Priemgetallen

Frans Oort

november / december 2013

HOVO-cursus wiskunde Utrecht

· · · prime numbers "grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout." Don Zagier

Inhoudsopgave.

Inleiding

Till now the mathematicians tried in vain to discover some order in the sequence of the prime numbers and we have every reason to believe that there is some mystery which the human mind shall never penetrate. To convince oneself, one has only to glance at the tables of primes which some people took the trouble to compute beyond a hundred thousand, and one perceives that there is no order and no rule. This is so much more surprising as the arithmetic gives us definite rules with the help of which we can continue the sequence of the primes as far as we please, without noticing, however, the least trace of order.

So wrote Euler about two centuries ago, yet the prime numbers may inspire the contemporary mathematician with the same feeling of mystery that Euler so vividly expressed.
Euler, twee eeuwen geleden. Zie [67].

Zo vaak zeggen mijn vrienden en kennissen dat ze graag wat meer over wiskunde willen weten en horen. Maar hoe kan ik dat doen op een bevattelijke manier zonder de waarheid geweld aan te doen? Al werkend aan deze cursus merk ik dat er inderdaad veel is wat op een begrijpelijk niveau de fascinerende schoonheid van wiskunde kan laten zien.

"Wat me trof in al mijn gesprekken met hen was de buitengewone nauwkeurigheid waarmee ze zich uitdrukten ... de precieze opbouw van het antwoord ... dat wiskundigen domweg een hekel hebben aan het doen van een onware uitspraak ... " Zie [78] pagina 12.

Iets uitleggen wil ik doen op een wiskundig juiste manier. Zo vaak wordt er in onze wereld populariserend geschreven en gesproken (daar heb ik niets op tegen). Maar de grens wordt overschreden als we daarbij onware uitspraken doen. En dit gehoor zal dat ongetwijfeld als storend ervaren.

Nadenken loont. – Ik denk dat materiaal van deze cursus kan worden uitgelegd aan iedereen die bereid is na te denken, ongeacht de voorkennis.

In deze cursus bestuderen we *priemgetallen*. We zijn vooral geïnteresseerd in de vraag

"hoeveel priemgetallen zijn er, en waar liggen ze"?

Die vraag zullen we eerst precies maken voor we er iets mee kunnen beginnen. Voor allerlei notaties, en voor definities, zie § 2.

(0.1) Definitie. Voor elke $x \in \mathbb{R}$ definiëren we $\pi(x)$ voor het aantal priemgetal dat kleiner dan of gelijk aan x is:

$$\pi(x) := \#\left(\{p \mid p \text{ is een priemgetal, } p \leq x\}\right);$$

$\#(V)$ staat voor het aantal elementen in de verzameling V.

Dit is een "trap-functie": voor $0 < x < 2$ is $\pi(x) = 0$; dan springt die functie naar $\pi(2) = 1$; voor $2 \leq y < 3$ geldt $\pi(y) = 1$, etc.; soms zijn er stapjes 1 omhoog vlak na elkaar, maar soms zijn er grote intervallen waar de functie constant is. Kunnen we iets zinnigs zeggen over deze grillige functie? Zie het artikel [93], waar plaatjes in staan:

één grafiek geeft $\pi(x)$ voor $x < 100$,
en we zien een grillig verloop: duidelijk een *trapfunctie*;

de andere grafiek geeft $\pi(x)$ voor $x < 50,000$
en het *lijkt* of $\pi(x)$ een *gladde functie* is.

Dat geeft de suggestie dat je over het globale gedrag van $\pi(x)$ wel degelijk iets kunt zeggen; dat werd vermoed door Gauss, maar door hem nooit gepubliceerd; uit een aantekening die hij maakte in zijn logaritme tabel toen hij 15 of 16 was:

"Im Jahr 1792 oder 1793 $\cdots$ Primzahlen unter $a(=\infty)\frac{a}{\ln(a)}$",

zoals hij in 1849 aan zijn vriend Encke schreef, zie [29]. Ook werd dit vermoed door Legendre in 1797/1798. Dat resultaat, de priem-getal-stelling (Prime Number Theorem, we korten het af als PNT), werd bewezen door Chebyshev, Hadamard en de la Vallée-Poussin (resultaten gepubliceerd in de periode 1848 - 1896). Het is een verbluffende (en ook diepe) stelling:

we weten vrij nauwkeurig hoeveel priemgetallen er liggen
(beneden een bepaalde grens, in een gegeven interval)
zonder dat we die priemgetallen zelf kennen.

Zo kunnen we het bestaan van priemgetallen met een bepaalde eigenschap bewijzen, kunnen we vrij nauwkeurig afschatten hoeveel priemgetallen er op een gegeven (groot) interval liggen. In § 10 citeren we dat resultaat (zonder dat we een bewijs geven van deze diepe stelling). Bovendien blijken er ook heel bruikbare, zwakkere vormen van die stelling te bestaan die bovendien wel heel eenvoudig te bewijzen zijn.

(0.2) Wat is de structuur achter de vraag ? Ik begin met het formuleren met een paar vragen. Probeer vooral om bij elke vraag te beslissen of u die vraag begrijpt, en of een antwoord gemakkelijk is of niet. Het zal blijken dat sommige vragen een heel eenvoudig te bewijzen antwoord hebben, terwijl andere vragen moeilijk en nog steeds onopgelost zijn.

Dit is kenmerkend voor het beoefenen van de wiskunde: een vraag stimuleert de nieuwsgierigheid. Soms zeg je al gauw "ja, natuurlijk dat is eenvoudig". Dan weer is er een "eenvoudige vraag", maar hoe meer je erover nadenkt, steeds verder lijkt een oplossing te liggen.

We zullen zien dat (veel) rekenen soms wel inzicht geeft (soms ook de verkeerde suggestie, zie § 16), en dat nadenken en het toepassen van abstracte methodes vaak verbluffende resultaten geeft.

Wiskundigen proberen de structuur te vinden die achter een vraag ligt. De wiskundige Yuri Manin zei onlangs in een interview "Good proofs are proofs that make us wiser":

" *I see the process of mathematical creation as a kind of recognizing a preexisting pattern*";

zie [53]. Probeer daarom in alles wat ik hieronder bespreek te bedenken: begrijp ik het patroon dat ten grondslag ligt aan dit verschijnsel?

Het blijkt dat voor het begrijpen van vragen uit de "elementaire getaltheorie" er vaak diepe theorie, prachtige structuren uit de algebra, meetkunde, analyse en nog veel meer andere wiskunde-specialismen nodig zijn. En dan blijven er nog vragen over, die o zo eenvoudig lijken, maar waar we kennelijk nog niet weten welke structuur we moeten begrijpen om dat probleem op te lossen.

(0.3) Hoe deze syllabus te gebruiken ?

- Begin met de vragen in § 1; probeer elk van die vragen te begrijpen, en probeer zelf een antwoord te vinden (de structuur van wiskundige argumenten, hoe moeilijk het is, wat er gebeurt begrijp je vaak pas als je het eerst zelf probeert). Denk na, doe een paar berekeningen, probeer te voelen wat die problemen echt zijn. Antwoorden (of het gebrek aan resultaten) zijn te vinden in §§ 3 - 8.

- Een vreemde paragraaf: in § 9 geef ik argumenten die soms overtuigen "dat een vermoeden dat we hebben wel waar móét zijn". Ruwweg gezegd: we doen alsof priemgetallen zich volledig willekeurig gedragen, alsof getallen die we bestuderen zich volledig willekeurig voordoen, en we passen eenvoudige kansrekening toe om onszelf te overtuigen wat de verdeling van die getallen is. Op zichzelf is dit onzin:

  "de *kans* dat een getal N priem is gelijk aan ... " is een rare uitspraak:
  dat getal is wél of is níet priem.

  Maar het blijkt dat we zo wel meer gevoel en intuïtief inzicht krijgen. Soms helpt het bij het vinden van het goede argument, het vinden van de juiste structuur.

- In § 10 zien we een prachtig onderwerp, waar we zien dat het vermoeden van Gauss en van Legendre juist is, een diepe stelling, die echter een heel bruikbare eenvoudige variant heeft; prachtige toepassingen. Hier zien we (een terugkerend thema):

  alhoewel we alle priemgetallen niet individueel kennen, kunnen we wel degelijk iets zeggen over hun gedrag

  ("hoe veel zijn er", "waar liggen ze" etc.). In § 11 een boeiende nieuwe ontwikkeling in de getaltheorie.

- In §§ 12 – 15 een (heel korte) samenvatting van basis-material dat we soms gebruiken om meer inzicht te krijgen.

- In § 18 geef ik een paar opgaven. Die kunnen gemaakt worden zonder veel voorkennis, maar soms moeten we wel iets slims doen.

- Probeer voorbeelden door te rekenen, en kijk of er zo meer inzicht komt (maar pas op: sommige van deze problemen zijn moeilijk, en in sommige gevallen geeft heel veel rekenwerk nog helemaal geen inzicht of resultaat).

- In de loop van de tijd zijn er allerlei vragen over priemgetallen van zelf onstaan uit problemen in de meetkunde, in de getaltheorie, en in nog veel meer aspecten van de wiskunde, maar ook daarbuiten. Neem een paar van die voorbeelden, en begrijp die vragen zo goed, dat u er over kunt nadenken en vooral voelen wat u erbij ervaart; zie §§ 5 - 6.

- In § 19 geef ik een lijst met een paar open problemen. Echter:

  grote wiskundigen komen daar nog niet uit ...
  wat is de onderliggende theorie die het probleem oplost en verklaart?

Er zijn in dit vak veel problemen die gemakkelijk te formuleren zijn, maar waar we eigenlijk nog helemaal geen vat op hebben: fascinerend.

"Elke formule in een tekst halveert het aantal geïnteresseerde lezers.
Als dit zo zou zijn dan heeft deze syllabus aan het eind bar weinig lezers over. Maar ik verwacht dat dít gehoor daar anders over denkt. Mooie wiskunde kun je nu eenmaal niet uitleggen zonder logische stappen te beschrijven met wiskundige terminologie, zonder de gedachten te preciseren in compacte formules. In vroegere wiskundige culturen werd soms wiskunde beschreven in lange teksten, die bovendien niet precies genoeg waren. In de moderne wiskunde kunnen we een hoge mate van precisie bereiken door de dingen die we beschrijven in eenvoudige en directe definities te vatten, en vervolgens met duidelijke formules de voortgang van de gedachten gang te ondersteunen. – Ja, dat kan wel eens abstract worden. Daarom is het zo goed als een wiskundige tekst gelardeerd wordt met uitleg, beschrijven van de achtergrond, benoemen van de wiskundige intuïtie, en vooral door het expliciet maken van "dwarsverbanden" (bij voorbeeld een algebraïsche formule meetkundig begrijpen, we zullen daar mooie voorbeelden van zien).

Hier en daar zal ik wat verder gaan dan elementaire voorkennis toestaat. Elk onderdeel waar iets meer voorkennis verondersteld wordt wordt met een * aangegeven. Zulke onderdelen kunt u gerust overslaan. *Al het andere materiaal hoop ik, verwacht ik, is geheel toegankelijk voor iedereen die durft na te denken, die bereid is abstracte gedachten toe te laten.*

De schoonheid van wiskunde bestaat eigenlijk uit twee totaal verschillende componenten.

Een ervan is die ongebreidelde stroom van nieuwe gedachten, vergezichten in een abstracte wereld, het plotseling eenvoudig worden van een probleem dat eerst onoplosbaar en erg moeilijk leek. Over de intuïtie van de wiskundige die hieraan ten grondslag ligt zal ik in de cursus af en toe komen te spreken.

Een ander aspect is het feit dat je al die vergezichten, die prachtige gedachten kunt vatten in precieze beschrijvingen, dat je moeilijke conclusies kunt bewijzen door middel van sluitende gedachtengangen. – Ik hoop en verwacht van alle deelnemers dat ze aan de slag gaan: niet alleen passief luisteren, maar ook vragen stellen, en vooral elke week tenminste één bewijs zelfstandig en volledig uitschrijven, en een paar vraagstukken maken. En vooral nieuwsgierig zijn en blijven. Zo krijgt u voeling met deze wondere wereld, zo ziet u hoe een nadenken inzicht kan geven, hoe de elegantie en schoonheid wonderlijke vergezichten opent.

Aspecten uit de geschiedenis van de wiskunde kun je op twee wezenlijk verschillende manieren beschrijven. Enerzijds kan men kiezen voor de methode de notatie, het gedachten-goed, de gevoelens van de periode die je beschrijft zorgvuldig te beschrijven in de taal en notatie van die tijd; een historicus zal in het algemeen deze weg volgen. Anderzijds kun je het historisch materiaal in moderne notatie en interpretatie weergeven. Hier heb ik voor voor deze tweede methode gekozen.

Zie de pagina vóór de lijst van referenties met lees-adviezen.

(0.4) Informatie op het internet. Daar is veel informatie te vinden. In deze syllabus staan verwijzingen. Die kunnen we ook vinden door met google te werken; voorbeeld: google <prime number theorem> en een verwijzing naar

`http://en.wikipedia.org/wiki/Prime_number_theorem`

komt direct boven. Zoek van allerlei onderwerpen die we bespreken op deze manier informatie op.

(0.5) Rekenadvies. Probeer van allerlei verschijnselen die besproken worden een aantal gevallen door te rekenen; in de syllabus vinden we allerlei suggesties daarvoor.

Hier zijn enkele sites waar hulpmiddelen staan om berekeningen uit te voeren, informatie te krijgen:

online calculator
`http://www.math.sc.edu/cgi-bin/sumcgi/calculator.pl`

a scientific calculator, b.v.:
`http://web2.0calc.com/#`

factoring numbers, e.g.:
`http://eng.numberempire.com/factoringcalculator.php`

vind het N-de priemgetal (voor $N < 10^{12}$):
`http://primes.utm.edu/nthprime/`

finding Collatz trees:
`http://www.nitrxgen.net/collatz.php`

om een rij gehele getallen te vinden waarvan we het begin weten:
`http://oeis.org/`

de som van de delers van een getal
`http://www.javascripter.net/math/calculators/divisorscalculator.htm`

curiosa: namen van allerlei priemgetallen
`http://en.wikipedia.org/wiki/List_of_prime_numbers`

Wiskundigen in de literaire fictie:
`http://kasmana.people.cofc.edu/MATHFICT/default.html`

“ *Its very simple, all you have to explain is this:*
other sciences seek to discover the laws that God has chosen;
mathematics seeks to discover the laws which God has to obey.
Jean-Pierre Serre,
Lettre du Collège de France, no 18 (déc. 2006); zie:
`http://www.abelprisen.no/binfil/download.php?tid=56994`, pagina 30, voetnoot 4.

1 Een paar vragen

Hieronder formuleer ik een paar vragen. Probeer de vraag te begrijpen, probeer elke vraag te beantwoorden. Is er een gemakkelijk antwoord? Probeer te voelen of dit interessant is of niet. Sommige van deze vragen zijn van groot belang, andere helemaal niet; ik heb ze expres dwars door elkaar heen gezet.

(1.1) Vraag 1. *Is de verzameling van alle priemgetallen eindig of oneindig*?
[Hoe beginnen we hier aan? Zo maar een lijst maken van veel priemgetallen, zou dat helpen?]
Voor een antwoord, zie § 3.

We gaan bestuderen of priemgetallen ver van elkaar af liggen of dicht bij elkaar liggen.

We zeggen dat N de lengte van een *gat in de rij van priemgetallen* is als er twee op een volgende priemgetallen $p < q$ zijn met $N = q - p$.

(1.2) Vraag 2. *Is de lengte van gaten in de rij van priemgetallen begrensd of onbegrensd*?
[Wat proberen we? Nadenken? Of voorbeelden maken?]
Zie (8.1).

We bestuderen de vraag of priemgetallen dicht bij elkaar kunnen liggen.

We spreken van een *priem-tweeling* als er priemgetallen $p < q$ zijn met $q - p = 2$.

We spreken van een *priem-drieling* als er priemgetallen $p < q < r$ zijn met $q - p = 2$ en $r - q = 2$.

(1.3) Vraag 3.
(2) *Is de verzameling van priem-tweelingen eindig of oneindig*?
(3) *Is de verzameling van priem-drielingen eindig of oneindig*?
[Voorbeelden maken? zou dat helpen?]
Zie (8.4), (8.5). Zie (19.4).

