Het ontbinden van grote getallen in priemfactoren

Voordracht gehouden op de NWD

H.W. Lenstra, Jr.
Department of Mathematics, University of California, Berkeley

Dit artikel is gebaseerd op een plenaire voordracht die ik tijdens de Nationale Wiskunde Dagen 1995 gehouden heb. Ik ben dank verschuldigd aan F. van der Blij voor het schrijven van een eerste versie en aan J. van de Craats voor het leveren van opbouwende kritiek.

In deze voordracht hoop ik het in de titel vermelde onderwerp van verschillende kanten te belichten, zodat de toehoorder in staat zal zijn tijdens beschaafde koffietafelgesprekken een welingelichte indruk te maken. Een aspect dat onderbelicht zal blijven is dat van de wiskundige details. Hiervoor, en voor vele andere zaken, kan men terecht in het boek *Cryptology and computational number theory*, geredigeerd door C. Pomerance en uitgegeven door de American Mathematical Society in 1990.
De benodigde voorkennis bestaat uit de volgende definitie: *een priemgetal is een geheel getal groter dan* 1 *dat geen delers behalve* 1 *en zichzelf heeft.* Van zo'n getal zegt men ook wel kortweg dat het *priem* is. Een getal heet *samengesteld* als het niet een priemgetal is, en groter dan 1. Merk op dat 1 geen priemgetal is, en ook niet samengesteld – wiskundigen weten dat deze afspraak in de loop van de tijd het meest geriefelijk is gebleken. (In andere kringen vat men de zaak wel eens als een geloofskwestie op, en de discussies kunnen dan hoog oplopen.) Het getal 101 is een priemgetal, maar $91 = 7 \cdot 13$ is samengesteld.

De hoofdstelling van de getaltheorie

Volgens de 'Hoofdstelling van de getaltheorie' is *elk positief geheel getal op precies één manier als produkt van priemgetallen te schrijven.* Zo heeft men de volgende ontbindingen in priemfactoren:

$$9191 = 7 \cdot 13 \cdot 101,$$
$$2178540 = 2^2 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 13 \cdot 19,$$
$$100895598169 = 112303 \cdot 898423.$$

Hier moet men het woord *produkt* ruim opvatten: neemt men het produkt van een verzameling die slechts uit een enkel priemgetal bestaat, dan krijgt men dit priemgetal zelf, en het getal 1 is het *lege* produkt.

Dat men ieder positief geheel getal inderdaad als produkt van een stel priemgetallen kan schrijven is gemakkelijk in te zien. Dat het maar op één manier kan, spreekt, anders dan men weleens denkt, allerminst vanzelf. In figuur 1 ziet men een bericht dat op 2 (!) april 1993 de ronde deed.

```
    |\^/|     MAPLE V
._|\|   |/|_.  Copyright (c) 1981-1990 by the University of Waterloo.
 \ MAPLE /    All rights reserved.  MAPLE is a registered trademark of
 <____ ____>  Waterloo Maple Software.
      |       Type ? for help.

> a := 34816783:
> b := 29698715047:
> c := 1209796049048786078889:
> d := 1031956000233747418830001:
> isprime(a);

                                   true

> isprime(b);

                                   true

> isprime(c);

                                   true

> isprime(d);

                                   true

> a*d;

                  35929388125686333158214572057783

> b*c;

                  35929388125686333158214572057783
```

fig. 1

In het computer-algebra systeem Maple worden vier verschillende getallen a, b, c, d ingevoerd, en het systeem beantwoordt de in gebroken Engels gestelde vraag of dit priemgetallen zijn bevestigend.Vervolgens worden de produkten ad en bc uitgerekend. Had men nu ook nog even het verschil genomen, dan was direct duidelijk geweest wat men nu pas na enig turen ziet: beide produkten zijn gelijk! Weerspreekt dit de hoofdstelling? Het geeft te denken dat men het experiment niet met de huidige versie van Maple kan herhalen.
Deze ervaring toont, wellicht ten overvloede, de noodzaak aan om de hoofdstelling te *bewijzen.* In de *Disquisitiones arithmeticae*, het boek waarmee Carl Friedrich

Gauss (1777-1855) in 1801 de moderne getaltheorie inluidde, is de hoofdstelling voor het eerst duidelijk geformuleerd en bewezen. Bij eerdere getaltheoretici, zoals Euclides van Alexandrië (circa 295 voor Chr.), Diophantos van Alexandrië (circa 250 na Chr.), Pierre de Fermat (1601-1665) en Leonhard Euler (1707-1783) zoekt men de hoofdstelling tevergeefs, hoewel Euclides in de buurt komt. Ik zal de priemfactorontbinding van een getal vaak in de vorm

$$\prod_p p^{a(p)}$$

schrijven, waarbij het produkt zich uitstrekt over alle priemgetallen p, en waarbij $a(p)$, voor ieder priemgetal p, een niet-negatief geheel getal is dat voor slechts eindig veel p verschillend van 0 is.

Het belang van de hoofdstelling

Men kan zich afvragen waar de stelling de naam *hoofd*stelling aan verdient. Dit ligt eraan dat vele vragen die men zich over gehele getallen kan stellen een antwoord toelaten in termen van de priemfactorontbinding. Ik geef twee voorbeelden.
Welke getallen laten zich als som van twee kwadraten schrijven? Antwoord:

$$\text{als } n = \prod_p p^{a(p)}$$

dan is n te schrijven als som van twee kwadraten van gehele getallen dan en slechts dan als $a(p)$ *even* is voor ieder priemgetal van de vorm $p = 4k - 1$. Met andere woorden: n is een som van twee kwadraten als elk priemgetal van de vorm $4k - 1$ een even aantal keren in n voorkomt, en deze voorwaarde is ook nodig. Deze mooie stelling is van Fermat afkomstig.
Voorbeelden: $175 = 5^2 \cdot 7$ is niet een som van twee kwadraten, want 7 komt een oneven aantal keren voor; maar $245 = 5 \cdot 7^2$ is wel een som van twee kwadraten: $245 = 49 + 196 = 7^2 + 14^2$.
De *som van de delers* van een getal n verheugt zich al sinds eeuwen in de belangstelling van rekenkundigen. Men schrijft $\sigma(n)$ voor deze som:

$$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$$

Hoe kan men $\sigma(n)$ snel bepalen? Antwoord:

$$\text{voor } n = \prod_p p^{a(p)} \text{ heeft men}$$

$$\sigma(n) = \prod_p \frac{p^{a(p)+1} - 1}{p - 1}.$$

Voorbeeld: voor $n = 175 = 5^2 \cdot 7$ vindt men

$$\sigma(175) = \frac{5^3 - 1}{5 - 1} \cdot \frac{7^2 - 1}{7 - 1} = 31 \cdot 8 = 248.$$

