Wat te bewijzen is (58)

Rubriek

Mijn leraar zei *algebra,* op de kaft van het boek stond *algebra*, maar op m'n rapport heette het *stelkunde*. Zo was dat tot diep in de jaren vijftig van de vorige eeuw. Stelkunde, ooit stelconst, zo genoemd door de zuidelijke Nederlander en taalpurist Simon Stevin, die toch gedacht zal hebben aan de kunst of kunde van het 'stellen', als bij 'ingeklede vergelijkingen'. Ook bij blote vergelijkingen kan er vaak met vrucht worden 'gesteld', daarmee bedoel ik dat een deelexpressie tijdelijk wordt voorzien van een één-letternaam. Formele substitutie zo gezegd, of in Jip-en-Janneketaal: de bordjesmethode.
Het principe van formele substitutie is al zo oud als de Babyloniërs, al gebruikten die geen lettersymbolen, maar woorden als lengte, breedte en oppervlakte. Een standaardprobleem uit die tijd luidt:

> Van een rechthoek weet je de som van lengte en breedte en ook de oppervlakte; wat zijn dan de afmetingen?

In algebrataal zeg je los x en y op, bijvoorbeeld uit:

$$\begin{cases} x+y = 100 \\ xy = 2331 \end{cases}$$

De klassieke methode is de volgende. Kijk eerst of x en y ook gelijk kunnen zijn (een vierkant is per slot een bijzondere rechthoek). Zo niet, stel x gelijk aan 'de halve som plus iets' en y gelijk aan 'de halve som min datzelfde iets'. Hier: $x = 50 + u$ en $y = 50 - u$.
$xy = 2331$ leidt dan (via een even belangrijk als merkwaardig product) tot $2500 - u^2 = 2331$ zodat $u^2 = 169$. Dat levert op: $(x, y) = (63, 37)$ of $(x, y) = (37, 63)$.

Het vraagstuk *'gegeven som en product van twee getallen, bepaal die getallen'* is equivalent met '*los deze of die vierkantsvergelijking op*'. Ik maak er geen geheim van dat ik de hier geschetste aanpak prefereer boven de *abc*-formule die voor de meeste leerlingen niet meer dan een dom recept is, waar ze niets van (hoeven te) begrijpen.

Zeg niet dat de som-productmethode niet efficiënt is: als mijn kleindochter aan de lijn is met een tweedegraadsvergelijking, kan ik die vrijwel altijd uit het hoofd oplossen zonder dat daar een a, b of c aan te pas komt. Maar wie rekent er nu nog uit het hoofd, opa, als je een rekenmachientje hebt...

Een Babylonisch staaltje stelkunde

Op het kleitablet AO 8862 staat het volgende probleem:

> Lengte en breedte heb ik vermenigvuldigd en zo de oppervlakte gevormd. Verder heb ik het overschot van de lengte over de breedte bij de oppervlakte opgeteld: 183. Verder heb ik de lengte en breedte opgeteld: 27. Gevraagd: lengte, breedte en oppervlakte.

Van der Waerden schrijft in zijn *Ontwakende Wetenschap* (wanneer wordt dat prachtwerk eens herdrukt?) dat men zich niet door de meetkundige woordkeus moet laten misleiden; het is immers onzin om bij een oppervlakte een lengtemaat op te tellen, en ... *'door het meetkundige gewaad heen ziet men de algebraïsche kern'*. Die kern is hier:

$$\text{Los } x \text{ en } y \text{ op uit: } \begin{cases} xy + x - y = 183 \\ x + y = 27 \end{cases}$$

Op het kleitablet worden eerst 183 en 27 bij elkaar opgeteld (= 210) en vervolgens wordt 27 met 2 vermeerderd. Daarmee blijkt het probleem teruggebracht tot een 'som-productprobleem'. Inderdaad:

$$\begin{array}{rcll} xy + x - y &=& 183 & \\ x + y &=& 27 & \longrightarrow \quad x + y + 2 = 29 \\ \hline + \quad xy + 2x &=& 210 & \longrightarrow \quad x(y + 2) = 210 \end{array}$$

Stel $z = y + 2$ en we krijgen te maken met: $x + z = 29$ en $xz = 210$. Na het 'breken van 29 in twee gelijke delen' werd $x = 15$ ('lengte') en $z = 14$ ('breedte') gevonden, met de conclusie: $y = 14 - 2 = 12$ ('echte breedte'). Dit alles zonder onze vertrouwde formules, kortom: Babylonische stelkunde, maar dan wel 'avant la lettre'.

