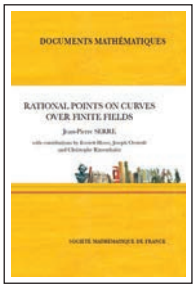
Boekbesprekingen

| Book Reviews

Redactie: Hans Cuypers en Hans Sterk

Review Editors NAW - MF 5.092
Faculteit Wiskunde & Informatica
Technische Universiteit Eindhoven
Postbus 513
5600 MB Eindhoven

reviews@nieuwarchief.nl
www.win.tue.nl/wgreview



Jean-Pierre Serre
with contributions by Everett Howe, Joseph Oesterlé and Christophe Ritzenthaler

Rational Points on Curves over Finite Fields

Documents Mathématiques, Vol. 18
Société Mathématique de France, 2020
x + 187 p., prijs € 45,00
ISBN 9782856299234

In 1985 gaf Jean-Pierre Serre een college aan Harvard University: 'The number of points on curves over a finite field'. De handgeschreven aantekeningen van F.Q. Gouvêa hebben veel wiskundigen inspiratie gegeven om aan dit prachtige onderwerp te werken. Het boek dat nu verschenen is geeft dat materiaal en nog veel meer: Serre heeft het materiaal opnieuw bekeken en op een aantal aspecten aangevuld, Everett Howe, Joseph Oesterlé en Christophe Ritzenthaler hebben nieuwe resultaten toegevoegd, en een groot aantal wiskundigen heeft geholpen met het verzorgen van de TeX-versie, zodat we nu dit prachtige boek met Alp Bassa, Elisa Lorenzo García, Christophe Ritzenthaler en René Schoof als editors tot onze beschikking hebben.

Over de vraag wat het aantal rationale punten op een algebraïsche kromme over een eindig lichaam is, schrijft Serre in zijn voorwoord: "After more than a century of general theorems in algebraic geometry, one should be able to answer such a concrete question." We beschrijven wat de bevindingen zijn van Serre (en veel andere wiskundigen) hierover, en we zullen zien dat die 'general theorems' lang niet altijd een antwoord geven zonder nog meer werk te verrichten.

In deze bespreking geef ik eerst wat achtergrondinformatie: meetkunde, getaltheorie en coderingstheorie.

We schrijven $q = p^e$ voor een macht van een priemgetal p. We weten dat er voor elke q een eindig lichaam is met q elementen, genoteerd als $\mathbb{F}_q$, eenduidig op isomorfie na. Voor een reëel getal t is $[t]$ het grootste gehele getal niet groter dan t. Voor elke algebraïsche variëteit V over een eindig lichaam $K = \mathbb{F}_q$ is het aantal punten op V met coördinaten in K eindig: $\#(V(\mathbb{F}_q)) < \infty$. Wat kunnen we zeggen over dit aantal, en waarom is het interessant? We nemen over van het boek: $N_q(g)$ *is het maximale aantal rationale punten op een kromme van geslacht* g *over* $\mathbb{F}_q$.

In een dagboekaantekening in 1814 beschreef Gauss een wonderlijk vermoeden over het aantal rationale punten op een specifieke kromme over een priemlichaam. Later bleek dat hij de precieze formule voor die gevallen juist had. We weten niet hoe Gauss tot dat diepe inzicht kwam. Kende en gebruikte Gauss de volgende observatie? De afbeelding die de coördinaten tot de macht q verheft geeft een afbeelding $F : V \to V$, die we de *Frobenius afbeelding* noemen. Was Hasse de eerste (in 1930) die deze afbeelding formuleerde? Het is eenvoudig in te zien dat voor V gedefinieerd over $\mathbb{F}_q$ de verzameling V^F van dekpunten van F gelijk is aan $V(\mathbb{F}_q)$. Deze meetkundige formulering blijkt de sleutel te zijn tot opmerkelijke ontwikkelingen.

We gaan een verband zien met het klassieke Riemann Vermoeden, we schrijven RH, dat Riemann formuleerde in 1895 voor de Riemann zetafunctie.

In zijn proefschrift in 1921 beschrijft Emil Artin een vermoeden hoe we het aantal rationale punten op een *elliptische kromme*

over $\mathbb{F}_p$ kunnen berekenen. Niet alleen ondersteunt Artin dit vermoeden door een veertigtal voorbeelden door te rekenen, maar vooral laat Artin in zijn proefschrift zien hoe dit vermoeden een analogon is van het klassieke RH. Om mogelijke verwarring te voorkomen zal ik het vermoeden over een eindig lichaam noteren als pRH. Aanvankelijk werd pRH als even moeilijk gezien als het klassieke RH, maar vanaf 1933 gaf H. Hasse verschillende bewijzen voor het pRH voor elliptische krommen.

In 1940–1949 generaliseerde André Weil dit vermoeden tot een indrukwekkend inzicht, geformuleerd in de *Weil-vermoedens*, voor variëteiten over een eindig lichaam. Weil bewees deze vermoedens voor algebraïsche krommen van willekeurig geslacht. Daaruit zien we de (Hasse-)Weil-grens: voor een kromme C van geslacht g over $\mathbb{F}_q$ zijn de eigenwaarden van Frobenius $\pi_1,\ldots,\pi_{2g}$ algebraïsche, gehele getallen en voor elke inbedding $\mathbb{Q}(\pi)\subset\mathbb{C}$ geldt $|\pi|=\sqrt{q}$; een dergelijk getal noemen we een q-Weil-getal; met behulp daarvan is bewezen dat

$$\#(C(\mathbb{F}_q)) = 1-S+q \le 1+[2g\sqrt{q}]+q, \quad \text{met } S := \sum_{1\le j\le 2g}\pi_j.$$

Voor $g=1$ zijn deze eigenwaarden π_j óf een geheel getal, e is even, en $\pi=\pm p^{e/2}$, óf $\pi\notin\mathbb{Z}$ en de complex geconjugeerden π en $\bar\pi = q/\pi$ komen voor. Met deze informatie is het niet moeilijk om voor het geval $g=1$ alle mogelijkheden op te schrijven.

