Paul Levrie
Faculteit Toegepaste Ingenieurswetenschappen
Universiteit Antwerpen
paul.levrie@uantwerpen.be

Rudi Penne
Faculteit Toegepaste Ingenieurswetenschappen
Universiteit Antwerpen
rudi.penne@uantwerpen.be

Vakantiecursus

Kettingbreuken, weefpatronen en de Kerststelling van Fermat

Op de vakantiecursus 2014 van het Platform Wiskunde Nederland hielden Paul Levrie en Rudi Penne de voordracht 'Priem!', over een onderwerp dat sinds het bewijs van Yitang Zhang over priemparen weer volop in de belangstelling staat. Een onderwerp ook waarover Levrie en Penne onlangs een boek publiceerden: *De pracht van priemgetallen*. **Voor de syllabus van de vakantiecursus schreven ze dit artikel, dat niet zo zeer een weergave van hun voordracht is, maar een voortborduursel op hun recente boek.**

Toen ons gevraagd werd om voor de syllabus van deze vakantiecursus een bijdrage te leveren over een onderwerp waar we net een boek [5] over hadden geschreven, leek het ons onzinnig om dubbel werk te leveren. Daarom grijpen we liever de kans om een nieuw hoofdstuk te breien aan dit boek. Ons verhaal over de priemgetallen is een mix van wiskunde, geschiedenis en leuke weetjes. Omdat het doelpubliek anders is dan dat van het boek, mag het wat meer wiskundig zijn, al zullen we de lezer onderweg verrassen met een heuse snit-en-naadtoepassing. Het begint allemaal met dit:

> Een priemgetal is een natuurlijk getal groter dan 1 dat enkel deelbaar is door 1 en door zichzelf.

En we gaan het hebben over een stelling die ons vertelt welke priemgetallen te schrijven zijn als een som van twee kwadraten. In het kader hiernaast vind je de geschiedenis van deze stelling.

Additieve getaltheorie en de stelling van Fermat

Dat getaltheorie verslavend kan zijn, kan je nu ook lezen in de laatste editie van het beroemde boek *An introduction to the theory of numbers*, van Hardy en Wright [3]. Je vindt er namelijk in de introductie:

> Thus chs. XII–XV belong to the 'algebraic' theory of numbers, Chs. XIX–XXI to the 'addictive', and Ch. XXII to the 'analytic' theories; while Chs. III, XI, XXIII, and XXIV deal with matters usually classified under the headings of 'geometry of numbers' or 'Diophantine approximation'.

Bedoeld wordt natuurlijk 'additive'. De additieve getaltheorie behandelt eigenschappen van getallen waarbij men deze probeert te schrijven als som van andere speciale getallen. Een van de mooiste resultaten op dit gebied is de Kerststelling van Fermat, die in haar meest ruwe vorm zegt:

Elk priemgetal van de vorm $4n+1$ is te schrijven als de som van twee kwadraten.

Iets meer verfijnd hebben we dit:

Een getal kan geschreven worden als de som van twee kwadraten als alle priemfactoren van de vorm $4n+3$ in de priemfactorisatie van het gegeven getal voorkomen met een even macht.

Dat de stap van de ruwe naar de verfijnde versie niet zo groot is, volgt uit twee dingen. Eerst en vooral is het eenvoudig in te zien dat een priemgetal van de vorm $4n+3$ niet te schrijven is als

1634 De minder bekende Franse wiskundige Albert Girard (1595–1632) schrijft een opmerking in de Franse vertaling van het werk van Simon Stevin:

ALB. GIR. *Determinaiſon d'un nombre qui ſe peut diviſer en deux quarrez entiers.*

I. Tout nombre quarré.
II. Tout nombre premier qui excede un nombre quaternaire de l'unité.
III. Le produict de ceux qui ſont tels.
IV. Et le double d'un chaſcun d'iceux.

1640 Pierre de Fermat (1601–1665) schrijft op kerstdag in een brief naar collega Marin Mersenne (1588–1648):

1° Tout nombre premier, qui surpasse de l'unité un multiple du quaternaire, est une seule fois la somme de deux quarrés, et une seule fois l'hypoténuse d'un triangle rectangle.

Fermat beweerde dat hij een onweerlegbaar bewijs had van deze stelling (zo kennen we hem).

1742 Leonhard Euler (1707–1783) schrijft op 30 juni in een brief aan Christian Goldbach:

seyn, welches aber nicht ist. Denn alle diese Zahlen sind in dieser formula $4m+1$ enthalten, welche so oft sie ein numerus primus ist, unfehlbar in duo quadrata, hocque unico modo, resolviret werden kann. So oft aber $4m+1$ kein

1749 Euler schrijft op 12 april naar Goldbach:

Nunmehr habe ich endlich einen bündigen Beweis gefunden, dass ein jeglicher numerus primus von dieser Form $4n+1$ eine summa duor. quadr. ist. Es sey $\boxed{2}$ das Zeichen der

1754 Euler publiceert een *Demonstratio theorematis Fermatiani omnem numerum primum formae 4n+1 esse summam duorum quadratorum*.

1848 Charles Hermite (1822–1901) en Joseph-Alfred Serret (1819–1885) vinden tegelijkertijd een efficiënt algoritme om een priemgetal van de vorm $4n+1$ te schrijven als de som van twee kwadraten.

1855 Henry John Stephen Smith (1826–1883) geeft een eerste eenvoudig bewijs van de stelling.

1867 Édouard Lucas (1842–1891) ziet een toepassing van de stelling van Fermat, die ook wel eens Fermat's Kerstmis-stelling wordt genoemd, bij het weven van satijn.

1940 Godfrey Harold Hardy (1877–1947) schrijft in zijn *A Mathematician's Apology* dit:

Another famous and beautiful theorem is Fermat's 'two square' theorem. The primes may (if we ignore the special prime 2) be arranged in two classes; the primes

5, 13, 17, 29, 37, 41, ...

which leave remainder 1 when divided by 4, and the primes

3, 7, 11, 19, 23, 31, ...

which leave remainder 3. All the primes of the first class, and none of the second, can be expressed as the sum of two integral squares: thus

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2,$$
$$17 = 1^2 + 4^2, \quad 29 = 2^2 + 5^2;$$

but 3, 7, 11, and 19 are not expressible in this way (as the reader may check by trial). This is Fermat's theorem, which is ranked, very justly, as one of the finest of arithmetic. Unfortunately, there is no proof within the comprehension of anybody but a fairly expert mathematician.

