Construeerbaarheid van regelmatige veelhoeken

Aleid Oosterwijk
Studentnummer 3593002
Universiteit Utrecht

Barbera Droste
Studentnummer 3676498
Universiteit Utrecht

Nathan Vos
Studentnummer 3692329
Universiteit Utrecht

20 september 2021

Inhoudsopgave

1 Inleiding

De construeerbaarheid van regelmatige veelhoeken is een fascinerend onderwerp wat al lange tijd voor vraagstukken in de wiskunde zorgt. Al in de Grieke oudheid werd aandacht eraan besteed. De Griekse wiskundigen hadden een passer en een lineaal zonder schaalverdeling tot hun beschikking en vele regels opgesteld waaraan de constructies moesten voldoen. De technieken waren over een groot gebied bekend. De Griekse wiskunidge Euclides heeft de kennis van geometrie van die tijd in een groot boekwerk verzameld: Euclides' elementen. Hierin beschrijft Euclides technieken om verschillende specifieke veelhoeken te construeren, zoals een gelijkzijdige driehoek, een vierkant, een regelmatige vijf- en zeshoek. Hij laat ook zien hoe je een regelmatige vijftienhoek kunt construeren door een gelijkzijdige driehoek en een regelmatige vijfhoek te construeren zodat hun omschreven cirkel hetzelfde is en ze één gelijk hoekpunt hebben. De twee vormen verdelen de cirkel dan in derden respectievelijk vijfden. Gebruik makend van het volgende diagram, kunnen we zien dat van de vijftien gelijke boog segmenten die de cirkel moet bevatten, drie bevat zijn in de boog AB en vijf in de boog AC. Dus, twee blijven achter in boog BC. Door de boog BC in twee gelijke delen te verdelen, is de zijde van een regelmatige vijftienhoek geconstrueerd. Vervolgens kan de gehele veelhoek worden geconstrueerd door deze lengte af te meten op de cirkel. Door deze technieken konden de volgende veelhoeken worden geconstrueerd: 3, 4, 5 en 15. Door twee deling ook: 6, 8, 10, 12, 16, 20 etc. Tot zover was men gekomen. Tot aan het eind van de achttiende eeuw waren wiskundigen zeker dat de enige regelmatige veelhoeken die geconstrueerd konden worden met passer en liniaal, de veelhoeken waren die al bekend waren bij de Grieken. Later bleken dit niet alle mogelijkheden te zijn. Wat wel alle mogelijkheden zijn, zal door ons besproken worden. Door het ontwikkelen van nieuwe wiskunde, *Galois theorie*, bleken elegante bewijzen gegeven te kunnen worden van stellingen over de construeerbaarheid van regelmatige veelhoeken die al lang bewezen waren, vanuit een heel andere hoek. Wij zullen een korte inleiding geven over dit veelzijdige onderwerp.
Wij hebben onderzocht welke regelmatige veelhoeken geconstrueerd kunnen worden met passer en lineaal. Daarvoor bespreken we eerst de Eulerfunctie en onstaat er een vermoeden voor een voorwaarde voor de construeerbaarheid. Vervolgens verduidelijken we het begrip constructie en bekijken we hoeveel oplossingen het stappenplan van een constructie geeft en hoeveel oplossingen daarvan daadwerkelijk verschillend zijn. Vervolgens bekijken we voor de regelmatige veelhoeken wat het verband is tussen het aantal hoeken, de eulerfunctie en de construeerbaarheid. Tenslotte behandelen we de Fermatgetallen en komen we tot een voorwaarde voor de construeerbaarheid.

2 De Euler functie

De wiskundige Leonard Euler was de eerste die opmerkte dat een belangrijke eigenschap van een geheel getal n is, wat het aantal positieve gehele getallen kleiner dan n en relatief priem aan n is. Om het voorgenoemde aantal voor een bepaalde n uit te drukken voerde hij de notatie $\phi(n)$ in en sinsdien staat de functie $n \mapsto \phi(n)$ bekend als de Euler functie. Bijvoorbeeld voor $n = 8$ zijn er 3 getallen kleiner en relatief priem tot n, namelijk $3, 5$ en 7, dus $\phi(8) = 3$.

Euler ondekte ook interessante eigenschappen van de functie, bijvoorbeeld het volgende: *Als m en n relatief priem zijn dan geldt de volgende gelijkheid:*

$$\phi(mn) = \phi(m) \cdot \phi(n) \tag{1}$$

Als n een priemgetal p is dan gebeuren er ook allerlei interessante dingen. Voor een priemgetal p geldt uiteraard dat alle positieve getallen kleiner dan p relatief priem zijn aan p, dus $\phi(p) = p - 1$. Voor p^2 geldt dat alle getallen met een gemene deler met p^2 veelvouden van p zijn, dus $p, 2p, 3p, ..., (p-1) \cdot p, p \cdot p$. Er zijn dus p getallen die *niet* relatief priem zijn aan p^2, m.a.w. $\phi(p^2) = p^2 - p = p(p-1)$. In het algemeen geldt dat voor p^m de getallen met gemene deler ook veelvouden van p zijn, dus $p, 2p, 3p, ..., p^{m-2}(p-1) \cdot p, p^{m-1} \cdot p$ en dat zijn dus p^{m-1} getallen. Dus voor een priemgetal p en een positief geheel getal m geldt:

$$\phi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1) \tag{2}$$

Deze twee eigenschappen maken het meteen gemakkelijk om $\phi(n)$ te berekenen voor kleine n. We doen er twee als voorbeeld:

$$\phi(14) = \phi(7) \cdot \phi(2) = 6 \cdot 1 = 6 \tag{3}$$

$$\phi(120) = \phi(15) \cdot \phi(4) \cdot \phi(2) = 10 \cdot 2 \cdot 1 = 20 \tag{4}$$