(1.4) Vraag 4. Fermat (priem)getallen. Bekijk de verzameling van getallen

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537, \cdots, \quad F_i := 2^{2^i} + 1.$$

Zij alle getallen in deze rij priem? *Zo nee, zijn er dan eindig of oneindig veel getallen in deze rij priem*?
[We zien dat voor een beetje grote i het getal F_i groot is; kunnen we hier aan rekenen? of willen we eerst nadenken? of wat gaan we anders doen om dit te begrijpen?]
Zie § 5 en (19.9).

(1.5) Vraag 5. Mersenne (priem)getallen. Een *Mersenne getal* is een getal van de vorm $M_n := 2^n - 1$. Zijn die getallen interessant? We zien dat $M_2 = 3$ en $M_5 = 31$. Komen er in de rij van alle Mersenne getallen slechts *eindig veel of oneindig veel priemgetallen voor*? Zie § 6, § 7 en (19.10).

(1.6) Vraag 6. We schrijven

$$p_1 = 2 < p_2 = 3 < \cdots < p_i < p_{i+1} < \cdots$$

voor de rij van álle priemgetallen geordend in opklimmende volgorde. *Is er een formule waarmee we voor elke i het i-de priemgetal p_i kunnen berekenen?*
[Is die vraag wel goed gesteld?]
Zie (8.7), (8.8); zie § 10.

(1.7) Vraag 7. We zien:

$$4 = 2 + 2, \quad 6 = 3 + 3, \quad 8 = 3 + 5, \quad \cdots, \quad 36 = 5 + 31 = 7 + 29, \quad \cdots (?)$$

Is het waar dat elk even getal $N = 2n \geq 4$ geschreven kan worden als som van twee priemgetallen?
[Voorbeelden maken? en wat concluderen we dan? Of hoe pakken we dit op een andere manier aan?]
Zie: *het vermoeden van Goldbach* (19.2), (19.3).

Een andere vraag.

$$2 = 5 - 3, \ 4 = 47 - 43, \ 6 = 13 - 7, \quad \cdots, 18 = 47 - 29, \cdots$$

Is elk even getal te schrijven als het **verschil** *van twee priemgetallen*?
Zie (19.5).

(1.8) Vraag 8. Bestaat er een priemgetal met 2013 cijfers?
[Waar te beginnen? Ik kan een getal van 2013 cijfers opschrijven; heeft het zin om dan te proberen of dit een priemgetal is? Is de kans erg groot dat ik door een willekeurige keuze te maken er een priemgetal komt?]
Zie (8.11), (10.3), (10.7).

(1.9) Vraag 9. Kunnen we getallen $A, a, D, d \in \mathbb{Z}_{\geq 2}$ vinden zodanig dat

$$A^a + 1 = D^d.$$

We zien dat $2^3 + 1 = 8 + 1 = 9 = 3^2$ een oplossing geeft van dit probleem. Zijn er nog andere oplossingen?
[Schrijf zuivere machten op: $1, 4, 8, 9, 16, 25, 27, 32, 36, \cdots$ en zie ik ergens een verschil van 1 optreden? Zou het helpen om zulke berekeningen uit te voeren? Is deze vraag moeilijk of gemakkelijk te beantwoorden? Waar past deze vraag in een algemener kader?]
Zie (8.12).

(1.10) Vraag 10. Een priemgetal p heet een *Sophie Germain priemgetal* als ook $q := 2p+1$ een priemgetal is. *Is het aantal Sophie Germain priemgetallen eindig of oneindig?*
Zie (19.11).

Deze getallen hebben deze naam gekregen, omdat Sophie Germain een speciaal geval van FLT bewees voor deze priem-exponenten. We zien dat 2, 3, 5, $, \cdots, 113, \cdots$ Sophie Germain priemgetallen zijn. Als we de rij $2, 3, 5, 11, 23, 29$ intoetsen op

`http://oeis.org/`, "The On-Line Encyclopedia of Integer Sequences",

dan komt er direct een lange rij van zulke priemgetallen te zien:
$2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293, 359,$
$419, 431, 443, 491, 509, 593, 641, 653, 659, 683, 719, 743, 761, 809, 911, 953, 1013, 1019,$
$1031, 1049, 1103, 1223, 1229, 1289, 1409, 1439, 1451, 1481, 1499, 1511, 1559$
verwijzingen, en nog veel meer.

(1.11) Vraag 11. Een oneven priemgetal is óf $p \equiv 1 \pmod 4$ óf $q \equiv 3 \pmod 4$. Dit geeft twee soorten oneven priemgetallen. Zijn er van elke soort even veel? of is er van de ene soort meer dan van de andere?
[Is die vraag wel goed gesteld? (nee) Is dit interessant? (ja)
We komen hier uitvoerig op terug.]
Zie (13.19).

(1.12) Vraag 12. Definieer de afbeelding

$$C : \mathbb{Z}_{>0} \longrightarrow \mathbb{Z}_{>0}$$

door:

$$C(2m) := m, \qquad C(2m+1) := 3(2m+1)+1;$$

dat wil zeggen: voor elke *even* n kiezen we $C(n) = n/2$, en voor elke *oneven* n kiezen we $C(n) = 3n+1$. Begin met een getal $a_1 \in \mathbb{Z}_{>0}$ en construeer de rij

$$\{a_1, a_2, \cdots \mid a_{i+1} := C(a_i)\}.$$

Verschijnt er voor elke keuze van a_1 het getal 1 ergens in die rij? Als dat het geval is, dan gaat de rij verder: $\{\cdots, 1, 4, 2, 1, \text{etc.}\}$.
[Wat gaan we doen? proberen, of nadenken? of iets anders? heeft het zin (veel) voorbeelden te maken?]
Zie (19.17).

2 Een paar definities

(2.1) We schrijven $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, 3, \cdots\}$ voor de verzameling van *gehele getallen*. Voor $a, b \in \mathbb{Z}$ zeggen we dat a een deler is van b als er een $d \in \mathbb{Z}$ bestaat met $da = b$.
Notatie: $a \mid b$ (en spreek uit: a deelt b).

Een getal $p \in \mathbb{Z}_{>1}$ heet een *priemgetal* als 1 en p de enige positieve delers zijn van p. Met andere woorden: als elke $1 < i < p$ niet een deler is van p.
Voorbeelden: 2, 3, 5, 7, 11, 13, 17, $19, \cdots$, 61, 67, $71, \cdots, 613$, 617, $619, \cdots$ etc.

(2.2) Grootste gemene deler. Gegeven zijn twee gehele getallen $m, n \in \mathbb{Z}$. Veronderstel dat $m \neq 0$. Beschouw de verzameling van gemeenschappelijk positieve delers:

$$\{d \in \mathbb{Z} \mid 1 \leq d,\ d \mid m,\ d \mid n\}.$$

Omdat $m \neq 0$ is deze verzameling eindig. Omdat $1 \mid m$ en $1 \mid n$ is deze verzameling niet leeg. Het grootste getal in deze verzameling noteren we als $\text{ggd}(m, m)$, de *grootste gemene deler van m en n*.
Opmerking. Bewezen kan worden dat voor $\text{ggd}(m, m) = d$ er bestaan $x, y \in \mathbb{Z}$ met $xm + yn = d$. Zie (13.6).

De eigenschap $\text{ggd}(m, n) = 1$ wordt wel verwoord als "m en n zijn onderling priem".
Gehele getallen zijn in priemfactoren te ontbinden, en een dergelijke ontbinding is uniek op volgorde van de factoren na; zie (13.3). Voor meer informatie over dit onderwerp, zie § 13.

(2.3) De logaritme. Logaritmen worden berekend met een grondtal. Voor $a \in \mathbb{Z}_{>1}$ schrijven we:

$$^a\log(x) = y \quad \Longleftrightarrow \quad x = a^y.$$

!! In deze syllabus schrijven we (en dat is de gangbare notatie onder wiskundigen):

$$\boxed{\log(x) :=^e \log(x)}\ ;\ \text{hier is } e \text{ de constante van Euler.}$$

Waarschijnlijk heeft u op de middelbare school geschreven $\ln(x) =^e \log(x)$ en $\log(x) =^{10} \log(x)$, maar dat doen we hier niet. (Een kwestie van afspraak, en van wennen.)
Zie `http://en.wikipedia.org/wiki/Logarithm`

3 Een bewijs van Euclides

(3.1) Stelling (Euclides). *Er zijn oneindig veel priemgetallen.*
Bewijs. Uitgaande van een eindige, niet-lege verzameling $\{P_1, \cdots, P_m\}$ van priemgetallen construeren we een priemgetal P dat niet in deze verzameling voorkomt. Als we dit laten zien, dan volgt dat de verzameling van alle priemgetallen niet eindig is.
Constructie. Beschouw het getal

$$M = P_1 \times \cdots \times P_m + 1.$$

Merk op dat $M > 1$; kies P als *de kleinste deler van* M *groter dan* 1; dan volgt dat P een priemgetal is (want als er een deler $1 < d < P$ zou zijn, dan is dat ook een deler van M, maar P is de kleinste deler van M met $P > 1$).
Bewering. *Het priemgetal* P *komt niet voor in* $\{P_1, \cdots, P_m\}$. Stel $P = P_i$ dan geldt

$$BP_i + 1 = M = AP \text{ met } B := P_1 \times \cdots \times P_{i-1} \times P_{i+1} \times \cdots \times P_m;$$

dus

$$(A - B)P = 1.$$

Hieruit volgt $B - A = \pm 1$, en $P = \pm 1$; tegenspraak met het feit dat $P > 1$. Dus geldt voor het priemgetal P dat $P \notin \{P_1, \cdots, P_m\}$. QED

Zie ook (5.1). Zie ook (4.13). Zie ook (13.16) en (13.19). Zie (13.21).

(3.2) Een vraag. Stel we beginnen met $P_1 = 2$ en construeren de rij $\{P_1, P_2, \cdots\}$ waar P_{m+1} het *kleinste* priemgetal is dat $M = P_1 \times \cdots \times P_m + 1$ deelt. Dan komt er de rij:

$$2,\ 3,\ 7,\ 43,\ 13,\ 53,\ 5,\ 6221671,\ 38709183810571,\ 139,\ 2801,\ 11, \cdots.$$

Mullin vroeg of elk priemgetal in deze rij voorkomt; dat is onbekend maar Shanks vermoedde dat dit wel het geval is. Verder is onbekend of dit effectief is, dat wil zeggen of we met zekerheid kunnen zeggen binnen hoeveel stappen een vooraf gegeven priemgetal in deze rij voorkomt.
Zie [7], `http://arxiv.org/abs/1107.3318`
Zie A000945 op `http://OEIS.org`

4 Convergente en divergente reeksen

Notatie. Als gegeven zijn $a_1, \cdots, a_m, b_1, \cdots, b_n$ (in $\mathbb{R}$ of in een andere ring), dan schrijven we

$$\sum_{i=1}^{i=n} a_i := a_1 + \cdots + a_m, \quad \prod_{j=1}^{j=n} b_j := b_1 \times \cdots \times b_n;$$

de notatie $X := Y$ betekent dat Y bekend is, en X wordt gedefinieerd door $X = Y$.

We gaan oneindige sommen en oneindige producten bespreken (a priori niet gedefinieerd).

(4.1) We nemen $a_1, \cdots, a_m, \cdots \in \mathbb{R}_{\geq 0}$ en gaan kijken of we een zinvolle betekenis kunnen geven aan $\sum_{i=1}^{i=\infty} a_i$. Denk aan:

$$\sum_{i=1}^{i=\infty} \frac{1}{i} \text{ (de harmonische reeks)}, \qquad \sum_{p \text{ priem}} \frac{1}{p}, \qquad \sum_{j=0}^{j=\infty} \frac{1}{r^j} \text{ (een meetkundige reeks).}$$

Definitie. Voor $a_i \in \mathbb{R}_{\geq 0}$ zeggen we dat $\sum_{i=1}^{i=\infty} a_i$ *divergent* is, of we zeggen dat som *onbegrensd* is, als voor elke $A \in \mathbb{R}$ er een index N is met

$$\sum_{i=1}^{i=N} a_i > A,$$

m.a.w. als deze som voor groeiende bovengrens onbeperkt groeit.

Voor $a_i \in \mathbb{R}_{\geq 0}$ zeggen we dat $\sum_{i=1}^{i=\infty} a_i$ *convergent* is met als limiet L als voor elke $\epsilon \in \mathbb{R}_{>0}$ er een index N is met

$$L - \epsilon \quad < \quad \sum_{i=1}^{i=N} a_i \quad \leq \quad L.$$

(4.2) Opmerking / Feit. Als $a_i \in \mathbb{R}$ (we staan negatieve getallen toe), dan kan het zijn dat de verzameling

$$\{ \sum_{1 \leq i \leq N} a_i \mid N \in \mathbb{Z}_{>0} \}$$

meerdere verdichtingspunten heeft. We zullen dit niet serieus gaan gebruiken. (Laat deze opmerking voor wat het is.)

Als slechts eindig veel van de a_1 ongelijk aan nul zijn, dan bestaat $\sum_{i=1}^{i=\infty} a_i$ (het is in wezen een eindige som).

Neem aan dat alle $a_i \in \mathbb{R}_{>0}$ (en dit is het interessante geval dat ons zal bezighouden). Dan zijn er twee mogelijkheden:
(begrensd) Als er een $M \in \mathbb{R}$ zodanig dat

$$\sum_{1 \leq i \leq N} a_i \quad \leq M, \qquad \forall\ N \in \mathbb{Z}_{>0},$$

dan zeggen we dat $\sum_{i=1}^{i=\infty} a_i$ *begrensd is.*
Feit. In dit geval is er een $L \in \mathbb{R}$ zodanig dat:
(1) $\forall\ N$ geldt $\sum_{1 \leq i \leq N} a_i \quad < L$ en

(2) voor elke $\epsilon \in \mathbb{R}_{>0}$ is er een N zodanig dat:

$$L - \epsilon \;\; < \sum_{1 \leq i \leq N} a_i \;\; < L$$

("de eindige sommen komen willekeurig dicht bij L"). In dit laatste geval zeggen dat de oneindige som bestaat, en we schrijven

$$\sum_{i=1}^{i=\infty} a_i = L.$$

In dit geval zeggen we ook wel dat de som *convergeert*.

(óf onbegrensd) Als voor elke $L \in \mathbb{R}$ er een N is zodanig dat

$$\sum_{1 \leq i \leq N} a_i \;\; > \;\; L$$

dan zegen we dat de oneindige som "*onbegrensd is*". In dit geval zeggen we ook wel dat de som *divergeert*.

(4.3) Stelling (de harmonische reeks). *De som*

$$\sum_{i=1}^{i=\infty} \frac{1}{i} \quad \textit{is divergent.}$$

Bewijs. Beschouw:

$$1 + \{\frac{1}{2} + (\frac{1}{3} + \frac{1}{4})\} + \{(\frac{1}{5} + \cdots + \frac{1}{8}) + (\frac{1}{9} + \cdots + \frac{1}{16})\} +$$
$$+ \cdots + (\frac{1}{2^k + 1} + \cdots + \frac{1}{2^{k+1}}) + \cdots.$$

We zien:

$$\sum_{i=1}^{i=2^{2m}} \frac{1}{i} \quad > m + 1.$$

QED

(4.4) Opgave. Dit resultaat heeft een amusante toepassing. Stel we hebben een groot aantal rechthoekige blokken (of kaarten van een kaartspel). We stapelen die blokken op een of andere manier op elkaar bij de rand van een tafel. Kunnen we het zo doen dat de bovenste buiten de rand van de tafel uitsteekt? Hoe ver kunnen we de bovenste buiten de rand laten uitsteken? Is daar een grens aan? of kunnen we (als we maar genoeg blokken hebben) willekeurig ver buiten de rand komen? Zie (18.30).

(4.5) Opgave. Een kever begint te lopen op een elastische draad die in het begin 1 meter is. De kever loopt elke seconde 1 centimeter, en aan het eind van elke seconde wordt de draad 1 meter uitgerekt. (Neem aan dat de draad zo elastisch is dat uitrekken heel lang kan doorgaan; neem aan dat de kever zo dapper en gezond is dat het doorlopen heel lang kan doorgaan.) Na 1 seconde heeft de kever 1 centimeter gelopen, wordt de draad 2 meter en daarvan heeft de kever 2 centimeter afgelegd. Na 2 seconden heeft de kever $2 \times 1 + 1$ centimeter afgelegd, wordt de draad 3 meter waarvan $(3/2) \times (3)$ door de kever is afgelegd, en zo voort. Bereikt de kever het eind van de draad? Zo nee, bewijs. Zo ja geef een schatting van een moment waarop we zeker weten dat de kever over de rand gelopen is. Dit is een puzzel van Gardner. Zie (18.31).

