Elliptische functies en krommen (2)

In het vorige artikel van dit tweeluik hebben we gekeken naar speciale functies die dubbel periodiek zijn. Deze functies worden ook wel elliptische functies genoemd. Een voorbeeld van zo'n functie is de functie die de uitwijking van een slinger beschrijft. Ook hebben we in het vorige artikel de naam Taniyama al laten vallen, en de relatie die hij vermoedde tussen speciale meetkundige objecten en deze fascinerende functies. In dit deel zullen we deze meetkundige objecten nader bekijken.

Afbeelding 1. Een slinger van Fouceault.Uit een fysisch eenvoudig systeem zoals een slinger volgt uiteindelijk

bijzonder diepgaande wiskunde. Afbeelding: Daniel Sancho.

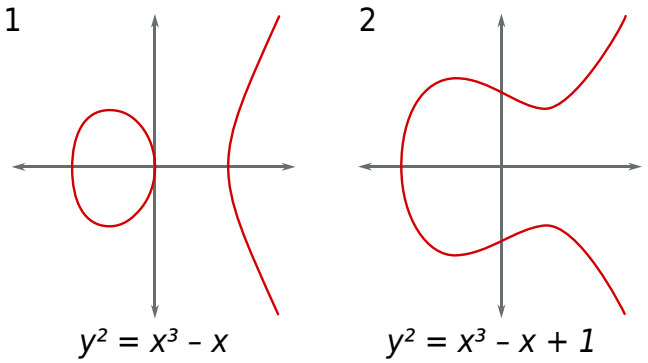
Veel mensen kennen de vergelijking voor een parabool, en die voor moeilijkere functies zoals

$$y=ax^3+bx+c,$$

maar ‘functies’ die de meeste mensen niet kennen zijn van de volgende vorm:

$$y^2=ax^3+bx+c.$$

Hoe de grafiek van zo’n functie eruitziet kun je zien in afbeelding 2 hieronder.



Afbeelding 2. Een elliptische kromme.Twee voorbeelden van elliptische krommen voor verschillende waarden van a, b en c. Afbeelding: Wikipediagebruiker SuperManu.

Aan de bovenstaande voorbeelden zie je dat dit soort functies er heel anders uitzien dan de functies die je kent uit je wiskundeboek. Ze kunnen uit verschillende delen bestaan, en normaalgesproken zou je ook niet de y^2 in de vergelijking laten staan. Om deze functie te plotten zou je eerder aan beide kanten de wortel nemen, en dus

$$y=\pm(ax^3+bx+c)^{1/2},$$

invoeren en dan bekijken hoe de functie eruitziet voor elk teken. Je ziet dus dat de functies waaraan je gewend bent erg anders zijn dan deze functies. We noemen deze functies ook wel *elliptische krommen*. Voordat ik verder ga wil ik eerste uitleggen waar deze naam vandaan komt. Ten eerste: *elliptisch*. Dit is een historisch gegroeide naam die zijn origine heeft in de omtrek bepalen van een ellips, zoals we al eerder tegenkwamen in het vorige artikel. Ten

tweede: *krommen*. Dit betekent niets anders dan een gekromde lijn, dus een cirkel of zelfs een rechte lijn kun je ook krommen noemen. We gebruiken hier het woord krommen omdat onze functies vaak niet uit één deel bestaan en om ze te plotten je twee delen aan elkaar moet plakken. In de rest van dit artikel zullen we deze meetkundige objecten, *elliptische krommen*, bestuderen.

Om de discussie wat gemakkelijker te maken wil ik focussen op één elliptische kromme, namelijk

$$\mathbf{y^2=x^3-4x^2+16,}$$

Om de connectie te maken met dubbelperiodieke functies, ofwel de elliptische functies, van het vorige artikel, wil ik naar de gehele getallen x en y kijken die aan de bovenstaande vergelijking voldoen. Ik wil echter niet zomaar naar oplossingen kijken – ik wil oplossingen *modulo een priemgetal* bekijken. Dat betekent dat als p een voorafgekozen priemgetal is, p + 2 voor ons hetzelfde is als 2. Ook elk veelvoud van het priemgetal dat ik bij 2 optel zien we als 'hetzelfde' als 2.