Door dezelfde twee eigenschappen is $\phi(n)$ ook sneller te berekenen voor grote n als de priemfactorisatie van die n bekend is. Bijvoorbeeld:

$$25\,876\,254\,764 = 2^2 \times 47 \times 137 \times 1\,004\,669 \tag{5}$$

$$\phi(25\,876\,254\,764) = 2 \cdot 46 \cdot 136 \cdot 1004668 = 12\,570\,406\,016 \tag{6}$$

Ter illustratie hebben we de $\phi(n)$ voor n van 1 tot 42 berekend en in een tabel gezet.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

n	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\phi(n)$	8	16	6	18	8	12	10	22	8	20	12	24	12	28	8

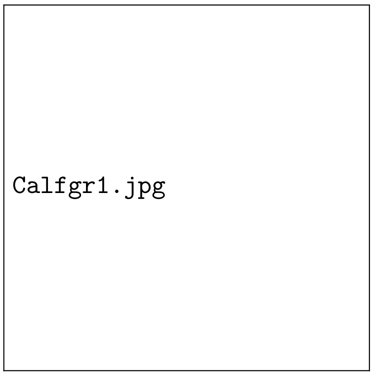
n	31	32	33	34	35	36	37	38	39	40	41	42
$\phi(n)$	30	16	20	16	24	12	36	18	24	16	40	12

Als we deze getallen vergelijken met de getallen waarvoor een regelmatige n-hoek kan worden geconstrueerd dan zien we een verband. Het lijkt alsof er geldt dat er een n-hoek kan worden geconstrueerd als $\phi(n)$ een macht van 2 is. We zullen later een intuitief argument geven waaruit blijkt dat deze eigenschap zowel nodig als voldoende is om een regelmatige n-hoek te construeren.

3 Wat betekent "Constructie"?

De oplossing van een constructieprobleem moet weergegeven worden als een opeenvolging van elementaire operaties, die lijken op een verzameling instructies voor een computer. Bijvoorbeeld, het probleem van het vinden van een bisectie van een lijnstuk AB kan als volgt opgelost worden:

1. Construeer met een passer een cirkel met middelpunt A en straal AB.
2. Construeer met een passer een cirkel met middelpunt B en straal AB.
3. Markeer de punten M,N waarop de cirkels elkaar snijden.
4. Trek de lijn MN met een liniaal.
5. Markeer het punt X waar de lijn MN en de lijn AB elkaar snijden.

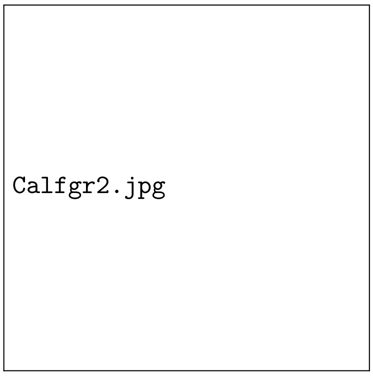


Figuur 1: Bisectie van een lijnstuk AB.

Nog een voorbeeld, waar een bisectrice van een hoek AOB wordt gevonden.

1. Construeer met een passer een cirkel met middelpunt O en zelfgekozen straal R.
2. Markeer het snijpunt M van de cirkel met de lijn OA.
3. Markeer het snijpunt N van de cirkel met de lijn OB.
4. Construeer met een passer een cirkel met middelpunt M en straal R.
5. Construeer met een passer een cirkel met middelpunt N en straal R.
6. Markeer het punt X (niet O) waar de cirkels elkaar snijden.
7. Trek de lijn OX met een liniaal.

Het probleem is hier echter dat opdracht 2 en 3 niet eenduidig zijn. De cirkel snijdt de lijnen OA en OB namelijk op twee plekken, en het is niet duidelijk welke er gekozen moet worden. Je zou kunnen zeggen dat OA en OB slechts lijnstukken zijn, en dus maar één snijpunt hebben met de cirkel, maar het concept van lijnstuk is niet elementair genoeg om begrepen te worden door



Figuur 2: Bissectrice van een hoek.

onze 'wiskundige machine'. Het begrijpt alleen het concept lijn.

Als 'het snijpunt' vervangen wordt door 'een snijpunt', krijg je twee keer zoveel snijpunten, namelijk ook aan de 'andere kant' van het punt O, en daarmee krijg je vier verschillende punten X_1, X_2, X_3 en X_4, omdat je vier cirkels in totaal krijgt, die elkaar in 8 punten snijden, waarvan 4 samenvallen met het punt O. Als je nu alle lijnen X_nO trekt, krijg je twee lijnen, omdat X_1 op de lijn X_3O ligt en X_2 op de lijn X_4O ligt, en andersom.

Hoeveel oplossingen kan een stappenplan om een constructie op te lossen produceren? Elk stappenplan van deze soort is opgebouwd uit elementaire bewerkingen, waarvan er vijf zijn:

1. Trek een lijn door twee gegeven punten.
2. Construeer een cirkel met gegeven straal en middelpunt.
3. Vind het snijpunt van twee gegeven lijnen.
4. Vind het snijpunt van een gegeven lijn en een gegeven cirkel.
5. Vind het snijpunt van twee gegeven cirkels.

De eerste drie operaties geven een enkele waarde (enkelwaardige operaties), maar de laatste twee kunnen ook twee oplossingen geven.
Als het stappenplan alleen enkelwaardige operaties bevat, zal de oplossing uniek zijn. Als er één tweewaardige operatie in zit, zullen er twee oplossingen zijn. In het algemeen geldt:

Stelling *als het programma k tweewaardige operaties bevat, zijn er 2^k oplossingen.*

We hebben gezien dat sommige van die oplossingen alsnog tot dezelfde oplossing kunnen leiden. Het tegen elkaar wegvallen van oplossingen gebeurt altijd zó dat de onbepaaldheid (hoeveelheid oplossingen) van de uiteindelijke oplossing altijd van de vorm $2^l, (l \leq k)$ is.

