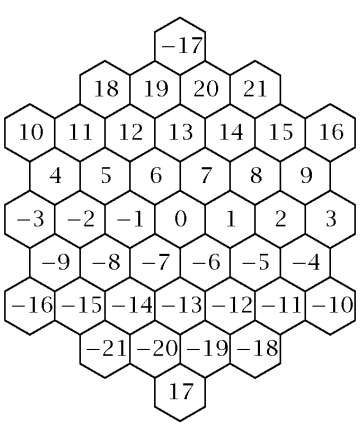
Hendrik Lenstra
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
hwl@math.leidenuniv.nl

Onderzoek

Ode aan het getal 43

Ieder mens is uniek, en ieder getal is dat ook. Naast de overvloedige belangstelling voor wereldberoemde getallen zoals π, is er over elk natuurlijk getal wel iets interessants te melden, als men maar goed zoekt. In deze bijdrage zet Hendrik Lenstra het getal 43 uitgebreid in het zonnetje.

In mijn Californische tijd gebeurde het een keer dat het gebied waar ik woonde en werkzaam was een ander netnummer kreeg: in plaats van 415 was het voortaan 510. Deze dramatische ingreep in het leven van miljoenen telefoongebruikers was voor een employé van de *Oakland Tribune* aanleiding ons *Department of Mathematics* te bellen met de vraag wat voor goeds er over het nieuwe nummer te melden viel. Direct greep ik mijn exemplaar van David Wells' *The Penguin dictionary of curious and interesting numbers* [14] van de plank, met het tevreden gevoel dat ik de aanschafprijs van dit speelse boekje terecht bij de beroepsonkosten had gerangschikt. Het stelde mijn verwachtingen echter teleur: het getal 510 stond er niet in, en we moesten zelf wat bedenken. We maakten de reporter gelukkig met de mededeling dat het voor $n = 510$ mogelijk is een regelmatige n-hoek met passer en liniaal te construeren, en dat getallen met deze mooie eigenschap dun gezaaid zijn; dat $n = 512$ en $n = 514$ er ook bij horen, hebben we maar voor ons gehouden.



Figuur 1. Met translaties van deze uit 43 zeshoekjes samengestelde rozet kan men het platte vlak betegelen. Schrijven we $\rho = e^{2\pi i/3}$, dan zijn de middelpunten van deze zeshoekjes de 43 elementen α van de ring $\mathbf{Z}[\rho] = \{a+b\rho : a, b \in \mathbf{Z}\}$ met de eigenschap $\alpha\bar{\alpha} < 13$. Deze 43 elementen representeren de restklassen van $\mathbf{Z}[\rho]$ modulo het ideaal $(6-\rho)$. De ring $\mathbf{Z}[\rho]/(6-\rho)$ kan men identificeren met de ring $\mathbf{Z}/43\mathbf{Z}$ van gehele getallen modulo 43; in het zeshoekje met middelpunt α staat de restklasse modulo 43 waar α mee correspondeert.

Het is Wells niet kwalijk te nemen dat niet ieder natuurlijk getal in zijn opus voorkomt. Naar men zegt probeert hij dit goed te maken door het kleinste dat ontbreekt steeds in de volgende druk op te nemen, zodat aan het eind der tijden alle natuurlijke getallen als *curious* of *interesting* te boek zullen staan. Het getal 43 valt de twijfelachtige eer te beurt het kleinste te zijn dat men in mijn eerste druk uit 1986 niet aantreft. Omdat ik het onder mijn persoonlijke vrienden tel, wil ik een poging tot rehabilitatie wagen. Figuur 1 vormt van deze poging een bescheiden begin.

Euclides' recept

Aan het welbekende bewijs van Euclides dat er oneindig veel priemgetallen bestaan (zie Figuur 2), ontleent men het volgende recept om getallen te genereren. Uitgaande van een eindige verzameling S van natuurlijke getallen, vormt men het product van alle getallen in S, telt hier 1 bij op, en voegt het aldus verkregen getal aan S toe. Met de nieuwe S begint men weer van voren af aan. Neemt men de lege verzameling als startpunt, dan krijgt men volgens dit recept achtereenvolgens de getallen

$$2,\ 3,\ 7,\ 43,\ 1807,\ 3263443,$$
$$10650056950807,\ \ldots .$$

We zullen het $n$de getal in deze rij met E_n aangeven, bijvoorbeeld

$$E_4 = (1+1)\cdot\Big((1+1)+1\Big)\cdot \Big((1+1)\cdot\Big((1+1)+1\Big)+1\Big)+1 = 43.$$

De lezer die op grond van Euclides' bewijs meent dat de getallen E_n allemaal priem zijn, en de eerste vier inderdaad als zodanig herkent, wordt uitgenodigd het product 13×139 uit te rekenen en te concluderen dat het getal 43 het eind van een illusie markeert. Het getal 3263443 is weer een priemgetal, maar misschien wel het laatste in de rij. De lezer die opmerkt dat E_n voor $n > 2$ alternerend 7 en 43 modulo 100 is, wordt voor meer gegevens naar Tabel 3 verwezen.

Men komt de getallen E_n tegen bij het bestuderen van Egyptische breuken. Een *Egyptische breuk* is een getal dat geschreven is als som van stambreuken, waarbij een *stambreuk* per definitie de inverse van een positief geheel getal is. Een voorbeeld van een Egyptische breuk is $1/4 + 1/5 + 1/120$. Een ander voorbeeld, met dezelfde waarde $11/24$, is $1/3+$

ΠΡΟΤΑΣΙΣ κ'.