(4.6) Stelling. *Voor $r \in \mathbb{R}_{>1}$ is de som*

$$\sum_{j=0}^{j=\infty} \frac{1}{r^j} \quad \textit{convergent.}$$

Bewijs. Beschouw (de eindige meetkundige reeks):

$$1 + \frac{1}{r} + \frac{1}{r^2} + \cdots + \frac{1}{r^m} = \frac{(\frac{1}{r})^{m+1} - 1}{\frac{1}{r} - 1} = \frac{r^{m+1} - 1}{r^{m+1} - r^m}.$$

Omdat $r > 1$ komt er:

$$\lim_{m\to\infty} \sum_{j=0}^{j=m} \frac{1}{r^j} = \lim_{m\to\infty} \frac{r^{m+1} - 1}{r^{m+1} - r^m} = \frac{r}{r-1} =: L.$$

We zien dat de (limiet van de) som gelijk is aan L. QED

Interessant / vraag:
de reeks $1 + (1/2) + \cdots + (1/i) + \cdots$ is divergent,
maar als we er voldoende termen uit laten dan krijgen we bij voorbeeld
de reeks $(1/3) + (1/9) + \cdots + (1/3^j) + \cdots$ die convergent is.
Wat gebeurt bij beschouwen van
de reeks $(1/2) + (1/3) + \cdots + (1/p) + \cdots$ (de noemers zijn alle priemgetallen)?

(4.7) De verkeerde manier. We kunnen proberen inzicht te krijgen door berekenen. We nemen een (heel snelle) computer, en laten die $\sum_{p<N}(1/p)$ berekenen (b.v. een eeuw lang) voor groeiende bovengrens N. Wat is de suggestie, en wat is de waarheid? We zien dat in het begin de som $\sum_{p<n}(1/p)$ wel groeit, maar het duurt heel lang voor die getallen een beetje groot worden. Zullen we "even" wachten tot die som boven de 6 komt? Dat maken we zelf niet meer mee (zie hieronder). We zouden tot de conclusie kunnen komen dat de oneindige som wel eens begrensd/convergent zou kunnen zijn. (?!)

(4.8) Stelling (Euler, 1737). *De som*

$$\sum_{p \text{ priem}} \frac{1}{p} \quad \textit{is divergent.}$$

Opmerking. Het lijkt vreemd dat we iets kunnen zeggen over deze som, terwijl we niet alle termen (precies) kennen.
Zie [37], II.2.6. Zie [5], Chapter 10. Zie
`http://en.wikipedia.org/wiki/Proof_that_the_sum_of_the_reciprocals_of_the_primes_diverges`
`http://en.wikipedia.org/wiki/Meissel%E2%80%93Mertens_constant`
Bewijs. (In dit bewijs gebruiken we het feit dat gehele getallen eenduidig in priemgetallen te ontbinden zijn, zie (13.3).) Neem aan dat deze som begrensd zou zijn. Dan bestaat er voor $\epsilon = 1/2$ een getal N zodanig dat

$$\sum_{p \text{ is priem, } p>N} \frac{1}{p} < \frac{1}{2}.$$

Denieer het getal

$$Q := \prod_{p \text{ is priem}, \ p \leq N} p.$$

Merk op dat voor elke $n \in \mathbb{Z}_{\geq 1}$ het getal $1 + nQ$ alleen maar factoren groter dan N geeft. Hieruit volgt dat voor elke $M \in \mathbb{Z}_{\geq 1}$ we de volgende ongelijkheid hebben:

$$\sum_{n=1}^{n=M} \frac{1}{1+nQ} \quad \leq \quad \sum_{t=1}^{\infty} \left(\sum_{p>N} \frac{1}{p} \right)^t ;$$

dit volgt want elke term links komt links maar één keer voor, en komt rechts ook voor (hier gebruiken we de eenduidigheid van factorontbinding). Uit

$$\sum_{t=1}^{\infty} \left(\sum_{p>N} \frac{1}{p} \right)^t \leq \sum_{t=1}^{\infty} \left(\frac{1}{2} \right)^t = 1$$

concluderen we dat

$$\sum_{n=1}^{\infty} \frac{1}{1+nQ}$$

convergent zou zijn, zie (4.2). Echter

$$\frac{1}{1+nQ} \geq \frac{1}{n+nQ} = \frac{1}{1+Q}\frac{1}{n}; \quad \text{dus} \quad \sum_{n=1}^{n=T} \frac{1}{1+nQ} \geq \frac{1}{1+Q} \sum_{n=1}^{n=T} \frac{1}{n}.$$

We maken gebruik van (4.3) en we zien dat $\sum_n 1/(1+nQ)$ divergeert; dit geeft een tegenspraak. We concluderen dat

$$\textstyle\sum_{p \text{ priem}} \frac{1}{p} \text{ niet begrensd is.}$$

QED

(4.9) Opmerking. Dit resultaat werd bewezen door Euler. Maar wat is nu de verklaring dat die som zo langzaam groeit, zoals we bij een lange computerberekening geconstateerd zouden hebben? Gauss vermoedde het volgende asymptotische gedrag in 1796 en Mertens bewees dit vermoeden in 1874:

$$\lim_{x \to \infty} \quad \left(\left(\sum_{p \text{ priem } \leq x} \frac{1}{p} \right) - \log(\log(x)) \right) = B_1,$$

waar de "Mertens constante" de waarde $B_1 \approx 0.26...$ heeft. We zullen verderop zien dat er zoiets als $p \sim (1/\log(p))$ geldt en het n-de priemgetal p_n is ongeveer $n \log(n)$; het integraalkenmerk geeft dat $\sum(1/\log(p))$ zoiets als $\log(\log(x))$ is; dit geeft een eerste, intuïtieve verklaring voor dit resultaat.

Bovenstaande asymptotische afschatting kan exact gemaakt worden. Er geldt:

$$\log(\log(N)) \quad < \quad \sum_{p<N} 1/p \quad < \quad \log(\log(N)) + B + \frac{1}{(\log(N))^2}, \quad B \approx 0.261497.$$

zie `http://primes.utm.edu/infinity.shtml`

(4.10) Opgave. Bereken $\sum_{p<100}\ 1/p$ en laat zien dat de bovenstaande afschatting aardig scherp is. Zie (18.36).

(4.11) Voorbeeld. Voor de bovengrens $x = 10^{100}$ komt er

$$\sum_{p\ \leq x} p \approx \log(\log(x)) + B + \frac{1}{(\log(N))^2} \approx 5.7.$$

We weten dat er onder $x = 10^{100}$ ongeveer 434×10^{95} priemgetallen zijn. Het aantal seconden per jaar is minder dan 4×10^7; een machine die elke seconde 1000 priemgetallen berekent en $1/p$ bij het vorige resultaat optelt (en dat is heel snel, vooral bij grote getallen) heeft er zoiets als $10^{100}/(4 \times 10^{10}) = 25 \times 10^{88}$ jaar voor nodig om de som $\sum_{p\leq x}\ (1/p)$ boven de 6 te krijgen (een ruwe of een bewezen schatting).

Een andere manier om er tegen aan te kijken: na 10 jaar zijn ongeveer de 12×10^9 priemgetallen onder de 10^{13} doorgerekend (als we de vorige schatting met een heel snelle computer aanhouden). De volgende dag bevat 86400 seconden, en er worden minder dan 10^8 nieuwe priemgetallen doorgerekend. Dat laat zien dat in die dag de som hooguit $10^8/10^{13}$ groeit; na 10 jaar zien we per dag de eerste 4 decimalen achter de komma niet veranderen (en dat is maar een ruwe schatting).

(4.12) We zien de verklaring waarom wachten op dat groeien van die som niet veel helpt aan de ene kant, maar dat aan de andere kant $\log(\log(x)) \to \infty$ voor $x \to \infty$. We zien dat

$$\sum_{p\ \leq x}\ \frac{1}{p}$$

extreem langzaam groeit, maar *niet begrensd is.* Zie
`http://mathworld.wolfram.com/MertensConstant.html`

Ik vind (4.8) een wonderlijk resultaat. Nadenken en het geven van abstracte bewijzen loont. En we begrijpen nu ook waarom een beetje (of veel) rekenen ons hier helemaal niet verder helpt.

(4.13) Een bewijs van (3.1), *er zijn oneindig veel priemgetallen,* volgt uit (4.8).

(4.14) Opmerking.* Euler constreerde de "zeta-functie":

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \sum_{n\geq 0}\ \frac{1}{n^s}.$$

Euler bestudeerde dergelijke reeksen in 1740, met s een geheel getal. Chebyshev nam voor s een reëel getallen (groter dan 1). Riemann bestudeerde deze functie voor s een complexe variabele en de naam "zeta-functie" is afkomstig van Riemann (maar ook voor een reële variabele is dit al interessant). Als het reële deel van s groter is dan 1, dan convergeert deze som, m.a.w. dan is $\zeta(s)$ gedefinieerd.

Interesante vraag: wat gebeurt er voor $s = 1$? Dan blijkt dat "$\zeta(1) > \sum_p\ 1/p$"; niet erg zonvol: de linkerkant en de rechterkant divergeren. We zien dat deze som net het interessante grensgeval is. Dit motiveerde Euler voor (4.8).
Zie `http://empslocal.ex.ac.uk/people/staff/mrwatkin/zeta/devlin.pdf`
Deze definitie van Euler was het begin van veel theorie, en het formuleren door Riemann van de RH.

(4.15) Zijn er oneindig veel tweelingen? zie (1.3), (8.4), (8.5), (19.4). We worden aangemoedigd door het feit dat divergentie van een som bewijst dat er oneindig veel priemgetallen zijn, zie (4.13). We proberen daarom of de volgende som

$$\sum_{p,\ \text{en}\ p+2\ \text{is ook priem}} 1/p$$

divergent is (of niet). In 1919 bewees V. Brun dat deze som *convergeert* (en deze som is ongeveer gelijk aan 1.902160583104). Hieruit volgt geen conclusie voor (on)eindig veel tweelingen. Voor verwijzingen voor het resultaat van Brun zie
`http://mathworld.wolfram.com/BrunsConstant.html`

(4.16) Waarschuwing, onzin. We hebben in deze paragraaf oneindige sommen gezien. Enige voorzichtigheid is geboden.
(1) Laten we schrijven $S = \sum_{0 \leq i < \infty} (1/2^i)$ (terwijl we ons er niet over bekommeren of dit wel bestaat). We gaan rekenen met S (alsof er niets aan de hand is, dubieuze praktijken):

$$\frac{1}{2} \times S = \frac{1}{2} \times \left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right) = \left(\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots\right) = -1 + S.$$

Uit $S/2 = -1 + S$ concluderen we $S = 2$. Mag dat wel, zo rekenen met oneindige sommen?

(2) Aangemoedigd door ons vorige succes doen we net zoiets: $T = \sum_{0 \leq i < \infty} 2^i$, We zien (?):

$$2T = 2 \times (1 + 2 + 4 + \cdots) = (2 + 4 + 8 + \cdots) = -1 + T.$$

We concluderen (?) uit $2T = -1 + T$ dat $T = -1$.

(3) Alsof dit niet al erg genoeg is: voor $U = \sum_{0 \leq i < \infty} (-1)^i$ komt er:

$$U = 1 + (-1 + 1) + (-1 + 1) + \cdots + (-1 + 1) + \cdots = 1 - U,$$

en ook

$$U = (1 - 1) + (1 - 1) + \cdots = 0.$$

Conclusie (??): $U = 1/2$ en ook $U = 0$.

(4) De redenering in (1) kan gerechtvaardigd worden, niet door de "berekening" hierboven, maar door zorgvuldige afschattingen van het verschil tussen de oneindige som met een eindige deelsom (het afschatten van "staarten"). Die berekening kan gedaan worden, en rechtvaardigt tenslotte ook het *resultaat* van de lichtzinnige redenering.

Voor de niet-convergente rijen in (2) en in (3) staat er onzin, die ook niet te repareren is. De reeks in (2) is divergent (onbegrensd), en de reeks in (3) is niet convergent (en een "som" ervan is niet gedefinieerd): de T en U zijn niet-bestaande objecten, en "rekenen" ermee zoals boven bewijst niets.

Een uitdrukking zoals $\sum_{1 \leq i < \infty} a_i$ moet als formele schrijfwijze opgevat worden, en geeft niet een getal of iets dergelijks zolang convergentie niet aangetoond is.

André Weil geeft in [89] een prachtige beschrijving van de geschiedenis van het sommeren van oneindige reeksen.

5 Fermat (priem)getallen

Beschouw de getallen - die we Fermat getallen noemen -

$$F_i := 2^{2^i} + 1, \quad i \in \mathbb{Z}_{\geq 0}.$$

Pierre de Fermat vroeg zich af of alle getallen in deze rij priem zijn. We zien dat

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

wel priem zijn. Maar Euler bewees in 1732:

$$F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417.$$

Zie ook (13.24).

Er is veel onderzoek en veel rekenwerk gedaan om nieuwe Fermat priemgetallen te vinden.
Zie `http://en.wikipedia.org/wiki/Fermat-number`
We kennen geen Fermat priemgetallen met $i > 4$. Voor veel waarden van i is bekend dat F_i niet priem is; zie:
`http://www.prothsearch.net/fermat.html`

(5.1) Opgave. Bewijs:
(1) Voor elke $i > 0$ geldt $F_i = F_0 \times \cdots \times F_{i-1} + 2$
(2) Voor $0 < i < j$ is $\text{ggd}(F_i, F_j) = 1$.
(3) Schrijf P_i voor de kleinste priemdeler van F_i. Laat zien dan $\{P_i \mid i \in \mathbb{Z}_{>0}\}$ een oneindige verzameling is (en zo bewijzen we weer dat de verzameling van priemgetallen niet eindig is).

(5.2) Opgave Als $2^m + 1$ een priemgetal is, dan is er een i met $m = 2^i$ (anders gezegd: als $2^m + 1$ priem is, dan is m even). Zie (18.32).
[De vraag naar primaliteit van getallen van de vorm 2^a waar a een oneven deler groter dan 1 heeft is niet zo interessant....]

(5.3) Opmerking / opgave. (1) (Euler). Het Fermatgetal $F_i := 2^{2^i} + 1$ is deelbaar door $a2^{i+1} + 1$ voor een goede keuze van $a \in \mathbb{Z}$.
(2) (Lucas). Voor $i \geq 2$ is $F_i := 2^{2^i} + 1$ is deelbaar door $b2^{i+2} + 1$ voor een goede keuze van $b \in \mathbb{Z}$.
Voorbeelden: $F_0 = 2 + 1$, $F_1 = 4 + 1$, $F_2 = 17 = 16 + 1$, $F_3 = 257 = 8{\cdot}32 + 1$, $F_4 = 1024{\cdot}64 + 1$, $F_5 = (5 \times 128 + 1) \times 6700417$;
$F_6 = (1017 \times 256 + 1) \times 67280421310721$, etc. ?

(5.4) Constructie van regelmatige veelhoeken. In de Griekse oudheid was bekend dat je met passer en liniaal een regelmatige 3-hoek, een regelmatige 5-hoek kunt construeren, en dat je elke gegeven hoek zo in twee gelijke delen kunt verdelen. Wat is de lijst van alle $n \in \mathbb{Z}_{>2}$ zodanig dat een regelmatige n-hoek met passer en liniaal geconstrueerd kan worden?

Gauss bewees op 29-maart-1796 (toen hij in de ochtend nog in bed lag, hij was toen 18 jaar), dat een regelmatige 17-hoek construeerbaar is. Later publiceert hij in [28], Hoofdstuk VII:

Stelling (Gauss, 1796). *Een regelmatige n-hoek is construeerbaar met passer en liniaal dan en slechts dan als $n \geq 3$ te schrijven is als*

$$n = 2^{\alpha} \times P_1 \times \cdots \times P_t$$

met $\alpha \in \mathbb{Z}_{\geq 0}$ en $P_1 < \cdots < P_t$ onderling verschillende Fermat priemgetallen.
We weten niet of Gauss inderdaad een bewijs had voor dit resultaat (een bewijs werd niet gepubliceerd door hem; het geval $n = 17$ bewijst hij door de lengte van de zijde van een regelmatige 17-hoek uit te rekenen). Een bewijs werd in 1837 door Pierre Wantzel gepubliceerd.