In Hoofdstuk 2 zien we hoe de Weil-grens

$$N_q(g) \le 1+[2g\sqrt{q}]+q$$

eenvoudig verscherpt kan worden tot

$$N_q(g) \le W(g) := 1+g\cdot[2\sqrt{q}]+q.$$

Bovendien, als we weten welke q-Weil-getallen $\{\pi_1,\ldots,\pi_{2g}\}$ optreden voor $C/\mathbb{F}_q$ dan zijn de q^m-Weil-getallen voor $C/\mathbb{F}_{q^m}$ precies $\{\pi_1^m,\ldots,\pi_{2g}^m\}$. Verbluffend: als we voor een elliptische kromme $E/\mathbb{F}_q$ weten wat $\#(E(/\mathbb{F}_q))$ is, dan kennen we π en q/π, en berekenen we eenvoudig het aantal $\#(E(\mathbb{F}_{q^m}))$ voor alle m.

We vermelden nog dat de Weil-vermoedens geformuleerd en gegeneraliseerd kunnen worden voor de zetafunctie van een algebra Λ van eindig type over $\mathbb{Z}$. Het geval $\Lambda=\mathbb{Z}$ geeft het klassieke RH, en is niet opgelost; de gevallen met $0=p\cdot 1\in\Lambda$ vallen onder de pRH. Een indrukwekkend aspect van twintigste-eeuwse wiskunde. Speciale gevallen zijn bewezen. Het algemene vermoeden, met daaronder het klassieke RH lijkt nog ver buiten ons bereik te liggen.

De Weil-vermoedens begonnen met de verrassende observatie van André Weil dat de formule

$$\#(C^F) = \#(C(\mathbb{F}_q)) = 1-S+q$$

lijkt op de 'dekpuntenstelling' van Lefschetz uit 1926, die het aantal dekpunten van een afbeelding $f:T\to T$ op een compacte topologische ruimte berekent als wisselsom van de sporen op de relevante homologiegroepen; een fascinerend aspect van de wiskunde van de twintigste eeuw. Vele jaren en vele pagina's prachtige, maar moeilijke wiskunde waren nodig om dit idee exact te kunnen formuleren in de algebraïsche meetkunde (welke cohomologiegroepen heb je nodig?) en te bewijzen (Weil, Grothendieck, Serre, Deligne en vele anderen). Compacte topologische ruimten enerzijds en variëteiten over een eindig lichaam anderzijds lijken begrippen die ver uiteen liggen.

We zullen zien dat de Weil-grens in veel gevallen niet bereikt wordt. Zelfs weten we niet voor gegeven $g\ge 3$ of het verschil tussen $N_q(g)$ en de Weil-grens begrensd is. Om de lezer een indruk te geven laten we een paar eenvoudige voorbeelden zien; ik hoop zo de complexiteit van het probleem duidelijk te maken.

$(g=1, q=p)$ Neem de nulpunten van $T^2+[2\sqrt{p}]T+p$; met behulp van de Honda–Tate-theorie zien we dat deze nulpunten p-Weil-getallen zijn van een elliptische kromme, en

$$N_p(1) = 1+[2\sqrt{p}]+p$$

is de Weil-grens. Een paar voorbeelden $(g=1,e=1)$: $p=2$, $\pi=-1\pm\sqrt{-1}$, $N_2(1)=5$; $p=3$, $\pi=(-3\pm\sqrt{-3})/2$,$N_3(1)=7$. Voor $p=19$ is $[2\sqrt{19}]=8$, en $\pi=-4\pm\sqrt{-3}$ geeft $N_{19}(1)=1+8+19=28$. Voor $p=23$ nemen we $\pi=(-9\pm\sqrt{-11})/2$, en $N_{23}(1)=1+9+23=33$.

Voor $N_q(1)$ met $q=p^e$, met $m=m(q):=[2\sqrt{q}]$, geeft Theorem 2.6.3:

$$q+m \le N_q(1) \le 1+m+q.$$

Meestal is m niet deelbaar door p, en de Weil-grens wordt wel bereikt door $N_q(1)$. Maar voor $p>3$ en m deelbaar door p wordt de Weil-grens niet bereikt: voor $q=2^7$ met $m=22$, $q=3^7$ met $m=93$, $q=5^9$ met $m=2795$, en $q=7^5$ met $m=259$ en $q=13^{17}$, is $m(q)$ deelbaar door p (de 'exceptionele gevallen'); in die gevallen is $N_q(1)=m+q$ en in deze gevallen wordt de Weil-grens niet bereikt. (Opgave voor de lezer: kies $p=11$; vind een oneven e zo dat $m(q)=[2\sqrt{11^e}]$ deelbaar is door 11.)

Een open probleem is het volgende: is er een priemgetal $p>7$ zo dat p een deler is van $[2\sqrt{p^5}]$? Een dergelijke p is groter dan 10^7, zie Remark 2.6.5. Een andere vraag luidt: is er voor elk priemgetal p een oneven e zo dat $m(p^e)=[2\sqrt{p^e}]$ deelbaar is door p? We geven wat nadere uitleg. Voor $q=3^7$ met $m=93$ is een nulpunt π van $T^2+93T+3^7$ wel een q-Weil-getal, π is niet een Frobeniuseigenwaarde op een elliptische kromme, maar wel een Frobeniuseigenwaarde van een abelse variëteit van dimensie 7.

We zien het onvoorspelbare gedrag van $N_q(1)$. Er lijkt geen 'algemene formule' te zijn voor $N_q(g)$.

$(g=2, q=2)$ De Weil-grens hier is $1+2[2\sqrt{q}]+2=7$; nagaan welke expliciete gevallen van 2-Weil-getallen mogelijk zijn, laat zien dat $\#(C(\mathbb{F}_2))\le N_2(2)=6$. Evenzo:

$$N_4(2) = 10 < 13 = 1+2[2\sqrt{4}]+4 = 13.$$

Voor een discussie van de waarden van $N_q(2)$ zie Theorem 3.2.3.