Dit is meer een algebraïsche stelling dan een geometrische, die uit de algebra van de *Galois theorie* komt. Het bewijs van deze stelling valt daarom buiten de strekking van deze paper.

Een voorbeeld van een constructie dat nu uitgewerkt zal worden, is dat van het vinden van een raaklijn aan twee cirkels. De cirkels noemen we ω_1 en ω_2, met middelpunten O_1 en O_2. De elementaire bewerkingen waarmee je zo'n raaklijn kan vinden zijn de volgende:

1. Trek een lijn α door O_1 en O_2.
2. Markeer de punten A_1 en A_2 waar α de cirkels ω_1 en ω_2 snijdt.
3. Teken een cirkel ω_3 met middelpunt A_1 en straal $|O_2A_2|$.
4. Markeer het punt B waar ω_3 en de lijn α elkaar snijden.
5. Teken een cirkel ω_4 met middelpunt O_1 en straal $|O_1B|$.
6. Teken een cirkel ω_5 met straal $|O_1O_2|$ en middelpunt O_1.
7. Teken een cirkel ω_6 met middelpunt O_2 en straal $|O_1O_2|$.
8. Markeer de punten C en C' waar ω_5 en ω_6 elkaar snijden.
9. Trek een lijn β door C en C'.
10. Markeer het punt D waar α en β elkaar snijden.
11. Teken een cirkel ω_7 met middelpunt D en straal $|DO_1|$
12. Markeer het punt E waar ω_4 en ω_7 elkaar snijden.
13. Trek een lijn γ door E en O_1.
14. Markeer het punt F waar γ en ω_1 elkaar snijden.
15. Teken een cirkel ω_8 met middelpunt F en straal $|O_1A_1|$.
16. Markeer de punten G en G' waar γ en ω_8 elkaar snijden.
17. Teken een cirkel ω_9 met middelpunt G en straal $|A_1A_2|$.
18. Teken een cirkel ω_{10} met middelpunt G' en straal $|A_1A_2|$.
19. Markeer de punten H en H' waar ω_9 en ω_{10} elkaar snijden.
20. Trek een lijn δ door H en H'.

Wat we nu merken, is dat als alle mogelijkheden worden uitgewerkt, er acht lijnen δ zijn, die dus de raaklijn aan beide cirkels zou moeten vormen. We zien dat vier van de lijnen daadwerkelijk raaklijnen zijn, de andere vier lijken geen raaklijn te zijn.
Echter, als je de cirkel ω_2 spiegelt in spiegelvlak k, zien we dat de overige gevonden lijnen δ raaklijnen vormen aan ω_2'. Het vermoeden wat hierdoor ontstaat is dat de formulering van het probleem niet duidelijk is: er zijn raaklijnen gevonden aan de twee cirkels, maar ook aan een andere cirkel. De verklaring voor

het feit dat die raaklijnen ook gevonden zijn, kan inderdaad gevonden worden door naar de vraagstelling te kijken. In de derde stap kies je welke van de twee cirkels ω_1 is, en waarmee je dus de constructie begint. Je kunt nu zowel de linker- als de rechtercirkel kiezen, waarbij het zo is dat je je assen altijd zo kunt kiezen dat de cirkels links en rechts van elkaar liggen, en niet bijvoorbeeld boven en onder elkaar. Doordat je dus niet weet aan welke kant van ω_1 ω_2 ligt, biedt de constructie uitkomst voor beide mogelijkheden, en daarom vind je ook oplossingen voor ω_2'.

Deze constructie is ook een mooi voorbeeld van het feit dat het uiteindelijke aantal oplossingen altijd van de vorm 2^l is, en de totale hoeveelheid oplossingen van de vorm 2^k. We zien namelijk dat:

1. Bij de eerste stap is er 1 oplossing
2. Bij de tweede stap zijn er twee punten A_1 en twee punten A_2.
3. Dit geeft 4 cirkels ω_3, waarvan er 2 verschillend zijn.
4. Voor elke cirkel zijn er twee punten B, dus in totaal 8 punten, waarvan 4 verschillend zijn omdat 2 cirkels ω_2 samenvallen.
5. Voor elk punt B is er een ω_4 dus in totaal 8 cirkels, maar omdat er maar 4 verschillende punten B zijn, zijn het er 4, en daarvan vallen er weer twee samen, dus in totaal zijn er 2 verschillend.
6. Er is 1 cirkel ω_5.
7. Er is 1 cirkel ω_6.
8. Er is 1 punt C en 1 punt C'.
9. Er is 1 lijn β.
10. Er is 1 punt D.
11. Er is 1 cirkel ω_7.
12. Er zijn 4 punten E, omdat er slechts twee verschillende cirkels ω_4 zijn. De totale onbepaaldheid kan maximaal 16 zijn.
13. Er zijn 4 lijnen γ, met een totale onbepaaldheid van 16.
14. Er zijn 8 punten F, met een totale onbepaaldheid van 32.
15. Er zijn 8 cirkels ω_8, met een totale onbepaaldheid van 32.
16. Er zijn 8 punten G en 8 punten G', met een totale onbepaaldheid van 32.
17. Er zijn 8 cirkels ω_9, met een totale onbepaaldheid van 32.
18. Er zijn 8 cirkels ω_{10}, met een totale onbepaaldheid van 32.
19. Er zijn 8 punten H en 8 punten H' met een totale onbepaaldheid van 32.
20. Er zijn 8 lijnen δ met een totale onbepaaldheid van 32.