Uit de laatste zin blijkt dat Hardy het bewijs van zijn landgenoot Smith, die evenals hijzelf de Savilian Chair of Geometry bekleedde in Oxford, niet kende.

1984 Roger Heath-Brown (1952) geeft een nieuw, kort bewijs van de stelling.

1990 Don Zagier (1951) publiceert zijn *A One-Sentence Proof That Every Prime p ≡ 1 (mod 4) Is a Sum of Two Squares*.

een som van twee kwadraten. Indien dit wel het geval zou zijn, dan moet het gaan om een kwadraat van een even getal en een kwadraat van een oneven getal. Een even getal kunnen we voorstellen door $2k$ bijvoorbeeld, en een oneven getal door $2m+1$. We hebben dan voor de som van de kwadraten:

$$(2k)^2 + (2m+1)^2 = 4k^2 + (4m^2 + 4m + 1) = 4(k^2 + m^2 + m) + 1,$$

en dit geeft dus steeds een viervoud plus 1, en nooit plus 3.

Verder kunnen we gebruik maken van de wonderbaarlijke eigenschap die ons toelaat een product van twee sommen van kwadraten te schrijven als een som van kwadraten:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

(eenvoudig te zien door uitwerking).

Voor een willekeurig getal dat voldoet aan de voorwaarden van de verfijnde stelling gaan we nu als volgt te werk:

- de factoren 2 schrijven we als $1^2 + 1^2$ en de priemfactoren van de vorm $4n+1$ schrijven we als som van twee kwadraten, en met de vorige eigenschap kunnen we dan het product van deze getallen voorstellen als som van twee kwadraten: $A^2 + B^2$;
- de andere factoren hebben een even macht, en zijn samen te herschrijven in de vorm C^2, en die kunnen we dan gewoon op de volgende manier 'binnenbrengen':

$$(A^2 + B^2)C^2 = (AC)^2 + (BC)^2.$$

Onze bedoeling is om in de rest van dit artikel het bewijs te geven van Henry Smith uit 1855 voor de ruwe vorm van de stelling van Fermat. We volgen in essentie de lijnen van [1], hoewel Smith gebruik maakte van *continuanten*, dingen waarvan de meeste mensen nooit gehoord hebben. In plaats daarvan zullen wij werken met *kettingbreuken*, die we onder andere kennen van [4]. Kettingbreuken hebben te maken met lineaire recursiebetrekkingen, en hierover is er een inleiding te vinden in appendix A. Het verband met de kettingbreuken lees je dan weer in appendix B. Dus als je alle details wil weten, lees dan de appendices. Maar je kan het verhaal ook volgen zonder de details van de appendices.

Eerst vertellen we wat meer over kettingbreuken, en in de volgende paragraaf geven we dan onze eigen versie van het bewijs van Smith. Daarna gaan we op zoek naar de twee kwadraten, wiskundig, met de kettingbreuken, maar ook grafisch, via de toepassing beschreven door Édouard Lucas in 1867 (zie geschiedkundig overzicht).

Eindige kettingbreuken

Voor elk niet-geheel rationaal getal kan je wat men noemt een eindige kettingbreuk vinden. We laten dit zien aan de hand van het voorbeeld $\frac{39}{16}$. We bepalen het grootste geheel getal dat in de breuk in kwestie past, en schrijven

$$\frac{39}{16} = 2 + \frac{7}{16} = 2 + \frac{1}{\frac{16}{7}}.$$

Met de noemer van de tweede term in het rechterlid gaan we dan op dezelfde manier verder:

$$\frac{39}{16} = 2 + \frac{1}{\frac{16}{7}} = 2 + \frac{1}{2 + \frac{2}{7}} = 2 + \frac{1}{2 + \frac{1}{\frac{7}{2}}} = 2 + \cfrac{1}{2 + \cfrac{1}{3 + \frac{1}{2}}}.$$

Dit proces eindigt altijd en de laatste noemer is steeds een geheel getal ≥ 2 (waarom kan dit niet gelijk zijn aan 1?).

De kettingbreuk van een positief niet-geheel rationaal getal heeft dus de volgende vorm:

$$b_1 + \cfrac{1}{b_2 + \cfrac{1}{\ddots + \cfrac{1}{b_k}}} \tag{1}$$

waarbij alle b's positieve gehele getallen zijn. We zullen de notatie $T_{1\to k}$ en $N_{1\to k}$ gebruiken voor de teller en de noemer van het rationaal getal dat we krijgen indien we deze kettingbreuk uitwerken:

$$b_1 + \cfrac{1}{b_2 + \cfrac{1}{\ddots + \cfrac{1}{b_{k-1} + \frac{1}{b_k}}}} = \frac{T_{1\to k}}{N_{1\to k}} \tag{2}$$

(dus $1 \to k$ betekent dat de b's geordend zijn van b_1 tot b_k).

Elke stap in deze uitwerking is van de vorm

$$b_j + \frac{1}{N} = \frac{T}{N}$$

met T, N gehele getallen, waarbij T en N geen gemeenschappelijke factor kunnen hebben. In onze notatie veronderstellen we dus dat $T_{1\to k}$ en $N_{1\to k}$ onderling ondeelbaar zijn.