Men bewijst de formule door een stel meetkundige reeksen met elkaar te vermenigvuldigen. In het gegeven voorbeeld geldt

$$\frac{5^3 - 1}{5 - 1} \cdot \frac{7^2 - 1}{7 - 1} = (1 + 5 + 5^2) \cdot (1 + 7)$$

en bij uitvermenigvuldiging verschijnen alle delers van $5^2 \cdot 7$.
De beide genoemde resultaten zijn pas bruikbaar als de priemfactorontbinding van n *bekend* is. Dit leidt tot de vraag hoe men van een gegeven getal n de priemfactorontbinding snel kan *vinden*. Dat is het voornaamste onderwerp van deze voordracht. Ik zal de tegenwoordige stand van zaken bespreken, de belangrijkste open problemen aangeven, en ingaan op de motieven die men in de loop van de geschiedenis gehad heeft om zich met het ontbinden van grote getallen bezig te houden.

Primaliteit en factorizatie

Het probleem om een gegeven getal in priemfactoren te ontbinden wordt vaak in twee deelproblemen gesplitst, die bekend staan onder de namen *primaliteit* en *factorizatie*. Het *primaliteits*probleem bestaat eruit te beslissen of een gegeven geheel getal $n > 1$ een priemgetal is of niet. Dit gebeurt met een zogenaamde *primaliteitstest*. Als het antwoord 'ja' luidt, dan is daarmee tevens de priemfactorontbinding van n gevonden: $n = n$. Is het antwoord 'nee', dan weet men zeker dat een deler d van n met $1 < d < n$ *bestaat*, maar de meeste primaliteitstests hebben de onaangename eigenschap dat ze geen enkele informatie geven over hoe zo'n deler d dan wel te vinden zou zijn. Daarmee komt men terecht bij het *factorizatie*probleem: gegeven een samengesteld getal $n > 1$, vind een deler d van n met $1 < d < n$. Dat probeert men te doen met een *factorizatiemethode*. Heeft men succes, dan kan men schrijven $n = d \cdot \frac{n}{d}$, en met de getallen d en $\frac{n}{d}$ begint men weer van voren af aan. Dit voert uiteindelijk tot de volledige priemfactorontbinding van n.
Men kan de huidige stand van zaken kort samenvatten door te zeggen dat primaliteit *gemakkelijk* is, en factorizatie *moeilijk*. Dit ga ik nader preciseren.

Testdelingen

De bekendste methode om n in priemfactoren te ontbinden bestaat uit het uitvoeren van een serie testdelingen. Voor deze methode legt men een tabel 'kleine' priemgetallen aan: 2, 3, 5, ... Deze priemgetallen worden op de rij af als mogelijke delers van n geprobeerd. Iedere gevonden priemdeler wordt zo vaak als mogelijk is uit het getal verwijderd. Men houdt op als men bij een priemgetal aankomt dat groter is dan de wortel van het overblijvende getal; dat laatste getal is dan vanzelf priem. Voorbeeld: voor $n = 19998$ vindt men achtereenvolgens de factoren 2, 3, 3, 11 en de overblijvende factor 101 is kleiner dan 11^2 en dus vanzelf priem: $n = 2 \cdot 3^2 \cdot 11 \cdot 101$.

Bij deze methode hoeft men nooit testdelingen door priemgetallen groter dan $\sqrt{n}$ uit te voeren. De rekentijd is op zijn hoogst

$$c \cdot \sqrt{n} \cdot (\log n)^2.$$

Hierbij is een c een positieve constante, die afhangt van de manier waarop men de tijd meet, van de snelheid van de computer die men gebruikt, en van het grondtal dat men bij de logaritme gebruikt. De factor $\sqrt{n}$ vormt een bovengrens voor het aantal uit te voeren testdelingen. De factor $(\log n)^2$ vormt een schatting voor de tijd die een enkele testdeling in beslag neemt; merk op dat $\log n$ ruwweg evenredig is met het aantal cijfers van n. De exponent 2 kan wat verbeterd worden, maar dat is nauwelijks van belang, want de logaritmische factor valt toch al bij $\sqrt{n}$ in het niet.

De testdelingen-methode doet primaliteit en factorizatie in één klap, maar heeft bijna alleen praktische waarde voor erg kleine getallen. Als n meer dan ongeveer 25 cijfers heeft – en dat is tegenwoordig nauwelijks groot te noemen! – dan kan men letterlijk eeuwig op het antwoord wachten, tenzij men in het gelukkige maar oninteressante geval verkeert dat alle priemfactoren van n tamelijk klein zijn. We kunnen de gegeven schatting voor de rekentijd echter gebruiken als maatstaf om andere methoden tegen af te zetten.

De 'beste' methode

Er zijn meer primaliteitstests en factorizatiemethoden in omloop dan ik hier op kan sommen, en de vraag naar de 'beste' is even zinloos als de vraag wat nu eigenlijk de beste auto is. Verschillende gebruikers stellen verschillende eisen, en men gaat niet in zijn boodschappenwagen op safari. Ik zal in mijn bespreking de nadruk leggen op technieken die nog het best met race-auto's te vergelijken zijn – technieken waar de wereldkampioenen hun records mee vestigen, maar die zelden geschikt zijn voor de consumentenmarkt.