Uit dit voorbeeld blijkt duidelijk hoe verschillende mogelijkheden kunnen samenvallen en daardoor er uiteindelijk minder oplossingen zijn. Ook is duidelijk dat zowel de hoeveelheid verschillende oplossingen (8) als de totale onbepaaldheid (32) een macht van 2 zijn.

Onderstaande plaatjes laten zien hoe de constructie werkt: De globale weergave laat zien hoe de constructie werkt, hoe je een raaklijn kan construeren met deze methode. De weergave van de volledige constructie laat zien wat het resultaat is van de constructie zoals hierboven weergegeven in een stappenplan. Hierin is goed te zien hoeveel oplossingen er zijn, en welke oplossingen uiteindelijk weer samenvallen, waardoor de onbepaaldheid niet gelijk is aan de hoeveelheid oplossingen. De weergave van alle raaklijnen, het spiegelvlak en ω_2' laat zien hoe de andere 4 oplossingen uiteindelijk toch goede oplossingen zijn, als je ω_2 spiegelt.

`Calfgr4.jpg`

Figuur 3: Globale weergave van de constructie van 2 van de raaklijnen aan beide cirkels.

We keren terug naar het probleem van het vinden van een bisectrice van een hoek. Als we proberen de bisectrice van hoek AOB te vinden, vinden we gelijk de bisectrice van de de andere, 'tegenovergestelde' hoek, die samen met de hoek AOB die we bedoelen een hoek van π maakt. Deze oplossing hoeft niet gezien te worden als overbodig, aangezien we in ons stappenplan het probleem formuleren aan de hand van twee snijdende lijnen, en de beide oplossingen dus even goed zijn.

Dit geldt in het algemeen:

Stelling *Alle 2^l oplossingen die gevonden worden met een stappenplan zijn 'echte' oplossingen,* als het probleem goed geformuleerd is.

Bijvoorbeeld, het probleem van het construeren van een ingeschreven cirkel in een gegeven driehoek kan opgelost worden met een stappenplan met een onbepaaldheid van 16 (er zijn 16 oplossingen), waarbij er vier *verschillende*

`Calveelcirkels.jpg`

Figuur 4: Weergave van de volledige constructie.

oplossingen zullen worden gevonden, één ingeschreven cirkel en drie omschreven cirkels. Deze oplossingen zijn allevier goed als we het probleem als volgt formuleren: Teken een raakcirkel aan drie gegeven rechte lijnen. Het onderscheid tussen ingeschreven en omschreven cirkel is afhankelijk van het concept van 'tussen', of 'binnen', wat niet te begrijpen is voor een computer.
De bovenstaande voorbeelden laten zien dat als een geometrisch constructieprobleem meerdere oplossingen heeft, dat het constructiestappenplan alle oplossingen zal geven. Dit geldt ook in het algemene geval:

Stelling *Elk geometrisch constructieprobleem dat opgelost kan worden met passer en lineaal heeft* 2^l *oplossingen.*

Deze bewering ziet er vrij eenvoudig uit, en toch duurde het tot de negentiende eeuw voordat hij ontdekt werd. Hoe komt het dat het zo lang geduurd heeft?
Een mogelijke verklaring hiervoor was de afwezigheid van een hedendaags, bereking-georienteerde formulering van het probleem. Een andere reden was de gescheiden behandeling van elk probleem, in plaats van dat het werd gezien als één groot probleem, zoals het probleem van het construeren van een regelmatige n-hoek voor elke n. Het is mogelijk dat dit onderwerp onderzocht zal

Calspiegel.jpg

Figuur 5: Alle raaklijnen weergegeven met ω_2' en het spiegelvlak erbij.

Calfgr3.jpg

Figuur 6: Bissectrice van een hoek inclusief de buitenhoek.

worden door geschiedkundigen en wiskundigen, en er een complete verklaring zal komen voor deze gemiste kans.

4 Regelmatige veelhoeken

We willen weten hoe je een regelmatige n-hoek construeert met behulp van een passer en liniaal. We gaan daarom onderzoeken op hoeveel mogelijke manieren een bepaalde n-hoek te construeren is. Om niet aan oneindig veel oplossingen te komen, stellen we een grootte en positie vast: we nemen aan dat de n-hoek is ingeschreven in een gegeven cirkel ω met middelpunt O en dat de positie van één van zijn hoeken, A_0, is gegeven. Vervolgens moeten we de posities $A_1, A_2, \ldots, A_{n-1}$ van de andere hoeken bepalen. Het is nu genoeg alleen de positie van A_1 te bepalen. Vervolgens worden de overige hoekpunten gevonden door de boog A_0A_1 af te tekenen op de cirkel.
De oplossing voor $n = 6$ is het gemakkelijkst, omdat we gebruik kunnen maken van het volgende lemma:

Lemma *De lengte van een zijde van een regelmatige zeshoek is gelijk aan de straal van de omgeschreven cirkel.*

Bewijs Bekijk een regelmatige zeshoek met zijden A,B,C,D,E,F en met omgeschreven cirkel (O;AO). Omdat het een regelmatige zeshoek is geldt: $AB = BC = CD = DE = EF = FA$, en dat $AO = BO = CO = DO = EO = FO$. Dus de driehoeken ABO, BCO, CDO, DEO, EFO, FAO zijn congruent. Hieruit volgt dat de hoeken AOB, BOC, COD, DOE, EOF, FOA gelijk zijn, en omdat een cirkel 360° bevat, is iedere hoek dus gelijk aan $\frac{360^\circ}{6} = 60^\circ$. Omdat de driehoek ABO gelijkbenig is (AO = BO) geldt dat $\angle ABO = \angle BAO = \frac{180^\circ - 60^\circ}{2} = 60^\circ$. Dus er geldt dat $\angle ABO = \angle BAO = \angle AOB = 60^\circ$. Hieruit volgt dat AB = OB = OA, dus AB is gelijk aan de straal van de omgeschreven cirkel. □

De constructie van een regelmatige zeshoek is dan als volgt:

1. Teken met een passer de cirkel ω_1 met middelpunt A_0 en straal $|OA_0|$.
2. Noem het snijpunt van de cirkels ω en ω_1 A_1.