Οἱ πρῶτοι ἀριθμοὶ πλείους εἰσὶ παντὸς τοῦ προτεθέντος πλήθους πρώτων ἀριθμῶν.

Εστωσαν οἱ προτεθέντες πρῶτοι ἀριθμοὶ, οἱ Α, Β, Γ· λέγω ὅτι τῶν Α, Β, Γ πλείους εἰσὶ πρῶτοι ἀριθμοί.

PROPOSITIO XX.

Primi numeri plures sunt omni proposità multitudine primorum numerorum.

Sint propositi primi numeri Α, Β, Γ; dico quam ipsi Α, Β, Γ plures esse primos numeros.

Α, 2. Β, 3. Γ, 5.
Ε 30. Δ Ζ

Figuur 2. Propositie 20 uit het negende boek van de *Elementen* van Euclides en het begin van zijn bewijs, volgens de editie van Peyrard [6]

$1/8$. In het proefschrift [13] van Kurt Vogel leest men hoe zulke breuken in de rekenkunde van de Egyptenaren figureerden. Het ging hun natuurlijk om *eindige* sommen van stambreuken, maar hier kijken we eerst naar *oneindige*.

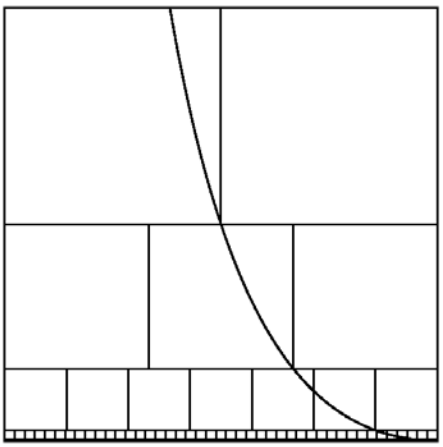
Stel dat men 1 wil schrijven als som van een oneindige rij stambreuken $1/m_n$. Dan kan men m_1, m_2, ... met de volgende 'gretige' methode bepalen: kies steeds, als m_1, ..., m_{n-1} al gekozen zijn zodanig dat $1/m_1 + \ldots + 1/m_{n-1} < 1$, de grootste stambreuk $1/m_n$ waarvoor geldt $1/m_1 + \ldots + 1/m_{n-1} + 1/m_n < 1$. Dit geeft achtereenvolgens $1/m_1 = 1/2$, $1/m_2 = 1/3$, $1/m_3 = 1/7$, en met inductie ziet men gemakkelijk in dat de getallen m_n identiek zijn met de getallen E_n. De rij $(E_n)_{n=1}^{\infty}$ is dus de 'lexicografisch kleinste' oplossing van de vergelijking $1 = \sum_{n=1}^{\infty} 1/x_n$ in positieve gehele getallen x_n (zie ook Figuur 4).

Ook bij *eindige* Egyptische breuken met waarde 1 hebben de getallen E_n een extreme eigenschap. Voor elke positieve gehele t heeft men $1 = \left(\sum_{n<t} 1/E_n\right) + 1/(E_t - 1)$, bijvoorbeeld $1 = 1/2+1/3+1/7+1/43+1/1806$. Het is een leerzame opgave om te bewijzen dat voor elke vaste t de vergelijking $1 = 1/m_1 + \ldots + 1/m_t$ maar eindig veel oplossingen in stambreuken $1/m_i$ heeft. Veel lastiger is het om aan te tonen dat de grootste m_i die bij deze oplossingen optreedt, gelijk is aan $E_t - 1$. Dus, als $1 = 1/m_1 + 1/m_2 + 1/m_3 + 1/m_4 + 1/m_5$, dan is elke m_i ten hoogste 1806. Dit werd bewezen door Curtiss [1].

De net genoemde resultaten hebben een leuke toepassing in de groepentheorie, die het eerst door Landau [3] is opgemerkt. Twee elementen g en h van een groep G noemt men *geconjugeerd* als er een x in G is met $g = x \cdot h \cdot x^{-1}$. Het gaat hier om een *equivalentierelatie* op G, waarvan de equivalentieklassen de *conjugatieklassen* van G heten. Stel nu dat de groep G *eindig* is. Dan zijn er ook maar eindig veel conjugatieklassen, zeg C_1, ..., C_t. Op een college groepentheorie leert men dat voor elke i het aantal elementen $\#C_i$ van C_i een *deler* van $\#G$ is, zeg $\#G = m_i \cdot \#C_i$. Omdat de C_i een partitie van G vormen, geldt $\#G = \#C_1 + \ldots + \#C_t$. Deelt men deze relatie door $\#G$, dan vindt men $1 = 1/m_1 + \ldots + 1/m_t$. Hiermee is 1 geschreven als som van evenveel stambreuken als er conjugatieklassen in G zijn. Omdat één van de C_i alleen uit het eenheidselement van G bestaat, komt $1/\#G$ onder deze stambreuken voor. De zojuist genoemde leerzame opgave impliceert dus dat er voor vaste t maar eindig veel mogelijkheden voor $\#G$ zijn, en vanwege het preciezere resultaat van Curtiss geldt zelfs $\#G \leq E_t - 1$. Voor $1 \leq t \leq 12$ is de grootste $\#G$ in feite gelijk aan

$$1,\ 2,\ 6,\ 12,\ 60,\ 168,\ 360,\ 720,$$
$$2520,\ 20160,\ 29120,\ 443520,$$

respectievelijk, zie [11]. Men krijgt de indruk dat de ongelijkheid $\#G \leq E_t - 1$ nog aanzienlijk verscherpt kan worden. Dat dit inderdaad het geval is, heeft Pyber met behulp van de classificatie van eindige simpele groepen bewezen [8]. Voor oneindige groepen liggen de zaken heel anders: met resultaten die men bij Serre [9, Ch. I, §1.3 en §1.4] aantreft, kan men voor elke gehele $t \geq 2$ een oneindige groep met precies t conjugatieklassen construeren. Hiermee hebben we het getal 43 echter wel uit het oog verloren.