Drie primaliteitstests

Eerst laat ik drie primaliteitstests de revue passeren. De eerste twee zijn in wiskundig opzicht tamelijk geavanceerd. De *Jacobi-somtest*, door L.M. Adleman en anderen omstreeks 1983 uitgevonden, berust op de hogere reciprociteitswetten uit de algebraïsche getaltheorie, en de *complexe vermenigvuldigingstest*, door A.O.L. Atkin en anderen omstreeks 1988 ontwikkeld, op de theorie der elliptische krommen. Als men bereid is zijn computer een paar maanden te laten draaien, is elk van beide methoden in de praktijk bruikbaar voor getallen van maximaal ongeveer 1500 cijfers, en in dit bereik ontlopen ze elkaar weinig in snelheid. Voor grotere n gaan beide methoden teveel tijd in beslag nemen, maar men verwacht wel dat de tweede methode uiteindelijk sneller is. Men heeft namelijk bewezen dat men met de Jacobi-somtest in het ergste geval tijd

$$(\log n)^{c \log\log\log n}$$

kwijt is, terwijl men vermoedt dat de complexe vermenigvuldigingstest niet meer dan tijd

$$c \cdot (\log n)^5$$

kost. In beide uitdrukkingen geeft c een positieve constante aan.
In de praktijk vertonen deze tests, net als bijna alle andere primaliteitstests, een opmerkelijk gedrag: als namelijk het getal n dat men onderzoekt *niet* een priemgetal is, dan komt de test daar bijna direct achter. Als de berekening lang duurt dan kan men er praktisch zeker van zijn dat n priem is – *praktisch* zeker, maar niet *wiskundig* zeker: de tijdrovende berekeningen moet men juist uitvoeren om voldoende gegevens voor een volledig sluitend bewijs dat n priem is bijeen te zamelen. Dat bewijs berust soms op geavanceerde wiskundige theorieën.
De net genoemde eigenschap kan men gebruiken om de rekentijd van primaliteitstests aanzienlijk te bekorten. Men laat de test namelijk slechts een beetje langer lopen dan nodig is om de niet-priemgetallen te herkennen, en als de test dan nog niet gestopt is, onderbreekt men hem toch, voordat met het tijdrovende gedeelte een aanvang gemaakt wordt. Men heeft dan niet een sluitend bewijs dat n priem is, maar wel de praktische zekerheid. Dat is wetenschappelijk gesproken onbevredigend, maar voor niet-wetenschappelijke doeleinden vaak goed genoeg. Wil men bijvoorbeeld priemgetallen verhandelen – en dat gebeurt tegenwoordig! – dan mogen er best een paar kapotte tussenzitten. Dat is met CD-spelers immers ook het geval, en met een coulante garantieregeling kan men toch de klant te vriend houden.

Eén van de bekendste methoden die niet meer dan praktische zekerheid geven is de *getuigentest* van G.L. Miller en M.O. Rabin (1976). De rekentijd is slechts $c \cdot (\log n)^3$, en men kan er getallen van tienduizenden cijfers mee testen. Andere aantrekkelijke eigenschappen van de methode zijn eenvoud van implementatie, bruikbaarheid door consumenten en algemene begrijpelijkheid van de onderliggende wiskunde. Men moet ten aanzien van de 'praktische zekerheid' echter wel weten wat men doet – het bovenverhaalde Maple-fiasco was hoogstwaarschijnlijk te wijten aan een al te optimistische variant van de getuigentest.
Voor getallen van een speciale vorm zijn vaak aparte tests beschikbaar. Op het ogenblik is het getal $2^{859433} - 1$, dat 258716 cijfers heeft, het grootst bekende priemgetal. Het (wiskundig sluitende) bewijs dat dit getal priem is, berust op een test die speciaal voor getallen van de vorm $2^m - 1$ is ontworpen.

Al met al is de situatie ten aanzien van primaliteitstests redelijk bevredigend. De voornaamste open problemen zijn van theoretische aard, bijvoorbeeld: kan men een wiskundig sluitende test bedenken waarvan men kan *bewijzen* dat de rekentijd niet meer dan $(\log n)^c$ is? (Voor de complexe vermenigvuldigingstest was dit slechts een *vermoeden*.) Met enige fantasie kan men zich ook wel een *praktische* situatie voorstellen waarin de tegenwoordige stand van de wetenschap tekort schiet. Stel bijvoorbeeld dat men een getal n van zo'n 7000 cijfers tegenkomt, dat niet een speciale vorm heeft, en waarvan men praktisch zeker is dat het een priemgetal is (bijvoorbeeld omdat de getuigentest dat zegt). Stel bovendien dat men dolgraag een *bewijs* zou willen hebben dat n priem is, bijvoorbeeld omdat men daar een beroemd open probleem mee zou kunnen oplossen. In deze situatie is er geen enkele bekende methode waarmee men geholpen is.

De elliptische krommen-methode

Bij primaliteitstests maakte ik onderscheid tussen wiskundig sluitende methoden en methoden die alleen praktische zekerheid bieden. Dit onderscheid bestaat niet bij factorizatiemethoden. Immers, een factorizatiemethode heeft tot taak om van een gegeven samengesteld getal n een niet-triviale deler d te vinden, en als deze taak is uitgevoerd, kan iedereen ogenblikkelijk controleren of d inderdaad een deler van n is. Hierbij hoeft men niet op de machine te vertrouwen of kennis te hebben van de wiskundige theorie die aan de methode ten grondslag ligt.