Omdat er twee mogelijkheden zijn voor A_1, bevat de constructie twee verschillende oplossingen, maar het resultaat is hetzelfde. Alleen de volgorde waarin de hoeken zijn genummerd is verschillend. Dit is te zien in figuur (7); wanneer je de procedure zou herhalen zou je zien dat A_2' overeenkomt met hoek A_4'' en zo verder.

Voor $n = 5$ en $n = 10$ is er echter wel een verschil tussen de verschillende oplossingen. We bekijken het geval voor $n = 10$. Als we de bissectrice A_1B van de hoek OA_1A_0 zouden construeren, zouden de resulterende driehoeken OA_1B en BA_1A_0 twee gelijke zijden hebben en de driehoeken OA_1A_0 en BA_1A_0 zouden dan gelijkvormig zijn. We willen nu natuurlijk A_1 vinden.
Beschouw de lijn OA_0 als getallenlijn waarbij het punt O correspondeert met 0 en het punt A_0 met 1. Laat het punt B corresponderen met het onbekende getal x. Vanwege de gelijkvormigheid geldt: $\frac{A_1B}{A_0B} = \frac{OA_0}{A_1A_0}$. Omdat $A_1B = A_1A_0 = OB = x$ en $A_0B = A_0O - OB = 1 - x$ komen we dan uit op de volgende vergelijking:

$$\frac{x}{1-x} = \frac{1}{x} \tag{7}$$

constrrzeshoek.jpg

Figuur 7: De constructie van een regelmatige zeshoek waarbij de hoekpunten worden gevonden door de straal van de omgeschreven cirkel af te meten

Of anders geschreven:

$$x^2 + x - 1 = 0 \tag{8}$$

Als we de vergelijking oplossen vinden we punt B. A_1 kan nu gevonden worden als het snijpunt van de gegeven cirkel ω en de cirkel met middelpunt A_0 en straal x. Er zijn twee snijpunten dus ook twee oplossingen: de punten A_1‘ en A_2“. De kwadratische vergelijking heeft echter ook twee oplossingen:
$x_1 = \frac{-1+\sqrt{5}}{2}$ en $x_2 = \frac{-1-\sqrt{5}}{2}$
x_2 is negatief, wat geometrisch gezien betekent dat het punt B aan de andere kant van O ligt en dus niet tussen O en A_0 in. Er zijn dus nog twee oplossingen voor A_1: A_1''' en A_1'''' We hebben vier verschillende posities voor A_1 gevonden die twee verschillende decagons geven: een convex (zie figuur 8) en een stervormige (zie figuur 9). Het is leuk om te weten dat als je de zijden van de convex doortekent, er ook een stervormig decagon tevoorschijn komt (maar deze is niet meer omschreven door cirkel ω) (zie figuur 10).

In het geval van $n = 5$, dus bij pentagons, gebeurt hetzelfde: er bestaan ook vier oplossingen, die leiden tot twee verschillende pentagons (met ook weer twee mogelijke nummeringen van hoeken).

We gaan nu kijken naar een willekeurige regelmatige n-hoek en proberen het aantal verschillende oplossingen te vinden. Laat x de lengte van de boog A_0A_1 zijn. Het punt A_1 is de oplossing als we na n keer de booglente A_0A_1 afmeten op de cirkel vanuit punt A_0 we weer precies uitkomen bij A_0, waarbij n het convex.jpg

Figuur 8: De constructie van een regelmatige tienhoek. Een van de oplossingen is een covex.

stervormige.jpg

Figuur 9: Een regelmatige tienhoek in de vorm van een ster convexster.jpg

Figuur 10: Als je de zijden van een regelmatige convex doortekent ontstaat er ook een ster

aantal hoeken van de n-hoek is. Anders geformuleerd staat hier, bij een omtrek van 1: Het getal nx is een geheel getal en de getallen $x, 2x, 3x, \ldots, (n-1)x$ zijn geen gehele getallen. Dus als $n = 10$, dan kan x gelijk zijn aan $\frac{1}{7}$, maar ook aan $\frac{7}{10}$ of $\frac{9}{10}$. Deze waarden corresponderen met de vier oplossingen die we hebben gevonden met de geometrie. Stel dat we $x = \frac{11}{10}$ kiezen, dan vinden we geen nieuwe geometrische oplossingen, omdat de positie van het hoekpunt op de cirkel niet afhangt van $x = \frac{k}{n}$, maar afhangt van de rest na deling van k door n.