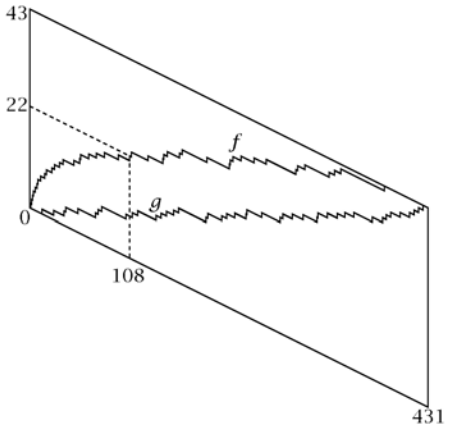


Figuur 4. Nestor Romeral Andres heeft een mooie manier bedacht om de identiteit $\sum_{n\geq 1} 1/E_n = 1$ meetkundig te verbeelden (zie [11]). De linkeronderhoek van het laatste vierkant op elke rij ligt op de grafiek $y = x + x^{-1} - 2$.

We keren terug tot de elementaire getaltheorie, en beschouwen een door Birkhoff gesuggereerde vraagstelling [2]. Laat n een positief geheel getal zijn. Als a, b, c, d gehele getallen zijn met $a \equiv b \bmod n$ en $c \equiv d \bmod n$, dan geldt ook $a + c \equiv b + d \bmod n$ en $a \cdot c \equiv b \cdot d \bmod n$. Als gevolg hiervan kan men op zinvolle wijze de som en het product van twee restklassen modulo n definiëren. Kan men ook *machtsverheffing* voor restklassen modulo n definiëren? Met andere woorden, als a,

n	basis 10	basis 2	basis 5
1	2	10	2
2	3	11	3
3	7	111	12
4	43	101011	133
5	1807	100001111	24212
6	3263443	111010011	313412233
7	056950807	000010111	034411212
8	361000443	111111011	404003233
9	485195807	000011111	202231212
10	645185443	110100011	131413233
11	213920807	000100111	230431212
12	453610443	111001011	111013233
13	545045807	100101111	012431212
14	183235443	101110011	402013233
15	388170807	000110111	332431212
16	018860443	110011011	312013233
17	291295807	000111111	032431212
18	884485443	101000011	412013233
19	994420807	001000111	032431212
20	400110443	101101011	412013233

Tabel 3. Bij het bestuderen van patronen in de eindcijfers van de getallen E_n in het tientallig stelsel, ligt het voor de hand ook naar de eindcijfers in basis 2 en basis 5 te kijken. Beide gevallen tonen een heel verschillend gedrag. De rijen $(E_{2n-1})_{n=1}^{\infty}$ en $(E_{2n})_{n=1}^{\infty}$ convergeren 5-adisch naar de beide 5-adische wortels uit -1, maar 2-adisch zijn de getallen $(E_n)_{n>1}$ gelijkverdeeld over de restklasse $3 \bmod 4$. Voor elke $n > 1$ heeft $E_n + 1$ precies twee factoren 2 meer dan $n - 1$.



Figuur 5. Deze illustratie laat zien hoezeer de ondergroep $\langle 2,3\rangle$ van $(\mathbf{Z}/431\mathbf{Z})^*$ uit het lood ligt. In perspectief ziet men de grafiek van $f(x) = \#\{n \in \mathbf{Z} : 0 < n \leq x,\ (n \bmod 431) \in \langle 2,3\rangle\}$ voor $0 < x < 431$. Omdat één op de tien elementen van $(\mathbf{Z}/431\mathbf{Z})^*$ tot $\langle 2,3\rangle$ behoort, zou men verwachten dat $f(x)$ dichtbij $x/10$ ligt, waarvan de grafiek door de diagonaal gegeven wordt. De grafiek van $f(x) - x/10$, die men niet-perspectivisch ziet, toont evenwel anders. Het middelste element van $\langle 2,3\rangle$ komt men al op een kwart van het interval tegen. Men krijgt $g(x)$ door $\langle 2,3\rangle$ te vervangen door zijn nevenklasse $26 \cdot \langle 2,3\rangle$, die veel gelijkmatiger verdeeld is.

b, c, d gehele getallen zijn met $a \equiv b \bmod n$ en $c \equiv d \bmod n$, en c en d positief, heeft men dan ook $a^c \equiv b^d \bmod n$? Voorbeelden tonen aan dat men deze conclusie niet in alle gevallen kan trekken, maar er zijn waarden voor n waarvoor dit toch kan, onafhankelijk van de keuze van a, b, c en d. Zulke getallen n zullen we, de betekenis van het woord δύναμις indachtig, *dynamisch* noemen. We gaan, in het voetspoor van Dyer-Bennet (zie [2; 10, Ch. VI, §6] maar ook [5]), alle dynamische getallen bepalen.