We zien dat een meetkundig probleem (welke regelmatige n-hoeken kunnen geconstrueerd worden met passer en liniaal?) eigenlijk een probleem is in de getaltheorie (welke Fermat getallen zijn priem ?).

6 Mersenne (priem)getallen

We introduceren de Mersenne getallen:

$$M_n := 2^n - 1$$

en vragen ons af of daar priemgetallen onder voorkomen.

(6.1) Opgave.

$$M_n \text{ is een priemgetal } \implies n \text{ is een priemgetal.}$$

Zie (18.37).

(6.2) Merk op dat de omkering niet geldt: 11 is een priemgetal, maar

$$23 \text{ is een deler van } M_{11}.$$

Inderdaad: $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$, zoals Hudalricus Regius in 1635 liet zien.

(6.3) Opmerking. Laat p een priemgetal zijn zodanig dat $q = 2p + 1$ ook een priemgetal is; Het priemgetal p heet dan *een Sophie Germain priemgetal*; zie ook (19.11). De volgende eigenschap zullen we niet bewijzen; het generaliseert het geval $23 \mid M_{11}$.

Feit. (6.3)(1)* *Als $q = 2n + 1$ een priemgetal is dan is n een deler van*

$$2^{q-1} - 1 = (2^n - 1)(2^n + 1).$$

Hoe kunnen we zien of q een deler is van $2^n - 1$ of van $2^n + 1$?
(6.3)(2)* *Als p priem is, $q = 2p + 1$ is ook een priemgetal, en $p \equiv 3 \pmod 4$ dan is q een deler van $2^p - 1$.*
Zie [5], Th. 5.4.1.

Een paar voorbeelden:
$q = 7 = 2^3 - 1$;
$q = 11$ deelt $2^5 + 1$:
we zagen al dat $q = 23$ een deler is van $2^{11} - 1$;
$q = 47$ deelt $2^{23} - 1$;
probeer zelf $p \in \{29,\ 41,\ 53,\ 83,\ 89\}$.
We zien dat $2^{21} + 1 = 43 \times 48771$; hier is $q = 43 = 2n + 1$ een deler van $2^n + 1$ en $q \equiv 3 \pmod 4$; is dit een tegenspraak met (6.3)(2)?

(6.4) Vroeger kwam de interesse voor Mersenne getallen door de volgende stelling.
Definitie (uit de Griekse oudheid). Een getal $N \in \mathbb{Z}_{>0}$ heet een *perfect getal* als de som van de positieve delers van N gelijk is aan $2N$; of: de som van de delers d van N met $1 \leq d < N$ is gelijk aan N:

$$\sum_{1 \leq d \leq N,\ \ d \mid N} d = 2n \quad \overset{\text{def}}{\iff} \quad N \text{ is perfect.}$$

Ga na:
$6 = 2 \cdot M_2$ is een perfect getal, $28 = 2^2 \cdot M_3$ is een perfect getal,
$496 = 2^4 \cdot M_5$ is een perfect getal, en verder $\cdots$?
Laat zien dat $2^{10} \cdot M_{11}$ niet een perfect getal is.

(6.5) (Euclides, Boek IX, Propositie 36 en Euler). *Een* even *getal $N = 2m$ is perfect dan en slechts dan als er bestaat een priemgetal p zodanig dat*

$$M_p \text{ is priem, en } N = 2^{p-1}\cdot(2^p - 1) = 2^{p-1}\cdot M_p.$$

Voorbeelden: $p = 2, 3, 5, 7, 13, 17, \cdots$;
$M_{31} = 2^{31} - 1 = 2147483647$ is een priemgetal (Euler, 1772) en dit geeft het perfecte getal

$$2^{30} \times M_{31} = 2305843008139952128.$$

Voor dit en voor fascinerende beschrijving van verdere vondsten zie
`http://primes.utm.edu/notes/by_year.html#31`

We zien dat het vinden van **even** *perfecte getallen*
equivalent is met het vinden van Mersenne priemgetallen.

(6.6) Het vinden van Mersenne priemgetallen houdt wiskundigen al heel lang bezig. Waarom? Het is een probleem dat wel omschreven is, en beslissen of er slechts eindig veel of oneindig veel Mersenne priemgetallen zijn is een mooie uitdaging.

Enerzijds zijn die getallen precies gedefinieerd, anderzijds groeien ze snel. "Met de hand rekenen" is al snel niet meer mogelijk. Wat is er nu bekend?

In (18.37) hebben we gezien dat M_n is priem impliceert dat n priem is. Dat beperkt het zoeken.

We weten nu dat M_p priem is als p een van de volgende priemgetallen is:

$$2,\ \ 3,\ \ 5,\ \ 7,\ \ 13,\ \ 17,\ \ 19,\ \ 31,\ \ \cdots,\ \ 3,021,377,\ \ \cdots\ \ 57,885,161, \qquad \text{(en verder ??)}\ ;$$

we kennen nu 48 Mersenne priemgetallen. Slimme algoritmes en veel, heel veel rekenwerk, een mooie geschiedenis van het vinden van Mersenne priemgetallen: Euclides, Regius, Cataldi, Fermat, Euler, en vele anderen, en het ontwerpen van een test door Lucas en Lehmer. Voor een volledige lijst van de nu bekende Mersenne priemgetallen, zie
`http://en.wikipedia.org/wiki/Mersenne_prime`
`http://primes.utm.edu/mersenne/`

Dit is een fascinerend onderwerp. Het rekenwerk is mooi, maar leren we er iets van? Ik heb de indruk dat we de "onderliggende structuur" nog niet begrijpen. Zie (19.9). In de paragraaf 9 laten we een (zeer speculatieve) benadering zien die, alhoewel niet gebaseerd op wiskundig juiste redeneringen, ons inzicht zou kunnen geven wat we mogen verwachten.

7 Som van de delers

In deze paragraaf bewijzen we (6.5):

(7.1) *Een* even *getal $N = 2m$ is perfect dan en slechts dan als er bestaat een priemgetal p zodanig dat*

$$M_p \text{ is priem, en } N = 2^{p-1}\cdot(2^p - 1) = 2^{p-1}\cdot M_p.$$

(7.2) **Notatie.** Voor een $N \in \mathbb{Z}_{>0}$ schrijven we $\sigma(N)$ voor de som van de positieve delers van N:

$$\sigma(N) := \sum_{d|M,\ \ 1\le d\le N} d.$$

Merk op:

$$N \text{ is perfect} \quad \stackrel{\text{def}}{\iff} \quad \sigma(N) = 2N.$$

We krijgen $\sigma : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$. We gaan een paar eigenschappen van deze functie bestuderen.

Op de site "sum of divisors"
`http://www.javascripter.net/math/calculators/divisorscalculator.htm`
kunnen we $\sigma(n)$ direct berekenen voor vele waarden van n.

(7.3) **Stelling.** (1) *Als $N, M \in \mathbb{Z}_{>0}$ met* $\text{ggd}(N, M) = 1$ *dan geldt:*

$$\sigma(NM) = \sigma(N)\sigma(M).$$

(2) *Als p een priemgetal is, en $n \in \mathbb{Z}_{>0}$ dan geldt:*

$$\sigma(p^n) = \frac{p^{n+1} - 1}{p - 1}; \text{ in het bijzonder } \sigma(p) = p + 1.$$

Merk op dat dit ons in staat stelt om op een snelle manier $\sigma(N)$ te berekenen zodra de factorizatie van N bekend is, b.v.:

$$\sigma(80) = \sigma(16)\sigma(5) = 31\cdot 6; \quad \sigma(66) = \sigma(2)\sigma(3)\sigma(11) = 3\cdot 4\cdot 12.$$

Opgave. Bereken zelf $\sigma(22)$, $\sigma(70)$, $\sigma(81)$, $\sigma(94)$.
Bewijs van (7.3). Als $\text{ggd}(N, M) = 1$ dan geldt voor elke deler D van NM dat er een unieke factorizatie is $D = de$, waar d een deler is van N en e een deler van M; zo komen ook al zulke producten de voor. We concluderen:

$$\sigma(MN) = \sum_{D|NM,\ \ 1\le D\le NM} D = \left(\sum_{|N,\ \ 1\le d\le N} d\right) \times \left(\sum_{e|M,\ \ 1\le e\le M} e\right) = \sigma(N)\sigma(M).$$

Dit bewijst (1).

We zien dat

$$\sigma(p^n) = 1 + p + \cdots + p^i + \cdots + p^n;$$

de som van deze meetkundig rij is inderdaad $(p^{n+1} - 1)/(p - 1)$. QED

De eigenschap (1) hierboven wordt wel samengevat als: "$\sigma(-)$ is een multiplicatieve functie".

(7.4) We bewijzen de implicatie reeds door Euclides bewezen:

$$M_p \text{ is priem } \implies \quad N := 2^{p-1}\cdot M_p \text{ is perfect.}$$

Inderdaad:

$$\sigma(2^{p-1}\cdot M_p) = \sigma(2^{p-1})\cdot\sigma(M_p) = (1+2+4+\cdots+2^{p-1})\cdot(1+M_p) = (2^p-1)\cdot 2^p = 2N.$$

QED

Nu:

$$M_p \text{ is priem } \impliedby \quad N := 2^{p-1}\cdot M_p \text{ is perfect.}$$

We weten dat M_p oneven is, en omdat bovendien N perfect is komt er:

$$\sigma(2^{p-1}\cdot M_p) = \sigma(2^{p-1})\sigma(M_p) = (2^p-1)\sigma(M_p) = 2\times 2^{p-1}\cdot M_p.$$

Omdat $2^p - 1 = M_p$ volgt

$$\sigma(M_p) = 1 + (\text{andere delers}) + M_p = 2^p.$$

We zien dat er geen "andere delers" zijn, en concluderen dat M_p priem is. QED

(7.5) Op een HOVO-cursus zei een van deelnemers tegen mij:

"de som van de delers van mijn leeftijd is een kwadraat".

Opgave. Wist ik toen de leeftijd van die deelnemer? Zie (18.38).

(7.6) Opgave. Is de volgende uitspraak waar (en geef een bewijs) of onjuist (en geef een tegenvoorbeeld) ? *Als voor $N > 81$ de som van de delers $\sigma(N)$ een kwadraat is, dan is N even* (?). Zie (18.39)

(7.7) Dit gaf aanleiding tot de vraag: komt het "vaak" voor dat de som van de delers van een geheel getal een kwadraat is? Probeer met methoden uit § 9 en gevoel te krijgen wat het anwoord zou moeten zijn.

(7.8) Stelling (Beukers, Luca en Oort, 2012). *Er zijn oneindig veel positieve gehele getallen N zodanig dat $\sigma(N)$ een kwadraat is.*
De vraag (7.5) was de aanleiding tot het zoeken en vinden van dit resultaat. Een bewijs is te vinden in [6].

Hopelijk vinden we tijd om het bewijs van deze stelling te zien. In het artikel [6] en in [18] vinden we ook de volgende, veel algemenere stelling:

(7.9) Stelling (Beukers, Luca en Oort, 2012; Freiberg, 2010). *Zij $k \in \mathbb{Z}_{>0}$. Er zijn oneindig veel positieve gehele getallen N zodanig dat $\sigma(N)$ de k-de macht van een geheel getal is.*

(7.10) Opgave. *Veronderstel dat we weten dat er oneindig veel Mersenne priemgetallen zijn* (onbekend, wel vermoed en verwacht waar te zijn). *Gebruik dit om het resultaat (7.9) te bewijzen.*

8 Een paar antwoorden

(8.1) Gaten in de rij van priemgetallen. Een antwoord op (1.2).
We bewijzen: voor elke $N \in \mathbb{Z}_{>0}$ bestaat er een paar opeenvolgende priemgetallen (p_i, p_{i+1}) met

$$p_{i+1} - p_i \geq N$$

(m.a.w. de lengte van gaten in de rij van priemgetallen is niet begrensd).
Hier is het **eenvoudige bewijs**. Beschouw

$$M := (N+1)! = 2 \times \cdots \times N \times (N+1).$$

Kies i zo dat p_i het grootste priemgetal is kleiner dan $M+2$. Merk op:

$$M+2, \quad M+3, \quad \cdots, \quad M+N, \quad M+N+1 \quad \text{zijn niet priem.}$$

Inderdaad, voor $2 \leq j \leq N+1$ is j een deler van M, en dus is voor die waarden het getal $M+j$ niet een priemgetal. We zien dat het volgende priemgetal

$$p_{i+1} \geq M+N+2, \quad p_i \leq M+1; \quad \text{dus } p_{i+1} - p_i \geq (M+N+2) - (M+2) = N.$$

QED

Het bewijs is dan wel kort, maar het geeft in veel gevallen niet de zuinigste manier om een lang genoeg gat te construeren.
Voorbeeld. Voor $1 \leq j \leq 33$ is $1327 + j$ niet een priemgetal. Dit gat van lengte 34 komt veel eerder dan het getal

$$34! \quad \approx \quad 2.95 \times 10^{38}.$$

Voorbeeld. Voor $p_i = 31397$ geldt $p_{i+1} - p_i = 72$, terwijl

$$72! \quad \approx \quad 6.12 \times 10^{103}.$$

Zie `http://en.wikipedia.org/wiki/Prime-gaps` Zie ook [30], pag. 10. Zie ook de laatste pagina van deze syllabus.

(8.2) Opmerking. We kunnen tegen de vraag of de lengte van gaten in de rij van priemgetallen begrensd zou zijn ook als volgt aankijken. Stel dat elk gat hooguit de lengte N heeft. Dan volgt dat élk interval van lengte N tenminste één priemgetal bevat. Daar zou uit volgen dat $\pi(x) > x/N$ voor alle $x \in \mathbb{R}$. Maar we zullen zien, zie § 10, dat er geldt $\pi(x) < B \cdot x/(\log(x))$ voor een of andere constante B; dit geeft een tegenspraak voor alle x met $B/(\log(x)) > N$.

We kunnen ons afvragen welke precieze lengtes van gaten in de rij van priemgetallen voorkomen. Komt elke positief geheel getal voor? We zien direct in dat een oneven getal groter dan 1 niet voorkomt als gat (waarom niet? geef een bewijs!). Komen alle even getallen voor? Zie (19.5).

Opmerking. *Eenvoudig in te zien: er bestaan geen priemgetallen p en q met $q - p = 7$.*
Bewijs. Als p en q even zijn dan is $q - p$ even en dus niet gelijk aan 7. Voor $p = 2$ is $q := 2 + 7 = 9$ niet een priemgetal. QED

(8.3) Opmerking / opzienbarende ontwikkeling. We zagen dat de lengte van gaten in de rij van priemgetallen niet begrensd is. Maar, ondertussen is ook bewezen:

Er zijn oneindig veel gaten begrensd door 7×10^7*:*

Y. Zhang, *Bounded gaps between primes.* Dit zal verschijnen in: Ann. Math. Merk op dat het vermoeden over oneindig veel tweelingen, zie (19.4), equivalent is met :"Er zijn oneindig veel gaten begrensd door 2".
`http://annals.math.princeton.edu/articles/7954`
`http://arxiv.org/abs/1305.6369`

(8.4) Tweelingen. Een antwoord op (1.3)(2)? Er zijn heel veel priemtweelingen bekend. We denken dat er oneindig veel zijn, zie (19.4). Heuristiek maakt duidelijk dat dit het goede antwoord zou moeten zijn. Asymptotische schattingen zijn gemaakt, en die kloppen wonderwel met het numerieke materiaal dat ondertussen rond dit probleem verzameld is. Toch hebben we het gevoel dat we inzicht missen, dat we niet begrijpen wat de structuur is die dit probleem kan verklaren en oplossen. Deze vraag is niet beantwoord.

(8.5) Drielingen. Een antwoord op (1.3)(3).
Voor $n \in \mathbb{Z}_{>1}$ is er in een rij $\{n, n+2, n+4\}$ precies één van die drie getallen deelbaar door 3 (waarom ? geef een bewijs !). Als we de definitie nemen van een drieling zoals in (1.3) dan is één van die drie priemgetallen deelbaar door 3, dus gelijk aan 3. We zien dat $\{3, 5, 7\}$ een priem-drieling is, en dat dit de enige is. Het aantal priem-drielingen is gelijk aan één.

De definitie was niet erg handig, niet erg nuttig, en we komen zo op een vraag die een eenvoudig antwoord heeft.
Kortom: de vraag (1.3)(2) naar tweelingen is zinvol, en die geeft aanleiding tot veel nieuwe inzichten, en tot een nog steeds onopgelost probleem, maar de vraag (1.3)(3) naar drielingen heeft geen zin.