Palindroom en polynoom

Het woordenboek Van Dale geeft als voorbeeld van een palindroom het woord 'parterretrap', dat van achter naar voren gelezen niet verandert. Een wat minder bekend voorbeeld van een palindroom is 'meetsysteem'. Het eerste voorbeeld bevat een even aantal letters (in het midden staan twee gelijke letters), het tweede heeft de eenzame y in het centrum; het aantal letters is oneven.

In oude algebraboeken kun je nog een paragraaf over 'wederkerige vergelijkingen' tegenkomen. Het betreft polynoomvergelijkingen in één onbekende (zeg x) waarbij de coëfficiënten van afnemende machten van x een 'palindromisch' rijtje getallen vormen.

Als de graad van het polynoom oneven is (er is dan geen middelste term), is er direct een oplossing te ‘zien’, namelijk $x = -1$. Kijk bijvoorbeeld naar:

$$x^5 - 4x^4 + 3x^3 + 3x^2 - 4x + 1 = 0$$

Noem het ‘parterretrap-polynoom’ in het linkerlid $P(x)$, dan zegt de zogenaamde *factorstelling* dat $P(x)$ deelbaar is door $x + 1$. Het quotiënt kan gevonden worden via het delingsalgoritme voor veeltermen, maar ook via:

$$P(x) = (x^5 + 1) - 4x(x^3 + 1) + 3x^2(x + 1)$$

Immers:

$$x^3 + 1 = (x + 1)(x^2 - x + 1)$$

$$x^5 + 1 = (x + 1)(x^4 - x^3 + x^2 - x + 1)$$

en hieruit volgt na wat rekenwerk:

$$P(x) = (x + 1)(x^4 - 5x^3 + 8x^2 - 5x + 1)$$

Het quotiënt blijkt ook een ‘wederkerig polynoom’ te zijn (nu van het type ‘meetsysteem’). Dat dit altijd zo is, kan elegant worden bewezen via het volgende criterium, dat eenvoudig is in te zien.

Een polynoom P(x) van de graad n is wederkerig, als (en alleen als) het polynoom $x^nP(x^{-1})$ *identiek is aan P(x).*

Stel nu $P(x) = x^nP(x^{-1})$ en $P(x) = (x + 1)Q(x)$.

Er volgt dan:

$$x^nP(x^{-1}) = x^n(x^{-1} + 1)Q(x^{-1}) = x^{n-1}(1 + x)Q(x^{-1})$$

zodat

$$(x + 1)Q(x) = x^{n-1}(1 + x)Q(x^{-1})$$

en dus

$$Q(x) = x^{n-1}Q(x^{-1})$$

Halvering van de graad

Nu kan een wederkerig polynoom $Q(x)$ van even graad $2k$ via een slimme formele substitutie worden omgevormd tot een polynoom $x^kR(y)$ waarbij $R(y)$ een polynoom van de graad k is. Die substitutie is: $y = x + x^{-1}$.

In ons voorbeeld gaat dat aldus:

$$x^4 - 5x^3 + 8x^2 - 5x + 1 = x^2[x^2 - 5x + 8 - 5x^{-1} + x^{-2}$$

Met $y = x + x^{-1}$ en $y^2 = x^2 + x^{-2} + 2$ kan het rechterlid dan worden omgewerkt tot $x^2(y^2 - 5y + 6)$. $R(y) = 0$ leidt dan tot $y = 2$ of $y = 3$.