Lemma *Zij $A_0A_1...A_{n-1}$ een regelmatige n-hoek en $x = \frac{k}{n}$ de booglengte A_0A_1 en de omtrek van de cirkel $= 1$. Dan hangt de positie van het hoekpunt op de cirkel hangt af van de rest na deling van k door n*

Bewijs

We kunnen k schrijven als $k = an+b$ met $a, b \in \mathbb{Z}, b > 0$. Dus $booglengte A_0A_1 = \frac{an+b}{n} = a + \frac{b}{n}$. We weten ook dat deze booglengte kleiner is dan 1 (omdat de omtrek gelijk is aan 1 en de booglengte tussen twee punten op de cirkel kleiner is dan de omtrek) en groter is dan 0 (omdat afstanden per definitie groter zijn dan 0). Dus $a = 0$, waaruit volgt dat, om de positie te bepalen, de positie van het hoekpunt alleen afhangt van $\frac{b}{n}$ en niet van a. Dus de positie van een hoekpunt op de cirkel hangt af van $b \equiv k(mod(n))$. □

Lemma *Zij $m < n$ en $x = \frac{m}{n}$. Alleen voor $ggd(m, n) = 1$ geldt dat kx alleen een geheel getal is als k een veelvoud is van n.*

Bewijs Zij $m < n$ en $x = \frac{m}{n}$

- Laat $kx \in \mathbb{N} \Leftrightarrow k = bn$ met $b \in \mathbb{N}$. Stel $ggd(m,n) = a$ met $a \neq 1$. Dan geldt $n = am$ en $a < n$. Dus $x = \frac{m}{am} = \frac{1}{a}$. Dus dan geldt $kx \in \mathbb{N}$ voor $k = a < n$. Dit is een tegenspraak dus $ggd(m,n) = 1$
- Laat $ggd(m,n) = 1$.
  Voor $k = bn$ met $b \in \mathbb{N}$, $kx = bn\frac{m}{n} = bm \in \mathbb{N}$.
  Stel nu $kx \in \mathbb{N}$ voor $k \neq bn$ met $b \in \mathbb{N}$. Dan $kx = \frac{km}{n} \in \mathbb{N}$, dus $\exists p \in \mathbb{N}$ zodat $\frac{km}{n} = p$. Dus $n = \frac{k}{p}m$, er geldt $n \in \mathbb{N}$, dus $\frac{k}{p} \in \mathbb{N}$ dus $ggd(m,n) = m$. Dit is een tegenspraak, dus $kx \in \mathbb{N} \Leftrightarrow k = bn$ met $b \in \mathbb{N}$. □

Dus ieder getal kleiner dan n en relatief priem aan n is een oplossing voor de constructie van een regelmatige n-hoek. Daarom wordt het aantal verschillende oplossingen gegeven door Euler's functie. Als we deze functie bekijken voor de door ons bekeken veelhoeken, vinden we $\phi(5) = \phi(10) = 4$ en $\phi(6) = 2$. Deze waarden zijn in overeenstemming met het aantal de door ons gevonden oplossingen. In het vorige hoofdstuk hebben we gezien dat een constructieprobleem dat kan worden opgelost met passer en liniaal 2^l verschillende oplossingen moet hebben. Hier vinden we de belangrijke voorwaarde van ons probleem:

Een regelmatige n-hoek kan alleen worden geconstrueerd met passer en liniaal als $\phi(n) = 2^l$, waarbij l een geheel getal is.

5 Fermat getallen

We hebben zojuist laten zien dat om een regelmatige n-hoek te construeren het nodig is dat

$$\phi(n) = 2^l \tag{9}$$

met l een geheel getal, maar nu we dit weten hebben we niet zomaar een oplossing voor ons probleem. We weten namelijk niet hoeveel getallen n er zijn waar de voorwaarde voor geldt, dus voor hoeveel n een regelmatige n-hoek is te construeren. We kunnen voor een n wel bepalen of deze aan de voorwaarde voldoet door simpelweg $\phi(n)$ te bepalen, maar het zou veel makkelijker zijn als er een goede beschrijving was van de verzamling voor alle n waarvoor vergelijking (9) geldt. Het beschrijven van deze verzameling is zelfs een groot probleem in de wiskunde en is nog steeds niet opgelost. We zullen de belangrijkste punten van het probleem beschrijven. Een manier om de verzameling te omschrijven kan door middel van ontbinding in priemfactoren.

$$n = p_1^{m_1} p_2^{m_2} \cdot \dots \cdot p_k^{m_k} \tag{10}$$

We hebben n als vermenigvuldiging van priemgetallen, dus door eigenschappen 1 en 2 te gebruiken kunnen we $\phi(n)$ bepalen.

$$\phi(n) = \phi(p_1^{m_1}) \cdot \phi(p_2^{m_2}) \cdot \dots \cdot \phi(p_k^{m_k}) \tag{11}$$

$$\phi(n) = p_1^{m_1-1} \cdot p_2^{m_2-1} \cdot \dots \cdot p_k^{m_k-1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1) \tag{12}$$

Om ervoor te zorgen dat $\phi(n)$ een macht van 2 is moet elk oneven priemgetal p_i een macht $m_i = 1$ hebben en moet p_i de vorm $2^t + 1$ hebben. Het bewijs hiervan geven we, maar daarvoor hebben we nodig dat iedere macht van 2 slechts deelbaar is door machten van 2.

Lemma 1 *Elk getal van de vorm 2^n is alleen deelbaar door getallen van de vorm 2^m met $m \leq n$.*

Bewijs We gaan dit lemma bewijzen met inductie.

- Voor $n = 0$ en $n = 1$ is het lemma waar, want $2^0 = 1$ en $2^1 = 2$.
- Neem aan dat het lemma waar is voor $n \leq k$. Voor $k + 1$ geldt dat $2^{k+1} = 2^1 \cdot 2^k$. Nu is $2^1 = 2$ en 2 is na 1 ook het kleinste getal waarmee 2^k vermenigvuldigd kon worden, dus 2^{k+1} is alleen deelbaar door 2 en alle getallen waar 2^k deelbaar door is en dat zijn alleen maar machten van 2. Dus volgens het principe van wiskundige inductie is het lemma bewezen. $\square$

Nu we dit weten kunnen we bewijzen dat p_i en m_i de eerdergenoemde vorm moeten hebben.