Er is een veel betere definitie die wél een interessante vraag geeft:
Definitie. Een drietal priemgetallen $\{p,\ q,\ r\}$ heet een *priem-triplet* als
$q = p + 2$ en $r = q + 4$, bij voorbeeld $\{5, 7, 11\}, \cdots, \{41, 43, 47\}, \cdots, \{857, 859, 863\}, \cdots$
of $q = p + 4$ en $r = q + 2$, bij voorbeeld $\{7, 11, 13\}, \cdots, \{613, 617, 619\}, \cdots$.
Maak zelf veel priem-tripletten.
Zie `http://en.wikipedia.org/wiki/Prime-triplet`

(8.6) Vermoeden. *Het aantal priem-tripletten is oneindig (?).* (Er is geen bewijs maar we kunnen ook niet bewijzen dat het aantal priem-tripletten eindig is.)

Voor een generalizatie van tweelingen en tripletten, zie "Forbes prime k tuples":
`http://en.wikipedia.org/wiki/Prime_k-tuple`

(8.7) Is er een formule waarmee je voor elke i het i-de priemgetal p_i kunt berekenen?
Deze vraag is niet precies genoeg geformuleerd. Het is belangrijk in de wiskunde om precies te formuleren (we laten vage formuleringen over aan politici en aan ...). Afhankelijk van de goede formulering het antwoord bevestigend of ontkennend:

Ja, zo'n formule bestaat als we alle priemgetallen al kennen.

Wat verwachten we van een formule zoals gevraagd?

(8.8) Voorbeeld. Er is een getal $\alpha \in \mathbb{R}$ zodanig dat:

$$p_n = \lfloor 10^{1+\cdots+n} \cdot \alpha \rfloor - 10^n \cdot \lfloor 10^{1+\cdots+(n-1)} \cdot \alpha \rfloor;$$

notatie: voor een getal $\beta \in \mathbb{R}$ staat $\lfloor \beta \rfloor$ voor het grootste gehele getal kleiner of gelijk aan β:

$$\lfloor \beta \rfloor = m \in \mathbb{Z} \quad \Longleftrightarrow \quad m \leq \beta < m+1.$$

Inderdaad, schrijf

$$\alpha = 0.203005000700011000013\cdots = \sum_{n=1}^{n=\infty} p_n \times 10^{f(n)}$$

waar $f(n)$ gelijk is aan $1+2+\cdots+n$-(het aantal cijfers van p_n). We gebruiken $p_n < 10^n$ (eenvoudig in te zien) om te bewijzen dat α goed gedefinieerd is. Laat zien dat de formule hierboven inderdaad klopt.

Zij we iets opgeschoten? Om het getal α precies genoeg te berekenen, heb je preciese informatie over veel priemgetallen nodig:

als we weten wat $p_1, \cdots, p_n$ precies zijn, dan kun je zo p_n berekenen

(ja allicht !). Het is gemakkelijk een formule te vinden die alle priemgetallen geeft als je alle priemgetallen al kent.
Zie `http://primes.utm.edu/glossary/xpage/FormulasForPrimes.html`

In H. Wilf – *What is an answer?* Amer. Math. Monthly, **89** (1982), 289–292 wordt de vraag gesteld: wat is het verschil tussen een formule en een goede formule?
Zie ook [39].

(8.9) Voorbeeld. Euler liet zien dat voor $0 \leq i \leq 39$ substitutie van $T = i$ in het polynoom $T^2 + T + 41$ een priemgetal geeft. Bestaat er een veelterm die "alle priemgetallen geeft"? Matijasevic bewees in 1971 dat er een veelterm bestaat waarvan alle positieve waarden een priemgetal zijn. Later, zie [40], werd een expliciet polynoom in 26 variabelen van graad 25 gevonden, waarvan alle positieve waarden een priemgetal zijn.

Zijn we iets opgeschoten? Ja, in abstracte zin; deze stelling was van groot belang in de logica. Kunnen we hiermee priemgetallen berekenen? Het blijkt moeilijk om ook maar één enkel priemgetal te berekenen langs deze weg; ik zie ook niet hoe je dit kunt gebruiken om van een getal te beslissen of het priem is.
Zie `http://primes.utm.edu/glossary/xpage/MatijasevicPoly.html`

(8.10) Met de moderne technologie en met het internet kunnen we heel snel alle priemgetallen beneden 10^{12} krijgen.
Zie `http://primes.utm.edu/nthprime/`
$p_{100} = 541$, $p_{500} = 3,571$, $p_{10,000} = 104,729$, $p_{1,000,000} = 15,485,863$,
$p_{100,000,000} = 2,038,074,743$, $p_{100,000,000,000} = 2,760,727,302,517,\cdots$.
Is dit interessant? Schieten we hier iets mee op?
Op die site kun je ook $\pi(x)$ berekenen voor $x < 3{\cdot}10^{13}$.

(8.11) Bestaat er een priemgetal met precies 2013 cijfers? Zou er een tabel bestaan waar we alle priemgetallen met hooguit 2013 cijfers kunnen opzoeken? Nee, beslist niet: het aantal priemgetallen tot 20^{2012} is ongeveer 10^{874}; geschat wordt dat het aantal elementaire deeltjes in ons heelal gelijk is aan zoiets als 10^{78}. Er is dus geen sprake van dat een dergelijke lijst bestaat.

Maar hoe kunnen we die vraag dan wel beantwoorden? We geven de functie $\pi : \mathbb{Z} \to \mathbb{Z}$ (het aantal priemgetallen onder een gegeven grens, zie (0.1)). We kunnen eenvoudig inzien, met behulp van resultaten vermeld in § 10, dat $\pi(10^{2012}) < \pi(10^{2013})$ (eenvoudige beschouwingen, geen diepe stelling gebruikt). Conclusie: er bestaat een priemgetal bestaande uit 2013 cijfers (elementaire beschouwingen geven een bewijs van het bestaan, maar we geven niet een expliciet voorbeeld). Zie (10.3), (10.7).

(8.12) Het vermoeden van Catalan.

$$A^a + 1 = D^d, \quad A, a, D, d \in \mathbb{Z}_{\geq 2}.$$

Eugène Charles Catalan formuleerde in 1844 het vermoeden dat $8 + 1 = 9$ de enige oplossing is van deze vergelijking met $A, a, D, d \in \mathbb{Z}_{\geq 2}$. Er werden veel berekeningen gedaan om te zien of dit weerlegd kon worden. Tot er een effectief resultaat kwam: Tijdeman bewees in 1976 dat er een bovengrens is aan alle mogelijke oplossingen. Die bovengrens, later werd er een door Langevin berekend, bleek wel erg groot: $\exp(\exp(\exp(\exp(730))))$ (waar $\exp(a) = e^a$ gebruikt wordt), een grens ver buiten het bereik van berekeningen. (Later werd die grens wel iets naar beneden gebracht, maar nog steeds ver buiten het bereik van computers.) Lang dachten we dat dit een probleem was waar we nog niet de methoden hadden om dit aan te pakken.

Het bleek dat bestaande methodes uit de algebra wel voldoende waren om het probleem op te lossen: inderdaad is $8 + 1 = 9$ de enige oplossing van het Catalan probleem, zoals Preda Mihăilescu in 2004 bewees; zie [55]. Nadenken en abstract denken triomferen weer over berekeningen.
Zie `http://en.wikipedia.org/wiki/Catalan\%27s-conjecture`.

9 Heuristiek

"*Clearly, no one can mistake these probabilistic arguments for rigorous mathematics and remain in a state of grace. Nevertheless, they are useful in making educated guesses as to how numbertheoretic functions should 'behave'.* " Zie [1], pagina 248.

We geven een discussie van "heuristic arguments", see
http://primes.utm.edu/glossary/xpage/Heuristic.html

Zulke "educated guesses" bewijzen in het algemeen niets. Maar we kunnen ons er wel door laten leiden wat betreft onze intuïtie. We zullen zien dat deze methode resultaten geven over schattingen die merkwaardig accuraat aansluiten bij de werkelijkheid zodra we de nodige berekeningen gemaakt hebben. Daarom denken we vaak dat we zo op het goede spoor zitten. Probeer de beschouwingen hierover te begrijpen en toe te passen. Maar bedenk wel dat schattingen zo gemaakt in de meeste gevallen niets bewijzen. Met deze voorzichtigheid in ons achterhoofd is de methode prachtig.

Beschouw de uitspraak:

"de kans dat een getal $n \in \mathbb{Z}_{>0}$ een priemgetal is, is gelijk aan $\frac{1}{\log n}$."

Dit is onzin: de "kans" dat $n = 1000$ een priemgetal is is gelijk aan 0 (het is niet een priemgetal), en de "kans" dat 997 een priemgetal is, is gelijk aan 1 (want het is wel een priemgetal).

Toch heeft deze onzin-uitspraak nut om het als leidraad te gebruiken.

De uitspraak kan precies gemaakt worden door een schatting te geven van het aantal priemgetallen op het interval $(n - \Delta/2, n + \Delta/2)$. Dat aantal is ongeveer $\Delta/\log n$, en deze uitspraak kan meer precies gegeven worden zodra een effectieve versie van de zwakke vorm van PNT gegeven is.

Ook gebruiken we de uitspraak om een gevoel te krijgen voor een mogelijk antwoord. beschouw bij voorbeeld alle Fermat getallen. We "bewijzen" (?!) dat er maar eindig veel Fermat priemgetallen zijn:

de kans (?) dat F_i priem is, is gelijk aan $1/\log(2^{2^i}) = (1/2^i)(1/\log 2)$; omdat

$$\sum_{0<i<\infty} \frac{1}{\log(2^{2^i})} = \frac{1}{\log 2} \sum_{0<i<\infty} \frac{1}{2^i} < 2 \cdot \frac{1}{\log 2}$$

convergent is, concluderen we (?) dat er maar eindig veel Fermat priemgetallen zijn.

Dit is onzin. Het bewijst niets. Maar het geeft wel een indruk aan ons gevoel: de Fermat getallen liggen nogal willekeurig (dat is niet helemaal waar); laten we daarom deze kansrekening toepassen, en er komt iets uit wat we als vermoeden kunnen formuleren; zie (19.9).

Hier is een afschrikwekkend voorbeeld .

Uitspraak (?) "er zijn oneindig veel even priemgetallen" (is dat waar ?!).
"Bewijs." De kans dat $2n$ een priemgetal is is gelijk aan $1/\log(2n)$ en
de som $\sum 1/\log(2n)$ is divergent.
(De laatste uitspraak is waar, maar deze kansrekening slaat nergens op, en we weten dat er precies één even priemgetal is.)

(9.1) Opgave. Pas deze heuristiek toe, en maak aannemelijk dat er oneindig veel Mersenne priemgetallen zijn. (Ondanks dat er nog maar weinig Mersenne priemgetallen bekend zijn, denken we toch dat er oneindig veel zijn. Schattingen waar "het volgende Mersenne priemgetal ligt" komen steeds merkwaardig goed uit, zie [9], Figure 1.)

(9.2) Opgave. Pas deze heuristiek toe, en maak aannemelijk dat er oneindig veel priemtweelingen zijn.

(9.3) Opgave. Pas deze heuristiek toe, en maak aannemelijk dat er oneindig veel Sophie Germain priemgetallen zijn.

(9.4) Opgave. Pas deze heuristiek toe, en maak aannemelijk dat er oneindig veel priemtripletten zijn.

(9.5) Opgave. Pas deze heuristiek toe, en krijg een gevoel voor (19.5)(1).

(9.6) Een voorbeeld. We vragen ons af hoeveel priemgetallen p er zijn met de eigenschap $p = n^2 + 1$ onder een gegeven grens x; laten we dit aantal noteren als $A(x)$; het vermoeden is, dat $A(x)$ onbegrensd is voor $x \to \infty$, zie (19.16). In [9], 3.8 vinden wat de heuristiek ons daarover als suggestie geeft:

$$A(x) \sim (1.3728134628\cdots) \times \frac{\sqrt{x}}{\log(x)} =: B(x).$$

Dit blijkt (in veel gevallen) heel goed te kloppen met de werkelijkheid, bij voorbeeld:

$$x = 10^{14}, \quad A(x) = 456362, \quad B(x) \approx 456404,$$

zie [9], Table 8; een verbluffende nauwkeurigheid van de heuristische methode in dit geval.

De methode van deze paragraaf is met succes toegepast op een schatting van het aantal priemtweelingen. Omdat we weten dat voor een oneven priemgetal p het getal $p + 2$ ook oneven is, denken we dat de kans dat dit getal ook priem is iets groter is dan $1/\log(p + 2)$. Dat verdisconteren we. Zo zijn er schattingen gemaakt van het aantal priemtweelingen op een interval, of beneden een gegeven grens, zie (19.4). Die schattingen komen merkwaardig goed overeen daar waar we door berekeningen weten hoeveel het er precies zijn op een gegeven interval. Dit geeft moed dat deze benadering niet helemaal onzin in (maar we blijven ons bewust dat er zo niet een bewijs gegeven wordt):

de benadering geschetst in deze paragraaf, hoe discutabel dan ook, levert ons een merkwaardig goed gevoel *wat "er waar zou moeten zijn", in welke richting we soms moeten zoeken.*

10 De priemgetal stelling (PNT)

(Voor de notatie $\log(x)$ zie (2.3).)
We bespreken in deze paragraaf een manier om het aantal priemgetallen onder een bepaalde grens te schatten: een diepe stelling die dat exact doet (een schitterend resultaat) "in de limiet", en een zwakkere vorm die uitstekend te gebruiken is in veel concrete situaties (en die heel gemakkelijk en elementair te bewijzen valt).

(10.1) Stelling* (Chebyshev, Hadamard en De la Vallée-Poussin).

$$\pi(x) \quad \sim \quad \frac{x}{\log x}.$$

Dit betekent:

$$\lim_{x\to\infty} \pi(x)/\frac{x}{\log x} = 1.$$

Een andere manier van formuleren: $\forall \epsilon \in \mathbb{R}_{>0} \quad \exists N \in \mathbb{Z}$ met:

$$x > N \Longrightarrow (1-\epsilon)\frac{x}{\log x} < \pi(x) < (1+\epsilon)\frac{x}{\log x}.$$

Dit is een diepe stelling, er zijn vele bewijzen, en elk daarvan is lang en moeilijk. Maar er is een versie die zwakker is, en die in heel veel gevallen goed bruikbaar is. Er zijn heel eenvoudige, elementaire bewijzen voor bepaalde waarden van ϵ. Ik noem een van de vele versies:

(10.2) Stelling.

$$x > 10 \quad \Longrightarrow \quad \frac{1}{3}\frac{x}{\log x} < \pi(x) < 3\frac{x}{\log x}.$$

Zie Th.10.2.1 in [5]; het bewijs is werkelijk elementair en eenvoudig. Er zijn veel scherpere varianten. Zie ook [93].

Voor een scherpere verzie en verwijzingen zie
`http://en.wikipedia.org/wiki/Prime_number_theorem`
Bij voorbeeld:

$$x \geq 55 \quad \Longrightarrow \quad \frac{x}{\log(x)+2} < \pi(x) < \frac{4}{\log(x)-4}.$$

(10.3) Een voorbeeld. Omdat

$$9 \times 2013 = 18117 < 10 \times 2012$$

volgt:

$$\pi(10^{2012}) \quad < \quad 3{\cdot}\frac{10^{2012}}{2012{\cdot}\log 10} \quad < \quad \frac{1}{3}{\cdot}\frac{10^{2013}}{2013{\cdot}\log 10} \quad < \quad \pi(10^{2013}).$$

Dus bestaat er een priemgetal met 2013 cijfers.

(10.4) Gevolg.* *Voor het n-de priemgetal geldt*

$$p_n \sim n \log n.$$

Er is een effectieve versie: er bestaan C, D, N (die je kunt uitrekenen) zodanig dat voor alle $n \geq N$ er geldt

$$A{\cdot}n\log n < p_n < B{\cdot}n\log n.$$

(10.5) Een voorbeeld. Een lange berekening leert: $p_{100,000,000,000} = 2,760,727,302,517$; een afschatting geeft: voor $n = 100,000,000,000$ geldt $n \log n \approx 2.302585093 \times 10^{12}$. We zien dat hier $p_n/(n \log n) \approx 1.198770$.

