Priemgetallen

Beschrijving

De priemgetallen lijken zo onregelmatig dat ze willekeurig gekozen lijken te zijn, en toch zijn ze exact bepaald. Deze mengeling van bijna-willekeurigheid en exact patroon heeft wiskundigen eeuwenlang verleid, zowel professionals als amateurs, om berekeningen te maken, patronen te herkennen, vermoedens te hebben en vervolgens proberen om die te bewijzen. Meestal waren hun vermoedens vals.

Veel vermoedens over priemgetallen zijn even elegant als eenvoudig, en de verleiding om te geloven dat je een patroon hebt ontdekt, kan overweldigend zijn â?? totdat je het tegenvoorbeeld ontdektâ?¦

Op de middelbare school werkte ik het volgende vermoeden voor het genereren van priemgetallen uit:

$2^{(2n-1)}-1$ *voor elk natuurlijk getal n* > 1.

- n = 2 geeft 2^3-1 = 7 is een priemgetal
- n = 3 geeft 2^5-1 = 31 is een priemgetal
- n = 4 geeft 2^7-1 = 127 is een priemgetal
- n = 5 geeft 2^9-1 = 511 is ***geen*** priemgetal
- n = 6 geeft 2^{11}-1 = 2047 is ***geen*** priemgetal

Helaas: ook mijn vermoeden blijkt onjuist.

Riemann-hypothese

Het meest bekende probleem in de wiskunde van vandaag, met algemene instemming, is een vermoeden, de *Riemann-hypothese*, die stamt uit een briljant artikel dat gepubliceerd werd in 1859. Wie het uiteindelijk bewijst, zal beroemder worden dan *Andrew Wiles*, die over de voorpaginaâ??s spatte
toen hij in 1994 eindelijk *de laatste stelling van Fermat* bewees.

Dit speculeren heeft een speciale rol gegeven aan de moderne elektronische rekenmachine of computer. In de goede oude tijd betekende â??*computer*â?? eigenlijk een persoon die rekende, en het was een lange, vervelende en moeilijke taak voor de wiskundige die geen menselijke rekenmachine was zoals
Euler of *Gaus*.

Gauss


default watermark

Euler

Tegenwoordig kunnen computers sneller gegevens genereren dan we ze kunnen lezen, en kunnen berekeningen voltooien in enkele uren die een menselijke rekenmachine jaren gekost zou hebben â?? en de computer maakt geen onzorgvuldige fouten. (Hoewel: de programmeur kan zich natuurlijk vergissen!) Computers plaatsen je ook in contact met de concrete werkelijke getallen, op een manier zoals een abstract bewijs dat niet doet.

Computers hebben nog twee andere effecten gehad. De pc moedigde duizenden amateurs aan om tijd en energie te steken in het verkennen van de wereld der priemgetallen. Het resultaat is een massa materiaal variÃ«rend van grappig maar triviaal tot serieus en belangrijk.
Het tweede effect is dat de zeer complexe berekeningen die nodig zijn om te bewijzen dat een groot getal een priemgetal is, of om de factoren ervan te vinden, plotseling binnen bereik zijn gekomen. *Ã?douard Lucas* bewees in 1876 dat 2^{127} â?? 1 een priemgetal is. Het grootste bekende priemgetal op dit moment is $2^{82.589.933}$ â?? 1. Dit getal heeft 24.862.048 cijfers. (*Beide voldoen aan mijn formule* $\mathbf{2^{(2n-1)}-1}$!)

Hoeveel priemgetallen zijn er?

Als je de distributie van priemgetallen binnen de reeks van natuurlijke getallen bekijkt, lijken ze steeds spaarzamer te worden. Maar komt er ooit een eind aan? Nee, is het antwoord. Maar hoe weten we dat zo zeker?

Dit weten wetenschappers door een even vernuftig als eenvoudig bewijs, waar de Griekse wiskundige *Euclides*[1] al in 300 voor Christus mee op de proppen kwam. Zijn bewijs uit het ongerijmde is analoog aan het volgende: je wilt aantonen dat er oneindig veel gehele getallen zijn. Neem dan om te beginnen het tegenovergestelde aan: er zijn Ã©indig veel gehele getallen. Dat betekent dat er Ã©Ã©n bepaald getal is, N, dat het grootste gehele getal zou moeten zijn. Maar ja, N + 1 is per definitie nog groter. En dat levert een tegenspraak! Dus de aanname kan niet kloppen en moeten er dus oneindig veel gehele getallen zijn.

Euclides ging voor zijn bewijs uit van 2 feiten:

- onder een priemgetal verstaan we een geheel getal (een â??integerâ??) dat je ***niet*** kunt schrijven als het product van twee andere integers.
- elk getal dat ***gÃ©Ã©n*** priemgetal is, kun je op zijn beurt schrijven als een vermenigvuldiging van priemgetallen (dat bewees Euclides al eerder).

Encryptie met priemgetallen

De versleuteling (encryptie) met openbare sleutels en methoden heeft priemgetallen van vitaal belang gemaakt voor het bedrijfsleven (en het leger). Dus de zoektocht naar priemgetallen gaat ook op commerciÃ«le basis verder.