Indien we de b's in de omgekeerde volgorde zetten, dan noteren we het resultaat zo:

$$b_k + \cfrac{1}{b_{k-1} + \cfrac{1}{\ddots + \cfrac{1}{b_2 + \frac{1}{b_1}}}} = \frac{T_{k\to 1}}{N_{k\to 1}}. \tag{3}$$

Merkwaardig genoeg is in beide gevallen de teller gelijk, dat wil zeggen $T_{1\to k} = T_{k\to 1}$. We kijken even terug naar het voorbeeld aan het begin van deze paragraaf. Als we de volgorde van de b's hierin omkeren, dan krijgen we dit:

$$2 + \cfrac{1}{3 + \cfrac{1}{2 + \frac{1}{2}}} = \frac{39}{17}$$

met inderdaad dezelfde teller. Deze eigenschap van kettingbreuken blijkt essentieel te zijn, en is een gevolg van (13) en (14). Meer algemeen zullen we de notaties $T_{i\to j}$ en $N_{i\to j}$ gebruiken voor de teller en de noemer van de (uitgewerkte) kettingbreuk waarbij de b's lopen van b_i tot b_j en waarbij $T_{i\to j}$ en $N_{i\to j}$ onderling ondeelbaar zijn.

Het bewijs van de stelling van Fermat

De stelling die we willen bewijzen zegt dit:

Elk priemgetal van de vorm $p = 4n + 1$ is te schrijven als de som van twee kwadraten.

De essentie van het bewijs is het feit dat de tellers in (2) en (3) aan elkaar gelijk zijn, in combinatie met de volgende merkwaardige formule:

$$T_{1\to k} = T_{j\to 1} \cdot T_{j+1\to k} + N_{j\to 1} \cdot N_{j+1\to k}. \tag{4}$$

Dit is formule (17) uit Appendix B. We kunnen ze ook zo schrijven (als $j + 2 \leq k$):

$$T_{1\to k} = T_{j\to 1} \cdot T_{j+1\to k} + N_{j\to 1} \cdot T_{j+2\to k}, \tag{5}$$

want we hebben natuurlijk dat

$$\frac{T_{j+1\to k}}{N_{j+1\to k}} = b_{j+1} + \cfrac{1}{b_{j+2} + \cfrac{1}{\ddots + \frac{1}{b_k}}} = b_{j+1} + \frac{1}{\frac{T_{j+2\to k}}{N_{j+2\to k}}},$$

en na uitwerking van het rechterlid volgt hieruit door het onderling ondeelbaar zijn van T en bijhorende N dat $N_{j+1\to k} = T_{j+2\to k}$.

We vertrekken van een priemgetal p dat één meer is dan een viervoud, en we stellen de kettingbreuk op voor breuken waarvan de teller gelijk is aan p. Stel dat zo'n kettingbreuk opgebouwd is met de getallen $b_1, b_2, \ldots, b_k$, dan worden (4) en (5) dus:

$$\begin{aligned} p &= T_{j\to 1} \cdot T_{j+1\to k} + N_{j\to 1} \cdot N_{j+1\to k} \\ &= T_{j\to 1} \cdot T_{j+1\to k} + N_{j\to 1} \cdot T_{j+2\to k} \end{aligned}$$

We beperken ons hierbij tot het geval dat $b_1 \geq 2$, dat blijkt voldoende te zijn voor het bewijs. Een gevolg van deze veronderstelling is dat de beide breuken in het rechterlid van (2) en (3) een noemer hebben die ligt tussen 2 en $2n$ (herinner je dat $p = 4n + 1$). Inderdaad, we hebben dan dat

$$\frac{p}{\text{noemer}} > 2 \quad \Rightarrow \quad p = 4n + 1 > 2 \cdot \text{noemer}.$$

Noemer = 1 sluiten we overigens uit, want dan hebben we geen breuk.

We bekijken de verschillende breuken eens voor $p = 13$, dus $n = 3$. Het gaat dan om breuken met teller 13 en noemer respectievelijk 2, 3, 4, 5, 6. Dit zijn de bijhorende kettingbreuken:

$$\frac{13}{2} = 6 + \frac{1}{2},\ \frac{13}{3} = 4 + \frac{1}{3},\ \frac{13}{4} = 3 + \frac{1}{4},\ \frac{13}{5} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}},\ \frac{13}{6} = 2 + \frac{1}{6}.$$

Let op het verband tussen de kettingbreuken die horen bij de breuken met noemers 2 en 6: de volgorde van de b's is omgewisseld. Ook die met noemers 3 en 4 komen op deze wijze met elkaar overeen. De overblijvende breuk, met noemer 5, valt op door het feit dat als je de volgorde van de b's in de kettingbreuk omkeert, dat deze niet verandert ten gevolge van een soort palindromisch effect.

Dit zal ook meer algemeen zo zijn: met elk getal uit $\{2, 3, 4, \ldots, 2n\}$ (= de mogelijke noemers) kunnen we een ander getal uit deze verzameling associëren op deze manier. Neem als getal j, bepaal de kettingbreuk voor $\frac{p}{j}$, keer de volgorde van de b's om zoals in (2) en (3), en dan is de noemer van de resulterende breuk opnieuw een getal uit $\{2, 3, 4, \ldots, 2n\}$.

Omdat het aantal elementen in de verzameling $\{2, 3, 4, \ldots, 2n\}$ gelijk is aan $2n - 1$, een oneven getal, en omdat we deze dus kunnen verdelen in groepjes van twee noemers die bij elkaar horen, zal er altijd één noemer overblijven, die dan ook deze palindromische eigenschap zal moeten hebben:

$$b_1 = b_k,\ b_2 = b_{k-1}, \ldots.$$

Hiermee werken we verder. We onderscheiden nu twee gevallen.

Ofwel is het aantal b's voor deze ene speciale breuk even, stel dus $k = 2j$. Dan ziet de breuk er zo uit:

$$b_1 + \cfrac{1}{\ddots + \cfrac{1}{b_j + \cfrac{1}{b_{j+1} + \cfrac{1}{\ddots + \cfrac{1}{b_k}}}}} = b_1 + \cfrac{1}{\ddots + \cfrac{1}{b_j + \cfrac{1}{b_j + \cfrac{1}{\ddots + \cfrac{1}{b_1}}}}},$$

want inderdaad geldt

$$b_{j+1} + \cfrac{1}{\ddots + \cfrac{1}{b_k}} = b_j + \cfrac{1}{\ddots + \cfrac{1}{b_1}}.$$

Nu kunnen we dit zo schrijven:

$$\frac{T_{j+1\to k}}{N_{j+1\to k}} = \frac{T_{j\to 1}}{N_{j\to 1}}, \tag{6}$$

en hieruit volgt wegens het onderling ondeelbaar zijn van tellers en noemers dat $T_{j+1\to k} = T_{j\to 1}$, noem dit geheel getal a, en ook $N_{j+1\to k} = N_{j\to 1}$, noem dit b.

