Wat te bewijzen is (25)

Rubriek

Neem de vier priemgetallen kleiner dan 10. Die kunnen op drie manieren worden verdeeld in twee paren. Bij elke verdeling vermenigvuldig ik de getallen van elk paar en tel ik de beide uitkomsten op. Dat geeft:

$$2 \times 3 + 5 \times 7 = 41$$
$$2 \times 5 + 3 \times 7 = 31$$
$$2 \times 7 + 3 \times 5 = 29$$

Drie nieuwe priemgetallen dus. Ik had de vier priemgetallen ook kunnen verdelen in een groepje van drie en een groepje van één om daarna een soortgelijke berekening uit te voeren:

$$2 \times 3 \times 5 + 7 = 37$$
$$2 \times 3 \times 7 + 5 = 47$$
$$2 \times 5 \times 7 + 3 = 73$$
$$3 \times 5 \times 7 + 2 = 107$$

Andermaal nieuwe priemgetallen.
Zou dit procédé - verdeel een aantal priemgetallen in twee disjuncte groepen, vermenigvuldig de getallen in elke groep en tel de beide uitkomsten op - altijd nieuwe priemgetallen opleveren? Het antwoord is ja, mits 'opleveren' goed wordt geïnterpreteerd. Zo geldt:

$$2 \times 3 + 5 \times 7 \times 11 = 391 = 17 \times 23$$

De uitkomst hoeft niet per se priem te zijn, maar de priemfactoren ervan verschillen zeker van de priemgetallen waarmee begonnen is. Het bewijs dat dit algemeen geldt, is niet moeilijk. Stel:

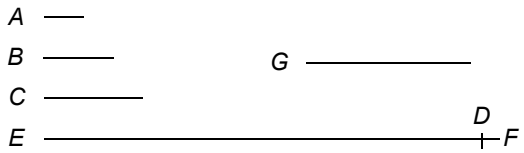
$$S = \underbrace{p_1 \times \ldots \times p_k}_{A} + \underbrace{p_{k+1} \times \ldots \times p_n}_{B}$$

waarbij $p_1, p_2, \ldots, p_n$ staan voor n verschillende priemgetallen. Dan is elk van die n priemgetallen of een deler van A en niet van B, of een deler van B en niet van A, en dus zeker geen priemfactor van $S = A + B$.
Bij elke eindige club priemgetallen kun je op deze wijze priemgetallen maken die (nog) geen lid van die club zijn. Deze redenering, afkomstig van de Nederlandse wiskundige Stieltjes, is een van de vele bewijzen dat er oneindig veel priemgetallen zijn. Het bewijs is zo eenvoudig dat het door jonge VWO/HAVO-leerlingen kan worden gesnapt.
In de loop der tijd zijn veel moeilijke en gemakkelijke bewijzen geleverd voor deze stelling. Blijkbaar daagt zij, net als bijvoorbeeld de stelling van Pythagoras, uit tot het vinden van alternatieve bewijsvoeringen.

Het bewijs van Euclides

Het begon allemaal bij Euclides. Propositie 20 van boek 9 van de *Elementen* zegt in de vertaling van Dijksterhuis: *De priemgetallen zijn meer dan elke voorgeschreven hoeveelheid priemgetallen.*

Euclides' bewijs luidt vrijwel letterlijk als volgt.
Laat A, B, C drie aangewezen priemgetallen zijn.
Ik zeg dat er meer priemgetallen zijn dan deze.
Want neem het kleinste getal dat door A, B en C gemeten wordt en noem het DE. Voeg de eenheid DF toe aan DE.



Dan is EF priem of niet priem.
Stel eerst dat EF priem is.
Dan hebben we de priemgetallen A, B, C, EF en dat is meer dan A, B, C.
Stel nu dat EF niet priem is; dus EF wordt gemeten door een of ander priemgetal G.
Ik zeg dat G niet gelijk is aan een van de drie A, B of C.
Want stel dat dit wel zo zou zijn. DE wordt gemeten door A, B, C en dan dus ook door G. Maar EF wordt ook gemeten door G. Dus het verschil, de eenheid DF, wordt gemeten door G en dat is absurd. Dus G is niet gelijk aan een van de priemgetallen A, B, C en er zijn meer priemgetallen dan deze. Q.E.D.