De priemgetallen worden toegepast in de zogenaamde asymmetrische cryptografie. Hierbij is er niet Ã©Ã©n sleutel, maar zijn er twee. Een publieke sleutel en een geheime sleutel. De publieke sleutel kan

door iedereen gebruikt worden om een bericht te coderen, maar alleen de ontvanger, die de publieke sleutel bekend heeft gemaakt, kan deze gecodeerde berichten ontcijferen. Het is als een hangslot. Iedereen kan het dichtklikken, maar alleen degene met de sleutel kan het weer openen.

Een uitleg met een voorbeeld met kleine priemgetallen maakt dit duidelijk (voor de echte codering worden priemgetallen van honderden cijfers gebruikt!)

Priemgetallen hebben een speciale eigenschap: elk natuurlijk getal (1,2,3,4 â?¦) kan op juist Ã©Ã©n manier worden ontbonden in priemfactoren (al bewezen door Euclides). Met andere woorden, elk natuurlijk getal kan gemaakt worden door bepaalde priemgetallen met elkaar te vermenigvuldigen en dit kan maar op ***Ã©Ã©n*** manier.
Zo bestaat 42 uit 2 Ã? 3 Ã? 7. Er is ***geen*** andere combinatie van priemgetallen denkbaar om 42 te vormen. En dit is precies het magische hangslot voor coderingen. Er is een wiskundige methode waarbij voor het coderen het natuurlijke getal (bijvoorbeeld 42) nodig is, maar voor het ontcijferen de unieke priemgetallen (hier dus 2, 3 en 7) nodig zijn. Dus 42 klikt het slot dicht en 2, 3 en 7 maken het open.

Het â??dichtklikkenâ?• is vrij makkelijk. Neem twee priemgetallen, bijvoorbeeld 19 en 29. De publieke sleutel is nu 551, want 19 Ã? 29 is 551. Iedereen kan nu met deze publieke sleutel een bericht coderen. Maar om dit bericht vervolgens te ontcijferen zijn 19 en 29 nodig. En die weet alleen de maker.
Probeer maar eens de priemgetallen te vinden die horen bij 3431 (de bijbehorende priemgetallen zijn kleiner dan 100).

Dit is een goede beveiliging, want twee grote priemgetallen zijn vrij makkelijk te vermenigvuldigen, maar om een groot getal te ontbinden in priemgetallen is heel moeilijk. Daarvoor voldoen op dit moment de beste computers niet eens. De boodschap is dus volstrekt veilig zolang de twee priemgetallen maar groot genoeg gekozen worden.

---

[1] *Euclides*, ook *Euclides van AlexandriÃ«* genoemd, was een wiskundige, die rond het jaar 300 v.Chr. werkzaam was in de bibliotheek van *AlexandriÃ«*.
Euclides wordt vaak de â??*vader van de meetkunde*â?• genoemd. Hij leefde tijdens het bewind van *Ptolemaeus de Eerste* (323-283 v.Chr.) in *AlexandriÃ«*.
Zijn *Elementen* is het meest succesvolle handboek en een van de invloedrijkste werken in de geschiedenis van de wiskunde. Het deed vanaf het tijdstip van publicatie tot in de late 19e of vroege 20e eeuw dienst als het belangrijkste leerboek voor het onderwijs in de wiskunde, vooral in de meetkunde. In dit werk worden de beginselen van wat nu de euclidische meetkunde wordt genoemd gededuceerd uit een kleine verzameling van axiomaâ??s. *Euclides* schreef ook werken over perspectief, kegelsneden, bolmeetkunde en getaltheorie.

Er is weinig bekend over het leven van *Euclides*, aangezien er in de overgebleven antieke werken slechts een handvol verwijzingen naar hem bestaan. In feite dateren de belangrijkste verwijzingen naar *Euclides*, van *Proclus* en *Pappos van AlexandriÃ«*, van eeuwen later. *Proclus* schreef in zijn commentaar op de *Elementen*, dat was in de 5e eeuw, maar kort iets over *Euclides*. Volgens hem was *Euclides* de schrijver van de *Elementen*, en werd hij genoemd door *Archimedes*.
Toen *Ptolemaeus I Euclides* vroeg of er geen kortere weg naar de meetkunde bestond dan de *Elementen*, antwoordde *Euclides* volgens *Proclus* dat â??*er geen koninklijke weg tot de meetkunde*

*bestaat*â??.
In de enige andere belangrijke verwijzing naar *Euclides* vermeldt *Pappos van AlexandriÃ«* in de vierde eeuw kort dat *Apollonius van Perga* â??*lange tijd doorbracht met de leerlingen van Euclides in AlexandriÃ«, en dat hij zich daar zijn natuurwetenschappelijke manier van denken eigen maakte*.â?• Het is volgens velen mogelijk dat *Euclides* in het oude *Athene* aan de *Akademeia* van *Plato* heeft gestudeerd.

Datum en plaats van de geboorte van *Euclides* en ook zijn sterfdatum en de omstandigheden van zijn dood zijn niet nauwkeurig bekend, evenmin als een beschrijving hoe hij eruit zag. Er bestaat al helemaal geen portret van hem. Portretten van later datum zijn verzonnen.

Datum aangemaakt
2023/03/07