = 2\cos\frac{8\pi}{17}$ } dus $\eta_{111} > \eta_{112} > 0$

$\eta_{111} + \eta_{112} = \eta_{11}$; $\eta_{111}\,\eta_{112} = r^5 + r^{-3} + r^3 + r^{-5} = \eta_{21}$

Dus η_{111} is de grootste wortel van $u^2 - \eta_{11}\,u + \eta_{21} = 0$.

Tenslotte is hiermede $\cos\frac{2\pi}{17}$ uitgedrukt met behulp van vierkantswortels. Uit het voorgaande is gemakkelijk een meetkundige constructie voor de zijde van de regelmatige 17-hoek af te leiden [1].

Bepaalt men gehele getallen a_k, welke voldoen aan $\sum \frac{a_k}{p_k} = \frac{1}{\prod p_k}$ (steeds mogelijk!), dan is hiermede het probleem van de cirkelverdeling in $\prod p_k$ gelijke delen opgelost, terwijl de verdere uitbreiding tot $2^h \prod p_k$ door voortdurende halvering volgt.

Wij willen dit gedeelte besluiten met enkele opmerkingen over de priemgetallen van de gedaante

$$2^{2^t} + 1.$$

Voor t = 1,2,3,4 vindt men inderdaad priemgetallen, n.l. 5, 17, 257 en 65537. Dit leidde Fermat tot het vermoeden, dat alle getallen van deze vorm priemgetallen waren. Dit is echter onjuist. Euler heeft reeds aangetoond, dat

$$2^{2^5} + 1 = 641 \cdot 6700417.$$

Ook meerdere volgende getallen uit deze rij zijn deelbaar gebleken. Het is nog een open vraag of deze rij een eindig of oneindig aantal priemgetallen bevat.

Wij zullen nu overgaan tot het tweede gedeelte, de noodzakelijkheid der gestelde voorwaarde, dus de negatieve kant van de zaak:

Slechts de veelhoeken van het bovenstaande type zijn met passer en lineaal te construeren. Wij merkten reeds op, dat Gauss ook dit probleem heeft opgelost, in 1801. Aan het slot van art. 365 van zijn in de zomer van 1801 verschenen "Disquisitiones arithmeticae" staat te lezen:

"Wanneer echter p-1 andere priemfactoren behalve 2 bevat, komen wij steeds op vergelijkingen van hogere graad, en wij kunnen met alle strengheid bewijzen, dat deze hogere vergelijkingen nooit vermeden kunnen worden, of tot vergelijkingen van lagere graad kunnen worden herleid; ofschoon de grenzen van dit boek niet veroorloven, dit bewijs hier mede te delen, menen wij toch daarop te moeten wijzen, opdat niet iemand nog andere verdelingen, behalve de door onze theorie geleverde, b.v. in 7, 11, 13, 19 delen op geometrische constructies hoopt terug te kunnen brengen, en daarmede zijn tijd onnut verkwist." De spatieringen in verschillende graad zijn afkomstig van Gauss.

---

1) [illegible]

Uit zijn dagboek is gebleken, dat Gauss dit bewijs eerst ontdekt heeft op 6 April 1801, tijdens de correctie van de laatste drukproeven, zodat bovenaangehaalde passus ongetwijfeld eerst op het laatste moment is ingevoegd. Hoe het door Gauss geleverde bewijs verloopt, is (nog) niet bekend.

Wij willen nu besluiten met een eenvoudig bewijs hiervan.

Gegeven: L_0 is het lichaam der rationale getallen.
α_1 is een getal uit $L_0 \neq$ kwadraat van getal uit L_0.
$L_1 = L_0(\sqrt{\alpha_1})$ is ontstaan uit L_0 door adjunctie van $\sqrt{\alpha_1}$.
α_2 is een getal uit $L_1 \neq$ kwadraat van getal uit L_1
$L_2 = L_1(\sqrt{\alpha_2}) = L_0(\sqrt{\alpha_1}, \sqrt{\alpha_2})$ ontstaat uit L_0 door achtereenvolgende adjunctie van $\sqrt{\alpha_1}, \sqrt{\alpha_2}$, etc.
$L_0(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots\ldots, \sqrt{\alpha_k})$ ontstaat uit L_0 door achtereenvolgende adjunctie van $\sqrt{\alpha_1}$ (α_1 in L_0, $\sqrt{\alpha_1}$ niet in L_0), $\sqrt{\alpha_2}$ (α_2 in L_1, $\sqrt{\alpha_2}$ niet) ..... $\sqrt{\alpha_k}$ (α_k in L_{k-1}, $\sqrt{\alpha_k}$ niet).