Bewijs

- Als $\phi(n) = p_1^{m_1-1} \cdot p_2^{m_2-1} \cdots p_k^{m_k-1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1) = 2^l$ dan is volgens lemma 1 elke factor van $p_1^{m_1-1} \cdot p_2^{m_2-1} \cdots p_k^{m_k-1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)$ een macht van 2.
- Als $p_i = 2$ dan is $p_i^{m_i-1}$ sowieso een macht van 2 en $(p_i - 1) = (2 - 1) = 1$, dus ook een macht van 2.
- Voor $p_i \neq 2$, dus als p_i oneven is, geldt dat $p_i^{m_i-1} = 2^s$ met s willekeurig, omdat p_i oneven is kan dit alleen als $m_i = 1$, want volgens lemma 1 kan 2^s niet gelijk zijn aan een macht van een ander getal dan 2, maar als $m_i = 1$ dan is $p_i^{m_i-1} = p_i^0 = 2^0 = 1$. Dat is dus de enige mogenlijkheid voor m_i. Ook moet gelden dat $(p_i - 1) = 2^t$ met t willekeurig, dus $p_i = 2^t + 1$

Nu weten we dus zeker wat de vorm van de priemgetallen moet zijn. $\square$

Merk op dat niet alle getallen van deze vorm priem zijn. Neem bijvoorbeeld $2^6 + 1 = 65$, dit is deelbaar door 5 en dus geen priemgetal. De voorwaarde waar t aan moet voldoen zodat $2^t + 1$ en we zullen nu laten zien dat dat zo is.

Lemma 2 *Als n een positief geheel getal is dan $a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$.*

Bewijs Dit volgt logisch als we $(a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$ uitschrijven. Eerst vermeningvuldigen we de som met $(a-b)$.

$$\begin{aligned}(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} &= \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} - \sum_{k=0}^{n-1} a^k b^{n-k} \\ &= a^n + \sum_{k=0}^{n-1} a^k b^{n-k} - \sum_{k=0}^{n-1} a^k b^{n-k} - b^n \\ &= a^n - b^n\end{aligned}$$

□

Stelling *Als 2^n+1 een oneven priemgetal is n een macht van 2*

Bewijs We bewijzen dit met contrapositie. Stel n is een geheel getal dat geen macht van 2 is, dan heeft n een oneven getal in de priemfactorisatie, dus $n = rs$ waarin $1 \leq r<n, 1<s<n$ waarin s oneven is. Uit Lemma 2 volgt dat, voor een geheel getal m,

$$(a-b)|(a^m - b^m)$$

Als we nu stellen $a = 2^r, b = -1$ en $m = s$, dan geeft dat,

$$\begin{aligned}(2^r - (-1)^s)|(2^{rs} - (-1)^s) \\ (2^r + 1)|(2^n + 1)\end{aligned}$$

Dus dan is 2^n+1 niet priem, dus volgens contrapostie is de stelling bewezen. □

Getallen van deze vorm worden Fermat getallen genoemd. De gebruikelijke notatie van deze getallen is F_n waarin n overeenkomt met n in $2^{2^n}+1$. Merk op dat dit geen priemgetallen hoeven te zijn. De eerste vijf Fermat getallen zijn dat wel, namelijk: 3, 4, 17, 257 en 65537, maar zoals Euler al opmerkte is het zesde getal niet priem, het is deelbaar door 641. Ook na Euler zijn er veel wiskundige bezig geweest met Fermat getallen. Één van de dingen die zijn ondekt door I.M. Pervushin in 1877 is dat $2^{2^{12}}+1 = 7 \cdot 2^{14}+1$. Er zijn ook na hem nog vele wiskundigen bezig geweest met het berekenen van priem factor ontledingen van Fermat getallen. De meest recente werd nog op 20 maart 2011 gevonden door Roman Maznichenko. Hij vond een priemfactor van F_{42}. Toch is het nog steeds niet bekend of het aantal Fermat getallen eindig is of niet.

We hebben dus laten zien dat een regelmatige n-hoek geconstrueerd kan worden met passer en liniaal als $n = 2^s \cdot p_1 \cdot p_2 \cdots \cdot p_k$ waarbij p_i paarsgewijs disjuncte Fermat priemgetallen zijn. Het omgekeerde, dat elk getal dat van de vorm $n = 2^l \Pi p_i$ is, waarin p_i verschillende Fermat-priemgetallen zijn, geconstrueerd kan worden, kan bewezen worden met behulp van Galois-theorie.

De functie $\sigma : K \to K$ die de wortel $e^{\frac{2\pi i}{p}}$ naar $e^{\frac{2\pi i j}{p}}$ stuurt, is een automorfisme van K. We weten dat $x^p - 1$ een veelterm is over $\mathbb{Q}$, en K een lichaamsuitbreiding van $\mathbb{Q}$ waarin $x^p - 1$ volledig ontbindt in lineaire factoren, aangezien $e^{\frac{2\pi ij}{p}}$ alle wortels van $x^p - 1$ geeft. Dus weten we dat $x^p - 1$ volledig splijt in K. De wortels brengen een deellichaam van K voort, dit noemen we het splijtlichaam van $x^p - 1$. Nu geldt dat elk automorfisme van K over $\mathbb{Q}$ gezien kan worden als een splijtlichaam van $x^p - 1$.

Elk element van K is algebraïsch over $\mathbb{Q}$, omdat het de oplossing is van een veeltermvergelijking over $\mathbb{Q}$, namelijk $x^p - 1$. Als elk element algebraïsch is, geldt dat de uitbreiding algebraïsch is, dus K is een algebraïsche uitbreiding, dus K over $\mathbb{Q}$ is een galoisgroep, want een galoisgroep is de groep van $\mathbb{Q}$-automorfismen van een algebraïsche uitbreiding.