Ik bespreek drie factorizatiemethoden. De eerste is de *elliptische krommen-methode*, die ik tien jaar geleden bedacht heb. Als ik voor iedere keer dat deze methode met succes gebruikt is een dubbeltje had gekregen dan had ik me nu op een comfortabel landgoed terug kunnen trekken. De populariteit van de methode is te danken aan een combinatie van aantrekkelijke eigenschappen die elk voor zich zeldzaam zijn bij factorizatiemethoden. Ten eerste is de methode bijzonder eenvoudig te implementeren, ondanks het feit dat de onderliggende gedachten uit de theorie der elliptische krommen afkomstig zijn. Ten tweede kan men de methode ook op kleine machines, die geen groot geheugen hebben, draaien. Ten derde is de methode bruikbaar voor getallen n uit een buitengewoon groot bereik, van slechts tien tot duizenden cijfers aan toe. Niet dat men voor de grootste van die getallen altijd *succes* heeft: de methode is gespecialiseerd in het vinden van betrekkelijk 'kleine' priemfactoren. In de praktijk betekent dit: priemfactoren van niet meer dan zo'n 35 cijfers. Op grond van theoretische analyses vermoedt men dat de methode ongeveer tijd

$$e^{\sqrt{(2+\varepsilon)\log p \log\log p}} \cdot (\log n)^2$$

nodig heeft om de priemfactor p van n te vinden; hier moet men de natuurlijke logaritme nemen, en ε is een getal dat naar 0 nadert voor $p \to \infty$. De van p afhangende uitdrukking is een nadere bestudering waard. Men kan eruit aflezen dat kleine priemfactoren sneller gevonden worden dan grote, en ook dat de methode sneller werkt dan de eerder besproken testdelingen-methode, die ongeveer tijd $p \cdot (\log n)^2$ nodig heeft om hetzelfde te doen.

In de praktijk is de elliptische krommen-methode vaak de eerste die men loslaat op een getal n dat men nooit eerder ontmoet heeft, om de kleine priemfactoren eruit te verwijderen. Als de methode enige tijd zonder succes gedraaid heeft, concludeert men dat n waarschijnlijk geen 'kleine' priemfactoren heeft. In dat geval heeft men als n niet te groot is – niet meer dan ongeveer 140 cijfers, met de tegenwoordige stand van zaken – nog een kans met een van de volgende twee methoden.

De kwadratische zeef

De *kwadratische zeef*, door C. Pomerance in 1982 uitgevonden, is in bijna alle opzichten de tegenpool van de elliptische krommen-methode. Het is een enigszins peuterig werk om er een programma voor te schrijven, hoewel de onderliggende wiskunde erg eenvoudig is. Men komt ook niet goed uit de voeten zonder een flink geheugen. De methode is toepasbaar op een veel bescheidener bereik: voor getallen van meer dan zo'n 130 cijfers loopt de rekentijd te hoog op. Daar staat tegenover dat deze rekentijd, anders dan bij de elliptische krommen-methode, in de praktijk heel goed voorspelbaar is. Deze tijd is namelijk niet afhankelijk van een onbekende grootheid, zoals de grootte van de priemfactoren van n, maar alleen van n zelf.
Er is goede reden om aan te nemen dat de rekentijd in de meeste gevallen gegeven wordt door een uitdrukking van de vorm

$$e^{\sqrt{(1+\varepsilon)\log n \log\log n}}$$

waarbij $\varepsilon \to 0$ voor $n \to \infty$. Het kost met deze methode dus evenveel tijd om kleine priemfactoren te vinden als grote! In feite vindt de methode *alle* priemfactoren op bijna hetzelfde moment. Dit mag vreemd klinken, zeker wanneer men een vergelijking trekt met de methode die op testdelingen berust en de elliptische krommen-methode. Het blijkt evenwel dat de meeste geavanceerde factorizatiemethoden deze eigenschappen met de kwadratische zeef delen – het is juist de elliptische krommen-methode die een uitzondering vormt.

Bestudeert men de bovengegeven uitdrukking voor de rekentijd dan ontdekt men dat de kwadratische zeef aanzienlijk sneller is dan de testdelingen-methode, maar veel langzamer dan de primaliteitstests die ik heb besproken. Het is een aardige opgave om te zien in welk bereik de rekentijd vergelijkbaar is met de tijd die de elliptische krommen-methode in beslag neemt.

De getallenlichamenzeef

De kwadratische zeef wordt de laatste jaren in toenemende mate overschaduwd door de *getallenlichamenzeef*, waarvan het basisprincipe in 1988 door J.M. Pollard werd aangegeven en waaraan sedertdien een hele groep mensen verbeteringen heeft aangebracht. De grondgedachten van de methode lijken erg op die van de kwadratische zeef, behalve dat men niet met elementaire getaltheorie maar met algebraïsche getaltheorie werkt; weliswaar slechts met de beginselen van deze theorie, zoals die al in de tweede helft van de negentiende eeuw bekend waren, maar omdat het hier een vak betreft waar de meeste getallen-ontbinders weinig mee vertrouwd zijn, heeft dit toch een vertragend element in de ontwikkeling van de methode gevormd. Het programmeren van de getallenlichamenzeef heeft tot verscheidene problemen aanleiding gegeven, die nu alle min of meer bevredigend zijn opgelost.
Nu de stofwolk enigszins is opgetrokken, begint duidelijk te worden dat de getallenlichamenzeef sneller werkt dan de kwadratische zeef zodra n meer dan ongeveer 105 cijfers heeft. Men heeft goede hoop dat de methode in elk geval bruikbaar zal zijn voor getallen van maximaal ongeveer 155 cijfers. Een theoretische analyse suggereert dat voor zeer grote n de rekentijd ongeveer

$$e^{1,923\,(\log n)^{\frac{1}{3}}\,(\log\log n)^{\frac{2}{3}}}$$

bedraagt, hetgeen uiteindelijk inderdaad minder is dan voor de kwadratische zeef.
De getallenlichamenzeef heeft nog een aantrekkelijke eigenschap: voor sommige getallen die een speciale vorm hebben, werkt hij extra snel. Een voorbeeld wordt gegeven door het getal

$$F_9 = 2^{2^9} + 1$$

dat men het *negende Fermatgetal* noemt. Het heeft 155 cijfers. Alle rekenkundigen hebben een speciale plaats in hun hart voor Fermatgetallen, en het ontbinden van Fermatgetallen is de droom van hun leven. In 1990 lukte het A.K. Lenstra en M.S. Manasse om F_9 met behulp van de getallenlichamenzeef in priemfactoren te ontbinden. Ze vonden dat

$$F_9 = p_7 \cdot p_{49} \cdot p_{99}$$

waarbij het aantal cijfers van p_7, p_{49} en p_{99} gelijk is aan 7, 49 en 99:

p_7 = 2 424833,
p_{49} = 7 455602 825647 884208 337395 736200 454918 783366 342657,
p_{99} = 741 640062 627530 801524 787141 901937 474059 940781 097519 023905 821316 144415 759504 705008 092818 711693 940737.