De eerste vergelijking in het kadertje wordt dan:

$$p = T_{j\to 1} \cdot T_{j+1\to k} + N_{j\to 1} \cdot N_{j+1\to k} = (T_{j\to 1})^2 + (N_{j\to 1})^2$$

of nog

$$p = a^2 + b^2.$$

In dit eerste geval is de zaak dus bewezen.

Ofwel is het aantal b's voor de speciale breuk oneven, stel dus $k = 2j + 1$. Dan ziet de breuk er zo uit:

$$\begin{aligned} b_1 + \cfrac{1}{\ddots + \cfrac{1}{b_j + \cfrac{1}{b_{j+1} + \cfrac{1}{b_{j+2} + \cfrac{1}{\ddots + \cfrac{1}{b_k}}}}}} &= b_1 + \cfrac{1}{\ddots + \cfrac{1}{b_j + \cfrac{1}{b_{j+1} + \cfrac{1}{b_j + \cfrac{1}{\ddots + \cfrac{1}{b_1}}}}}}, \end{aligned}$$

en dus geldt

$$b_{j+2} + \cfrac{1}{\ddots + \cfrac{1}{b_k}} = b_j + \cfrac{1}{\ddots + \cfrac{1}{b_1}}.$$

Dit laatste kunnen we nu zo schrijven:

$$\frac{T_{j+2\to k}}{N_{j+2\to k}} = \frac{T_{j\to 1}}{N_{j\to 1}},$$

en hieruit volgt dan onmiddellijk dat $T_{j+2\to k} = T_{j\to 1}$. Uit het tweede deel van de vergelijking in het kadertje volgt dan:

$$p = T_{j\to 1} \cdot T_{j+1\to k} + N_{j\to 1} T_{j+2\to k} = T_{j\to 1} \cdot (T_{j+1\to k} + N_{j\to 1}),$$

waarbij $T_{j\to 1}$ niet gelijk kan zijn aan 1. Uit deze laatste uitdrukking volgt dat p niet priem is, wat in strijd is met het gestelde.

We zijn er dus nu zeker van dat p te schrijven is als de som van twee kwadraten, en dat k in dit geval even is. Hiermee is het bewijs klaar.

Op zoek naar de twee kwadraten

We willen natuurlijk ook graag weten van welke twee kwadraten het priemgetal $p = 4n+1$ de som is. Hiervoor proberen we meer te weten te komen over de noemer in de palindromische kettingbreuk, we stellen deze noemer voor door d. Hierbij gebruiken we de formule (16) uit Appendix B:

$$N_{1\to k} \cdot T_{1\to k-1} - T_{1\to k} \cdot N_{1\to k-1} = (-1)^{k-1} = -1, \tag{7}$$

die we hier toepassen met k even. Hierbij is $T_{1\to k} = p$ en $N_{1\to k} = d$. Uit (2):

$$\frac{p}{d} = \frac{T_{1\to k}}{N_{1\to k}} = b_1 + \cfrac{1}{b_2 + \cfrac{1}{\ddots + \cfrac{1}{b_{k-1} + \cfrac{1}{b_k}}}} = b_1 + \frac{1}{\frac{T_{2\to k}}{N_{2\to k}}},$$

en uit het onderling ondeelbaar zijn van T en bijhorende N volgt dat d de teller is van de volgende kettingbreuk:

$$\frac{T_{2\to k}}{N_{2\to k}} = b_2 + \cfrac{1}{b_3 + \cfrac{1}{\ddots + \cfrac{1}{b_{k-1} + \cfrac{1}{b_k}}}}.$$

Maar we hebben vroeger gezien dat de teller van zo'n kettingbreuk niet verandert als we de volgorde van de b's omkeren. We krijgen dan de volgende kettingbreuk, die we anders kunnen schrijven door gebruik te maken van het palindromisch karakter van de b's:

$$b_k + \cfrac{1}{b_{k-1} + \cfrac{1}{\ddots + \cfrac{1}{b_3 + \cfrac{1}{b_2}}}} = b_1 + \cfrac{1}{b_2 + \cfrac{1}{\ddots + \cfrac{1}{b_{k-2} + \cfrac{1}{b_{k-1}}}}},$$

vermits $b_k = b_1$, $b_{k-1} = b_2$, enzovoort. De teller van deze laatste kettingbreuk is dus ook gelijk aan d. Dit betekent dat $T_{1\to k-1} = d$. De vergelijking (7) wordt dan:

$$\begin{aligned} d^2 - pN_{1\to k-1} = -1 \quad &\Leftrightarrow \quad d^2 + 1 = pN_{1\to k-1} \\ &\Rightarrow \quad d^2 + 1 \text{ is deelbaar door } p. \end{aligned}$$

Het is niet moeilijk om in te zien dat er maar één getal d kan zijn tussen 2 en $2n$ met deze eigenschap. Stel namelijk dat er zo twee zijn, d_1 en d_2, met $d_1 > d_2$, met zowel d_1^2+1 als d_2^2+1 deelbaar door p. Dan volgt onmiddellijk dat ook het verschil $d_1^2 - d_2^2 = (d_1+d_2)(d_1-d_2)$ deelbaar zal zijn door het priemgetal p, maar beide factoren zijn kleiner dan p, dus dat kan niet.