$(g>1, q=p^e$ met $e=2s)$ Als $\#(C(\mathbb{F}_q)) = 1+2g\cdot\sqrt{q}+q$, dan is e even en er geldt $\pi_j=-\sqrt{q}$. Dan is $\pi_j^2=q$ en uit

$$1-2gq+q^2 = \#(C(\mathbb{F}_{q^2})) \ge \#(C(\mathbb{F}_q))$$

volgt eenvoudig $2g\le q-\sqrt{q}$. We zien: voor *even* e en grote g wordt de Weil-grens $W(g)$ niet bereikt.

Over het verbeteren van grenzen op $\#(C(\mathbb{F}_q))$ is veel onderzoek gedaan. Een groot deel van het boek is besteed aan de vraag: *kunnen we een scherpe bovengrens bepalen voor het maximale aantal rationale punten $N_q(g)$ als g en q gegeven zijn*?

Coderingstheorie. Hoe kun je een bericht coderen, zodat bij kleine verstoring een verminkte code nog hersteld kan worden. Een lineaire code van type $[n,k,d]$ wordt gegeven door een lineaire deelruimte van dimensie k van de eindigdimensionale vectorruimte $V=(\mathbb{F}_q)^n$; schrijf d voor het minimale aantal niet-nulcoördinaten

in een niet-nul element van V. We zoeken codes met d en k groot (je wilt veel fouten kunnen corrigeren), en n zo klein mogelijk (je wilt kleine gecodeerde woorden). In 1970 en in 1982 liet V.D. Goppa zien hoe een kromme van klein geslacht met veel rationale punten een efficiënte lineaire code geeft. Voor een beschrijving zie § 1.2, pp. 2–4, in het boek. We gebruiken graag $\mathbb{F}_2$ als grondlichaam.

In 1981 bespreekt Yu.I. Manin "What is the maximum number of points on a curve over $\mathbb{F}_2$?" Is dit een moeilijk probleem? Voor wie dit onderwerp niet kent: probeer het maar eens voor $g = 7$ over $\mathbb{F}_2$; de Weil-grens geeft

$$N_2(7) \leq 1 + 7 \cdot [2\sqrt{2}] + 2 = 17.$$

We laten zien hoe $N_2(7)$ bepaald wordt (en we zien dat het een lastig probleem is).

We zien dat $N_2(g)$ momenteel berekend is voor slechts 17 waarden van g, zie Table 2 op pagina 169.

In 1972/1975 werd de Gilbert–Varshamov-grens geformuleerd, ook wel bekend als de Gilbert–Shannon–Varshamov-afschatting. Ik weet nog hoe het een schok was toen in 1982 M.A. Tsfasman, S.G. Vlădut en Th. Zink lieten zien dat de methode van reductie modulo p van modulaire krommen en van Shimura-variëteiten een verscherping van de GV-grens geeft. Ideeën, standaard in het ene vak, waren plotseling relevant in een heel andere tak van wiskunde.

Nu richten we ons op algemene methoden. Een *abelse variëteit* is een projectieve algebraïsche variëteit A waarvan de punten een groep vormen. In het werk van Abel komen punten op sommige A voor als waarden van een bepaalde integraal van een differentiaalvorm op een Riemann-oppervlak, vandaar de naam. Zo zien we dat elke kromme C van geslacht g aanleiding geeft tot een abelse variëteit $A = \mathrm{Jac}(C)$ van dimensie g. Vaak geeft meetkunde van $\mathrm{Jac}(C)$ waardevolle informatie over C. Over de constructie van $C \mapsto \mathrm{Jac}(C)$ en uitwisseling van eigenschappen van C en van $\mathrm{Jac}(C)$ bestaat veel literatuur.

T. Honda en J.T. Tate lieten in 1986 zien dat voor elk q-Weil-getal π er een abelse variëteit A over $\mathbb{F}_q$ bestaat waarvan π een eigenwaarde van de Frobenius $\mathrm{Frob}_{A/\mathbb{F}_q} = F_A : A \to A$ is. Tate liet in 1966 zien hoe aritmetische eigenschappen van π invarianten van A bepalen, waaronder de dimensie van A. Een krachtig hulpmiddel om langs deze weg abelse variëteiten over een eindig lichaam te construeren. Die algemene stelling, de Honda–Tate-theorie, is goed begrepen.

Hoe kunnen we dit gebruiken om krommen te vinden met veel rationale punten? Voor $g \leq 3$ 'komt elke abelse variëteit af van een kromme'; echter, voor $g > 3$ zijn er 'veel meer' abelse variëteiten dan algebraïsche krommen.

Hoe zien we welke π met $|\pi| = \sqrt{q}$ gerealiseerd wordt door een kromme? 'General theorems' zoals Serre dat noemt in zijn voorwoord, zijn voor dit geval niet direct toepasbaar in het probleem van rationale punten op krommen van geslacht $g > 3$. En, zoals Serre het formuleert in zijn introduction: "When one reads Mumford's booklet *Curves and their Jacobians*, one realizes the sad fact that we have 'no reasonable effective way' to describe the curves with ... a large genus."

Bijvoorbeeld, hoe krijgen we expliciete informatie over 'alle' krommen van geslacht 7 over $\mathbb{F}_q$, die we zouden kunnen gebruiken om $N_q(7)$ te bepalen? We zullen zien dat reeds voor $q = 2$ dit een lastig probleem is. We zien diepe, algemene stellingen en constructies die wel bovengrenzen, echter niet een formule voor $N_q(g)$ lijken te geven, het beginpunt van dit boek.

We geven een korte samenvatting van (een deel van) de inhoud van dit boek. Algemene methoden geven niet in alle gevallen de scherpste grenzen voor het maximale aantal rationale punten $N_q(g)$. Betere grenzen worden bestudeerd met behulp van *meetkunde* (van algebraïsche krommen), met behulp van *getaltheorie* (eigenschappen van Weil-getallen), en met behulp van methoden uit de *analytische getaltheorie* (zie Hoofdstuk 6). We zien dat een merkwaardige en ingenieuze mix van deze methoden verscherpingen van bestaande grenzen geeft. In een aantal gevallen geven constructies van expliciete voorbeelden aan dat die scherpe bovengrens ook gerealiseerd wordt; in die gevallen wordt $N_q(g)$ bepaald.