Deze ontbinding nam vier maanden in beslag en maakte gebruik van honderden over de hele wereld verspreide computers. Wie hier meer over wil weten, verwijs ik naar het artikel 'The factorization of the ninth Fermat number', dat verschenen is in *Mathematics of Computation, vol. 61* (1993), pp. 319-349.

De toekomst

Als men de rekentijd van bestaande factorizatiemethoden onderzoekt, ontdekt men dat deze zo snel toeneemt met het getal dat men wil ontbinden, dat het nauwelijks zoden aan de dijk zet wanneer men een snellere computer koopt. Stel bijvoorbeeld dat n een samengesteld getal is van 210 cijfers, en dat de eer van de mensheid ermee gemoeid is om n in priemfactoren te ontbinden, net zoals in de jaren zestig de Amerikaanse eer gemoeid was met het plaatsen van een mens op de maan. Wat te doen? Als n een kleine priemfactor bezit, heeft men met de elliptische krommen-methode een kans, maar als dit niet zo is dan is er geen enkele bekende methode waarmee de klus geklaard kan worden, zelfs niet met de beste politieke wil van de wereld. Als n maar 190 cijfers heeft, ligt het anders: het is goed voorstelbaar dat men een getal van die grootte met bestaande technische en algoritmische middelen kan ontbinden, zij het dat men aanzienlijke organisatorische en financiële problemen zal hebben te overwinnen.

Wie getallen van meer dan zo'n 200 cijfers wil ontbinden, kan er alleen maar op hopen dat iemand een snellere methode bedenkt. Dat is dan ook het voornaamste open probleem in dit vakgebied. Een ander open probleem, dat van meer theoretische aard is, bestaat eruit om de rekentijdanalyses die ik aan heb gegeven streng te bewijzen.

Factorizatie door de eeuwen

In vroeger eeuwen achtten de grootste getaltheoretici het niet beneden hun waardigheid zich bezig te houden met het ontwerpen en toepassen van methoden om grote getallen in factoren te ontbinden. In de loop van de negentiende eeuw, na Gauss, werd dit anders. Topwiskundigen hadden andere dingen om handen, en factorizatieproblemen begonnen te behoren tot het domein van de mindere goden, inclusief amateur-wiskundigen. Eén van de origineelste van de geleerden die zich toen met het onderwerp bezig hielden, was de Fransman Edouard Lucas (1842-1891), wiens naam een begrip is bij iedereen die in wiskundige puzzels geïnteresseerd is. Uit deze puzzelhoek heeft het onderwerp zich gedurende het grootste deel van de twintigste eeuw niet kunnen losmaken. Wiskundigen die zich erop toelegden, bewogen zich in de marge van de wetenschap, en hun fronsende collega's konden moeilijk verhelen dat ze de hele onderneming in intellectueel opzicht even uitdagend vonden als het verzamelen van sigarenbandjes.

Pas tegen het eind van de jaren zeventig kwam er, door twee gelijktijdige ontwikkelingen, een omslag. Eén van deze ontwikkelingen had plaats in de *cryptografie*. In 1977 vonden R.L. Rivest, A. Shamir en L.M. Adleman een systeem uit waarmee men geheime boodschappen kan versturen dat grote voordelen had ten opzichte van eerdere systemen. Meer bijzonderheden over dit zogenaamde *RSA-systeem*, dat gebruik maakt van getaltheorie, zijn te vinden in het aan het begin genoemde boek van Pomerance. Voor de constructie van de hulpgetallen die het systeem gebruikt, is het essentieel dat primaliteit een gemakkelijk probleem is, en de onbreekbaarheid van het systeem berust op de praktische onoplosbaarheid van het factorizatieprobleem voor grote getallen.

Het ligt voor de hand dat dit geleid heeft tot een sterk toegenomen belangstelling voor het vakgebied, onder andere van de kant van geheime diensten. Zuiver-wiskundigen die toepassingen toch maar vulgair vinden, moeten wel bedenken dat het hier om een toepassing van hun *onkunde* gaat: als ze het factorizatieprobleem oplossen, verdwijnt de toepassing en wordt de zuiverheid van de getaltheorie hersteld.

De tweede ontwikkeling was de opkomst van de *theoretische informatica*. In deze tak van wetenschap bestudeert men rekenmethoden niet door ze uit te proberen maar door er in een luie stoel over na te gaan denken. Eén van de dingen waar men over nadenkt is, of men kan voorspellen hoeveel tijd een computer nodig heeft om een bepaald probleem met een bepaalde methode op te lossen. Met behulp van dergelijke *rekentijdanalyses* is men in staat 'op het droge' te beslissen welke van twee methoden de beste is. Dit leidt vervolgens tot de vraag om voor een gegeven probleem een rekenmethode te ontwerpen waarbij de schatting van de rekentijd zo gunstig mogelijk uitvalt.
Het probleem om getallen in factoren te ontbinden heeft in dit verband vanwege zijn eerwaarde ouderdom en zijn fundamentele karakter altijd op de speciale belangstelling van theoretisch-informatici kunnen rekenen.

Als resultaat van deze ontwikkelingen hebben primaliteit en factorizatie hun centrale plaats in de getaltheorie opnieuw ingenomen. Men ontleent technieken aan de algebraïsche meetkunde en de algebraïsche getaltheorie, en de rekentijdanalyses berusten op analytische getaltheorie. De sigarenbandjes kunnen weer zonder schroom getoond worden.

Perfecte getallen

Men kan zich afvragen wat mensen ertoe dreef om getallen te ontbinden in de tijd dat er nog geen sprake was van cryptografische toepassingen of computers. In figuur 2 ziet men het antwoord van Gauss, aan zijn *Disquisitiones arithmeticae* ontleend.