Voor het bepalen van de unieke noemer d gaan we dan als volgt te werk: bepaal het kwadraat van de getallen $2, 3, \ldots$ en tel er 1 bij op. Indien het resultaat deelbaar is door p, dan heb je d gevonden. Voor $p = 29$ vinden we voor die kwadraten plus 1 het volgende, op veelvouden van 29 na:

1	→	2	7	→	21
2	→	5	8	→	7
3	→	10	9	→	24
4	→	17	10	→	14
5	→	26	11	→	6
6	→	8	12	→	0

We besluiten dat $d = 12$. We bepalen nu de kettingbreuk voor $29/12$:

$$\frac{29}{12} = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \frac{1}{2}}}$$

(palindromisch!) en we berekenen dit deel ervan:

$$2 + \frac{1}{2} = \frac{5}{2},$$

en met de teller en de noemer kunnen we 29 schrijven als een som van twee kwadraten:

$$29 = 2^2 + 5^2.$$

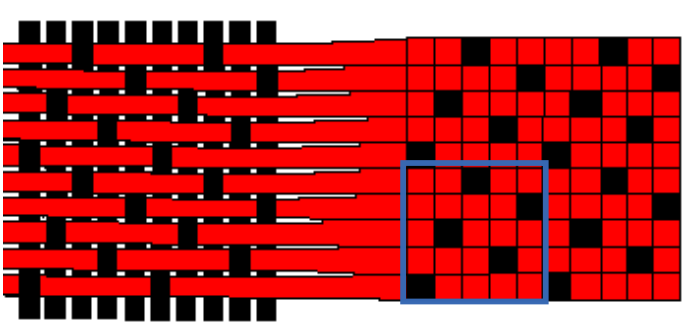
Dit laatste volgt uit (6), want we hebben bewezen dat teller en noemer van het rechterlid de twee getallen zijn die we zoeken.

De methode van Édouard Lucas

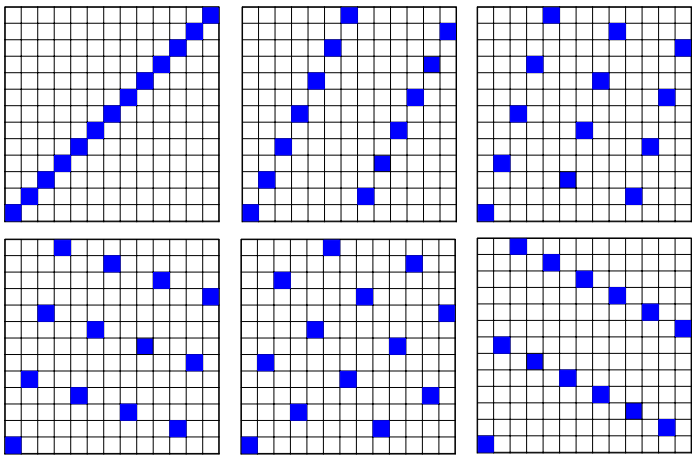
We kunnen de getallen a en b ook op een andere manier bepalen. Édouard Lucas bracht in 1867 de stelling van Fermat in verband met het weven van draden tot textiel. Hierbij worden verticale en horizontale draden met elkaar vervlochten, zoals aan de linkerkant van Figuur 1. Het gaat hier om een zogenaamde satijnbinding. Bij satijn kruisen wat men noemt de ketting- en de inslagdraden elkaar op een speciale manier. Als de zwarte kettingdraad op een bepaalde plaats boven ligt, dan ligt bij minstens vier van de volgende kruisingen de rode inslagdraad boven. Op de figuur zijn het er precies vier. Het patroon herhaalt zich, en kan daarom voorgesteld worden zoals rechts in de figuur, met wat in het blauwe vierkant te zien is, een vierkant opgebouwd uit 5×5 kleine vierkanten, waarvan er als volgt een aantal zwart gekleurd zijn: kleur het vierkantje linksonder in, ga dan één kolom opzij en twee rijen omhoog en kleur daar het vierkantje in, ga weer naar rechts en twee omhoog enzovoort. Kom je uit boven de 5, dan tel je van onderen te beginnen verder.

Omdat de zijde van het vierkant een priemgetal is, zal het toepassen van deze methode er steeds voor zorgen dat er op elke rij en kolom precies één vierkant is ingekleurd, één per rij en één per kolom.

In Figuur 2 is een voorbeeld te zien in het geval we niet vier maar twaalf opeenvolgende kruisingen hebben met de inslagdraad boven, het gaat dan om een vierkant van 13×13. Dit kan op verschillende manieren, zoals je kan zien op Figuur 2. In de verschillende delen van de figuur gaat men respectievelijk met stappen van $1, 2, 3, 4, 5$ en 6 naar boven, steeds startend linksonder in een vierkant. Zo ontstaan



Figuur 1



Figuur 2

patronen. Lucas merkte op dat het patroon in het midden onderaan het mooiste is omdat er allerlei vierkanten in te zien zijn. Bovendien is het het enige dat niet verandert als je het een kwartslag draait. Merk op dat we bij dit patroon stijgen in stappen van 5. En 5 was precies de noemer die hoorde bij het priemgetal 13 waarvan de kettingbreuk palindromisch was!

Lucas bewees ook dat een dergelijke symmetrie niet voorkomt indien het aantal vierkantjes per zijde een priemgetal is van de vorm $4n+3$.

We doen het nog even opnieuw voor $p = 29$, en de bijhorende noemer 12. Kleur in een vierkant van 29×29 het vierkantje linksonder in, ga dan één kolom opzij en twaalf rijen omhoog en kleur daar het vierkantje in, ga weer naar rechts en twaalf omhoog, enzovoort (Figuur 3, links).

Opnieuw ontstaan er vierkanten, waarvan er één is aangeduid op de figuur. Het wordt duidelijker indien we de blauwe vierkantjes vervangen door roosterpunten in een rooster van 29×29 (Figuur 3, rechts). Via de stelling van Pythagoras vinden we dan dat het kwadraat van de zijde van het aangeduide vierkant te schrijven is als $5^2 + 2^2 = 29$.

Bijna 250 jaar na de eerste formulering van de stelling van Fermat door Girard, vond Lucas [6–7] er zo een echte praktische toepassing van! Voor Lucas werd het zelfs een heel nieuwe tak van de meetkunde, die hij *Géométrie plane des tissus* (Vlakke meetkunde van de stoffen) doopte. Hij vond hierbij navolging bij andere wiskundigen, waarvan de meest bekende Pafnuty Chebyshev (1821–1894) is, met zijn ongepubliceerd artikel 'Sur la coupe des vêtements' uit 1878 waarin hij berekent welke vorm je uit een stuk stof moet uitknippen om er een boloppervlak volledig mee te kunnen 'aankleden'.