Vaak wordt de vraag naar het aantal rationale punten op twee manieren gesteld: óf kies g vast en laat alle mogelijke $q = p^e$ toe, óf kies q vast en bestudeer alle mogelijke g. Beide benaderingen vinden we hier terug. Serre behandelde deze twee onderwerpen op twee verschillende dagen in zijn college.

In het eerste deel worden 'kleine' g bestudeerd. We zien, Hoofdstuk 2, dat voor $g = 1$ resultaten bekend zijn (Deuring, Waterhouse, Tate). Extra aandacht voor de gevallen waar de verscherpte Weil-grens bereikt wordt (storende drukfout op pagina 24: "voor $q = p^e = 2^3$ is p een deler van $m := [2\sqrt{q}]$": we zien $[2\sqrt{8}] = 5$).

Voor $E/\mathbb{F}_q$ schrijven we $E'/\mathbb{F}_q$ voor de kwadratische $\mathbb{F}_{q^2}/\mathbb{F}_q$-twist van E. Voor maximale $E/\mathbb{F}_q$ is $E'/\mathbb{F}_q$ minimaal (storende drukfout in de vijfde regel van 2.6.5). Zo zien we dat hier 'algemene stellingen' mooie antwoorden geven.

In Hoofdstuk 3 worden allerlei algemene methoden ontwikkeld, en wordt het geval $g = 2$ besproken. Resultaten over $N_q(2)$ bewees Serre in 1982 en 1983 (zie vooral ook de brieven hierover van Serre aan Tate). Het resultaat, Theorem 3.2.3, bespreekt alle gevallen; in het bijzonder geldt voor $g = 2$:

$$\big(1 + 2 \cdot [2\sqrt{q}] + q\big) - N_q(2) \leq 3;$$

we zien dat voor $g = 2$ de waarde $N_q(2)$ weinig afwijkt van de Weil-grens. Het bewijs in dit boek van deze stelling bestaat uit een bespreking van algemene methoden en de bestudering van bijzonder gevallen en het kost veertig bladzijden. Dit geeft een mooi beeld van de moeilijkheden in dit onderwerp: dit geval van een kleine g, waar bovendien elke abelse variëteit van dimensie 2 'afkomstig' is van een kromme vergt al zoveel inspanning om tot een complete beschrijving van $N_q(g)$ te komen.

Hoofdstuk 4 bespreekt $g = 3$. Voor $q \leq 29$ geeft het boek een tabel voor de exacte waarde van $N = N_q(3)$. Jaap Top beschreef in 2003 alle gevallen $g = 3$ en $q < 100$. Hier helpt de meetkunde: we weten dat elke kromme C van geslacht drie óf hyperelliptisch is óf dat de kanonieke afbeelding $C \to \mathbb{P}^2$ een isomorfisme geeft met een vlakke kromme van graad 4. In dit laatste geval spelen (een twist) van de Klein-kromme, nulpunten van $X^3Y + Y^3Z + Z^3X$, en (een twist) van de Fermat-kromme, nulpunten van $X^4 + Y^4 + Z^4$ in $\mathbb{P}^2(\mathbb{F}_q)$, een belangrijke rol bij het vinden van voorbeelden. In Conjecture 4.3.1 wordt gevraagd of

$$\big(1 + 3 \cdot [2\sqrt{q}] + q\big) - N_q(3)$$

begrensd is, misschien wel ≤ 6 voor $g = 3$ en alle q? Uit het eerste deel van het boek zien we: een 'algemene formule' die $N_q(g)$ geeft lijkt niet te bestaan, zelfs niet voor kleine g.

In een serie van artikelen en tabellen vanaf 1993 geven Gerard van der Geer en Marcel van der Vlugt een grote hoeveelheid schattingen van $N_q(g)$ en krommen met het maximale aantal rationale punten.

Deel twee van dit boek beschrijft algemene methoden voor grote g. Algemene methoden worden ontwikkeld, en allerlei expliciete voorbeelden geconstrueerd. Uit het rijke palet van technieken en resultaten noem ik een paar aspecten.

Hoofdstuk 7 is gewijd aan een poging om de vraag van Manin "What is the maximum number of points on a curve over $\mathbb{F}_2$?" te beantwoorden. Hier is $q=2$ vast, maar we beschouwen 'alle' g. Om een indruk te geven van technieken en resultaten neem ik over uit het boek de gevallen $g=7$, $g=50$ en $g=120$ met grondlichaam $\mathbb{F}_2$.

In Hoofdstuk 5, en in Hoofdstuk 6 met methodes hoofdzakelijk ontwikkeld door J. Oesterlé, vinden we een indrukwekkende hoeveelheid techniek, die culmineert in het vinden van veel scherpere grenzen op $N_2(g)$. Dat is de ene kant van de benadering van het probleem. We zien bij voorbeeld, een combinatie van allerlei schattingen: $N_2(7)\leq 11<17$, $N_2(50)\leq 40<103$, $N_2(120)\leq 82<243$, aanzienlijke verscherpingen van de Weil-grens gegeven door $1+g\cdot[2\sqrt{2}]+2=2g+3$.

Nu komt de andere benadering van het probleem: het bestaan van voorbeelden met 'veel' rationale punten. Voor $g=7$ wordt er bewezen dat er *wel* een kromme C over $\mathbb{F}_2$ bestaat met $N(C)=10$, zie 7.3.5, zie een discussie verderop, maar er bestaat *niet* een kromme C van geslacht 7 over $\mathbb{F}_2$ met $N(C)=11$, zie 7.2; omdat de Oesterlé-grens bewijst dat $N_2(7)\leq 11$ krijgen we de conclusie: $N_2(7)=10$. Kortom: een lastige schatting en een gecompliceerd voorbeeld geven samen een bewijs dat $N_2(7)=10$. De lezer krijgt bij het bepalen van $N_2(7)$ een beeld van de complicaties van dit probleem.