329. Problema, numeros primos a compositis dignoscendi, hosque in factores suos primos resoluendi, ad grauissima ac vtilissima totius arithmeticae pertinere, et geometrarum tum veterum tum recentiorum industriam ac sagacitatem occupauisse, tam notum est, vt de hac re copiose loqui superfluum foret.

praetereaque scientiae dignitas requirere videtur, vt omnia subsidia ad solutionem problematis tam elegantis ac celebris sedulo excolantur.

fig. 2

In het Nederlands:

> 'Het probleem om priemgetallen van samengestelde te onderscheiden, en de laatste in hun priemfactoren te ontbinden, behoort tot de belangrijkste en nuttigste van de gehele rekenkunde. Wiskundigen van alle tijden hebben hun ijver en wijsheid eraan gespendeerd. Dit alles is zo welbekend, dat het niet nodig is er uitgebreid bij stil te staan. (...). Bovendien lijkt men het aan de waardigheid van de wetenschap verschuldigd te zijn om alle hulpmiddelen voor de oplossing van een zo elegant en beroemd probleem met vlijt te cultiveren.'

De waardigheid van de wetenschap! Wie dat antwoord niet wil horen moet de vraag niet stellen.
Het 'nut' waar Gauss op doelt, beperkt zich tot toepassingen in de getaltheorie zelf, zoals bij de berekening van de som van de delers van een getal. Waarom men die berekening wil uitvoeren, zal ik nu uitleggen.
Men noemt een getal *perfect* als het gelijk is aan de som van zijn echte delers; 'echt' betekent dat het getal zelf niet wordt meegeteld. Voorbeelden zijn 6 en 28:

$$6 = 1 + 2 + 3 \qquad 28 = 1 + 2 + 4 + 7 + 14$$

Het gaat hier om een van de oudste begrippen uit de wiskunde[1]. Al bij Euclides vinden we een recept voor het maken ervan (zie figuur 3).

ΠΡΟΤΑΣΙΣ λς'.

Ἐὰν ἀπὸ μονάδος ὁποσοιοῦν ἀριθμοὶ ἐξῆς ἐκτεθῶσιν ἐν τῇ διπλασίονι ἀναλογίᾳ, ἕως οὗ ὁ σύμπας συντεθεὶς πρῶτος γένηται, καὶ ὁ σύμπας ἐπὶ τὸν ἔσχατον πολλαπλασιασθεὶς ποιῇ τινα· ὁ γενόμενος τέλειος ἔσται.

PROPOSITIO XXXVI.

Si ab unitate quotcunque numeri deinceps exponantur in duplâ analogiâ, quoad totus compositus primus fiat, et totus in ultimum multiplicatus faciat aliquem; factus perfectus erit.

fig. 3

In het Nederlands:

als $2^m - 1$ priem is, dan is $2^{m-1}(2^m - 1)$ perfect.

De voorbeelden 6 en 28 krijgt men door m gelijk te nemen aan 2 en 3. Met $m = 859433$ krijgt men het grootste bekende perfecte getal, $2^{1718865} - 2^{859432}$, dat 517430 cijfers heeft. De voorspelling die P. Barlow in 1811 deed (zie figuur 4) is dus niet uitgekomen.

The difficulty, therefore, of finding perfect numbers, arises from that of finding prime numbers, of the form $2^n - 1$, which is very laborious. Euler ascertained, that $2^{31} - 1 = 2147483647$ is a prime number; and this is the greatest at present known to be such, and, consequently, the last of the above perfect numbers, which depends upon this, is the greatest perfect number known at present, and probably the greatest that ever will be discovered; for, as they are merely curious without being useful, it is not likely that any person will attempt to find one beyond it.

fig. 4

In een artikel van Euler dat pas in 1849 gepubliceerd werd (66 jaar na zijn dood!) werd bewezen dat alle *even* perfecte getallen door de formule van Euclides gegeven worden. Of er *oneven* perfecte getallen bestaan is een beroemd open probleem.

Meervoudig perfecte getallen

Er zijn eigenlijk te weinig perfecte getallen om plezier aan te beleven. Hierin heeft men aanleiding gevonden de eis van perfectheid wat af te zwakken. Een getal heet *meervoudig perfect* als het een *deler* is van de som van zijn delers. Met andere woorden, n is meervoudig perfect als er een geheel getal k is met

$$k \cdot n = \sigma(n)$$

waar $\sigma(n)$ de som van de delers van n aangeeft, inclusief n zelf. Met $k = 2$ krijgt men de perfecte getallen. Het getal 120 is een voorbeeld van een meervoudig perfect getal dat niet perfect is, want $\sigma(120) = 360 = 3 \cdot 120$.

Zelf meervoudig perfecte getallen maken

Het fabriceren van meervoudig perfecte getallen was in het midden van de zeventiende eeuw een populaire hobby van Fermat en zijn correspondenten, zoals men in het tweede deel van Fermat's verzameld werk kan nalezen. Het is erg leuk om te doen, en bijzonder aan te bevelen voor wie tijdens een vervelende voordracht de tijd wil verdrijven.

We willen een oplossing van de vergelijking $k \cdot n = \sigma(n)$ vinden. Vervangen we n door zijn priemfactorontbinding en $\sigma(n)$ door de eerder gegeven formule, dan staat er

$$k \cdot \prod_p p^{a(p)} = \prod_p \frac{p^{a(p)+1} - 1}{p - 1}.$$

Men gaat nu een tabel aanleggen van priemmachten p^a die men eventueel links wil opnemen. Naast iedere priemmacht p^a zet men de corresponderende factor

$$\frac{p^{a+1} - 1}{p - 1} \; (= \sigma(p^a))$$

van het rechterlid. In figuur 5 ziet men een voorbeeld van zo'n tabel.