Stelling *Als de keten $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset K_3 = K$ aan de volgende eigenschappen voldoet, met $a_1, ..., a_n$ een stel construeerbare reële getallen:*

1. *K een deellichaam is van $\mathbb{R}$*
2. *$a_1, ..., a_n \in K$*
3. *voor i$= 0, ..., n-1$ geldt $K_{i+1} = K_i(\sqrt{r_i})$ met $0 < r_i \in K_i$ en $\sqrt{r_i} \notin K_i$*

dan is elk element van K construeerbaar.

Bewijs Aan deze voorwaarden wordt voldaan:

1. Er geldt dat K een deellichaam is van $\mathbb{R}$:
   (a) Omdat $1 \in \mathbb{Q}$ en $\mathbb{Q} \subset K$, geldt $1 \in K$.
   (b) Omdat voor alle $a, b \in K$ geldt dat $a - b \in K$
   (c) Omdat voor alle $a, b \in K$ met $b \neq 0$ geldt dat $ab^{-1} \in K$.
2. Er geldt dat $a_1, ..., a_n \in K$
3. Omdat in dit geval de keten bestaat uit $\mathbb{Q} \subset K$, en $K = \mathbb{Q}(\sqrt{r_i})$, geldt de derde eigenschap ook.

Dus geldt dat elk element van K construeerbaar is. □

Stelling *Voor een lichaam K met de eigenschappen zoals in de vorige stelling geldt dat $[K : \mathbb{Q}] = 2^m$.*

Bewijs Zij K het laatste lichaam in een toren met eigenschappen zoals in de vorige stelling, dan geldt $[K : \mathbb{Q}] = 2^m$ vanwege de torenformule.

Dus de Galois groep (K/$\mathbb{Q}$) is van de orde 2^m en is oplosbaar.

Wanneer dit wordt gereduceerd tot een compositie serie en gebruikmakend van de Galois correspondentie heeft men een toren van velden, elk van graad twee over zijn voorganger, precies wat nodig is voor construeerbaarheid.
We komen dan tot de volgende oplossing van ons probleem:
Een regelmatige n-hoek kan worden geconstrueerd met passer en liniaal dan en slechts dan als $n = 2^s \cdot p_1 \cdot p_2 \cdots p_k$ waarbij p_i paarsgewijs disjuncte Fermat priemgetallen zijn.

6 Conclusie

We hebben gezien dat Euler het bij het rechte eind had toen hij veronderstelde dat een belangrijke eigenschap van een geheel getal n is de hoeveelheid getallen kleiner en relatief priem aan zichzelf het heeft, gegeven door $\phi(n)$. Hoewel je dit een rekenkundige eigenschap zou noemen, heeft het dus ook geometrisch een betekenis. Een regelmatige n-hoek kan alleen worden geconstrueerd als $\phi(n) = 2^l$ waarbij l een geheel getal is. Dit komt doordat ieder geometrisch probleem dat opgelost kan worden met passer en lineaal 2^l oplossingen heeft. We hebben vervolgens bewezen dat als $\phi(n) = 2^l$ dat n dan van de vorm $2^s \cdot p_1 \cdot p_2 \cdots p_k$ is waarbij p_i paarsgewijs disjuncte Fermat priemgetallen zijn; priemgetallen van de vorm $2^{2^n} + 1$. Met behulp van Galoistheorie kunnen we ook bewijzen dat als $n = 2^s \cdot p_1 \cdot p_2 \cdots p_k$, een regelmatige n-hoek geconstrueerd kan worden. We komen dan uiteindelijk tot de volgende conclusie: *Een regelmatige n-hoek kan worden geconstrueerd met passer en liniaal dan en slechts dan als $n = 2^s \cdot p_1 \cdot p_2 \cdots p_k$ waarbij p_i paarsgewijs disjuncte Fermat priemgetallen zijn.*

7 Referenties

1. Kirillov, A., *On Regular Polygons, Euler's Function and Fermat Numbers*, translated by N.K. Kulman, Boersma,S., Fokkema, T., Kupers, S., Steenstra, J., *De construeerbaarheid van regelmatige veelhoeken*, 14 maart 2006, Universiteit Utrecht, "http://www.phys.uu.nl/~3021009/kaleidoscoop/De%20construeerbaarheid%20van%20regelmatige%20veelhoeken%20%28verbeterde%20versie%29.pdf"

2. Bishop, H., *How to Construct a Regular Polygon*, The American Mathematical Monthly, Vol. 85, No. 3 (Mar., 1978), pp. 186-188,"https://mail.google.com/mail/u/1/?ui=2&ik=9cdfc5e165&view=att&th=12efd2e2723137f0&attid=0.1&disp=vah&realattid=8ea6e395fd6eaca8_0.1&zw"

3. Krizek, M.,*17 necessary and sufficient conditions for the primality of Fermat numbers*, Acta Mathematica Universitatis Ostraviensis, Vol. 11 (2003), No. 1, 73–79 "https://mail.google.com/mail/u/1/?ui=2&ik=9cdfc5e165&view=att&th=12efd2e2723137f0&attid=0.2&disp=vah&realattid=8ea6e395fd6eaca8_0.2&zw"

4. Christian Gottlieb (1999). *The Simple and Straightforward Construction of the Regular 257-gon.* Mathematical Intelligencer 21 (1): 31–37

5. C. M. van der Straaten, *Getallentheorie.*

6. B. van Geemen, J. Top, *Ringen en Galoistheorie* zoals bewerkt naar: H. W. Lenstra, F. Oort, *Ringen en Lichamen*, versie V: 1.I.2008.

7. E. T. Eekhoff, *Construcibility of Regular Polygons*, http://orion.math.iastate.edu/dept/thesisarchive/MSM/EekhoffMSMSS07.pdf