Neem aan dat n dynamisch is, en laat p een priemdeler van n zijn. Kiezen we $a = b = p$, $c = n+1$, $d = 1$, dan blijkt uit $a^c \equiv b^d \bmod n$ dat n een deler van $p^{n+1} - p$ is, en daarom maar een enkele factor p bezit. Bijgevolg is n *kwadraatvrij*, dus $n = \prod_{p \in V} p$ voor een of andere eindige verzameling V van priemgetallen. We bewijzen nu de opmerkelijke formule

$$p - 1 = \prod_{q \in V, q < p} q \qquad \text{voor elke } p \in V.$$

Hiertoe nemen we voor a een primitieve wortel modulo p, en $b = a$, $c = n+1$, $d = 1$. Uit $a^c \equiv b^d \bmod n$ volgt dan $a^n \equiv 1 \bmod p$, dus $p-1$ deelt $n = \prod_{q \in V} q$ en daarom $p - 1 = \prod_{q \in V_p} q$ voor een zekere deelverzameling V_p van V. Omdat alle priemdelers van $p-1$ kleiner dan p zijn, geldt $q \in V_p \Rightarrow q < p$. Om de verlangde omkering hiervan te bewijzen, voor $p, q \in V$, passen we een dubbele inductie toe, die ons in staat stelt aan te nemen dat voor *kleinere* p de omkering waar is, en ook bij dezelfde p voor kleinere q. Dan bevat V_p om te beginnen alle priemgetallen in V die kleiner dan q zijn, en deze hebben product $q-1$. Zou q niet in V_p zitten, dan zouden de andere $r \in V_p$ allemaal *groter* dan q zijn, en wegens $q \in V_r$ zou men dan $r \equiv 1 \bmod q$ krijgen, zodat $p - 1 = (q-1) \cdot \prod_{r \in V_p \setminus V_q} r \equiv -1 \bmod q$ en $p \equiv 0 \bmod q$, een kennelijke tegenspraak.

Als we met $p_1, \ldots, p_t$ de priemfactoren van het dynamische getal n aangeven, stijgend gerangschikt, dan kunnen we de net bewezen opmerkelijke formule ook als volgt uitdrukken:

$$p_i = 1 + \prod_{j<i} p_j \qquad \text{voor alle } i \leq t.$$

Met andere woorden: de p_i worden door het recept van Euclides gegeven! Dan moet $p_i = E_i$ voor alle $i \leq t$. Omdat E_5 niet een priemgetal is, geldt dit niet voor $i = 5$, dus we hebben $t < 5$. Voor n blijven er dan maar vijf mogelijkheden over, namelijk de getallen $E_{t+1} - 1$ voor $0 \leq t < 5$:

$$n \in \{1, 2, 6, 42, 1806\}.$$

De lezer mag zelf, met de kleine stelling van Fermat in de hand, nagaan dat deze vijf getallen inderdaad dynamisch zijn. De conclusie is dat er precies vijf dynamische getallen bestaan. We hadden er zeven gehad als 1807, welbeschouwd een groter ongeluksgetal dan zijn factor 13 (zie [7]), niet samengesteld was geweest. Het heeft in ieder geval niet gelegen aan onze held 43, die hiermee de grootste priemfactor van het grootste dynamische getal is geworden.

n	$\#\{p < 10^9 : i(p) = n\}$	$50847533 \cdot r_n$	$\#\{p < 10^9 : j(p) = n\}$	$50847532 \cdot s_n$
1	19014787	19014730,57	35467375	35466222,65
2	14261183	14261047,93	10430967	10431241,95
3	3381013	3380396,55	2008321	2008979,93
4	2377108	2376841,32	1043450	1043124,20
5	961678	960744,28	355482	355378,72
6	2534422	2535297,41	502717	502244,98
7	454193	454309,14	120982	120692,23
8	1782836	1782630,99	304163	304244,56
9	375048	375599,62	74271	74406,66
10	719997	720558,21	104372	104523,15
11	172816	173005,36	29219	29313,13
12	422427	422549,57	125176	125561,25
≥ 13	4390025	4389822,05	281037	281598,60

Tabel 6. Er zijn 50847534 priemgetallen p met $p < 10^9$. Voor elke $n > 1$ is bij deze priemgetallen de kans op $i(p) = n$ duidelijk groter dan de kans op $j(p) = n$. Beide kansen zijn goed in overeenstemming met het in het kader rechts geformuleerde vermoeden.

Curieuze congruenties

De restklasse $(-2 \bmod 3^3)$ behoort tot de verzameling van 9 restklassen $(a \bmod 3^3)$ waarvoor de congruentie $a \equiv 1 \bmod 3$ geldt. Deze verzameling vormt een groep onder vermenigvuldiging, dus de stelling van Lagrange uit de groepentheorie vertelt ons $(-2)^9 \equiv 1 \bmod 3^3$. Op dezelfde manier toont men aan $(-3)^4 \equiv 1 \bmod 2^4$. Deze beide feiten impliceren dat het getal $2^9 - 3^4 + 1$ deelbaar is door zowel 2^4 als 3^3, dus eveneens door hun product $2^4 \cdot 3^3$. Omdat $2^9 - 3^4 + 1$ positief is, en wegens $2^9 < 2^5 \cdot 3^3$ ook kleiner dan *twee*maal $2^4 \cdot 3^3$, is het *gelijk* aan $2^4 \cdot 3^3$. Zo hebben we de treffende identiteit

$$2^9 - 3^4 = 2^4 \cdot 3^3 - 1$$

geconstrueerd, die het startpunt van onze bespiegelingen vormt. Beide zijden zijn in feite gelijk aan 431. Kennelijk geldt $2^9 \equiv 3^4 \bmod 431$ en $2^4 \cdot 3^3 \equiv 1 \bmod 431$, en deze congruenties schrijven we eenvoudshalve als gelijkheden