Stelling: Wanneer θ een willekeurig getal uit L_k is, dat niet behoort tot L_{k-1}, dan is θ een wortel van een onherleidbare L_0- vergelijking van de graad 2^k.

Bewijs: (volledige inductie)

De stelling is uitteraard waar voor k=1.

Neem aan, dat de stelling geldt voor k-1, dus dat θ als element van $L_1(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots\ldots \sqrt{\alpha_k})$ voldoet aan een onherleidbare L_1-vergelijking van de graad 2^{k-1}: $F(x) = 0$. De coëfficienten van deze vergelijking zijn getallen uit $L_1 = L_0(\sqrt{\alpha_1})$, dus de gedaante $b + c\sqrt{\alpha_1}$, (waarin b en c $\in L_0$). Dus $F(x) \equiv r(x) + s(x)\sqrt{\alpha_1}$, waarin r(x) en s(x) veeltermen in x zijn van de graad $\leq 2^{k-1}$, met coëfficienten uit L.
Zonder beperking kunnen wij de eerste coëfficient van F(x), dus de coëfficient van $x^{2^{k-1}}$ gelijk aan 1 nemen, zodat r(x) van de graad 2^{k-1} is, en s(x) van lagere graad.

θ is dan een wortel van een L_0-vergelijking:

$$G(x) = \{r(x)\}^2 - \alpha_1\{s(x)\}^2 = 0. \text{ (graad } 2^k)$$

Wanneer wij bewijzen, dat deze vergelijking onherleidbaar is in L_0, is alles bewezen.
Zij $\varphi(x)$ een factor van G(x) van een graad > 0 en $< 2^k$.
$F(x) = r(x) + s(x)\sqrt{\alpha_1}$ is onherleidbaar in L_1, dus deelbaar op, of onderling ondeelbaar met $\varphi(x)$ (ook L_1-polynoom).
Met $r(x) + s(x)\sqrt{\alpha_1}$ is ook $r(x) - s(x)\sqrt{\alpha_1}$ L_1-onherleidbaar, want iedere ontbinding van $r(x) - s(x)\sqrt{\alpha_1}$ in 2 L_1-polynomen levert een analoge ontbinding van $r(x) + s(x)\sqrt{\alpha_1}$, door vervanging van $+\sqrt{\alpha_1}$ door $-\sqrt{\alpha_1}$. Dus ook $r(x) - s(x)\sqrt{\alpha_1}$ is of deelbaar op, of

onderling ondeelbaar met $\varphi(x)$. Uit de onherleidbaarheid in L_1 van $r(x) + s(x)\sqrt{\alpha_1}$ volgt, dat $r(x)$ en $s(x)$ onderling ondeelbaar zijn. Hieruit volgt, dat ook $r(x) + s(x)\sqrt{\alpha_1}$ en $r(x) - s(x)\sqrt{\alpha_1}$ onderling ondeelbaar zijn in L_1, want iedere gemeenschappelijke factor zou in hun som en verschil, dus in $r(x)$ en $s(x)\sqrt{\alpha_1}$ begrepen zijn, waardoor in tegenspraak met de aanname $r(x) + s(x)\sqrt{\alpha_1}$ herleidbaar (L_1) zou zijn.

Aangenomen is:

$\varphi(x)$ is <u>eigenlijk</u> deelbaar (L_0) op

$$G(x) = \left\{r(x) + s(x)\sqrt{\alpha_1}\right\}\left\{r(x) - s(x)\sqrt{\alpha_1}\right\}$$

dus de graad van $\varphi(x)$ zou $< 2^k$ moeten zijn.

$\varphi(x)$ kan dan niet onderling ondeelbaar zijn met beide factoren van $G(x)$.

Dus $\varphi(x)$ zou (eventueel op een constante factor na) identiek moeten zijn met

$r(x) + s(x)\sqrt{\alpha_1}$ of met $r(x) - s(x)\sqrt{\alpha_1}$

Dit is in strijd met de aanname, dat $\varphi(x)$ een L_0-veelterm is.

Dus: <u>$G(x)$ is onherleidbaar L_0, w.t.b.w.</u>

Gevolgen:

1) Een onherleidbare verg. in L_0, waarvan de graad $\neq 2^k$ ($k = 1,2,3\ldots$ kan nooit een wortel bezitten, die door vierkantswortels is uit te drukken (m.a.w. met passer en lineaal te construeren).
2) Een regelmatige p-hoek (p priem, $p-1 \neq 2^k$) is <u>niet</u> met passer en lineaal construeerbaar. De algebraische oplossing voert n.l. tot een in L_0 <u>onherleidbare</u> vergelijking van de graad $p-1 \neq 2^k$.