Afgezien van de taal ('deelbaar door' is in de Griekse wiskunde 'wordt gemeten door') valt op dat Euclides een paradigma hanteert: hij bewijst dat er meer dan 'drie' priemgetallen zijn, maar het is duidelijk dat die 'drie' kan worden vervangen door elk willekeurig natuurlijk getal.
Euclides is zuinig bij de constructie van het getal dat nieuwe priemgetallen oplevert: 'neem het kleinste getal dat deelbaar is door A, B en C ... '
Een minder zuinige variant is de volgende. Stel, er is een grootste priemgetal P en bekijk het getal $P! + 1$.
$P!$ is deelbaar door elk van de priemgetallen 2, 3, 5, ... , P en $P! + 1$ geeft bij deling door elk van die getallen rest 1.
De priemfactoren van $P! + 1$ zijn dus groter dan P.
Merk op dat de getallen: $P! + 2$, $P! + 3$, $P! + 4$, ..., $P! + P$ zeker niet priem zijn (want deelbaar door respectievelijk 2, 3, 4, ... , P). Zo ontstaat een rij van $P - 1$ opvolgende niet-priemen en de conclusie is dat de rij van priemgetallen willekeurig grote sprongen bevat! Is het niet merkwaardig dat als het ware in één adem de oneindigheid van de rij priemgetallen en het bestaan van willekeurig grote gapingen in diezelfde rij kan worden bewezen?

De zeef van Eratosthenes

Priemgetallen worden in het huidige Nederlandse wiskundeonderwijs nauwelijks nog serieus genomen, en dat is betreurenswaardig te noemen. Vroeger besprak ik de

oneindigheid van de rij priemgetallen al in de brugklas en dat was dan de eerste (en geslaagde) kennismaking met een echt bewijs. Daar liet ik de zeef van Eratosthenes aan voorafgaan. Het principe is eenvoudig. Deel een honderdveld (vierkant met honderd genummerde hokjes) uit; 2 is het eerste priemgetal, dat hokje blijft wit. Alle hokjes van volgende tweevouden kunnen nu geblindeerd worden. Herhaal dit voor 3, 5, 7, en dan worden in één klap alle priemgetallen onder de 100 zichtbaar. (Het eerste elfvoud dat in aanmerking komt om geschrapt te worden is 121, en dat is groter dan 100. Ed de Moor heeft wel eens voorgesteld om een andere tabel te nemen, namelijk een van zes hokjes breed. Hieronder is het resultaat van die werkwijze te zien voor een tabel van 6 bij 24.

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
61	62	63	64	65	66
67	68	69	70	71	72
73	74	75	76	77	78
79	80	81	82	83	84
85	86	87	88	89	90
91	92	93	94	95	96
97	98	99	100	101	102
103	104	105	106	107	108
109	110	111	112	113	114
115	116	117	118	119	120
121	122	123	124	125	126
127	128	129	130	131	132
133	134	135	136	137	138
139	140	141	142	143	144

Het leuke van deze tabel is dat, afgezien van 2 en 3, alle priemgetallen in slechts twee kolommen opduiken.
Ieder priemgetal dat groter is dan 3 is of een zesvoud + 1 of een zesvoud –1 (ofwel: is congruent 1 of –1 modulo 6). Omdat er oneindig veel priemgetallen zijn, moeten er in ten minste een van beide 'priemkolommen' oneindig veel hokjes wit blijven. Dat de 5-kolom oneindig veel priemgetallen bevat, is gemakkelijk te bewijzen. Dat gaat in Euclidische trant.

Bij elk eindige serie priemgetallen $p_1, p_2, ..., p_n$ uit de 5-kolom vinden we ten minste één nieuw priemgetal p dat niet in de serie voorkomt, maar wel in die kolom zit.
Beschouw namelijk het getal $q = 6p_1\, p_2 \ldots p_n - 1$.
Dit getal dat thuishoort in de 5-kolom, is zeker niet deelbaar door een van de getallen $p_1, p_2, ..., p_n$
De priemfactoren van q kunnen echter niet allemaal uit de 1-kolom komen. Immers, elk product van getallen uit de 1-kolom zit weer in die kolom. Dat volgt gemakkelijk met schoolalgebra:

$$(6m + 1) \cdot (6n + 1) = 6(6mn + m + n) + 1$$

of via modulorekenen: $1 \times 1 = 1 \pmod 6$
Dus q bezit ten minste één priemfactor die uit de 5-kolom stamt en niet gelijk is aan een van de getallen $p_1, p_2, ..., p_n$
De conclusie is dat er steeds weer nieuwe priemgetallen in de 5-kolom kunnen worden gevonden, en daarmee is aangetoond dat er oneindig veel priemgetallen van de vorm $6n - 1$ zijn.
Als je de 5-kolom en de 1-kolom vergelijkt, doen ze weinig voor elkaar onder wat betreft het aantal witte vakjes. Maar ja, dat is nog slechts een pril begin. Dat kan verderop wel heel anders worden. Zouden er in de 1-kolom ook oneindig veel priemgetallen voorkomen?
Het is waar, maar bovenstaande gedachtengang is helaas niet overdraagbaar. Er geldt namelijk:

$$(6m - 1) \cdot (6n - 1) = 6(6mn - m - n) + 1$$

Ofwel: het product van twee (of meer) getallen uit de 5-kolom zit juist in de 1- kolom.