Voor $g=50$ wordt bewezen dat er een C bestaat met $N(C)=40$; we komen hier op terug; conclusie: $N_2(50)=40$. De schattingen geven $N_2(120)\leq 82$, en het is onbekend wat $N_2(120)$ precies is.

Als antwoord op de vraag van Manin zien we dat een algemene uitspraak over de waarde van $N_g(2)$ voor slechts zeventien waarden van g bekend is.

Twee relevante meetkundige technieken.

(1) *'Plakken' van algebraïsche krommen,* zie § 3.3 en § 4.2. Laat ik een voorbeeld geven. Neem elliptische krommen E_1 en E_2 over een lichaam van karakteristiek ongelijk 2, beschouw $\varphi_1: E_1\to\mathbb{P}^1=S$ van graad twee, vertakt in vier punten, en idem $\varphi_2: E_2\to\mathbb{P}^1=S$. Kies coördinaten op $\mathbb{P}^1$ zo dat drie vertakkingspunten van φ_1 en drie van φ_2 boven eenzelfde punt op $\mathbb{P}^1$ liggen en de andere vertakkingspunten boven twee verschillende punten van $\mathbb{P}^1$. De kromme $C:=E_1\times_S E_2$ is een kromme van geslacht twee; eigenschappen van C kunnen afgelezen worden uit eigenschappen van E_1 en E_2. Deze methode, besproken in § 3.3 en § 4.2, geeft een rijk arsenaal aan nieuwe voorbeelden.

(2) *Klasselichamentheorie voor algebraïsche krommen.* In 1959 beschreef Serre deze methode over een algebraïsch gesloten grondlichaam, en in Hoofdstuk 5 vinden we hier een verdere uitleg. Een kromme Y wordt gegeven, en een abelse overdekking $X\to Y$ wordt geconstrueerd, waar de Galois-groep en een (mogelijk vertakte) overdekking gekozen wordt. Eigenschappen van Y en van de overdekking X/Y geven toegang tot eigenschappen van X.

Laat ik als voorbeeld geven de constructie van $g(C)=7$ over $\mathbb{F}_2$ met $N(C)=10$, zie Table 2, pagina 160. Kies een elliptische kromme E over $\mathbb{F}_2$ met een punt $Q\in E(\mathbb{F}_{2^6})$ zo dat dit een gesloten punt $Q_6\subset E/\mathbb{F}_2$ geeft van graad 6 en kies $C\to E/\mathbb{F}_2$ met $\mathrm{Gal}(C/E)=\mathbb{Z}/2$ met vertakking in $2Q_6$ zodat er precies $n=5$ rationale punten op E totaal splitsen in C/E; zo komt er $N(C)=10$; zie Case 2 van 7.3.5 op pagina 169. De Riemann–Hurwitz-formule geeft $2g-2=2(2-2)+2.6.(2-1)$, dus $g(C)=7$. We weten al $N_2(7)\geq 10$; conclusie: $N_2(7)=10$.

Voor $g=50$ wordt een keuze gemaakt met een elliptische kromme E, met $2Q_7\subset E$, en $\mathrm{Gal}(C/E)\cong(\mathbb{Z}/2)^3$ met $n=5$. Een berekening levert $g(C)=50$ en $N(C)=8\cdot 5=40$; conclusie: $N_2(50)=40$.

Dit boek laat me weer nadenken over de manieren van wiskundig denken en werken. Een simplificatie: als we een probleem proberen op te lossen, dan kunnen we óf algemene methoden ontwikkelen, óf zoveel concreet materiaal (voorbeelden) beschrijven dat we 'zien' wat de oplossing is. Grothendieck was een voorbeeld van de eerste methode: generaliseer een probleem, en los dat dan op; er is veel mee bereikt, en velen van ons vinden dat de juiste manier van werken.

Maar wat te doen als algemene methoden niet een antwoord geven? Ik ken gevallen waar de algemene aanpak leek te falen, maar waar concrete informatie in de vorm van voorbeelden ons liet zien hoe het probleem wel op te lossen is.

Andrew Wiles zegt in een beschrijving van zijn zoektocht naar een bewijs van de Laatste Stelling van Fermat: "Perhaps I could best describe my experience of doing mathematics in terms of entering a dark mansion. One goes into the first room, and it's dark, completely dark. One stumbles around bumping into the furniture, and gradually, you learn where each piece of furniture is, and finally, after six months or so, you find the light switch. You turn it on, and suddenly, it's all illuminated. You can see exactly where you were."

Dit boek geeft een voorbeeld hoe je verder kunt gaan als algemene methoden niet lijken te werken: doorrekenen van speciale gevallen, voorbeelden maken, verschillende technieken combineren. Toepassingen in de coderingstheorie zijn in dit geval het resultaat. Maar ik vraag me af of we wel de goede vragen stellen in het probleem van aantallen rationale punten over een eindig lichaam.

Ook hebben we in het verleden gezien dat methoden uit het ene vakgebied soms een verrassend inzicht geven in een andere tak van wiskunde. De manier waarop Weil de Lefschetz dekpuntenstelling gebruikte als bron van inspiratie is daar een voorbeeld van. Een ander voorbeeld is het inzicht dat Deligne kreeg bij het lezen van een artikel van Rankin: het bleek de sleutel te geven voor het vinden van een bewijs van de Weil-vermoedens.

In een prachtig interview met Elisa Lorenzo García en Christophe Ritzenthaler vertelt Serre hoe het vergelijken van de discriminant $\mathrm{discr}(K/\mathbb{Q})$ en de graad $[K:\mathbb{Q}]$ van een algebraïsch getallenlichaam K leidt tot interessante beschouwingen (en hoe Serre en Hendrik Lenstra daar een interessante briefwisseling over hebben: maak K met kleine discriminant en grote graad); er is een analogie met geslacht — aantal rationale punten op een algebraïsche kromme over een eindig lichaam. Dit was een van de motivaties om aan dit onderwerp te gaan werken; voor een uitleg zie Remark 5.3.1 van het boek.