Het is dan nog zaak om de vergelijkingen $x + x^{-1} = 2$ en $x + x^{-1} = 3$ op te lossen. Ik begin met de laatste, dat komt neer op het vinden van getallen met ‘som’= 3, ‘product’ = 1.

Breek 3 in tweeën, dat geeft $1\frac{1}{2}$, stel de getallen $1\frac{1}{2} \pm u$, dat leidt tot $u^2 = \frac{5}{4}$, en zo krijg ik dan de oplossingen $1\frac{1}{2} \pm \frac{1}{2}\sqrt{5}$ voor x.

Bij $x + x^{-1} = 2$ volstaat het ‘eerlijk delen van de som 2’ en de enige oplossing is hier $x = 1$.

Conclusie: de oorspronkelijke vergelijking van de vijfde graad heeft de wortels -1, 1, $1\frac{1}{2} \pm \frac{1}{2}\sqrt{5}$, waarbij 1 als een ‘dubbele’ wortel’ kan worden gezien.

Dergelijke vraagstukken behoorden zo’n zestig jaar geleden nog tot de examenstof van het voortgezet onderwijs en ik moet bekennen dat substitutie met de ‘reciproke’, zoals mijn leraar dat noemde, mij zeer aansprak en ik ben die elegante ‘stelkunstgreep’ ook nooit vergeten.

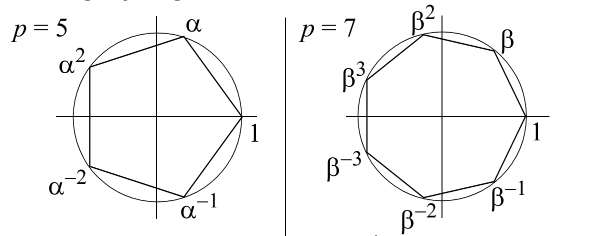
De regelmatige *p*-hoek

Wederkerige polynomen zijn in de wiskunde bijna even exotisch als palindromen in de taal, en daarom is het niet verbazend dat dit onderwerp na 1958 niet meer voorkwam in de schoolboeken. Er zijn wel een paar situaties bekend waarbij de wederkerige vergelijking een rol speelt. Eén daarvan heeft te maken met de vraag naar de construeerbaarheid met passer en liniaal van regelmatige veelhoeken, in het bijzonder van die waarbij het aantal zijden een priemgetal p is. Sinds de uitvinding van de complexe getallen kan deze kwestie algebraïsch worden opgevat als vraag naar de construeerbaarheid van de wortels ($\neq 1$) van de ‘cirkeldelingsvergelijking’ $z^p - 1 = 0$ of, na deling door $z - 1$, van de wortels van de wederkerige vergelijking:

$$z^{p-1} + \ldots + z + 1 = 0 \qquad (*)$$

De Grieken wisten al dat het construeren lukt bij $p = 3$ en bij $p = 5$. In het eerste geval is (*) een tweedegraadsvergelijking met construeerbare wortels en in het tweede geval kan (*) via de substitutie $w = z + z^{-1}$ gereduceerd worden tot een tweedegraadsvergelijking in w.

Als $\alpha = \cos\frac{2\pi}{5} + i \cdot \sin\frac{2\pi}{5}$, zijn $\alpha + \alpha^{-1}$ en $\alpha^2 + \alpha^{-2}$ de (met passer en liniaal construeerbare) wortels van die vergelijking in w.



$\alpha + \alpha^{-1}$ *construeerbaar* | $\beta + \beta^{-1}$ ***niet*** *construeerbaar*

Voor $p = 7$ lukt het echter niet! Dat volgt uit onderzoek van de vergelijking

$$z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0$$

ofwel:

$$z^3 + z^2 + z + 1 + z^{-1} + z^{-2} + z^{-3} = 0$$

Naast $y = z + z^{-1}$ en $y^2 - 2 = z^2 + z^{-2}$ gebruik ik nog

$$\begin{aligned} z^3 + z^{-3} &= (z + z^{-1})(z^2 + z^{-2}) - (z + z^{-1}) \\ &= y(y^2 - 2) - y = y^3 - 3y \end{aligned}$$

Dit alles gesubstitueerd geeft:

$$y^3 + y^2 - 2y - 1 = 0$$

en deze vergelijking heeft geen rationale wortels!