Het bewijs dat de 1-kolom oneindig veel priemgetallen bevat, is een stuk lastiger, en doet een beroep op een wat specialistischer hoofdstuk uit de getaltheorie, namelijk de theorie van de kwadraatresten - in het bijzonder de zogenaamde reciprociteitsstelling van Gauss - en dat valt buiten het kader van deze rubriek (zie bijvoorbeeld het boek *Getaltheorie voor beginners* van Frits Beukers).
Het feit dat er oneindig veel priemgetallen van de vorm $6n + 1$ bestaan is misschien niet zo verbazingwekkend, maar wat te denken van bijvoorbeeld de rij: 1001, 2001, 3001, ... ? De lezer kan het geloven of niet, maar ook deze rij bevat oneindig veel priemelementen.

Dirichlet heeft, met vernuftig gebruik van analytische middelen, bewezen dat *iedere* rekenkundige rij natuurlijke getallen, waarvan de beginterm en het het verschil onderling ondeelbaar zijn, oneindig veel priemgetallen bevat. Kortom voor elk paar onderling ondeelbare getallen a en b bestaan er oneindig veel priemgetallen van de vorm $an + b$. Deze stelling van Dirichlet (met bewijs) is bijvoorbeeld te vinden in *Analytic Number Theory* van Tom Apostol. Slechts voor een paar bijzondere gevallen is een elementair bewijs te leveren, zoals bij $a = 6$, $b = 5$.
De wiskundewereld heeft zich eigenlijk altijd al bezighouden met het zoeken naar formules van rijen die oneindig veel priemgetallen bevatten. Befaamd in dit verband

is de rij $t_n = n^2 + 1$, waarvan, behalve t_1, alleen de termen met even rangnummer priemkandidaten zijn, dus 5, 17, 37, 65, 101, ... Men vermoedt dat deze rij oneindig veel priemgetallen bevat, maar het bewijs van deze hypothese is nog niet gevonden. Dat de rij oneindig veel niet-priemen bevat is eenvoudig aan te tonen: $(10k + 8)^2 + 1$ is deelbaar door 5.

Een andere historische kwadratische rij is die welke wordt gedefinieerd door $n^2 - n + 41$ ofwel $n(n - 1) + 41$. Dit van Euler afkomstige voorbeeld is daarom zo attractief, omdat de eerste 40 termen priem blijken te zijn.
Voor $n = 41k$ of $41k + 1$ is $n(n - 1) + 41$ duidelijk deelbaar door 41, dus ook deze rij bevat oneindig veel niet-priemen. Dat volgt nog op andere wijze uit een onverwachte eigenschap van de rijen van het type $t_n = n^2 - n + p$, te weten dat het product van twee opvolgende termen ook tot de rij behoort. Kijk maar:

$$t_n t_{n+1} = [n^2 - n + p][n^2 + n + p] = (n^2 + p)^2 - n^2 = (n^2 + p)^2 - (n^2 + p) + p = t_{n^2+p}$$

Voor alle rijen $t_n = an^2 + bn + c$ waarbij a, b en c natuurlijke getallen zijn, zodat $ac \neq 0$, $a + b$ en c niet beide even zijn en ten slotte $b^2 - 4ac$ geen kwadraat is, bestaat tot op heden hoogstens het vermoeden dat zij oneindig veel priemgetallen bevatten.

Fermatgetallen
Een andere rij waarvan ooit gedacht is dat zij oneindig veel priemgetallen bevat, is die van de zogenaamde Fermatgetallen, dat wil zeggen, getallen van de vorm $2^m + 1$ waarbij m een macht van 2 is. Van de eerste vier Fermatgetallen is eenvoudig vast te stellen dat ze priem zijn:

$$F_0 = 2^1 + 1 = 3$$
$$F_1 = 2^2 + 1 = 5$$
$$F_2 = 2^4 + 1 = 17$$
$$F_3 = 2^8 + 1 = 257$$

$F_4 = 2^{16} + 1 = 65537$ vraagt wat meer inspanning, maar wanneer je als een ijzeren Hein alle priemgetallen onder 257 probeert te delen op 65537 blijkt ook F_4 een priemgetal te zijn. Deze recht-toe-recht-aan methode is praktisch onuitvoerbaar bij het priemonderzoek van F_5.
In 1732 bewees Euler via slim rekenwerk dat $2^{32} + 1$ deelbaar is door 641.Vandaag de dag hoef je niet zo slim te zijn en vraag je de ontbinding gewoon aan de TI-89, en het antwoord komt snel: $641 \cdot 6700417$.
De ontbinding van $2^{64} + 1$ (kleinste van de twee priemfactoren is 274177) laat even op zich wachten, maar zij verschijnt na een minuutje op het scherm. Dan is zo ongeveer de grens van zijn kunnen bereikt, en zijn er krachtiger programma's nodig.
Een manier om met potlood en papier aan te tonen dat F_5 deelbaar is door 641 is de volgende:
Merk op dat $641 = 2^4 + 5^4$ en $640 = 2^7 \cdot 5$.
Uit deze beide identiteiten volgt: $641 \times 2^{28} = 2^{32} + 640^4$
Dit 641-voud kan ook worden geschreven als:
$(2^{32} + 1) + (640^4 - 1)$. Als de tweede vorm tussen haakjes deelbaar is door 641, geldt dit ook voor de eerste vorm.
Welnu: $640^4 - 1 = (640^2 + 1)(640 + 1)(640 - 1)$ en daarmee is aangetoond dat $2^{32} + 1$ een veelvoud is van 641.

Dat de eerste vijf getallen van de rij $F_0, F_1, F_2, \ldots$ priemgetallen zijn, zegt uiteraard niets over het vervolg. Toch kan die rij dienen om de oneindigheid van de verzameling priemgetallen aan te tonen. Daartoe dient een mooie eigenschap van de Fermatgetallen die zichtbaar wordt als je het begin van de rij bekijkt. Er geldt namelijk:

$$F_0 = 3 = F_1 - 2$$
$$F_0 \times F_1 = 15 = F_2 - 2$$
$$F_0 \times F_1 \times F_2 = 255 = F_3 - 2$$
$$F_0 \times F_1 \times F_2 \times F_3 = 65535 = F_4 - 2$$

Dat dit patroon zich voortzet, volgt uit:

$$F_{n+1} - 2 = 2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1) = F_n(F_n - 2)$$

Herhaalde toepassing van deze recursieregel geeft:

$$F_{n+1} - 2 = F_n(F_n - 2) = F_n F_{n-1}(F_{n-1} - 2) = \ldots$$

Ten slotte komt er als laatste factor $F_1 - 2$ en dat is juist gelijk aan F_0. Uit $F_{n+1} - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_n$ volgt dat een eventuele gemeenschappelijke deler van F_{n+1} en F_i $(0 \leq i \leq n)$ deelbaar moet zijn op 2.
Omdat alle Fermatgetallen oneven zijn, volgt nu dat elke twee Fermatgetallen onderling ondeelbaar zijn. Een Fermatgetal heeft priemfactoren die al zijn voorgangers vreemd zijn, en omdat er oneindig veel Fermatgetallen zijn, bestaan er dus ook oneindig veel priemgetallen.
Dit bewijs is bijvoorbeeld te vinden in de bundel '*Proofs from the BOOK*' (Aigner en Ziegler). Dat boek, een eerbetoon aan de Hongaarse getaltheoreticus Erdös, opent met zes bewijzen over de oneindigheid van de rij priemgetallen. Warm aanbevolen!

Prime time for ever
In de *NRC* van 8 mei jongstleden lees ik onder het kopje *Priemgetallen bestaan in oneindig veel regelmatige rijen* dat er een oud vermoeden bewezen is, namelijk dat de rij van priemgetallen willekeurig lange rekenkundige deelrijtjes bevat. Het simpelste voorbeeld van zo'n 'equidistant' rijtje is 3, 5, 7; maar andere rijtjes zijn snel te vinden in de tabel op de vorige bladzijde (neem bijvoorbeeld alleen al de witte kolommetjes van meer dan 3 cellen, dat levert rijtjes met tussenruimte 6). Het bewijs van Green en Tao (48 bladzijden) moet nog gecheckt worden en dat kan nog wel even duren. Maar het geeft weer eens aan dat de priemgetallen regelmatig in het nieuws komen.
Voor wie op de hoogte wil blijven van de actuele ontwikkelingen, is er de website *http://primes.utm.edu*.

Martin Kindt, martin@fi.uu.nl