Gedeeld en toch geheim

Een man heeft twee zonen en een kluis met flink wat geld. Er zit hem wat dwars. Als hem iets overkomt, kan niemand de kluis meer openmaken. Hij zal de code dus met zijn zoons moeten delen. Maar het probleem is: hij vertrouwt ze niet. Hij wil hoe dan ook voorkomen dat de ene zoon zonder medeweten van de ander de kluis leeghaalt.

Deze man zoekt dus naar een manier om de code van de kluis aan zijn zoons te geven, maar op zo'n manier dat ze alleen samen de kluis open kunnen maken. Ze krijgen dus ieder een stukje van de code. Een zo'n stukje is waardeloos, maar als je samenwerkt, gaat de kluis open. Er bestaat een wiskundige truc om dit voor elkaar te krijgen.

Zo deel je een geheim

Laten we aannemen dat de code van de kluis 1234 is. De man verzint nu een willekeurige rechte lijn die de y-as in 1234 snijdt. Bijvoorbeeld de lijn $y = 377x + 1234$. Of de lijn $y = 630x + 1234$. Of $y = 411x + 1234$.

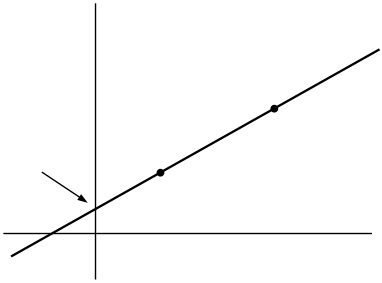
De man kiest voor de lijn $y = 377x + 1234$. Hij geeft nu elke zoon een punt op deze lijn, maar niet het punt bij $x = 0$. Zijn ene zoon krijgt bijvoorbeeld het punt (5, 3119), de andere zoon krijgt (15, 6889). Reken zelf maar uit dat deze twee punten inderdaad op de lijn liggen.

Als de eerste zoon het punt (5, 3119) krijgt, kan hij daar helemaal niets mee. Op geen enkele manier kan hij het snijpunt met *y*-as bepalen. Ook de andere zoon heeft niets aan zijn punt (15, 6889). Ook hij kan met geen mogelijkheid bepalen waar de lijn de *y*-as snijdt. Bedenk goed dat de vader met iedere zoon wel een punt op de lijn heeft gedeeld, maar de formule voor de lijn geheim gehouden heeft.

Maar wat gebeurt er als de zoons zouden samenwerken? Nu weten ze ineens twee punten op de lijn van vader: (5, 3119) en (15, 6889). En als je twee punten weet die op een rechte lijn liggen, dan weet je precies hoe die lijn loopt.

De twee zonen rekenen nu eenvoudig de richtingscoëfficiënt van de lijn uit. Deze is

$$\frac{\Delta y}{\Delta x} = \frac{6889 - 3119}{15 - 5} = 377$$



De vergelijking van de lijn van vader is dus $y = 377x + b$, waarbij b het snijpunt met de y-as is, tevens code van de kluis. De zoons vullen een van beide punten in en vinden: $3119 = 377 \cdot 5 + b$, dus $b = 1234$.

Meer dan twee

Hoe mooi is dat? Je hebt een geheim (de code van de kluis) gedeeld met twee mensen. Afzonderlijk weten ze niks. Alleen samen kunnen ze de kluis openen. Met een klein beetje wiskunde los je het probleem op. Maar kun je het geheim ook met meer dan twee mensen delen? Bijvoorbeeld met vijf mensen van wie er ten minste drie moeten samenwerken?

Je kunt hetzelfde trucje uithalen, maar dan een beetje ingewikkelder. Je weet dat twee punten genoeg zijn om een rechte lijn helemaal vast te leggen. Zoiets kan ook met drie punten. Met drie punten leg je altijd een parabool volledig vast, dus een functie van de vorm $y = ax^2 + bx + c$.

Het kunstje werkt op dezelfde manier. Vader bedenkt een willekeurige parabool (dat noemen we ook wel: een tweedegraads polynoom) en zorgt dat de code van de kluis eruit komt als je $x = 0$ invult. Bijvoorbeeld de functie $y = 24x^2 + 37x + 1234$. Nu geeft hij zijn vijf zonen elk een punt op deze parabool. Bijvoorbeeld: (2, 1404), (5, 2019), (7, 2669), (11, 4545) en (13, 5771).

Als nu willekeurig drie van deze vijf zonen gaan samenwerken, kunnen ze de code van de kluis achterhalen. Een zoon kan dat niet en twee ook niet. Stel dat de punten (5, 2019), (7, 2669) en (13, 5771) bij elkaar gelegd worden. Je zoekt een onbekende parabool van de vorm $y = a\,x^2 + b\,x + c$. De drie punten geven je de volgende informatie:

$2019 = a \cdot 5^2 + b \cdot 5 + c = 25\,a + 5\,b + c$
$2669 = 49\,a + 7\,b + c$
$5771 = 169\,a + 13\,b + c$

Het kost wat moeite, maar met deze drie vergelijkingen kun je de waarden van *a*, *b* en *c* vinden. En de waarde van *c* is precies de code van de kluis!

Een snelle oplossing

Er bestaat een manier om snel achter de formule voor de parabool te komen. Je hoeft dan niet het stelsel van drie vergelijkingen op te lossen. We nemen weer de punten (5, 2019), (7, 2669) en (13, 5771). Kijk nu eens naar de volgende functie:

$$f_5(x) = \frac{(x-7)(x-13)}{(5-7)(5-13)}$$

Als je goed kijkt, zie je dat deze functie nul oplevert als $x = 7$ of $x = 13$. In dat geval is immers of de linker of rechter factor nul. Maar er is nog een bijzonderheid. Bij $x = 5$ is deze functie precies één!

Zo kunnen we nog twee functies maken, namelijk:

$$f_7(x) = \frac{(x-5)(x-13)}{(7-5)(7-13)} \quad \text{en} \quad f_{13}(x) = \frac{(x-5)(x-7)}{(13-5)(13-7)}$$

De functie $f_5(x)$ is nul voor $x = 7$ of $x = 13$, maar juist één bij $x = 5$.
De functie $f_7(x)$ is nul voor $x = 5$ of $x = 13$, maar juist één bij $x = 7$.
De functie $f_{13}(x)$ is nul voor $x = 5$ of $x = 7$, maar juist één bij $x = 13$.

Nu is het heel eenvoudig om een functie te maken waarvoor geldt $f(5)=2019$, $f(7)=2669$ en $f(13)=5771$.

We kiezen dan: $f(x)=2019\cdot f_5(x)+2669\cdot f_7(x)+5771\cdot f_{13}(x)$

Herinner je je nog dat de functie bij $x=0$ precies de geheime code was? Die is gemakkelijk uit te rekenen. Reken maar even mee:

$$f_5(0)=\frac{(0-7)(0-13)}{(5-7)(5-13)}=\frac{91}{16} \qquad f_7(0)=-\frac{65}{12} \qquad f_{13}(x)=\frac{35}{48}$$

En dus vinden we voor $f(0)$:

$$f(0)=2019\cdot\frac{91}{16}-2669\cdot\frac{65}{12}+5771\cdot\frac{35}{48}=\ldots\ldots\ldots \qquad 1234$$

En dat is weer precies de code van de kluis. Merk op dat we uit de vijf verschillende punten ook drie andere hadden kunnen nemen. Elke set van drie punten op de parabool is voldoende om te bepalen waar deze de *y*-as snijdt.

Deze methode staat bekend onder de naam Shamir's Secret Sharing.

Martijn Leisink @ www.wiskunstelaar.nl