Conclusie. Een prachtig boek. Het plezier in wiskundebeoefening straalt je tegemoet. Een bron van inspiratie. *Frans Oort*

Jan Guichelaar, Paul Levrie, Roosmarij Vanhommerig

De dikke pythagoras

Lannoo, 2020
304 p., prijs € 19,99
ISBN 9789401471831

Zoals u op de foto rechtsonder ziet, liggen diverse jaargangen vanaf het begin van de jaren zestig op tafel. De eerste twee jaargangen ontbreken. De derde jaargang komt overeen met het jaar dat ik in de derde klas zat van de hbs. Dat was het schooljaar 1963–64. Vanaf die tijd heb ik het redelijk compleet. Hier en daar ontbreekt een nummer. Van sommige bezit ik meerdere exemplaren.

Wat opvalt is dat de zevende jaargang geheel oranje gekleurd is. Waarom? Ik weet het niet. Als leerling heb ik geworsteld, soms nu nog, met de opgaven in *Pythagoras*, als wiskunde-natuurkundestudent begon ik het belang van het tijdschrift in te zien en werd ik gebiologeerd door een artikel waarin een schaakbord binnenstebuiten (inversie) wordt gekeerd. *Pythagoras* heb ik tijdens mijn werk als docent ervaren als een grote rijkdom. Ik heb er vaak opgaven voor mijn lessen of testen uitgehaald. Het tijdschrift, met lezers en auteurs zowel in Nederland als België, bestaat zestig jaar zoals u waarschijnlijk weet. De redactie van nu laat ons weten dat zestig voor hen belangrijker is dan vijftig. Waarom? Het oude Babylonië (rond 3000 v. Chr.) wordt beschouwd als de geboorteplaats van de wiskunde en de Babyloniërs gebruiken een talstelsel op basis van 60. Ondertussen zijn er al meer dan 360 nummers van het tijdschrift uitgebracht. Toch was 2011 ook een mijlpaal, ter gelegenheid waarvan het boek *De Pythagoras Code* werd uitgebracht. Dit boek werd al een schatkamer genoemd. Denkertjes, puzzels, spellen, maar ook de nodige artikelen over geschiedenis van de wiskunde, meetkunde, getallen en op het eind van het boek de oplossingen.

Vergeleken met de speciale uitgave uit 2011 is *De dikke pythagoras*, 303 pagina's rijk, sowieso fysiek van een ander formaat maar ook van een andere opzet. Foto's zul je er niet in aantreffen, maar wel grappige, gekleurde tekeningen. Ook dit boek bevat geen echte artikelen, maar naast de talloze puzzels en problemen (601) — net als in *Pythagoras* wordt de moeilijkheidsgraad met 1, 2 of 3 bolletjes aangegeven — heel veel 'Wist je dit' of 'Wist je dat' wiskundige weetjes. Er wordt dan een probleem uit de doeken gedaan waarvan niet altijd de oplossing wordt gegeven. Dat zet aan tot echt denken en puzzelen. Overigens van veel problemen — meetkundig van aard, bord-roosterpuzzels, getal- en rekenpuzzels, verdeelproblemen, kans- en telproblemen, logische problemen — staan de oplossingen achterin, deel 2 van het boek. Liefst 87 pagina's zijn er voor uitgetrokken. Vaak zijn de uitwerkingen van een tekening voorzien. Ook wordt jaargang en nummer van de *Pythagoras* vermeld waar de opgave vandaan komt. De naam van de ontwerper van een opgave wordt niet genoemd. In die zestig jaar is er een keur van redacteuren en (vaste) medewerkers aan de slag gegaan. Op pagina 9, en dat schrijven we als $-1+12-2$, staat een trots overzicht. U zult er heel wat bekende namen aantreffen, zoals van een van de oprichters Bruno Ernst (pseudoniem van Hans de Rijk), auteur van heel veel wiskundeboeken en artikelen. Hij schreef ruim 250 werken. Een bekende uitspraak van hem is: "Ik weet niets maar ben nieuwsgierig naar alles." Ik beschouw het als een van de fundamenten van dit tijdschrift.

Hier een greep van drie puzzels in bolletjesvolgorde. Voor elk wat wils. We beginnen met opgave (136) die van één bolletje is voorzien. "Boer Japiks fokte kippen met vreemdsoortige eieren, soms met 1 dooier, soms met 2 dooiers en dan weer zonder dooier. Boer Japiks hield hiervan een boekhouding bij, maar na het 5000ste ei raakte hij zijn gegevens kwijt. Hij herinnerde zich alleen nog dat de meeste van de eieren slechts 1 dooier bevatten en precies de helft van de resterende eieren 2 dooiers had. Hoeveel dooiers zaten er in totaal in deze 5000 eieren?"

De auteurs schrijven in de inleiding dat de *éénbolletjesopgaven* met gezond verstand en eenvoudig rekenwerk op te lossen zijn. Ik zou zelf willen toevoegen: "Eerst heel goed lezen en dan een schetsje maken."

Kijken we naar pagina 60, het wordt genoteerd als $(1+1+2)*((2+3)*3$, dan zien we in opgave 140, een *tweebolletjesopgave*, het 'Zes Gelijke Gebieden probleem'. Jawel, het getal 6 speelt weer een rol. Bij dit soort opgave kan wiskundekennis uit de onderbouw nodig zijn. Je moet een driehoek tekenen met zijn drie zwaartelijnen. Er wordt meegedeeld dat de zwaartelijnen door één punt gaan (kennis onderbouw). Er staat een tekening van de driehoek bij. Ik noem de driehoek: $\triangle ABC$. De drie zwaartelijnen verdelen $\triangle ABC$ in zes kleinere driehoeken. Je moet nu aantonen dat de zes driehoeken dezelfde oppervlakte hebben. Achter in het boek staat een uitwerking met tekening. Soms zou je willen dat er meer strategieën worden gegeven. Maar misschien moet dat toch maar de taak van de docent blijven.