Voor de geïnteresseerde lezer, je doet het zoals in Figuur 4 wordt gedemonstreerd. Bovenaan zie je de vorm die je uit de stof moet snijden, onderaan het aankleden van de bol. (Met dank aan Étienne Ghys [2] voor de bovenste afbeelding, en aan Jos Leys voor de andere.)

Appendix A. Lineaire recursiebetrekkingen

Een lineaire recursiebetrekking (van de tweede orde) is een vergelijking die het verband geeft tussen drie opeenvolgende termen van een oneindige rij getallen $y_{-1}, y_0, y_1, \ldots, y_n, \ldots$ Zo'n vergelijking neemt de volgende vorm aan:

$$y_k = b_k \cdot y_{k-1} + a_k \cdot y_{k-2} \quad \text{voor } k = 1, 2, 3, \ldots$$

De getallen $a_1, a_2, a_2, \ldots$ en $b_1, b_2, b_3, \ldots$ zijn hierbij gegeven.

Het bekendste voorbeeld van een lineaire recursiebetrekking is dit:

$$y_k = y_{k-1} + y_{k-2} \quad \text{voor } k = 1, 2, 3, \ldots$$

waarbij alle a's en b's gelijk zijn aan 1.

In feite staan hier oneindig veel vergelijkingen, waarvan de eerste gegeven zijn door:

$$y_1 = y_0 + y_{-1}\,, \quad y_2 = y_1 + y_0\,, \quad y_3 = y_2 + y_1\,, \ldots$$

Merk op dat je met deze vergelijkingen inderdaad een oneindige rij getallen genereert, op voorwaarde dat je de eerste twee getallen y_{-1} en y_0 vastlegt. Voor deze recursiebetrekking is de standaardkeuze $y_{-1} = y_0 = 1$ (we spreken van beginvoorwaarden). We krijgen dan de volgende rij getallen:

$$y_{-1} = 1, y_0 = 1, y_1 = 2, y_2 = 3, y_3 = 5, y_4 = 8, y_5 = 13, y_6 = 21, \ldots$$

Deze rij is beroemd en wordt de rij van Fibonacci genoemd.

Als we andere beginvoorwaarden kiezen, dan krijgen we een andere rij getallen.

Een mooie eigenschap van dit soort recursiebetrekkingen is dat als je al twee oplossingen berekend hebt, dat alle andere oplossingen dan te vinden zijn uit die twee. Het is ideaal als je eerst deze twee specifieke oplossingen berekent:

$$\text{oplossing } A_k \text{ met } A_{-1} = 1, A_0 = 0,$$

$$\text{oplossing } B_k \text{ met } B_{-1} = 0, B_0 = 1,$$

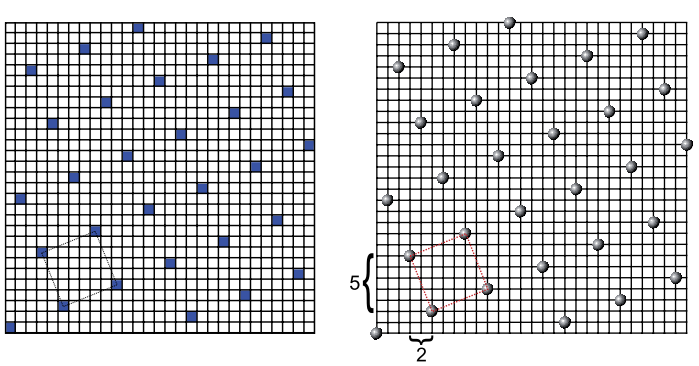
In Tabel 1 zie je de eerste paar termen van beide rijen. Door de speciale keuze van de beginvoorwaarden kunnen we nu elke andere oplossing y_k van de recursiebetrekking schrijven met behulp van deze twee. Je ziet in de tabel dat als je de oplossing A_k vermenigvuldigt met y_{-1} en daar B_k, vermenigvuldigd met y_0, bij optelt, dat je dan de eerste 2 waarden van y_k krijgt.

Door de lineariteit van de recursiebetrekking is het dan eenvoudig in te zien dat voor elke k geldt:

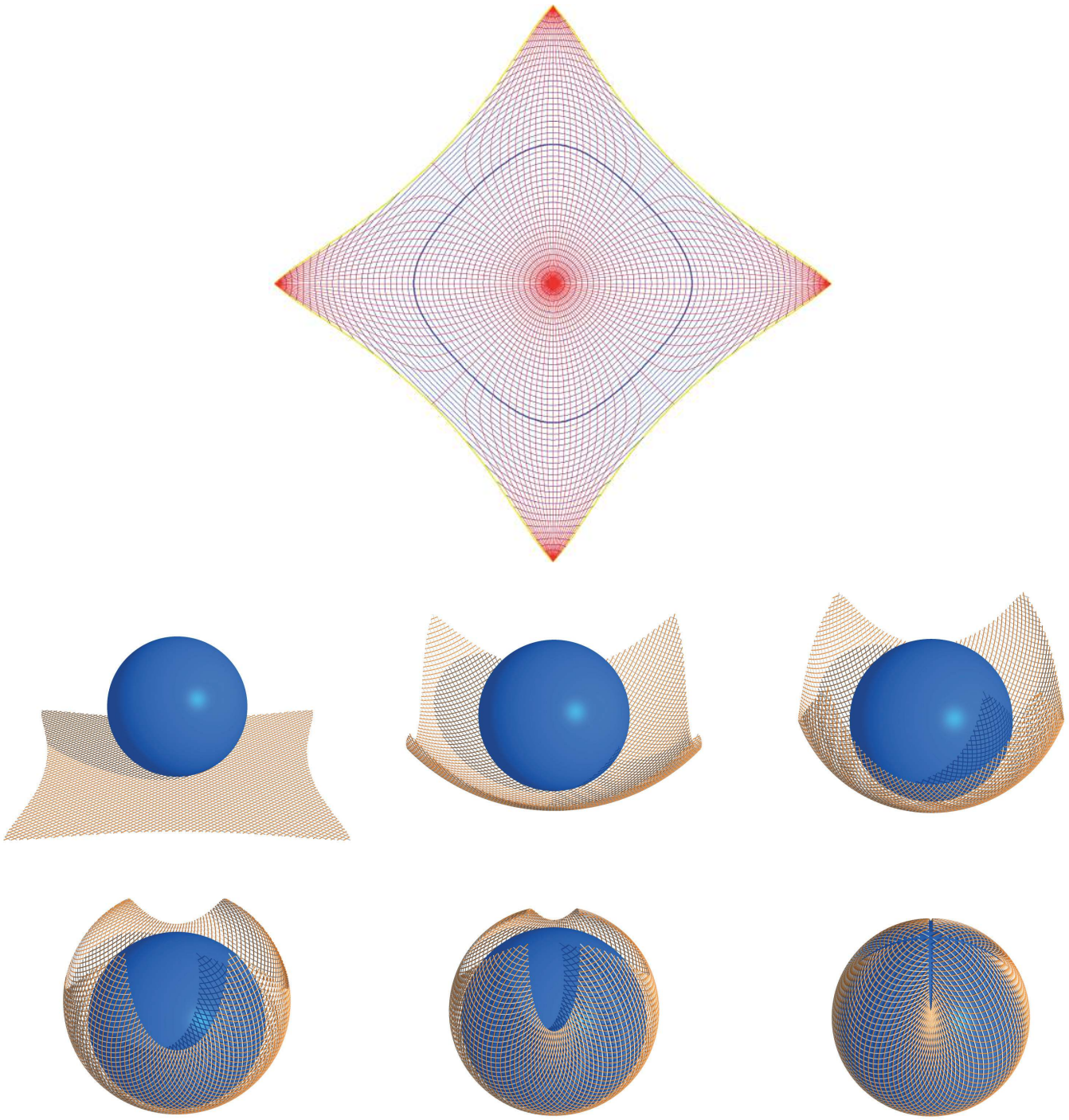
$$y_k = y_{-1}A_k + y_0 B_k.$$

We hebben de volgende eigenschap nodig, eveneens een gevolg van de lineariteit:

$$A_k B_{k-1} - A_{k-1} B_k = (-1)^{k-1} \cdot a_1 \cdot a_2 \cdot \cdots \cdot a_k. \qquad (8)$$



Figuur 3



Figuur 4

Dit kunnen we bewijzen per inductie, en daarvoor gebruiken we eigenschappen van determinanten:

$$\begin{vmatrix} A_k & A_{k-1} \\ B_k & B_{k-1} \end{vmatrix} = \begin{vmatrix} b_k A_{k-1} + a_k A_{k-2} & A_{k-1} \\ b_k B_{k-1} + a_k B_{k-2} & B_{k-1} \end{vmatrix} = -a_k \cdot \begin{vmatrix} A_{k-1} & A_{k-2} \\ B_{k-1} & B_{k-2} \end{vmatrix}$$

met

$$\begin{vmatrix} A_0 & A_{-1} \\ B_0 & B_{-1} \end{vmatrix} = -1.$$

Vanaf nu zullen we enkel nog werken met recursiebetrekkingen waarbij $a_k = 1$ voor elke waarde van k:

k:	-1	0	1	2	$\dots$	n	$\dots$
A_k:	1	0	a_1	b_2a_1	$\dots$	A_n	$\dots$
B_k:	0	1	b_1	$b_2b_1 + a_2$	$\dots$	B_n	$\dots$
y_k:	y_{-1}	y_0	y_1	y_2	$\dots$	y_n	$\dots$

Tabel 1

$k:$	-1	0	1	2	$\dots$	$j-1$	j	$j+1$	$\dots$	n	$\dots$
$B_k^{(1)}:$	0	1	b_1	$B_2^{(1)}$	$\dots$	$B_{j-1}^{(1)}$	$B_j^{(1)}$	$B_{j+1}^{(1)}$	$\dots$	$B_n^{(1)}$	$\dots$
$B_k^{(2)}:$	1	0	1	b_2	$\dots$	$B_{j-1}^{(2)}$	$B_j^{(2)}$	$B_{j+1}^{(2)}$	$\dots$	$B_n^{(2)}$	$\dots$
$B_k^{(3)}:$		1	0	1	$\dots$	$B_{j-1}^{(3)}$	$B_j^{(3)}$	$B_{j+1}^{(3)}$	$\dots$	$B_n^{(3)}$	$\dots$
$\vdots$											
$B_k^{(j)}:$					$\dots$	1	b_j	$B_{j+1}^{(j)}$	$\dots$	$B_n^{(j)}$	$\dots$
$B_k^{(j+1)}:$					$\dots$	0	1	b_{j+1}	$\dots$	$B_n^{(j+1)}$	$\dots$
$B_k^{(j+2)}:$					$\dots$	1	0	1	$\dots$	$B_n^{(j+2)}$	$\dots$

Tabel 2

$$y_k = b_k \cdot y_{k-1} + y_{k-2} \quad \text{voor } k = 1, 2, 3, \dots$$

We definiëren een aantal basisoplossingen zoals in Tabel 2. De positie van de twee opeenvolgende waarden 0 en 1 karakteriseert de verschillende basisoplossingen waarvan je de naam kan lezen in de eerste kolom. Om te beginnen kan je opmerken dat $B_k^{(1)} = B_k$ en $B_k^{(2)} = A_k$, en dus wordt eigenschap (8):

$$B_k^{(2)} B_{k-1}^{(1)} - B_{k-1}^{(2)} B_k^{(1)} = (-1)^{k-1}. \tag{9}$$

Verder is er natuurlijk voor elke waarde van j voldaan aan de recursiebetrekking:

$$B_k^{(j)} = b_k B_{k-1}^{(j)} + B_{k-2}^{(j)}. \tag{10}$$

Uit deze tabel kunnen we twee interessante relaties tussen deze oplossingen aflezen. We baseren ons hiervoor op de waarden van $B_k^{(j+1)}$ en $B_k^{(j+2)}$ in de kleine rechthoek. Om te beginnen kijken we naar $B_k^{(1)}$, en je ziet dan dat deze oplossing de volgende lineaire combinatie is van de twee onderste oplossingen:

$$B_k^{(1)} = B_j^{(1)} B_k^{(j+1)} + B_{j-1}^{(1)} B_k^{(j+2)}. \tag{11}$$

Voor $B_n^{(j)}$ vinden we op dezelfde manier:

$$B_n^{(j)} = b_j B_n^{(j+1)} + B_n^{(j+2)}. \tag{12}$$

Deze recursiebetrekking verbindt drie onder elkaar staande getallen in de tabel, en heeft als onmiddellijk gevolg dat twee opeenvolgende elementen van een kolom geen gemeenschappelijke factor kunnen hebben. Hadden ze wel een gemeenschappelijke factor, dan volgt uit (12) dat deze factor de hele kolom deelt, wat niet mogelijk is door het voorkomen van het getal 1 in elke kolom.