Vul maar $y = m/n$ in, met m, n geheel en onderling ondeelbaar, en via eigenschappen van deelbaarheid leidt dit dan tot tegenspraak. In aflevering 56 van deze rubriek is aangetoond dat de wortels van een derdegraadsvergelijking die geen rationale oplossingen kent, niet construeerbaar zijn met passer en liniaal. Klaar.

Sinds Gauss is bekend dat een regelmatige *p(riem)*-hoek dan en alleen dan construeerbaar is als het aantal hoekpunten een priemgetal van Fermat is, dat wil zeggen $p = 2^m + 1$ (waarbij m een macht van 2 is).

Deze stelling kan met Galois-theorie worden bewezen (zie bijvoorbeeld Ian Stewart's boek *Galois Theory*). Nu zijn Fermat-priemgetallen dun gezaaid. Er zijn er slechts vijf bekend: 3, 5, 17, 257 en 65537. Gauss zag kans op redelijk jonge leeftijd de regelmatige zeventienhoek te construeren en hij was daar zo trots op dat hij definitief besloot wiskundige te worden.

De construeerbare zeventienhoek

Het nu volgende bewijs van de construeerbaarheid van de regelmatige zeventienhoek berust op wat ik de 'som-productconstructie' zou willen noemen. Als van twee getallen zowel de som s als het product p construeerbaar zijn op de getallenlijn, dan zijn die beide getallen dat zelf ook.

Dit volgt met name uit de construeerbaarheid van de vierkantswortel uit een construeerbaar getal (constructie met de halve cirkel, zie aflevering 56 van deze rubriek). Voor het onderzoek naar de construeerbaarheid van de regelmatige zeventienhoek bekijk ik nu de vergelijking

$$z^{16} + z^{15} + \ldots + z + 1 = 0 \qquad (**)$$

Het getal $\alpha = \cos\frac{2\pi}{17} + i \cdot \sin\frac{2\pi}{17}$ is een wortel van (**); de andere wortels zijn dan $\alpha^2, \alpha^3, ..., \alpha^{16}$, waarbij geldt: $\alpha^{16} = \alpha^{-1}, \alpha^{15} = \alpha^{-2}, \ldots, \alpha^9 = \alpha^{-8}$.

Via de inmiddels vertrouwde substitutie kan de graad van (**) worden gehalveerd en komt er een achtstegraadsvergelijking in w waarvan de wortels zijn:

$$w_1 = \alpha + \alpha^{-1}, w_2 = \alpha^2 + \alpha^{-2}, \ldots, w_8 = \alpha^8 + \alpha^{-8}$$

De som van deze acht (reële!) getallen is bekend:

$$\sum_{k=1}^{8} w_k = \sum_{k=1}^{16} \alpha^k = -1 \qquad \text{(I)}$$

Verder merk ik op dat het product van elk tweetal van die wortels gelijk is aan de som van een ander tweetal. Bijvoorbeeld:

$$\begin{aligned} w_1 \cdot w_3 &= (\alpha + \alpha^{-1})(\alpha^3 + \alpha^{-3}) \\ &= \alpha^4 + \alpha^{-4} + \alpha^2 + \alpha^{-2} = w_4 + w_2 \end{aligned}$$

In het algemeen (met $k < m$) geldt:

$$w_k \cdot w_m = w_{m+k} + w_{m-k} \qquad \text{(II)}$$

waarbij men moet bedenken dat in het geval $m + k > 8$, die index vervangen wordt door $17 - (m + k)$.