$$2^9 \cdot 3^{-4} = 1,$$
$$2^4 \cdot 3^3 = 1,$$

te interpreteren in de ring $\mathbf{Z}/431\mathbf{Z}$, of beter gezegd in de groep $(\mathbf{Z}/431\mathbf{Z})^*$ van inverteerbare elementen van deze ring. Het getal 43 doet nu zijn intrede als de determinant van de exponentenmatrix $\left(\begin{smallmatrix} 9 & -4 \\ 4 & 3 \end{smallmatrix}\right)$. Vermenigvuldigt men de derde macht van de eerste gelijkheid met de vierde macht van de tweede, dan vindt men $2^{43} = 1$, en op vergelijkbare wijze krijgt men $3^{43} = 1$, $2 = 3^{10}$, $3 = 2^{13}$, allemaal in $(\mathbf{Z}/431\mathbf{Z})^*$. In die groep brengen 2 en 3 dus dezelfde ondergroep voort, en die ondergroep, waar Figuur 5 aan gewijd is, heeft orde 43.

Uit $2^{43} \equiv 1 \bmod 431$ kan men snel opmaken dat 431 een priemgetal is. Modulo elke deler d van 431 met $d > 1$ heeft de ondergroep $\langle 2 \bmod d\rangle$ van $(\mathbf{Z}/d\mathbf{Z})^*$ voortgebracht door $(2 \bmod d)$ namelijk orde 43, zodat geldt $d > 43$; elke deler groter dan 1 van 431 is dus groter dan 43, en wegens $43^2 > 431$ is 431 nu een priemgetal.

De connaisseurs onder mijn lezers weten

misschien wel wat er aan de congruenties

$$2^{43} \equiv 3^{43} \equiv 1 \bmod 431$$

zo curieus is. Voor een priemgetal p en een getal k dat klein is ten opzichte van p is het niet te verwachten dat 2^k en 3^k allebei congruent met 1 modulo p zijn, en de ontdekking dat dit voor $p = 431$, $k = 43$ toch gebeurt, is bepaald niet alledaags. Ook het geval $p = 3^8 - 2^3 = (2^{15} - 3)/5 = 6553$, $k = \det\left(\begin{smallmatrix} 15 & -1 \\ -3 & 8 \end{smallmatrix}\right) = 117$ is een overdenking waard.

Ter toelichting kijk ik eerst naar machten van 2 modulo priemgetallen. Toen Fermat dit in 1640 ook deed, in de context van volmaakte getallen, ging hem een groot licht op; "mi par di veder un gran lume", schreef hij aan Mersenne (zie [12, brief XL]). Fermat had ontdekt dat de kleinste positieve k met $2^k \equiv 1 \bmod p$, waarvoor we $d(p)$ zullen schrijven, een deler is van $p-1$. Als men een aantal van deze $d(p)$ uitrekent, bijvoorbeeld

$$d(5) = 4,\ d(7) = 3,\ d(23) = 11,\ d(431) = 43,$$

dan observeert men dat $d(p)$ doorgaans een in multiplicatief opzicht tamelijk *grote* deler van $p-1$ is, in de zin dat het getal $i(p)$ gedefinieerd door $d(p) \cdot i(p) = p - 1$ meestal aan de kleine kant is:

$$i(5) = 1,\ i(7) = 2,\ i(23) = 2,\ i(431) = 10;$$

zie ook Tabel 6. Men kan $d(p)$ en $i(p)$ interpreteren als de *orde* en de *index* van de ondergroep $\langle 2 \bmod p \rangle$ van $(\mathbf{Z}/p\mathbf{Z})^*$.

Er zijn niet al te veel heuse stellingen die de timmermanswijsheid onderbouwen dat $d(p)$ groot is en $i(p)$ klein. Uit $2^{d(p)} \equiv 1 \bmod p$ volgt $2^{d(p)} \geq p + 1$, dus

$$d(p) \geq \frac{\log(p+1)}{\log 2}.$$

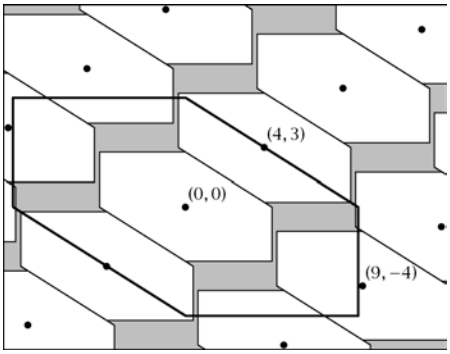
Deze logaritmische ondergrens is voor de meeste p zeer ver van de waarheid, hetgeen niet wegneemt dat het gelijkheidsteken geldt voor vermoedelijk oneindig veel priemgetallen p; het gaat hier om de notoire *Mersenne-priemgetallen*, die 1 minder zijn dan een macht van 2. Men heeft bijvoorbeeld $d(31) = 5$, $i(31) = 6$ en $d(8191) = 13$, $i(8191) = 630$. Ook zonder naar Mersenne-priemgetallen te kijken, kan men oneven priemgetallen p met $d(p) < i(p)$ bij de vleet vinden, maar dat er oneindig veel dergelijke priemgetallen zijn, is nog onbewezen. Ik vermoed dat ook $d(p) = i(p)$ oneindig vaak voorkomt; alle priemgetallen met die eigenschap zijn van de vorm $p = (16m)^2 + 1$, met m een positief geheel getal, maar $m = 1$ geeft het enige bekende voorbeeld.