Je kunt ook zeggen dat ik naar oplossingen x en y kijk en dan van x en y net zolang p af haal todat ik een geheel getal overhoud dat kleiner is dan p. Laten we dit eens bekijken bij de bovenstaande elliptische kromme en het priemgetal 3. Voeren we $x=0$ in, dan krijgen we $y^2=16$. Maar we willen alleen maar getallen hebben kleiner dan 3 en van 16 kunnen we vijf keer 3 afhalen en dus zeggen we dat 16 gelijk is aan 1 als we *modulo 3* rekenen. Het getal 17 zou dan bijvoorbeeld gelijk zijn aan 2. Dus voor $x=0$ vinden we de oplossing $y^2=1$, dus $y=\pm 1$.

Als we kijken naar $x=1$, dan vinden we dat $y^2 = 13$ ofwel $y^2=1$, want van 13 kun je vier keer 3 halen. Dus krijgen we wederom $y=\pm 1$. Voor $x=2$ vinden we (probeer het zelf uit!) geen gehele y als oplossingen. Het getal $x=3$ hoeven we niet te proberen, want we zijn alleen in oplossingen modulo 3 geinteresseerd. Aangezien 3 gelijk is aan 0 modulo 3, en we $x=0$ al hebben doorgerekend, is dat inderdaad overbodig. We vinden dus in totaal 4 verschillende oplossingen, namelijk $(x,y)=(0,\pm 1)$ en $(1,\pm 1)$.

Nu komt het magische! Tellen we nu het aantal oplossingen voor elk priemgetal, dan krijgen

we een lijstje met daarin het aantal oplossingen modulo het gekozen priemgetal. Laten we nu het aantal oplossingen voor elk priemgetal p met A_p noteren. We willen nu een nieuwe functie maken van de vorm

$$\mathbf{F(z) = N_1\, q + N_2\, q^2 + N_3\, q^3 + N_4\, q^4 + \ldots}$$

waarin q afhangt van de (complexe) variabele z als $q = exp(2\pi iz)$. De coefficienten N_p in deze functie kiezen we als volgt. Voor priemgetallen p nemen we $N_p = p\text{-}A_p$, dus p min het hierboven berekende aantal oplossingen. (Dus uit onze berekening hierboven volgt $N_3 = 3 - 4 = -1$.) Verder zijn de overige coefficienten N_k met k een niet-priemgetal uniek bepaald door ook nog aan te nemen dat $F(z)$ speciale transformatie-eigenschappen heeft die *modulaire invariantie* heten. Het artikel zou helaas veel te lang en technisch worden als we die speciale transformaties ook uit zouden leggen, maar het resultaat is verrassend en eenvoudig: de resulterende functie $F(z)$ is een dubbel periodieke functie! Dit verbazende resultaat is de essentie van het Taniyama theorema en geldt voor elke elliptische kromme.

Nu we hebben laten zien hoe elliptische krommen gerelateerd zijn aan dubbel periodieke functies, zul je je misschien afvragen hoe het omgekeerde verhaal gaat. Het blijkt ook mogelijk te zijn om uit een dubbel periodieke functie een elliptische kromme af te leiden; dit gebeurt met behulp van de zogeheten *Weierstrass elliptische functie*. Ook deze constructie zullen we hier niet in detail uitleggen, maar elders (bijvoorbeeld op Wikipedia) kun je vinden hoe die in zijn werk gaat.

In dit tweeluik hebben we besproken hoe elliptische krommen en dubbel periodieke functies aan elkaar gerelateerd zijn. Wiskundig gezien is deze stelling erg diep en bevat heel erg veel interessante feiten, waaronder Fermat's beroemde laatste stelling. Natuurkundig gezien zijn er niet direct toepassingen van de stelling van Taniyama zelf, maar elliptische krommen en dubbel periodieke functies vormen een significant deel van de snaartheorie. Daarover ongetwijfeld meer in een toekomstig artikel!