Hier is $\log n + \log(\log n) \approx 35.709281077$. We zien dat in dit geval de volgende afschatting geldt.

(10.6) Een scherpere versie van de zwakke vorm. Voor $n \geq 6$ hebben we:

$$\log n < \frac{p_n}{n} < \log n + \log(\log n).$$

Zie `http://en.wikipedia.org/wiki/Prime_number_theorem`

(10.7) Een toepassing. Kies $n = 22 \times 10^{2007}$. We zien:

$$\log(n) \approx 4624 \quad \text{en} \quad 22 \cdot \log(n) \approx 101728;$$

dus

$$1.01 \times 10^{2012} < n \log n < p_n.$$

Verder geldt $\log(\log n) \approx 8.4$; dus

$$p_n < n(\log n + \log(\log n)) \approx 22 \cdot 10^{2007} \cdot (4624 + 8.4) \approx 101926 \cdot 10^{2007} < 1.02 \times 10^{2012}.$$

Conclusie:

$$10^{2012} + 10^{2010} < p_n < 10^{2012} + 2 \cdot 10^{2010}.$$

We zien dat inderdaad dit priemgetal p_n precies 2013 cijfers heeft. We zien dat de schattingen (die bewezen zijn, geen heuristiek) laten zien dat er tenminste één priemgetal op dit interval ligt. Maar we weten niet "hoe dat priemgetal eruit ziet".

Er liggen vast nog meer priemgetallen in dit interval (hoeveel ongeveer?); dat is iets moeilijker te bewijzen; ik denk dat het exacte aantal niet met abstracte methodes te bepalen is.

(10.8) Conclusie. 1. Er zijn oneindig veel priemgetallen. Naarmate we grotere getallen beschouwen zijn er steeds minder (exact: het aantal priemgetallen op een interval van vaste lengte gaat asymptotisch naar nul naarmate we steeds grotere getallen beschouwen).
2. Het verschijnen van priemgetallen in de rij van gehele getallen lijkt chaotisch, maar de functie $\pi(x)$ lijkt (op grove schaal) een "gladde functie".
3. De afstand tussen twee opeenvolgende priemgetallen is onbegrensd; echter, we denken dat het aantal priem-tweelingen (paren van twee priemgetallen p en $p+2$) oneindig is ("opeenvolgende priemgetallen liggen vaak ver van elkaar, en liggen vermoedelijk oneindig vaak vlak bij elkaar").
4. Het is vaak moeilijk om te beslissen of een (erg) groot getal een priemgetal is; echter we kunnen wel in veel gevallen iets zeggen "hoeveel priemgetallen er liggen op een gegeven interval" (zonder de individuele priemgetallen te kennen, zonder een lijst te maken).

11 Het ABC vermoeden

Deze paragraaf gaat over een "eenvoudig" vermoeden, dat mogelijk nu opgelost is. Dit zou wel eens een revolutie in de getaltheorie kunnen betekenen. Het probleem is zo eenvoudig te formuleren. Het ABC vermoeden wordt ook wel het Oesterlé-Masser vermoeden (1985/1988) genoemd. Als het waar is dan zijn de gevolgen enorm. Shinichi Moichizuki claimt een bewijs met behulp van een nieuwe methodes.

(11.1) We beschouwen $A, B, C \in \mathbb{Z}_{>0}$ met

$$A + B = C \quad \text{met} \quad \text{ggd}(A, B) = 1 \quad (*)$$

(dat is toch wel heel eenvoudig ....). Voor een dergelijk drietal positieve gehele getallen definiëren we de *conductor*, ook wel genoemd het *radicaal*:

$$\text{Cond}(A, B, C) := \prod_{p|ABC} p,$$

het product genomen over alle priemgetallen (tot de macht één, !!) die of A of B of C delen. Het ABC vermoeden zegt iets over het vergelijken van de grootste van die drie getallen en $\text{Cond}(A, B, C)$.
Zie `http://en.wikipedia.org/wiki/Abc_conjecture`
`http://www.math.leidenuniv.nl/~desmit/papers/naw_abc.pdf`
We beginnen met een heel eenvoudige vorm van het vermoeden (mogelijk te sterk geformuleerd als we α "te klein" nemen):

(11.2) Zij $\alpha \in \mathbb{R}_{>1}$.

$$(\text{ABC})_\alpha \qquad \forall\ (A, B, C, *) \quad \stackrel{?}{\Longrightarrow} \quad C < \text{Cond}(A, B, C)^\alpha.$$

(11.3) Eerste verrassing. Voor een α die een beetje groot is, is het moeilijk om tegenvoorbeelden te vinden. In het bijzonder:

Voorbeeld (Reyssat, 1987) $\quad 2 + 3^{10} \times 109 = 23^5, \quad 23^5 < (2{\cdot}3{\cdot}109{\cdot}23)^{1.63}$;

er zijn geen voorbeelden bekend die de uitspraak

$$C \quad \stackrel{?}{<} \text{Cond}(A, B, C)^{1.63}$$

tegenspreken. Is $(\text{ABC})_2$ waar?

Voor nog veel meer voorbeelden van drietallen bekend, die geconstrueerd zijn om inzicht in dit vermoeden te krijgen; zie:
Zie `http://www.math.leidenuniv.nl/ desmit/abc/index.php?set=1`
Dat project berekent speciale gevallen. De uitkomsten zijn spectaculair.

(11.4) De kwaliteit van een drietal. Een ander manier van formuleren: de *kwaliteit* van een drietal (A, B, C) is het getal β met

$$C = (\text{Cond}(A, B, C))^\beta, \quad \text{qual}(A, B, C; *) = \beta.$$

Er zijn geen drietallen gevonden met $\mathrm{qual}(A,B,C;*) > 1.63$ (ondanks veel rekenwerk). Bij dat rekenwerk werden slimme algoritmen ingezet (met name het LLL algoritme .... ik geef hier geen uitleg).

De kwaliteit is laag als er weinig hoge machten van priemfactoren van ABC zijn; voorbeeld: $\mathrm{qual}(4,127,1313) \approx 0.468$, $\mathrm{qual}(1,37,38) = \log(38)/\log(37{\cdot}2{\cdot}17) \approx 0.50184$.

De kwaliteit is hoog als er veel hoge machten van priemfactoren van ABC zijn, zoals in het (tot nu toe mooiste) voorbeeld van Reyssat:

$$\mathrm{qual}(2, 3^{10}{\cdot}109, 23^5) \approx 1.6299.$$

Voor meer voorbeelden zie `http://www.math.leidenuniv.nl/~desmit/abc/?set=2`
`http://www.math.leidenuniv.nl/~desmit/abc/?set=1`

(11.5) De laatste stelling van Fermat. Hierover zal ik iets vertellen. Hier is de uitspraak:

$$x,y,z,n \in \mathbb{Z},\ n \geq 3,\quad x^n + y^n = z^n \quad \stackrel{?!}{\Longrightarrow} \quad xyz = 0.$$

Voor $n = 1$ en voor $n = 2$ heeft deze vergelijking veel oplossingen. De uitspraak hierboven zegt: voor $n \geq 3$ heeft de vergelijking $X^n + Y^n = Z^n$ geen oplossingen in positieve gehele getallen. Dit werd vermoed door Fermat. In (13.9) bespreek ik wat ik denk dat het bewijs was dat Fermat voor ogen zweefde (maar hij heeft daarover niets gepubliceerd, behalve dat hij de uitspraak als stelling in de kantlijn van een boek vermeldde.) Vele eeuwen is er naar een oplossing gezocht. Indrukwekkend veel theorie, heel veel berekeningen (die FLT bewezen voor $3 \leq n \leq 1,500,000$), speciale gevallen werden beschouwd, deelresultaten, tot tenslotte Andrew Wiles in 1995 bewees dat Fermat inderdaad gelijk had: een van de meest spectaculaire resultaten in de wiskunde van de laatste jaren.

(11.6) Tweede verrassing. Onderstel er bestaat een α waarvoor $(\mathrm{ABC})_\alpha$ waar is. Als bovendien $n > 3{\cdot}\alpha$ dan geldt:

$$(\mathrm{FLT})_n: \quad a,b,c \in \mathbb{Z}_{\geq 0},\quad a^n + b^n = c^n \Longrightarrow abc = 0$$

("de Fermat vergelijking voor deze n heeft geen oplossingen voor positieve gehele getallen").
Bewijs. Onderstel dat $(\mathrm{ABC})_\alpha$ waar is, en $n > 3{\cdot}\alpha$. Onderstel dat er bestaan $a,b,c \in \mathbb{Z}_{>0}$ met $a^n + b^n = c^n$. Schrijf $A = a^n$, $B = b^n$, en $C = c^n$. Dan geldt enerzijds:

$$\mathrm{Cond}(A,B,C) = \mathrm{Cond}(a,b,c) \leq abc < c^3;$$

anderzijds zegt $(\mathrm{ABC})_\alpha$ dat

$$c^n = C < \mathrm{Cond}(A,B,C)^\alpha = \mathrm{Cond}(a,b,c)^\alpha \leq (abc)^\alpha < (c^3)^\alpha.$$

De conclusie $c^n < c^{3\cdot\alpha}$ is in tegenspraak met $c > 1$ en $n > 3{\cdot}\alpha$. QED

We zien dat de juistheid van dit vermoeden, in deze sterke vorm (11.2), waar α berekend kan worden, vérstrekkende gevolgen zou hebben.

(11.7) Het ABC vermoeden. Dit vermoeden werd voor het eerst geformuleerd door D. Masser (1985) en door J. Oesterlé (1988). Voor meer informatie, en voor uitgebreide literatuur verwijzingen zie:
`http://en.wikipedia.org/wiki/Abc_conjecture`

Formulering I. *Voor elke $\varepsilon \in \mathbb{R}$ met $\varepsilon > 0$ zijn er maar* **eindig** (?) *veel drietallen (A,B,C) die voldoen aan $(*)$ zodanig dat $C > \mathrm{Cond}(A,B,C)^{1+\varepsilon}$.*

(11.8) Formulering II. *Voor elke* $\varepsilon \in \mathbb{R}$ *met* $\varepsilon > 0$ *is er een constante* $\gamma = \gamma(\varepsilon) \in \mathbb{R}$ *zodanig dat voor elke drietal* (A, B, C) *dat aan* $(*)$ *voldoet geldt:*

$$C \overset{?}{<} \gamma(\alpha) \times (\mathrm{Cond}(A, B, C))^{1+\varepsilon}.$$

Deze "ineffectieve formuleringen" (het bestaan van de constante γ geeft nog niet wat die constante is) zijn niet voldoende om FLT te bewijzen.

(11.9) Formulering III. *Voor elke* $\varepsilon \in \mathbb{R}$ *met* $\varepsilon > 0$ *zijn er maar* **eindig** (?) *veel drietallen* (A, B, C) *die aan* $(*)$ *voldoen met* $\mathrm{qual}(A, B, C) > 1 + \varepsilon$.

(11.10) Opmerking. Er zijn oneindig veel (A, B, C) die aan $(*)$ voldoen met $\mathrm{qual}(A, B, C) > 1$:
Opgave. Bewijs dat

$$q_n := \mathrm{qual}(1, \quad 9^n - 1, \quad 9^n) > 1 + \frac{1}{8n} \quad \text{voor alle} \quad n \in \mathbb{Z}_{>0},$$

zie `http://www.math.leidenuniv.nl/~desmit/papers/naw_abc.pdf`

Voorbeeld, zie `http://en.wikipedia.org/wiki/Abc_conjecture`: het aantal $(A, B, C; *)$ met $C < 10^{18}$ en $1 < \mathrm{qual}(A, B, C) < 1.05$ is 12129960.

(11.11) Nieuwe ontwikkelingen. Formuleringen van het ABC-vermoeden, en van gerelateerde vermoedens zijn te vinden in [86]. Shinichi Moichizuki (Kyoto, Japan) heeft in een manuscript van ongeveer 500 pagina's manuscript (4 delen) gebaseerd bovendien op 10 eerdere artikelen van dezelfde auteur geclaimd dat het ABC-vermoeden juist is; zie
`http://www.kurims.kyoto-u.ac.jp/~motizuki/top-english.html`
Deze bewijzen zijn nog door niemand anders begrepen. Er wordt hard aan gewerkt. Zowel het resultaat, als de methoden, indien correct, betekenen een grote doorbraak in de getaltheorie.

(11.12) Opgave. Is het waar dat $7^{100} + 1 = 19^{66}$?
Geeft dit een tegenvoorbeeld tegen $(\mathrm{ABC})_{38}$?

12 Appendix A: Notaties en symbolen

Wiskundigen gebruiken sommige notaties, symbolen. Die zijn bedoeld als stenografie. Ze geven een snelle en preciese manier om informatie compact weer te geven. Ik zal me in deze cursus van een paar aspecten van wiskundige notatie bedienen. Het stroomlijnt tekst en uitleg en het maakt wiskundige beweringen vaak nauwkeuriger.

Hieronder leg ik een paar aspecten van wiskundige notatie uit. Maar ik geef niet een college logica of verzamelingen-leer.

(12.1) Het esti-symbool. *We schrijven: $x \in V$; uit de notatie volgt dat V een verzameling is, dat x een element is, en dat het element x in de verzameling V zit.*
Bij voorbeeld, x is de persoon Anne Frank, V is de verzameling van mensen die in de 20ste eeuw geboren zijn; we zien dat $x \in V$ een uitspraak is die waar is, en die we kunnen lezen als: "Anne Frank is in de 20ste eeuw geboren".

We gebruiken het symbool $\notin$ om aan te geven dat het element links ervan niet bevat is in de verzameling rechts daarvan. Zij y de persoon Johann Sebastian Bach. De uitspraak $y \in V$ is niet waar, en $y \notin V$ is wel waar.

(12.2) Inclusie. We gebruiken het symbool $\subset$ om aan te geven dat er links daarvan een verzameling staat, die bevat is in de verzameling die er rechts van staat. Bij voorbeeld laat W de verzameling van vrouwelijke Nederlanders zijn geboren in de 20ste eeuw. De uitspraak $W \subset V$, met V als hierboven, is een ware uitspraak.
Pas op. De uitspraak $x \subset V$ is grammaticaal onjuist: het element x wat links staat is niet een verzameling.

(12.3) We geven met $\{\cdots\}$ een verzameling aan, waar tussen te haken gepreciseerd wordt welke elementen beschouwd worden.
Voorbeeld: $\{x\} \subset V$ is een uitspraak equivalent met $x \in V$.
$\{2, 5\} \subset \{1, 2, 3, 4, 5, 6\}$ is een uitspraak die juist is.

(12.4) Gehele getallen. Met $\{z \mid \cdots\}$ geven we aan de verzameling van alle elementen z die voldoen aan de restricties rechts van $|$.
Voorbeeld: met $\{n \mid n \text{ is een geheel getal}\}$ geven we aan de verzameling van alle gehele getallen. Die verzameling zullen we noteren als $\mathbb{Z}$.
$\frac{2}{7} \notin \mathbb{Z}$ en $0 \in \mathbb{Z}$ zijn juist, en $\{-3, 5, 18\} \subset \mathbb{Z}$ is juist.

(12.5) Rationale getallen. De verzameling van *breuken van gehele getallen* geven we aan met $\mathbb{Q}$. Een dergelijk getal wordt een *rationaal* getal genoemd. Merk op dat bij voorbeeld de regel $2/7 = (3{\cdot}2)/(3{\cdot}7)$ geldt. Merk op dat $\mathbb{Z} \subset \mathbb{Q}$; inderdaad een geheel getal $n \in \mathbb{Z}$ kan ook gezien worden als breuk $n/1 \in \mathbb{Q}$. (Verzoek: spreek niet van rationele getallen.)