Laten we de *kans* dat $i(p)$ gelijk is aan een gegeven positief geheel getal n definiëren als de limiet, voor $x \to \infty$, van het aantal oneven priemgetallen $p \leq x$ met $i(p) = n$, gedeeld door het totale aantal oneven priemgetallen p met $p \leq x$. Onder aanname van een bepaalde generalisatie van de Riemann-hypothese kan men bewijzen dat de limiet bestaat en gegeven wordt door een gecompliceerde formule; aan de hiertoe benodigde "analytische algebraïsche getaltheorie" heb ik ooit een deel van mijn proefschrift gewijd (zie [4]). De formule, die men in het onderstaande kader aantreft, neemt voor elke n een positieve waarde r_n aan, en er geldt $\sum_{n=1}^{\infty} r_n = 1$. Met andere woorden, men beschikt over een zeer plausibel vermoeden dat inderdaad uitdrukt dat $i(p)$ doorgaans klein is. Aan de andere kant kan men, zonder enige onbewezen aanname, een formule geven voor de kans dat $i(p)$ *deelbaar* is door een gegeven getal n. Deze op analoge wijze gedefinieerde kans is namelijk gelijk aan $2/\big(\varphi(n) \cdot n\big)$ of $1/\big(\varphi(n) \cdot n\big)$ al naar gelang n deelbaar door 8 is of niet, waar $\varphi(n)$ de orde van de groep $(\mathbf{Z}/n\mathbf{Z})^*$ aangeeft.

In het bijzonder kan $i(p)$ willekeurig groot zijn, en men kan zelfs afleiden dat er een positieve constante b is met de eigenschap dat voor elke n geldt

$$\liminf_{x\to\infty} \frac{\#\{p \in \mathcal{P}_x : i(p) \geq n\}}{\#\mathcal{P}_x} \geq \sum_{m=n}^{\infty} r_m \geq \frac{b}{n},$$

waar $\mathcal{P}_x = \{p : p \text{ priem}, 2 < p \leq x\}$. Uit de divergentie van $\sum_{n\geq 1} b/n$ volgt nu dat



Figuur 7. Dit is een plaatje van het rooster $L = \{(n,m) \in \mathbf{Z} \times \mathbf{Z} : 2^n \cdot 3^m = 1 \text{ in } (\mathbf{Z}/p\mathbf{Z})^*\}$, voor $p = 431$. De determinant $d(L)$ van L, die men kan definiëren als de index van L in $\mathbf{Z} \times \mathbf{Z}$, is gelijk aan de orde van de ondergroep $\langle 2, 3\rangle$ van $(\mathbf{Z}/p\mathbf{Z})^*$. De grote zeshoek begrenst de symmetrische convexe open verzameling $V = \{(x,y) \in \mathbf{R} \times \mathbf{R} : \max\{2^x, 2^{-x}, 3^y, 3^{-y}, 2^x 3^y, 2^{-x} 3^{-y}\} < p + 1\}$, waarvan de oppervlakte opp V gelijk is aan $\frac{3\cdot(\log(p+1))^2}{(\log 2)\cdot\log 3}$. Men ziet gemakkelijk in dat $L \cap V$ alleen het punt $(0,0)$ bevat. Volgens Minkowski's roosterpuntenstelling, waarvan het bewijs erop berust dat de translaties $r + \frac{1}{2}V$ van $\frac{1}{2}V$ over de punten $r \in L$ paarsgewijs disjunct zijn, geldt dan $d(L) \geq (\text{opp } V)/4$. De orde van de ondergroep $\langle 2, 3\rangle$ van $(\mathbf{Z}/p\mathbf{Z})^*$ is dus tenminste $\frac{3\cdot(\log(p+1))^2}{4\cdot(\log 2)\cdot\log 3}$.

de verwachting van $i(p)$ *oneindig* is. Zo extreem klein is $i(p)$ dus helemaal niet!

De situatie verandert als we 3 in het spel brengen, en de ondergroep $\langle 2 \bmod p\rangle$ van $(\mathbf{Z}/p\mathbf{Z})^*$ vervangen door $\langle 2 \bmod p, 3 \bmod p\rangle$, voor priemgetallen p die groter dan 3 zijn. De orde van die laatste groep, die tevens de kleinste positieve k met $2^k \equiv 3^k \equiv 1 \bmod p$ is, geven we aan met $e(p)$, bijvoorbeeld $e(431) = 43$; het is een deler van $p-1$ die deelbaar is door $d(p)$. De index

Vermoedelijke kansen

Laat $i(p) = \#(\mathbf{Z}/p\mathbf{Z})^*/\langle 2 \bmod p\rangle$ en $j(p) = \#(\mathbf{Z}/p\mathbf{Z})^*/\langle 2 \bmod p, 3 \bmod p\rangle$, voor priemgetallen $p > 2$ en $p > 3$, respectievelijk. Voor vaste n voldoet een willekeurig gekozen p vermoedelijk met kans r_n aan $i(p) = n$ en met kans s_n aan $j(p) = n$. Met het getoonde formularium kan men r_n en s_n uitrekenen. Het getal r_1 staat bekend als de *Artin-constante*. In eerste benadering zijn r_n en s_n proportioneel met respectievelijk $1/n^2$ en $1/n^3$, voor $n \to \infty$, en er geldt $\sum_{n=1}^{\infty} r_n = \sum_{n=1}^{\infty} s_n = 1$. De correctiefactoren b_d en c_d vinden hun oorsprong in de identiteiten $(\zeta_8 + \zeta_8^{-1})^2 = 2$ en $(\zeta_{12} + \zeta_{12}^{-1})^2 = 3$, waarbij ζ_m een primitieve $m$de machts eenheidswortel aangeeft.