p^a	$\frac{p^{a+1} - 1}{p - 1}$
7^2	$57 = 3 \cdot 19$
3	$4 = 2^2$
19	$20 = 2^2 \cdot 5$
5	$6 = 2 \cdot 3$
3^2	13
13	$14 = 2 \cdot 7$
2	3
2^2	7
2^3	$15 = 3 \cdot 5$
2^4	31

fig. 5

De tabel is als volgt gemaakt. De priemmacht $p^a = 7^2$ uit de eerste regel is willekeurig gekozen. Met deze keuze geeft men te kennen dat men uit is op een meervoudig perfect getal dat twee factoren 7 heeft. In de rechterkolom krijgt men nu $\sigma(7^2) = 57$, hetgeen men in priemfactoren ontbindt: $57 = 3 \cdot 19$. Men ziet dus dat een factor 7^2 in de linkerkolom rechts een factor 3 en een factor 19 geeft. Deze moeten links verantwoord worden, dus 3 en 19 moeten elk ofwel in k ofwel in n voorkomen. Maar schrijft men de vergelijking als

$$k = \prod_p \frac{1 - \frac{1}{p^{a(p)+1}}}{1 - \frac{1}{p}}$$

dan ziet men dat k in het algemeen niet al te groot zal zijn en dus ook niet veel priemfactoren zal hebben. Men moet daarom serieus rekening houden met de mogelijkheid dat 3 en 19 in n zelf voorkomen. Dat geeft aanleiding tot de tweede en derde regel van de tabel, met $p^a = 3^1$ en $p^a = 19^1$, waarbij men weer de corresponderende getallen $\sigma(p^a)$ uitrekent en in factoren ontbindt. Machten van 2 zijn van later zorg, maar de factor 5 uit $\sigma(19) = 20$ geeft aanleiding tot een nieuwe regel in de tabel, met $p^a = 5^1$. De factor 3 in $\sigma(5)$ doet het vermoeden rijzen dat n wel

eens *twee* factoren 3 zou kunnen hebben, zodat men niet 3^1 maar 3^2 moet gebruiken. Deze 3^2 leidt dan weer tot een 13, die zelf een 7 geeft. Dat is veelbelovend, want de twee zevens waarmee we begonnen zijn moesten immers rechts nog verantwoord worden. Er mist nu nog een enkele 7, en het is tijd om eens te gaan kijken of de tot nog toe veronachtzaamde factoren 2 hier wellicht voor gebruikt kunnen worden. Probeert men wat machten van 2 uit (de laatste vier regels van de tabel) dan ziet men dat $p^a = 2^2$ precies levert wat we nodig hebben. We zamelen de factoren 7^2, 19, 5, 3^2, 13, 2^2 bijeen, en vinden het meervoudig perfecte getal

$$n = 2^2 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 13 \cdot 19 = 2178540$$

dat voldoet aan

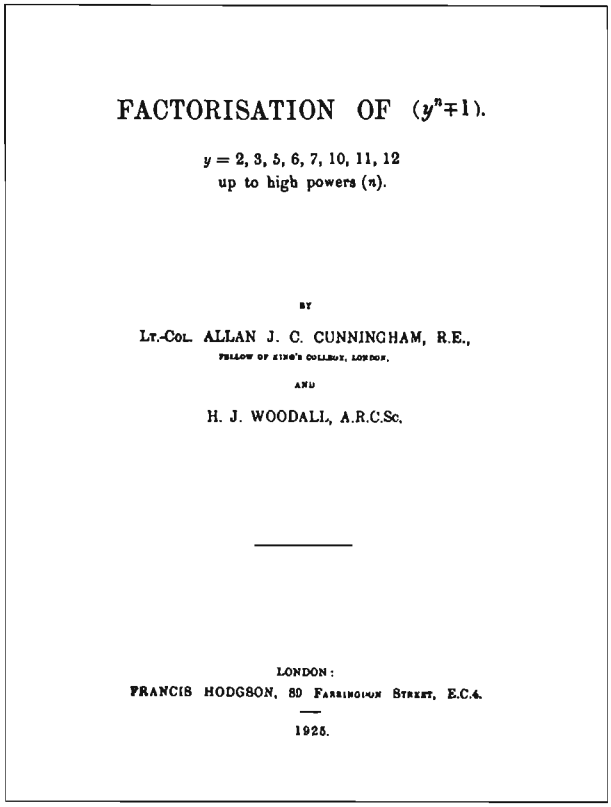
$$\sigma(n) = 4n.$$

Wie aardigheid krijgt in het vervaardigen van meervoudig perfecte getallen komt er snel achter dat het nuttig is om wat hulptabellen ter beschikking te hebben. De machten van 2 waar figuur 5 mee eindigt, komt men bijna altijd tegen, dus men kan deze eens en voor altijd in een aparte tabel zetten, zoals in figuur 6.

a	$2^a - 1$
1	1
2	3
3	7
4	$15 = 3 \cdot 5$
5	31
6	$63 = 3^2 \cdot 7$
7	127
8	$255 = 3 \cdot 5 \cdot 17$
9	$511 = 7 \cdot 73$
10	$1023 = 3 \cdot 11 \cdot 31$
11	$2047 = 23 \cdot 89$
12	$4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$

fig. 6

(In plaats van $2^{a+1} - 1$ verschijnt hier $2^a - 1$, wat natuurlijk dezelfde getallen geeft. Deze kleine opschuiving zal straks echter belangrijk zijn.) Vergelijkbare tabellen voor andere kleine priemgetallen 3, 5, ... bewijzen op een gegeven ogenblik ook hun nut.
Het treft dat er boeken zijn met dergelijke tabellen. Figuur 7 toont de titelpagina van zo'n boek uit 1925. Het is nu moeilijk te vinden, maar in 1983 werd een tabel gepubliceerd die veel verder gaat; in figuur 8 ziet men dat er in de tussenliggende 58 jaar ook in typografisch opzicht veel gebeurd is. Volgens de titelpagina's gebruikt men eveneens grondtallen die *geen* priemgetallen zijn, namelijk 6, 10 en 12: men is kennelijk langzamerhand de historische oorsprong van deze tabellen vergeten.



FACTORISATION OF $(y^n \mp 1)$.

$y = 2, 3, 5, 6, 7, 10, 11, 12$
up to high powers (n).