(12.6) Reële getallen*. We kunnen nog en algemener getal begrip invoeren (we geven een definitie die niet helemaal compleet is). Dit kunnen we doen door de verzameling van alle decimale breuken te beschouwen, waar we oneindig veel decimalen achter de komma toelaten (met nog een afspraak, die bijvoorbeeld zegt dat $1.9999\cdots = 2$). Een dergelijk getal wordt *een reëel getal genoemd*. De verzameling van reële getallen wordt aangegeven met $\mathbb{R}$. We schrijven $\mathbb{C}$ voor de verzameling van complexe getallen: alle getallen van de vorm $a + b\sqrt{-1}$ met $a, b \in \mathbb{R}$. Merk op $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

(12.7) *Er zijn reële getallen die niet rationaal zijn.*
Bewering. $\sqrt{2} \notin \mathbb{Q}$.
Bewijs. (Bewijs uit het ongerijmde.) Veronderstel dat er gehele getallen $m, n \in \mathbb{Z}$ zijn zodanig dat $\sqrt{2} = m/n$. Kwadrateren geeft: $m^2 = 2{\cdot}n^2$. We weten dat ontbinden van gehele getallen in priemfactoren uniek is. Het aantal factoren 2 in n^2 is *even*. We zouden concluderen dat het aantal factoren 2 in $2{\cdot}n^2 = m^2$ *oneven* zou zijn. Deze tegenspraak bewijst de bewering. QED

Opmerking. In de oude Griekse wiskunde was dit een schok: dat er getallen bestaan die niet rationaal zijn. Gehele getallen en quotiënten daarvan werden gezien als bouwstenen. Dat er ook andere getallen bestaan werd eerst niet vermoed, en later in de Griekse wiskunde als vreemd ervaren.

(12.8) Opmerking. Getallen die beschreven kunnen worden als oplossing van een polynoom-vergelijking worden *algebraïsche getallen* genoemd. Gebruikmakend van het begrip *aftelbaarheid*, zie (12.9), kan worden aangetoond dat de verzameling van algebraïsche getallen *aftelbaar* is. Omdat het diagonaal-principe van Cantor aantoont dat $\mathbb{R}$ niet aftelbaar is, zie (12.10), concluderen we: *er zijn reële getallen die niet algebraïsch zijn.* Dit bewijs construeert niet zulke getallen. Het is doorgaans niet zo gemakkelijk constructief het bestaan van zulke getallen aan te tonen.
Voorbeeld. Het getal π is *niet een rationaal getal*, d.w.z. $\pi \notin \mathbb{Q}$ (Lambert 1761; Legendre 1794; Hermite 1873). Pas veel later werd bewezen dat π niet een algebraïsch getal is (Lindemann 1882). Dit resultaat loste een eeuwen-oud probleem op, de kwadratuur van de cirkel: *het is niet mogelijk met passer en liniaal een vierkant te construeren waarvan de oppervlakte gelijk is aan die van een gegeven cirkel.*

(12.9) Aftelbaar. We zeggen dat een verzameling V *aftelbaar oneindig* is als alle elementen daarvan genummerd kunnen worden met behulp van de positieve gehele getallen $1, 2, 3, \cdots$. Anders gezegd: als er een bijectieve afbeelding $\mathbb{Z}_{>0} \to V$ bestaat.

Voorbeeld/Opgave: $\mathbb{Q}$ is aftelbaar oneindig.
Aanwijzing. Laat zien dat het voldoende is om dit te bewijzen voor alle $a/b \in \mathbb{Q}$ met $0 \leq a/b < 1$; zet al die getallen in een (aftelbare) lijst, bij voorbeeld als volgt: $0, 1/2, 1/3, 2/3, 1/4, 3/4, 1/5, 2/5, \cdots$.]

Cantor bewees dat $\mathbb{R}$ niet aftelbaar is, zie (12.10). Hier is dat principe zoals dat door Cantor ontwikkeld werd. Bij voorbeeld zie
http://en.wikipedia.org/wiki/Cantor's_diagonal_argument

(12.10) Stelling (Cantor). *De verzameling $\mathbb{R}$ is overaftelbaar.*
Dit wil zeggen: als $\alpha_1, \alpha_2, \alpha_3, \ldots$ een rij reële getallen is, dan bestaat er een $\beta \notin \mathbb{R}$.
Bewijs. Het is al voldoende om te bewijzen dat de verzameling $\{\gamma \in \mathbb{R} \mid 0 \leq \gamma < 1\}$ overaftelbaar is. Veronderstel een dergelijk rij als boven is gegeven met bovendien $0 \leq \alpha_i < 1$ voor alle i. Van elk van deze getallen schrijven we de decimale ontwikkeling uit:

$$\alpha_1 = 0,\ a_{1,1}\ a_{1,2}\ a_{1,3}\ a_{1,4} \cdots,$$

$$\alpha_2 = 0,\ a_{2,1}\ a_{2,2}\ a_{2,3}\ a_{2,4}\ \cdots,$$

$$\alpha_3 = 0,\ a_{3,1}\ a_{3,2}\ a_{3,3}\ a_{3,4}\ \cdots,$$

etc.. We construeren positieve gehele getallen $b_1, b_2, \cdots \in \{0,1\}$ zo dat $b_1 \neq a_{1,1}, \quad b_2 \neq a_{2,2}$, $\cdots b_i \neq a_{i,i}$ voor alle i, b.v. door: als $a_{i,i} > 0$ dan kiezen we $b_i = 0$ en als $a_{i,i} = 0$ dan kiezen we $b_i = 1$. (Dit heet het "Diagonalverfahren".) Schrijf

$$\beta := 0,\ b_1\ b_2\ b_3 \cdots .$$

Omdat $b_i \neq a_{i,i}$ volgt $\beta \neq \alpha_i$ voor elke i; dus komt β niet in bovenstaande lijst voor. We hebben bewezen dat $\mathbb{R}$ overaftelbaar is. QED

(12.11) We geven met $\Rightarrow$ een logische implicatie aan. Bij voorbeeld $x = 1 \Rightarrow x > 0$ is grammaticaal juist en bovendien een ware uitspraak.

Met $\Longleftrightarrow$ geven we een equivalentie van beweringen aan. Met $\wedge$ geven "en" aan en met $\vee$ het zwakke "of". Voorbeeld: $x^2 = 1 \Rightarrow (x \leq +1) \vee (x \geq -1)$ is een ware uitspraak.

Het symbool $\cap$ wordt gebruikt voor de doorsnede van verzamelingen (de verzameling van gemeenschappelijke elementen), en met $\cup$ geven we de vereniging aan (de verzameling van elementen die in een van beide ligt, of in allebei).
Voorbeelden: $\{x \mid x \in \mathbb{Z}, \quad x \geq 0\} \cap \{x \mid x \in \mathbb{Z}, \quad x \leq 0\} = \{0\}$,
$\{x \mid x \in \mathbb{Z}, \quad x \geq 0\} \cup \{x \mid x \in \mathbb{Z}, \quad x \leq 7\} = \mathbb{Z}$.

(12.12) Met $f : V \to W$ geven we aan dat V en W verzamelingen zijn, en dat f een afbeelding is van V naar W; dat betekent dat f aan elk element van v een element van W toevoegt.

Bij voorbeeld $f : \mathbb{R} \to \mathbb{R}$ gedefiniëerd door $f(x) = x^2$. Dit kan ook weergegeven worden door $x \mapsto x^2$. Let op, de notatie $x \to V$, waar x een element is, is grammaticaal onjuist (aan beiden kanten van $\to$ moet een verzameling staan); de notatie $\{x\} \to V$ is grammaticaal wel juist.

We zeggen dat f injectief is als voor alle $v, v' \in V$ geldt $v \neq v' \Rightarrow f(v) \neq f(v')$; schrijfwijze: $f : V \hookrightarrow W$.

We zeggen dat $f : V \to W$ surjectief als elk element in W het beeld is van een element in V; notatie $f : V \twoheadrightarrow W$.

Ga na: $f : \mathbb{R} \to \mathbb{R}$ gedefiniëerd door $f(x) = x^2$ is niet injectief, en is niet surjectief.

(12.13) $\exists$: er betaat/er bestaan; $\forall$: voor alle.

Met $x := 3$ bedoelen we: "we definiëren x als gelijk te zijn aan 3". Bij het symbool $:=$ staat links een nog niet gedefiniëerd begrip, en rechts ervan iets wat we al kennen.

Met $a \equiv b \pmod{c}$, spreek uit "a is equivalent met b modulo c", bedoelen we: het verschil $a - b$ is deelbaar door c.
Voorbeeld: $1 \equiv 7 \pmod{3}$ is een juiste uitspraak. Ook $2 \not\equiv 7 \pmod{3}$ is juist.
De volgende uitspraak is juist: $(a \equiv 0 \pmod{2}) \Longleftrightarrow (a \text{ is even})$.

Voor een eindige verzameling V schrijven we $\#(V)$ voor het aantal elementen van die verzameling.

Veronderstel dat $a_1, \cdots, a_n$ getallen zijn. De som daarvan wordt genoteerd als

$$\sum_{1 \leq i \leq n} a_i := a_1 + \cdots + a_n.$$

Samenvatting

$x \in V$ het element x is bevat in de verzameling V; $y \notin V$;
$W \subset V$ deelverzameling; $V \cap W$ doorsnede; $V \cup W$ vereniging;
$\{z \mid \cdots\}$ verzameling van elementen die aan de voorwaarde(n) $\cdots$ voldoen;
$\mathbb{Z}$ verzameling van gehele getallen, $\mathbb{Q}$ van rationale getallen,
$\mathbb{R}$ van reële getallen, $\mathbb{C}$ van complexe getallen;
$f : V \to W$ afbeelding tussen verzamelingen; $\hookrightarrow$ injectief; $\twoheadrightarrow$ surjectief;
$\Longrightarrow$ logische implicatie; $\Longleftrightarrow$ logische equivalentie;
:= links wordt gedefiniëerd door middel van wat er rechts staat;
$a \equiv b \pmod{c}$ "a is equivalent met b modulo c".

13 Appendix B: De ring van de gehele getallen

De paragrafen §§ 13, 14 en 15 geven een paar van de basis-technieken in elementaire algebra. Deze paragrafen bevatten onvoldoende bewijzen. Als u alle resultaten wilt begrijpen inclusief de bewijzen, dan kunt u literatuur over algebra en over elementarie getaltheorie raadplegen; we noemen: [87], [83], [5], [47], [48], [37], [8], [46], [81], [48], [22]

In deze paragraaf bespreken we een paar eigenschappen van de ring $\mathbb{Z}$, en van het rekenen "modulo n", m.a..w. rekenen in $\mathbb{Z}/n$. (In § 14 geven we een formele definitie van de begrippen "groep", "ring", "lichaam").

(13.1) Definitie. We zeggen dat $d \in \mathbb{Z}$ een *deler* is van $a \in \mathbb{Z}$ als er bestaat een $d' \in \mathbb{Z}$ zodanig dat $d \cdot d' = a$. We noteren dit als $d \mid a$; als c niet een deler is van a dan noteren we dit als $c \nmid a$.

Een getal $p \in \mathbb{Z}$ heet een *priemgetal* als $p \in \mathbb{Z}_{>1}$ en als elke $1 < i < p$ niet een deler is van p. M.a.w. de enige positieve delers van p zijn 1 en p.

(13.2) Opmerkingen. Er zijn oneindig veel priemgetallen (zoals Euclides al heel lang geleden bewees). Probeer een bewijs te vinden (of lees § 3).

Euler, bij voorbeeld, beschouwde 1 ook als een priemgetal; daar is niets op tegen, maar formuleringen worden eenvoudiger als we eisen dat dit niet als priemgetal gezien wordt, zoals nu gebruikelijk is.

Een van de moeilijke problemen in computer-technologie: gegeven een (heel groot) getal, ga na of het een priemgetal is, en zo nee, vind een factorizatie in priem factoren. In theorie geen probleem (het is wel een priemgetal of je kunt het factoriseren), maar in de praktijk bar lastig.

Belangrijke eigenschap, veel gebruikt in bewijzen:

(13.3) Stelling. *Beschouw $n \in \mathbb{Z}_{>1}$;*

(1) *n kan ontbonden worden als een product van priemgetallen;*

(2) *die ontbinding in priem factoren is uniek op de volgorde na.* Hiermee bedoelen we: *als*

$$n = p_1 \times \cdots \times p_s = \ell_1 \times \cdots \times \ell_t,$$

waar alle p_i en alle ℓ_j priemgetallen zijn, dan is $s = t$ en na eventueel omnummeren geldt $p_1 = \ell_1, \quad \cdots \quad , p_s = \ell_s$.

We ontwikkelen een methode om dit te bewijzen.

(13.4) Lemma (deling met rest). *Laat gegeven zijn gehele getallen $n, d \in \mathbb{Z}$ met $d > 0$. Dan bestaan er $q, r \in \mathbb{Z}$ zodanig dat:*

$$n = q \cdot d + r \quad \textit{met} \quad 0 \leq r < d.$$

Bewijs. Voor elke $j \in \mathbb{Z}$ beschouw

$$I_j = \{jd, jd+1, \cdots jd+d-1\} = \{m \in \mathbb{Z} \mid jd \leq m < (j+1)d\}.$$

Duidelijk: als $j \neq k$ dan is $I_j \cap I_k = \emptyset$ en

$$\mathbb{Z} = \cdots \cup I_{-1} \cup I_0 \cup I_1 \cup I_2 \cup \cdots \ .$$

Hieruit volgt dat er voor elke $n \in \mathbb{Z}$ er precies één $q \in \mathbb{Z}$ is met $n \in I_q$. Dit is equivalent met $n = q{\cdot}d + r$ met $0 \leq r < d$. QED

(13.5) De grootste gemene deler. Voor $a \in \mathbb{Z}$ definiëren we $\mid a \mid$, de absolute waarde van a als volgt: als $a \geq 0$ dan is $\mid a \mid = a$; als $a \leq 0$ dan is $\mid a \mid = -a$.

Zij gegeven $a,\ b \in \mathbb{Z}$, waar tenminsten één van beide niet gelijk is aan 0. We definiëren de grootste gemene deler d van a en b als volgt: beschouw

$$\{\delta \quad | \quad 0 \leq \delta \leq \mid a \mid, \quad 0 \leq \delta \leq \mid b \mid, \quad \delta \text{ deelt } a, \quad \delta \text{ deelt } b\};$$

merk op dat deze verzameling niet leeg is (het bevat het getal 1). Bovendien is deze verzameling eindig. Het grootste getal in deze verzameling noteren we als $\mathrm{ggd}(a, b)$, de *grootste gemene deler* $d = \mathrm{ggd}(a, b)$ van a en b. Merk op: voor $a = 0$ geldt $\mathrm{ggd}(0, b) = \mid b \mid$; er geldt $\mathrm{ggd}(a, b) > 0$. Als $\mathrm{ggd}(a, b) = 1$, dan zeggen we dat a en b *onderling ondeelbaar* zijn.

(13.6) Lemma. *Zij gegeven $a,\ b \in \mathbb{Z}$. Schrijf $d := \mathrm{ggd}(a, b)$. Er bestaan $x, y \in \mathbb{Z}$ zodanig dat*

$$xa + yb = d.$$

Bewijs. Als $a = 0$ of $b = 0$, dan is de uitspraak waar (ga na). Neem aan dat $\mid a \mid \geq \mid b \mid$ (zo niet, verwissel dan a en b). Als $\mid b \mid = d$ dan voldoet $x = 0$ en $y = \pm 1$. Neem aan dat $\mid b \mid > d$.

Beschouw alle paren gehele getallen (α, β) zodanig dat $\mid \alpha \mid \geq \mid \beta \mid > 0$ en $\mathrm{ggd}(\alpha, \beta) = d$. We nemen aan (inductie hypothese) dat de uitspraak van het lemma waar is voor alle paren (α, β) als boven met $\mid b \mid > \mid \beta \mid \geq d$. Uit (13.4) volgt dat er bestaat:

$$a = q{\cdot}b + r \quad \text{met} \quad 0 \leq r < \mid b \mid .$$

Ga na: $\mathrm{ggd}(a, b) = \mathrm{ggd}(b, r)$. De inductie hypothese zegt dat we kunnen kiezen $x', y' \in \mathbb{Z}$ met

$$x'{\cdot}b + y'{\cdot}r = d; \quad \text{dus} \quad y'{\cdot}a - q{\cdot}b + x'{\cdot}b = d.$$

Voor $x := y'$ en $y := -q + x'$ krijgen we de gevraagde uitspraak. QED

(13.7) Het algoritme van Euclides. Hier is een meer inzichtelijke vorm van het bewijs van het bovenstaande lemma. Begin met $a_1 = a \geq b = a_2 > 0$ en schrijf $a_1 = q_1 a_2 + a_3$, met $0 \leq a_3 < a_2$. Ga inductief verder

$$a_i = q_i a_{i+1} + a_{i+2}, \quad 0 \leq a_{i+2} < a_{i+1}.$$

Merk op dat $d = \mathrm{ggd}(a_1, a_2) = \ldots = \mathrm{ggd}(a_{i+1}, a_{i+2}) = \cdots$. De rij $a_2 > a_3 > \cdots \geq 0$ is strict dalend en we stoppen als $a_s > 0$ en $a_{s+1} = 0$. "Het algoritme stopt":

$$\cdots, a_{s-2} = q_{s-1}a_{s-1} + a_s, \qquad a_{s-1} = q_{s-1}a_s + 0.$$

Dan volgt $d = \mathrm{ggd}(a_{s-1}, a_s) = a_s$. we passen nu inductie van s naar 2. We zien dat $1{\cdot}a_{s-1} - q_{s-1}{\cdot}a_s = d$. Als

$$\xi{\cdot}a_{i+1} + \eta{\cdot}a_{i+2} = d$$

dan volgt

$$d = \xi{\cdot}a_{i+1} + \eta{\cdot}(a_i - \eta q_i a_{i+1}) = \eta{\cdot}a_i + (\xi - \eta q_i)a_{i+1}.$$

Inductie bewijst dat $d = \mathrm{ggd}(a_1, a_2)$ geschreven kan worden als $d = xa_1 + ya_2$ met $x, y \in \mathbb{Z}$.