Appendix B. Verband met kettingbreuken

Met de resultaten uit Appendix A kunnen we laten zien (zie verder) dat we het volgende resultaat hebben:

$$\frac{T_{1\to k}}{N_{1\to k}} = b_1 + \cfrac{1}{b_2 + \cfrac{1}{\ddots + \cfrac{1}{b_{k-1} + \cfrac{1}{b_k}}}} = \frac{B_k^{(1)}}{B_k^{(2)}}, \tag{13}$$

waarbij de b's de coëfficiënten zijn in de recursiebetrekking in Appendix A.

Uit het feit dat beide breuken (links en rechts) niet te vereenvoudigen zijn, volgt dan dat $T_{1\to k} = B_k^{(1)}$ en $N_{1\to k} = B_k^{(2)}$.

Verder hebben we ook:

$$\frac{T_{k\to 1}}{N_{k\to 1}} = b_k + \cfrac{1}{b_{k-1} + \cfrac{1}{\ddots + \cfrac{1}{b_2 + \cfrac{1}{b_1}}}} = \frac{B_k^{(1)}}{B_{k-1}^{(1)}} \tag{14}$$

voor de kettingbreuk waarin de b's in de omgekeerde volgorde staan. Dus $T_{k\to 1} = B_k^{(1)}$ en $N_{k\to 1} = B_{k-1}^{(1)}$.

Formule (13) kunnen we veralgemenen tot:

$$\frac{T_{j+1\to k}}{N_{j+1\to k}} = b_{j+1} + \cfrac{1}{b_{j+2} + \cfrac{1}{\ddots + \cfrac{1}{b_k}}} = \frac{B_k^{(j+1)}}{B_k^{(j+2)}}. \tag{15}$$

De formules (13) en (15) volgen uit (12). We herschrijven deze vergelijking als volgt:

$$B_k^{(j)} = b_j B_k^{(j+1)} + B_k^{(j+2)} \quad \Rightarrow \quad \frac{B_k^{(j)}}{B_k^{(j+1)}} = b_j + \cfrac{1}{\cfrac{B_k^{(j+1)}}{B_k^{(j+2)}}}.$$

We starten nu met $j = 1$:

$$\frac{B_k^{(1)}}{B_k^{(2)}} = b_1 + \frac{1}{\frac{B_k^{(2)}}{B_k^{(3)}}} = b_1 + \frac{1}{b_2 + \frac{1}{\frac{B_k^{(3)}}{B_k^{(4)}}}}$$

$$= b_1 + \cfrac{1}{b_2 + \cfrac{1}{\ddots + \cfrac{1}{b_{k-1} + \cfrac{1}{\frac{B_k^{(k)}}{B_k^{(k+1)}}}}}} = b_1 + \cfrac{1}{b_2 + \cfrac{1}{\ddots + \cfrac{1}{b_{k-1} + \cfrac{1}{b_k}}}}.$$

De laatste stap volgt uit de beginvoorwaarden in combinatie met de recursiebetrekking. We hebben namelijk dat $B_k^{(k)} = b_k$ en $B_k^{(k+1)} = 1$.

Voor (14) vertrekken we van de vergelijking (10) met $j = 1$ en herschrijven deze als volgt:

$$B_k^{(1)} = b_k B_{k-1}^{(1)} + B_{k-2}^{(1)} \quad \Rightarrow \quad \frac{B_k^{(1)}}{B_{k-1}^{(1)}} = b_k + \frac{1}{\frac{B_{k-1}^{(1)}}{B_{k-2}^{(1)}}}.$$

We vervangen dan in de linkse vergelijking k door $k-1$ en herhalen het procedé.

Formule (9) kunnen we nu herschrijven als

$$N_{1\to k} \cdot T_{1\to k-1} - T_{1\to k} \cdot N_{1\to k-1} = (-1)^{k-1}. \tag{16}$$

Formule (11) wordt

$$T_{1\to k} = T_{j\to 1} \cdot T_{j+1\to k} + N_{j\to 1} \cdot N_{j+1\to k}. \tag{17}$$

⇦

Referenties

1 F.W. Clarke, W.N. Everitt, L.L. Littlejohn en S.J.R. Vorster, H.J.S. Smith and the Fermat two squares theorem, *Amer. Math. Monthly* 106(7) (1999), 652–665.

2 É. Ghys, Sur la coupe des vêtements: variation autour d'un théorème de Tchebychev [On the cutting of garments: variation on a theme of Chebyshev], *Enseign. Math. (2)* 57(1–2) (2011), 165–208.

3 G.H. Hardy en E.M. Wright, *An Introduction to the Theory of Numbers*, Roger Heath-Brown, Joseph Silverman en Andrew Wiles (red.), Oxford University Press, 2008.

4 M. Kindt en P. Lemmens, *Ontwikkelen met kettingbreuken*, Zebra-reeks, deel 33, Epsilon Uitgaven, Amsterdam, 2011.

5 P. Levrie en R. Penne, *De pracht van priemgetallen*, Prometheus, Amsterdam, 2014.

6 É. Lucas, *Application de l'arithmétique à la construction de l'armure des satins réguliers*, G. Retaux, Paris, 1867.

7 É. Lucas, Les principes fondamentaux de la géométrie des tissus, *Congrès de l'Association française pour l'avancement des sciences* 40(2) (1911), 72–88.