BY

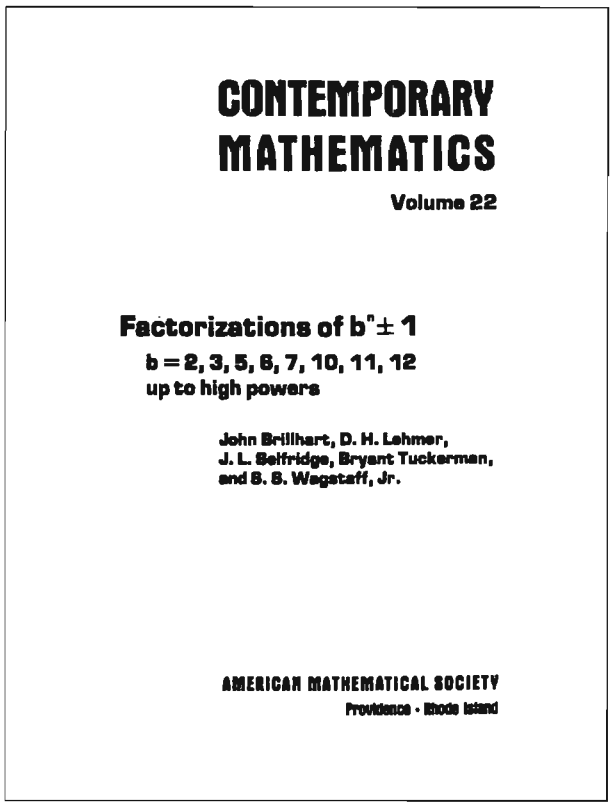
LT.-COL. ALLAN J. C. CUNNINGHAM, R.E.,
FELLOW OF KING'S COLLEGE, LONDON.

AND

H. J. WOODALL, A.R.C.Sc.

LONDON:
FRANCIS HODGSON, 89 FARRINGDON STREET, E.C.4.
1925.

fig. 7 Titelpagina van een boek over factorizatie uit 1925



CONTEMPORARY MATHEMATICS

Volume 22

Factorizations of $b^n \pm 1$
b = 2, 3, 5, 6, 7, 10, 11, 12
up to high powers

John Brillhart, D. H. Lehmer,
J. L. Selfridge, Bryant Tuckerman,
and S. S. Wagstaff, Jr.

AMERICAN MATHEMATICAL SOCIETY
Providence · Rhode Island

fig. 8 Titelpagina van een boek over factorizatie uit 1983

De kleine stelling van Fermat

Het lijdt geen twijfel dat Fermat zelf ook een tabel als in figuur 6 vervaardigde. Wie zorgvuldig tussen de regels van zijn correspondentie doorleest, kan precies volgen wat er door hem heenging toen hij de tabel bekeek. Hij merkte bijvoorbeeld op dat in de rechterkolom om de andere regel een factor 3 voorkwam; met andere woorden, $2^a - 1$ is deelbaar door 3 dan en slechts dan als a even is. Heeft men dit eenmaal opgemerkt, dan is het niet lastig te bewijzen. Op dezelfde manier komt er om de vier regels een factor 5 voor. Informatie van dit soort is natuurlijk erg handig als men de tabel naar beneden toe wil voortzetten. Een factor 7 komt om de *drie* regels voor.

Fermat kwam snel achter de wetmatigheid: als p een oneven priemgetal is, dan is de kleinste a waarvoor $2^a - 1$ een factor p heeft een deler van $p - 1$, en de andere waarden van a waarvoor $2^a - 1$ een factor p heeft, zijn juist de veelvouden van deze kleinste a. De laatste bewering is gemakkelijk te bewijzen. De eerste vereist wat meer werk, en kan als volgt geformuleerd worden: *als p een oneven priemgetal is, dan is* $2^{p-1} - 1$ *deelbaar door p.* Fermat slaagde erin zijn empirisch ontdekte resultaat te bewijzen, niet alleen voor 2 maar ook voor andere grondtallen: *als p een priemgetal is, en m is een geheel getal niet deelbaar door p, dan is* $m^{p-1} - 1$ *deelbaar door p.* Dit is de beroemde 'kleine stelling van Fermat', die uit 1640 dateert. Voorbeeld: 7 deelt $3^6 - 1 = 728 = 7 \cdot 104$. Zonder overdrijving kan men de kleine stelling van Fermat de op één na belangrijkste stelling uit de getaltheorie noemen, na de hoofdstelling. Men kan zonder deze stelling geen serieuze getaltheorie bedrijven. Alle primaliteitstests berusten erop, het RSA-systeem maakt er gebruik van, en – aan de andere kant van het spectrum – een vak als aritmetische algebraïsche meetkunde is ondenkbaar zonder de kleine stelling van Fermat. Het is met technieken uit dit laatste vakgebied dat de *laatste* of *grote* stelling van Fermat in 1994 uiteindelijk is bewezen. Die dateert uit ongeveer 1638, dus van vóór de kleine stelling, die bijgevolg geen rol kan hebben gespeeld in het wonderbaarlijke bewijs dat Fermat zelf voor zijn laatste stelling meende te bezitten.

In sommige getaltheorieboeken leest men dat de Chinezen de kleine stellingvan Fermat al eeuwen voor Christus kenden, althans voor het grondtal 2. Bij nader onderzoek blijkt dit verhaal niet te kloppen; de stelling is inderdaad in China onafhankelijk ontdekt, maar dit gebeurde pas in 1872, door Lǐ Shànlán. Er is gesuggereerd dat het misverstand teruggaat op een vertaalfout van een oud Chinees manuscript. In het algemeen ontdekt men geen belangrijke stellingen door oude Chinese manuscripten verkeerd te vertalen. Dan kan men beter iets frivools doen als meervoudig perfecte getallen bestuderen.

H.W. Lenstra, Jr.
Department of Mathematics #3840, University of California, Berkeley, CA 94720-3840, U.S.A.
email: hwl@math.berkeley.edu

Noot

Noot van de redactie:

[1] In het artikel '33550336: Een volmaakte voltreffer' van N. Brokamp, *Nieuwe Wiskrant 14* (3), april 1995, is beschreven hoe een hele schoolklas in de ban raakte van de perfecte getallen.