$$r_1 = \prod_{p \text{ priem}} \frac{p^2 - p - 1}{p^2 - p} \doteq 0{,}373955813619$$

$$r_n = \frac{r_1}{n^2} \cdot b_{\gcd(n,8)} \cdot \prod_{p \text{ priem}, p \mid n} \frac{p^2 - 1}{p^2 - p - 1}$$

$$b_1 = 1, \quad b_2 = 1, \quad b_4 = \tfrac{2}{3}, \quad b_8 = 2$$

$$s_1 = \prod_{p \text{ priem}} \frac{p^3 - p^2 - 1}{p^3 - p^2} \doteq 0{,}697501358496$$

$$s_n = \frac{s_1}{n^3} \cdot c_{\gcd(n,24)} \cdot \prod_{p \text{ priem}, p \mid n} \frac{p^3 - 1}{p^3 - p^2 - 1}$$

$$c_1 = 1, \quad c_2 = \tfrac{120}{119}, \quad c_4 = \tfrac{96}{119}, \quad c_8 = \tfrac{32}{17},$$
$$c_3 = 1, \quad c_6 = \tfrac{6}{7}, \quad c_{12} = \tfrac{12}{7}, \quad c_{24} = 4$$

p	$j(p)$	$e(p)$	$h(p)$
5	1	4	0
23	2	11	0,289065
431	10	43	0,612194
6553	56	117	0,845276
11321831	2834	3995	0,958596

Tabel 8. Schrijf $h(p) = \big(\log j(p)\big)/\log e(p)$, met $e(p) = \#\langle 2 \bmod p, 3 \bmod p\rangle$ en $j(p) = (p-1)/e(p)$, voor priemgetallen $p > 3$. De tabel toont alle $p < 6 \cdot 10^{11}$ waarvoor $h(p)$ groter is dan alle $h(p')$ met $p' < p$. Een gedurfd vermoeden zegt dat h een maximum aanneemt dat groter dan 1 is, met $\limsup_p h(p) = 1$.

$j(p) = (p-1)/e(p)$ van de ondergroep deelt $i(p)$. In nog sterkere mate dan voor $i(p)$ en $d(p)$ het geval is, lijkt $j(p)$ doorgaans veel kleiner te zijn dan $e(p)$. Tabel 6 spreekt in dezen boekdelen. Tastbare stellingen zijn evenwel opnieuw schaars.

Als analogon van de ondergrens $d(p) \geq \big(\log(p+1)\big)/\log 2$ heeft men nu de grotere maar nog steeds zwakke ondergrens $e(p) \geq 3 \cdot \big(\log(p+1)\big)^2/(4 \cdot (\log 2) \cdot \log 3)$ (zie Figuur 7). Het analogon van de Mersennepriemgetallen lijkt te ontbreken, in de zin dat een oneindige verzameling priemgetallen p waarop $e(p)/\big(\log(p+1)\big)^2$ begrensd is, niet voor het oprapen ligt. Wellicht bestaat zo'n verzameling helemaal niet. Voor $p = 431$ is de gegeven ondergrens voor $e(p)$ ongeveer $36{,}269654$, wat goed in de buurt van de juiste waarde $e(431) = 43$ ligt, en voor $p = 6553$ is de ondergrens ongeveer $76{,}057079$, terwijl $e(6553) = 117$.

De beschikbare empirische informatie lijkt te bevestigen dat j gemiddeld duidelijk kleinere waarden aanneemt dan i. Net als in het geval van $i(p)$, heeft men een plausibele formule voor de kans dat $j(p)$ gelijk is aan een gegeven positief geheel getal n (zie kader), en een bewezen formule voor de kans dat $j(p)$ deelbaar is door n. Die laatste kans bestaat en is gelijk aan $a_n/\big(\varphi(n) \cdot n^2\big)$, waar a_n het aantal delers van n onder de getallen $1, 8, 12, 24$ is. Dit is maar liefst $n/2$ dan wel n keer zo klein als de corresponderende kans voor $i(p)$, al naar gelang n deelbaar door 12 is of niet. Evenals i is j onbegrensd, maar het argument waarmee men kan bewijzen dat i een oneindige verwachting heeft, blijkt voor j iets heel anders te geven. Men vindt namelijk dat er een positieve c is zodat, met $\mathcal{Q}_x = \{p : p \text{ priem}, 3 < p \leq x\}$ en s_m als in het kader, voor alle n geldt

$$\liminf_{x\to\infty} \frac{\#\{p \in \mathcal{Q}_x : j(p) \geq n\}}{\#\mathcal{Q}_x} \geq \sum_{m=n}^{\infty} s_m \geq \frac{c}{n^2},$$

en ook

$$\liminf_{x\to\infty} \frac{1}{\#\mathcal{Q}_x} \cdot \sum_{p\in\mathcal{Q}_x} j(p) \geq \sum_{n=1}^{\infty} n \cdot s_n = \frac{5 \cdot 59 \cdot \pi^2}{2^6 \cdot 3^3} \doteq 1{,}684915.$$

Bovendien impliceert de gegeneraliseerde Riemann-hypothese dat de eerste en de laatste van deze drie ongelijkheden gelijkheden zijn, met een $\liminf$ die een limiet is. Als dat klopt, dan heeft $j(p)$ een eindige en zelfs tamelijk kleine verwachting, maar een oneindige spreiding.