Op pagina 206 ($=(11-2)\times 23\times(-3+4)$) hebben we een van de *driebolletjesopgaven*. Volgens de auteurs vergt zo'n opgave

goed inzicht en denk- en/of puzzelwerk. Maar ook wiskunde uit de bovenbouw. De titel van opgave 577 luidt: 'Allemaal vierkanten'. Het gaat om een serie steeds kleiner wordende vierkanten die op eenzelfde basislijn staan. Het grootste vierkant heeft zijde 1. Als je naar rechts gaat, is elk vierkant half zo hoog als het vorige. De linkeronderhoek ligt steeds op twee derde deel van de onderzijde van het vorige vierkant. Bepaal de totale oppervlakte van het gebied dat door de vierkanten wordt bedekt.

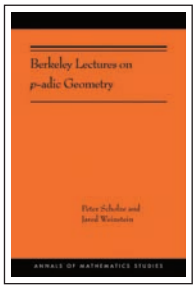
De opgave komt uit een *Pythagoras* van februari 2017. Het gaat om nummer 4 van de 56ste jaargang. Er is in dat nummer een mooie afbeelding toegevoegd. Je ziet zeven verschillend gekleurde vierkanten. In het boek moeten we het doen met één kleur en zes vierkanten, maar de afbeelding is veel groter. Ook de hoekpunten rechtsboven van de vierkanten zijn met een stippellijn verbonden. En dat maakt een verschil. Dat ziet u zo.

Op pagina 73 vind je een van de aardigste puzzels van 'Wist je dat'. Het 'Probleem van Leuven' verscheen in 1914, het beginjaar van de Eerste Wereldoorlog en wel in het Britse tijdschrift *The Strand*. Dat magazine kreeg bekendheid door de publicatie van de verhalen van Sherlock Holmes. Van zijn detectivewerk is ook veel verfilmd. Maar nu het huisnummerprobleem. De tekst luidt als volgt: "'I was talking the other day,' said William Rogers to the other villagers gathered round the inn fire, 'to a gentleman about that place called Louvain, what the Germans have burnt down. He said he knowed it well — used to visit a Belgian friend there. He said the house of his friend was in a long street, numbered on his side one, two, three, and so on, and that all the numbers on one side of him added up exactly the same as all the numbers on the other side of him. Funny thing that! He said he knew there was more than fifty houses on that side of the street, but not so many as five hundred. I made mention of the matter to our parson, and he took a pensil and worked out the number of the house where the Belgian lived. I don't know how he done it.' Perhaps the reader may like to discover the number of that house."

Dit is een probleem waarbij de meeste leerlingen halverwege zullen stagneren. Maar is dat erg? Mag er geworsteld worden? Met wat gereken met rekenkundige rijen kom je wel bij de oplossing, maar een sluitend bewijs vinden is niet zo simpel. Bij deze opgave is achterin het boek geen uitwerking te vinden. Is dat erg? Natuurlijk niet, maar het zou toch heel leuk zijn als de lezer zijn of haar pogingen zou doorsturen naar de redactie. Het zou weer een mooi artikel kunnen opleveren.

Het is niet geheel duidelijk voor wie dit boek geschreven is. In het voorwoord richt men zich niet meteen tot de leerling. De leraar functioneert nu als intermediair. Sommige opgaven zouden in een college 'Probleem Oplossen' of bij 'Wiskundige Denkactiviteiten' goede diensten kunnen bewijzen. Er zijn veel puzzels met verschillenden oplossingsstrategieën. En dat maakt het zo boeiend. Je lost het op en ziet achteraf een elegantere aanpak. Dat noem ik winst en rijkdom. Maar sommige aanpakken staan ver weg van de leerling. Jammer dat je niet echte leerlingenuitwerkingen ziet. Al waren er maar een paar van afgedrukt. Kwam ik bij dit boek doorwerken omissies tegen? Op bladzijde 115 moeten acht koninginnen op het schaakbord staan. Die staan er ook, maar vier ervan zijn op het zwarte vlakje nauwelijks te zien! Op pagina 155 onderaan moet staan 'Wist je dat 4 april(4–4), enz.'

Ten slotte wil ik nog even de verdienste vermelden van Matthijs Wielders, oud-docent van de Open Universiteit, met wie ik de ervaringen van het maken van diverse opgaven heb uitgewisseld. *De dikke pythagoras* hoort sowieso in de mediatheek van een school maar hoort ook in de boekenkast van elke wiskundedocent naast *De Pythagoras Code* te staan. Naast dit boek zou ook een bundeling van de zestig interessantste artikelen en de zestig mooiste of opvallendste uitwerkingen van leerlingen uit de ruim 360 nummers niet misstaan. *Jacques Jansen*



Peter Scholze, Jared Weinstein

Berkeley Lectures on p-adic Geometry

Princeton University Press, 2020
x + 250 p., prijs $75.00
ISBN 9780691202082

Dit boek is gebaseerd op een college dat Scholze — toen 26 jaar oud — in het najaar van 2014 gaf in Berkeley. Het onderwerp was p-adische meetkunde. Dit speelt een grote rol in de aritmetische meetkunde omdat het de brug slaat tussen meetkunde over lichamen van karakteristiek 0 en van karakteristiek p. Er is dan ook een lange lijst met belangrijke resultaten waarin p-adische meetkunde een rol speelt.

Twee jaar eerder was Scholzes zeer invloedrijke artikel over perfectoïde ruimten verschenen. Je zou kunnen denken dat zijn college in Berkeley gewijd was aan een uitleg van die moeilijke theorie. Niet dus. Een van de fascinerende aspecten van Scholzes werk is dat hij bezig is met een groot programma en dat hij het vermogen heeft om zich, ondanks de soms meer dan formidabele technische obstakels, met mokerslagen een weg vooruit te banen. Het hoofdthema van dit boek is niet de theorie van perfectoïde ruimten maar een wezenlijke uitbreiding daarvan, die gaat over zogenoemde 'diamonds'. Kort gezegd zijn dergelijke diamanten quotiënten van perfectoïde ruimten onder equivalentierelaties, ongeveer zoals algebraïsche ruimten quotiënten zijn van schema's.