Stel nu:
$$\begin{aligned} u_1 &= w_1 + w_2 + w_4 + w_8 \\ u_2 &= w_3 + w_6 + w_5 + w_7 \end{aligned}$$

De twee rijtjes van vier indices zijn verkregen door stap voor stap te verdubbelen, waarbij 12 is vervangen door 5 (= 17 – 12) en 10 door 7.

Ik toon nu eerst aan dat u_1 en u_2 beide op de getallenlijn kunnen worden geconstrueerd met passer en liniaal.

Er blijkt namelijk: $u_1 + u_2 = -1$ en $u_1 \cdot u_2 = -4$

De eerste gelijkheid volgt direct uit (I). Voor de tweede gebruik ik regel (II) en de vermenigvuldigingstabel:

$\cdot$	w_1	w_2	w_4	w_8
w_3	w_4+w_2	w_5+w_1	w_7+w_1	w_6+w_5
w_6	w_7+w_5	w_8+w_4	w_7+w_2	w_3+w_2
w_5	w_6+w_4	w_7+w_3	w_8+w_1	w_4+w_3
w_7	w_8+w_6	w_8+w_5	w_6+w_3	w_2+w_1

Het product $u_1 u_2$ is gelijk aan de som van alle sommen uit de tabel en dat is (even checken ...) precies vier keer de som van alle w_k's dus $4 \cdot -1 = -4$. Uit $u_1 + u_2 = -1$ en $u_1 \cdot u_2 = -4$ volgt (Babylonische methode):

$$u_{1,2} = -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{17}$$

Vervolgens splits ik u_1 en u_2 en wel zó:

$$u_1 \left\langle \begin{array}{l} v_1 = w_1 + w_4 \\ v_2 = w_2 + w_8 \end{array} \right. \qquad \left. \begin{array}{l} v_3 = w_3 + w_5 \\ v_4 = w_6 + w_7 \end{array} \right\rangle u_2$$

Bekijk nu som en product van de paren v_1, v_2 en v_3, v_4.

De sommen weet ik al: $v_1 + v_2 = u_1$ en $v_3 + v_4 = u_2$. Voor de producten bekijk ik twee tabellen:

$\cdot$	w_1	w_4
w_2	w_3+w_1	w_6+w_2
w_8	w_8+w_7	w_5+w_4

$\cdot$	w_3	w_5
w_6	w_8+w_3	w_6+w_1
w_7	w_7+w_4	w_5+w_2

Uit die tabellen volgt:

$$v_1 \cdot v_2 = v_3 \cdot v_4 = \sum_{k=1}^{8} w_k = -1$$

Van v_1 en v_2 zijn zowel som als product construeerbaar en dat betekent dat beide getallen te construeren zijn. Hetzelfde geldt voor het paar v_3, v_4.

De finish is nu in zicht, want:

$$w_1 + w_4 = v_1 \text{ en } w_1 \cdot w_4 = w_5 + w_3 = v_3$$

Nog één keer de som-productgedachte toegepast; met het paar v_1, v_3 is ook het paar w_1, w_4 en daarmee de regelmatige zeventienhoek construeerbaar!

De volhardende rekenaars kunnen desgewenst, via de hier gedemonstreerde procedure, het getal $w_1 = 2\cos\frac{2\pi}{17}$ uitdrukken in gestapelde vierkantswortels.

Martin Kindt, M.Kindt@uu.nl

MEDEDELING

Nationale Wiskunde Dagen

Op vrijdag 1 en zaterdag 2 februari 2013 worden de 19e Nationale Wiskunde Dagen gehouden in Congrescentrum de Leeuwenhorst te Noordwijkerhout.

Kosten per persoon: € 385,00 bij overnachting op een tweepersoonskamer en € 420,00 bij overnachting op een eenpersoonskamer.

Begin september is de programmafolder met aanmeldingsformulier naar de scholen gestuurd. Meer informatie over de NWD is ook al te vinden op http://www.fisme.science.uu.nl/nwd/.

Inlichtingen:
Ank van der Heiden, telefoon: 030 253 56 54 of e-mail: nwd@fi.uu.nl.