We zagen net dat de kans op $j(p) \geq n$ tenminste c/n^2 is. Dit geldt voor vaste n, maar er is ongetwijfeld een vergelijkbaar resultaat waarin n een voldoend langzaam groeiende functie van p is. De avontuurlijke keuze $n = \lceil\sqrt{p}\rceil$ zou dan tot de voorspelling leiden dat er oneindig veel priemgetallen p zijn met $e(p) < j(p)$ (zie Tabel 8). Zelfs met een enkel dergelijk priemgetal heb ik nog nooit kennisgemaakt, maar de gedachte dat het misschien ooit zal gebeuren, is al bijna even opwindend als het curieuze stel congruenties $2^{43} \equiv 3^{43} \equiv 1 \bmod 431$ waar het verhaal mee startte.

Epiloog

Bij het raadplegen van een latere druk van Wells' boekje kwam ik tot mijn verrassing een oude bekende tegen, die me deed beseffen dat het getal 43 al lang voor ik naar het Wilde Westen vertrok, mijn pad gekruist had. In de jaren '70 definieerde F. Göbel de rij $(x_n)_{n\geq 0}$ door $x_0 = 1$ en $x_n = \big(1 + \sum_{i=0}^{n-1} x_i^2\big)/n$ voor $n > 0$, en hij vroeg zich na berekening van een aantal beginwaarden zoals

$$x_1 = 2, \quad x_2 = 3, \quad x_3 = 5, \quad x_4 = 10, \quad x_5 = 28, \quad x_6 = 154$$

tevergeefs af of alle getallen x_n geheel zijn. Het antwoord luidt "nee"; in feite is x_n geheel dan en slechts dan als $n < 43$. Wat dit interessant maakt, is dat x_{42} en x_{43} veel te groot zijn om zelfs met moderne hulpmiddelen expliciet uit te rekenen, zodat een indirecte aanpak vereist is. De lezer die met de hand wil verifiëren dat x_{43} niet geheel is, kan daarvoor goed de in Figuur 9 getoonde rekenmachine gebruiken.

10	-20	-3	6	-12	-19	-5
16	11	21	1	-2	4	-8
17	9	-18	-7	14	15	13

Figuur 9. Met behulp van deze tabel kan men gemakkelijk twee elementen van het lichaam $\mathbf{Z}/43\mathbf{Z} = \{0, \pm 1, \pm 2, \ldots, \pm 21\}$ via vectoroptelling vermenigvuldigen. In het midden van de tabel bevindt zich de oorsprong 1. Ten opzichte van de oorsprong heeft -12 coördinaten $(1,1)$, en 13 heeft coördinaten $(3,-1)$. Met de x-coördinaat rekent men modulo 7, en met de y-coördinaat modulo 3, dus $(1,1) + (3,-1) = (-3,0)$. Op positie $(-3,0)$ staat 16, en dit betekent $-12 \times 13 = 16$ in $\mathbf{Z}/43\mathbf{Z}$. De benodigde vermenigvuldiging van de tekens doet men uit het hoofd, evenals vermenigvuldigingen met 0. Op analoge manier kan men delingen uitvoeren; uit $(1,1) - (3,-1) = (-2,-1)$ ziet men bijvoorbeeld $12/13 = -9$. De lezer mag zelf ontdekken hoe de tabel voor het trekken van vierkantswortels te gebruiken is.

Nawoord

Met dank aan Peter Kluit, Dirard Mikdad, Willem Jan Palenstijn, Jan Rozendaal en Cameron Stewart.

Referenties

1 D. R. Curtiss, 'On Kellogg's Diophantine problem', *Amer. Math. Monthly* **29** (1922), pp. 380–387.

2 J. Dyer-Bennet, 'A theorem on partitions of the set of positive integers', *Amer. Math. Monthly* **47** (1940), pp. 152–154.

3 E. Landau, 'Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante', *Math. Ann.* **56** (1903), pp. 671–676.

4 H. W. Lenstra jr., 'On Artin's conjecture and Euclid's algorithm in global fields', *Invent. Math.* **42** (1977), pp. 201–224.

5 H. W. Lenstra jr., 'Solution of problem 649', *Nieuw Arch. Wisk.* (4) **1** (1983), pp. 97–99.

6 F. Peyrard, *Les œuvres d'Euclide*, 3 vols, Patris, Paris, 1814/1816/1818.

7 A. Ponsen, E. van der Vlist (red.), *Het fataal evenement. De buskruitramp van 1807 in Leiden*, Uitgeverij Ginkgo, Leiden, 2007.

8 L. Pyber, 'Finite groups have many conjugacy classes', *J. London Math. Soc.* (2) **46** (1992), pp. 239–249.

9 J.-P. Serre, *Arbres, amalgames,* SL_2, Société Mathématique de France, 1977.

10 W. Sierpiński, *Elementary theory of numbers*, Państwowe Wydawnictwo Naukowe, Warszawa, 1964.

11 N. J. A. Sloane, *The on-line encyclopedia of integer sequences*, published electronically at ⟨ www.research.att.com / ~njas / sequences/ ⟩, 2006.

12 P. Tannery, C. Henry, *Oeuvres de Fermat*, tome deuxième, Gauthier-Villars, Paris, 1894.

13 K. Vogel, *Die Grundlagen der ägyptischen Arithmetik*, Michael Beckstein, München, 1929.

14 D. Wells, *The Penguin dictionary of curious and interesting numbers*, Penguin Books Ltd, Harmondsworth, 1986.