Deze theorie is niet ontwikkeld om er maar een beetje op los te generaliseren maar met een helder doel. Een van de spraakmakende ontwikkelingen van de laatste jaren is een door Fargues en Fontaine ontwikkelde totaal nieuwe visie op p-adische Hodgetheorie en de daarop gebaseerde 'geometrisatie' van het lokale Langlandsvermoeden door Fargues en Scholze. Het komt erop neer dat resultaten uit de p-adische Hodgetheorie, die voorheen gebaseerd waren op Fontaines 'periodenringen' (die niet erg intuïtief zijn), nu geïnterpreteerd kunnen worden als uitspraken over vectorbundels op een kromme — de 'Fargues–Fontaine-kromme', soms gewoon 'la courbe' genoemd. De grote winst is hier vooral dat dingen veel conceptueler worden gemaakt. Bovendien blijken ideeën te kunnen worden overgenomen uit het bewijs van het locale Langlandsvermoeden in karakteristiek p (V. Drinfeld, L. Lafforgue) en uit het meetkundige Langlandsprogramma. Voorlopig hoogtepunt hierin is het recente werk van Fargues en Scholze, dat voor willekeurige reductieve groepen over p-adische locale lichamen een zeer conceptuele meetkundige manier geeft om aan gladde irreducibele representaties L-parameters te associëren.

De interpretatie van ‘la courbe’ als een diamant speelt hierin een belangrijke rol.

Prachtige wiskunde, en het einde van al deze ontwikkelingen is nog lang niet in zicht. Het is wel verschrikkelijk technisch allemaal en wie bij wil blijven heeft al snel een enorme stapel literatuur op zijn bureau liggen. (Alleen al Fargues–Fontaine en Fargues–Scholze is zo’n 750 pagina’s.) Fijn dus wel dat er ‘lecture notes’ zijn waar je een begin mee kan maken. Deze Berkeley Lectures zijn uitgewerkt door Scholze samen met Jared Weinstein. De stijl is meer die van ‘lecture notes’ dan die van een definitieve tekst, en voor preciezere technische details is een andere tekst van Scholze (weer 165 pagina’s erbij…) de aangewezen bron. De lezer wordt in hoog tempo door de theorie geloodst maar door de grote nadruk op de intuïtie en motivatie is dit boek een heel nuttige toevoeging aan de literatuur. Als preprint was deze tekst al langer beschikbaar maar juist in een veld dat zich explosief ontwikkelt is het fijn om ook in boekvorm wat steunpunten te hebben op de steile weg omhoog.

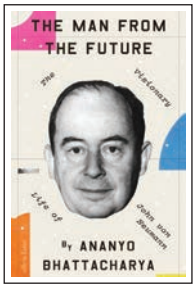
Ben Moonen

Recent verschenen publicaties. Als u een van deze boeken wilt bespreken of als u suggesties heeft voor andere boeken voor deze rubriek, laat dit dan per e-mail weten aan reviews@nieuwarchief.nl.

Edward van de Vendel, Ionica Smeets

Rekenen voor je leven

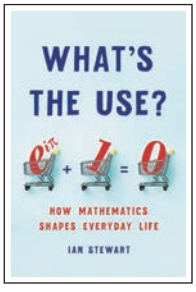
Uitgeverij Nieuwezijds, 2021
ISBN 9789057125188
nieuwezijds.nl/boek/rekenenvoorjeleven



Ananyo Bhattacharya

The Man from the Future
The Visionary Life of John von Neumann

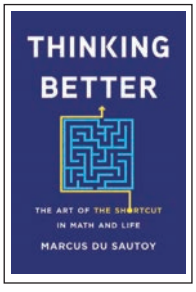
Penguin books, Imprint Allen Lane, 2021
ISBN 9780241398852
penguin.co.uk/books/313/313705/the-man-from-the-future/9780241398852.html



Ian Stewart

What’s the Use?
How Mathematics Shapes Everyday Life

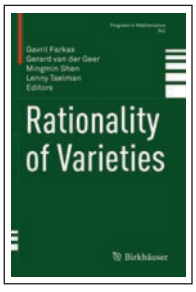
Basic Books, 2021
ISBN 9781541699489
basicbooks.com/titles/9781541699489



Marcus Du Sautoy

Thinking Better
The Art of the Shortcut in Math and Life

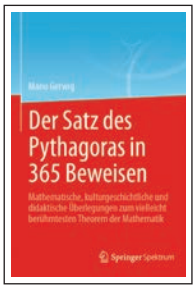
Basic Books, 2021
ISBN 9781541600362
basicbooks.com/titles/9781541600362



Gavril Farkas, Gerard van der Geer, Mingmin Shen, Lenny Taelman

Rationality of Varieties

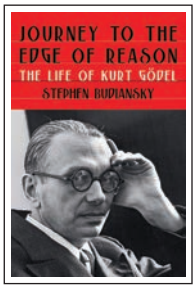
Birkhäuser, 2021
ISBN 9783030754204
springer.com/978-3-030-75420-4



Mario Gerwig

Der Satz des Pythagoras in 365 Beweisen

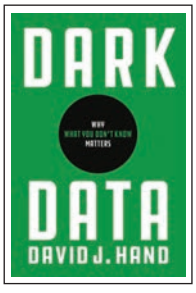
Springer, 2021
ISBN 9783662628850
springer.com/978-3-662-62885-0



Stephen Budiansky

Journey to the Edge of Reason
The life of Kurt Gödel

W. W. Norton & Company, 2021
ISBN 9781324005445
wwnorton.com/books/9781324005445



David J. Hand

Dark Data
Why What You Don’t Know Matters

Princeton University Press, 2022
ISBN 9780691234465
press.princeton.edu/books/paperback/9780691234465/dark-data