Een voorbeeld/toepassing. Zij $a = p$ een priemgetal en beschouw $b \in \mathbb{Z}$. Als p een deler is van b dan geldt $\mathrm{ggd}(p, b) = p$. Als p niet een deler is van b dan geldt $\mathrm{ggd}(p, b) = 1$ en er bestaan $x, y \in \mathbb{Z}$ met $xp + yb = 1$.

Bewijs van (13.3)**(1)**. Als n een priemgetal is dan is factorizatie mogelijk (met één priemfactor). Onderstel dat $n > 1$ niet een priemgetal is, en dat factorizatie mogelijk is voor alle m met $1 < m < n$. Omdat n niet een priemgetal is, zijn er echte delers, d.w.z. we kunnen schrijven $a = b{\cdot}b'$ met $1 < b$ en $1 < b'$. Voor b en voor b' is priemfactorizatie mogelijk (de inductie hypothese). Dus volgt factorizatie voor n. Dit bewijst het bestaan van priem factorizatie voor alle $n \in \mathbb{Z}_{>1}$. Nu nog de eenduidigheid.
(2) Neem aan dat $p_1 \times \cdots \times p_s = \ell_1 \times \cdots \times \ell_t$ met $1 \leq s \leq t$ (anders links en rechts verwisselen). Neem als inductie-hypothese aan dat *eenduidigheid bewezen is voor factorizaties van getallen waar ontbinding als een product van i priemgetallen met $1 \leq i < s$ mogelijk is.* Die inductie hypothese is juist als $i = 1$ (in dat geval is n een priemgetal). Schrijf $p = p_1$.
Bewering. Er is een index $1 \leq j \leq t$ zodanig dat $p = \ell_j$.
Bewijs. Als dit niet het geval zou zijn, dan zijn er x_i, y_i met $x_i p + y_i \ell_i = 1$ voor alle $1 \leq i \leq t$. Dan zou gelden

$$p{\cdot}(p_2 \times \cdots \times p_s)(y_1 \times \cdots \times y_t) = (1 - x_1 p) \times \cdots \times (1 - x_t p).$$

Dit kunnen we herschrijven als

$$p{\cdot}A = 1 + p{\cdot}B, \qquad A, B \in \mathbb{Z}; \qquad (A - B){\cdot}p = 1.$$

Deze tegenspraak bewijs de bewering.

We zien dat

$$p_2 \times \cdots \times p_s = \ell_1 \times \cdots \times \ell_{j-1} \times \ell_{j+1} \cdots \times \times \ell_t.$$

Uit de inductie-hypothese volgt dat hier eenduidigheid op volgorde na geldt. Dit bewijst ook die eenduidigheid voor $p_1 \cdots p_s = \ell_1 \cdots \ell_t$. Dit bewijst **(2)**. QED(13.3)

(13.8) Waarom zoveel aandacht geven aan iets dat eigenlijk zo vanzelf spreekt?

Er zijn ringen waar het analogon van (13.3) niet juist is. We kunnen natuurlijk flauwe voorbeelden nemen zoals een ring $\mathbb{Q}[a, b, c]$ met $ab = 2 = bc$. Maar hier is een serieuzer voorbeeld.

Voorbeeld. Zij $R = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5}\}$. In die ring geldt:

$$2{\cdot}3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Eenvoudig is in te zien dat voor elk van de factoren in beide producten geldt dat $\pm$ die factor en ± 1 de enige delers zijn (m.a.w. die factoren zijn elk niet verder te ontbinden). De eenduidigheid faalt.

Voorbeeld. Anderzijds, zij $R = \mathbb{Z}[\sqrt{-1}]$, de "ring van gehele getallen van Gauss". Met de afbeelding $N : R \to \mathbb{Z}$, met $N(a + b\sqrt{-1}) := a^2 + b^2$, de "norm afbeelding, kunnen we

het analogon van (13.6) in deze ring afleiden, en unieke factorizatie in deze ring geldt: op eenheden na, $\pm 1, \pm\sqrt{-1}$, en op volgorde na. Het is niet zo moeilijk om in te zien dat de priem elementen, op eenheden na, in deze ringen alle getallen zijn van de vorm: of $1+i$ of p, of een rationaal priemgetal $p \equiv 3 \pmod 4$, of $a+b\sqrt{-1}$ waar $N(a+b\sqrt{-1})$ een priemgetal is met $\equiv 1 \pmod 4$. Zie verder § 15.

(13.9) Een speculatie. Wat was het "wonderlijke bewijs" dat Fermat had van zijn stelling (vermoeden) FLT?

Schrijf ζ_p voor een complex getal met $\zeta_p \neq 1$ en $(\zeta_p)^p = 1$. Schrijf $\mathbb{Z}[\zeta_p]$ voor de kleinste deelring van $\mathbb{C}$ die $\mathbb{Z}$ en die ζ_p bevat. Het is niet zo moeilijk om in te zien dat als eenduidigheid van van factorizatie (op eenheden en op volgorde na) geldt in $\mathbb{Z}[\zeta_p]$, en $p > 2$ is een priemgetal, dan volgt FLT_p. Ik speculeer dat Fermat dit wist (een dergelijk bewijs lag geheel binnen zijn mogelijkheden), en dat Fermat veronderstelde (?!) dat eenduidigheid van factorizatie in $\mathbb{Z}[\zeta_p]$ geldt voor alle priemgetallen p; dit is niet waar; deze "fout" is later in de geschiedenis vaker voorgekomen, ook op een serieus wetenschappelijk niveau (Lamé), en pas na de waarschuwing van Kummer weten we dat het bewijs van FLT zo echt niet gaat. Wel werden allerlei gevalen van FLT zo bewezen met een uitgebreide bestudering van factorizaties in $\mathbb{Z}[\zeta_p]$. Een prachtig stuk wiskunde.

In de rest van de paragraaf noemen we een paar aspecten over rekenen modulo n. Dit is een mooie, effectieve methode die eigenlijk heel eenvoudig is. Bovendien werkt iedereen er al mee: we weten best dat een afsprak om 20 : 00 uur plaats vindt om 8 : 00 's avonds, rekenen modulo 12.

(13.10) Rekenen modulo n. Gegeven is een getal $n \in \mathbb{Z}_{>1}$. Beschouw de symbolen

$$\mathbb{Z}/n := \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}.$$

In deze verzameling definiëren we optellen, aftrekken en vermenigvuldigen. We schrijven $\overline{m} = \overline{m - in}$ voor elke $i \in \mathbb{Z}$, en we bestuderen de afbeelding

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n, \quad m \mapsto \overline{m}.$$

Met andere woorden: voor $m \in \mathbb{Z}$ schrijven we $m = dn + r$ met $0 \leq r = r(m) < n$ (delen door n met rest) en we beelden $m \in \mathbb{Z}$ af op $\overline{r(m)} = \overline{r}$. We schrijven $\overline{a} + \overline{b} = \overline{a+b}$ ("optellen modulo n"), en analoog voor $\overline{ab}$ en $\overline{a-b}$.

We kunnen ook zeggen (in terminologie die later ontwikkeld zal worden): $\mathbb{Z}/n$ is een ring, en de natuurlijke afbeelding $\mathbb{Z} \to \mathbb{Z}/n$ is een ring-homomorfisme.
Als we willen benadrukken dat we modulo n werken schrijven we $\overline{m} = m \bmod n$.
Maak goed onderscheid tussen enerzijds $(m \bmod n) \in \mathbb{Z}/n$ (de residu klasse van m modulo n) en anderzijds $a \equiv b \pmod n$ (en dat wil zeggen dat $a - b$ deelbaar is door n.

(13.11) In veel gevallen is rekenen modulo n en mooi hulpmiddel. Een getal dat $\equiv 2 \pmod 3$ is niet een kwadraat (waarom niet ?). Ga na.

Een voorbeeld. Heeft de vergelijking $T^2 = 47440033367001212$ een oplossing in $\mathbb{Z}$? [Reken modulo 3.]
Een andere methode: op welke decimaal cijfers eindigen kwadraten in $\mathbb{Z}$? [D.w.z. reken modulo 10.]

Een kwadraat in $\mathbb{Z}$, uitgeschreven in het 10-tallig stelsel eindigt op een van de cijfers: $0, 1, 4, 5, 6, 9$. Geef een bewijs. Zie (18.22).

Verder zien we: *voor elk priemgetal p heeft elke $0 \neq \overline{a} \in \mathbb{Z}/p$ een inverse.*
Probeer dit te bewijzen. In technische termen: $\mathbb{Z}/n$ is een lichaam dan en slechts dan als n is een priemgetal is.

We zullen vaak de volgende stelling gebruiken:

(13.12) Stelling (de Chinese rest-stelling). *Voor $m, n \in \mathbb{Z}$ met $\text{ggd}(m, n) = 1$ is de natuurlijke afbeelding*

$$\mathbb{Z}/(mn) \quad \xrightarrow{\sim} \quad \mathbb{Z}/m \times \mathbb{Z}/n$$

een isomorfisme (een bijectieve afbeelding die $+$ en $\times$ en $-$ behoudt).

(13.13) Voor een getal $n \in \mathbb{Z}_{>0}$ geschreven in het 10-tallig stelstel $n = a_1 a_2 \cdots a_m$ schrijven we $s(n)$ voor de som van die cijfers, d.a..z

$$s(n) = \sum_{i=1}^{i=m} a_i.$$

Merk op dat in dit geval $s(n) \leq 9m$. We zien dat er voor elke n een j is met $0 < s^j(N) < 10$.
Opgave. Bewijs:
als $s^j(n) = 3, 6, 9$ dan is n deelbaar door 3;
als $s^j(n) = 9$ dan is n deelbaar door 9.
Zie (18.59). Zie (18.23).

(13.14) Voor een getal $n \in \mathbb{Z}$ geschreven in het 10-tallig stelstel $n = a_1 a_2 \cdots a_m$ schrijven we $a(n)$ voor de alternerende som van de decimale cijfers van n:

$$a(n) = \pm(a_1 - a_2 + a_3 - a_4 + \cdots) = \frac{\mid n \mid}{n} \sum_{i=1}^{i=m} (-1)^{i-1} a_i.$$

We zien dat er voor elke n een j is met $-10 < s^j(N) < 10$.
Opgave. Bewijs:
(n is deelbaar door 11) $\iff$ $(\exists j : \ a^j(n) = 0)$.
Zie (18.60). Zie (18.24).

(13.15) Opmerking.* Vaak kunnen we aantonen dat een vergelijking geen oplossingen heeft door te reduceren modulo een geheel getal $n > 1$, en dan eerst te bewijzen dat er modulo n geen oplossing is. In sommige gevallen geeft dit toegang tot het probleem.

We kunnen proberen het proces om te draaien: bewijs dat de vergelijking een oplossing heeft modulo m voor elke $m > 0$, en los de vergelijking ook op over $\mathbb{R}$; we spreken van het Hasse principe als het bestaan van een oplossing in elk van die gevallen impliceert dat de oorspronkelijke vergelijking een oplossing heeft. Echter Selmer gaf de vergelijking

$$3X^3 + 4Y^3 + 5Z^3 = 0; \quad \text{zijn er oplossingen met} \quad X, Y, Z \in \mathbb{Z}, \quad XYZ \neq 0?$$

Hij bewees daarover: de vergelijking heeft voor elke $n \in \mathbb{Z}_{>1}$ een oplossing in $(\mathbb{Z}/n)^3 - \{0, 0, 0\}$, en er is een oplossing in $\mathbb{R}^3 - \{0, 0, 0\}$, maar er is geen oplossing in $\mathbb{Z}^3 - \{0, 0, 0\}$. Zie [74]. Dat was een doorbraak, en nieuwe methoden werden ontwikkeld om verder te komen.

(13.16) Priemgetallen modulo 4. We gaan zien dat eenvoudig te bewijzen is:
(13.16)(3). *Er zijn oneindig veel priemgetallen* $p \equiv 3 \pmod 4$.
Bewijs. We weten dat $7 \equiv 3 \pmod 4$. Als we een niet-lege verzameling $\{P_1, \cdots, P_n\}$ hebben met alle $P_i \equiv 3 \pmod 4$, dan construeren we een (nieuw) priemgetal Q met $Q \equiv 3 \pmod 4$ en $Q \notin \{P_1, \cdots, P_n\}$ (via een variant op het bewijs van Euclides): kies

$$M := (P_1 \times \cdots \times P_n)^2 + 2.$$

We zien dat $M > 1$ en $M \equiv 3 \pmod 4$. Daarom hebben niet alle priemdelers van M de eigenschap $\equiv 1 \pmod 4$; dus is er een priemdeler Q van M met $Q \equiv 3 \pmod 4$. QED

Iets moeilijker is:
(13.16)(1). *Er zijn oneindig veel priemgetallen* $p \equiv 1 \pmod 4$; zie (13.18).

(13.17) Propositie* (sommen van kwadraten) *Zij* $A, B \in \mathbb{Z}_{>0}$ *en zij* p *een priemgetal dat wel* $A^2 + B^2$ *deelt maar niet* A *deelt* (en dus ook niet B deelt). *Dan geldt*

$$p \not\equiv 3 \pmod 4.$$

De * geeft aan dat het bewijs niet helemaal elementair is (we gebruiken het begrip groep en een paar eigenschappen uit de groepentheorie).
Bewijs. Als $p = 2$ dan geldt $p \not\equiv 3 \pmod 4$. Neem aan dat p oneven is.
Schrijf

$$a = \overline{A} =: A \bmod p, \quad b = \overline{B} =: B \bmod p, \quad c = b^{-1} \in \mathbb{F}_p := \mathbb{Z}/p.$$

Uit $p \mid A^2 + B^2$ volgt $a^2 + b^2 = 0 \in \mathbb{F}_p$. Dus $(ca)^2 + 1 = 0 \in \mathbb{F}_p$. We zien dat

$$-1 = (ca)^2 \quad \text{een kwadraat is in } \mathbb{F}_p;$$

bovendien is dit kwadraat ongelijk aan nul. Beschouw $(\mathbb{F}_p)^* := \mathbb{F}_p - \{0\}$. Dit is een (multiplicatieve) groep. Deze groep bevat een element van orde 4, want $(ca)^2 = -1 \neq 1$ en $(ca)^4 = 1$. Uit de stelling van Lagrange, zie (14.7), volgt dat 4 een deler is van $\#((\mathbb{F}_p)^*) = p - 1$. QED

Nu een bewijs van (13.16)(1).

(13.18) Gevolg =(13.16)(1). *Er zijn oneindig veel priemgetallen* p *met* $p \equiv 1 \pmod 4$.
Bewijs. Veronderstel dat $P_1, \cdots, P_t$ oneven priemgetallen zijn, met $t > 0$. We bewijzen dat er een priemgetal P bestaat met

$$P \equiv 1 \pmod 4 \quad \text{en} \quad P \notin \{P_1, \cdots, P_t\};$$

als dit bewezen is dan volgt de uitspraak van het gevolg.
Neem

$$M := (P_1 \times \cdots \times P_t)^2 + 4.$$

Merk op dat M oneven is. We zien uit (13.17) dat elk priemgetal P dat M deelt de eigenschap $P \equiv 1 \pmod 4$ heeft. Als $P \in \{P_1, \cdots, P_t\}$ zou gelden, dan is

$$P \text{ een deler van } M - (P_1 \times \cdots \times P_t)^2 = 4,$$

en dat is een tegenspraak; dus geldt $P \notin \{P_1, \cdots, P_t\}$; zo construeren we een nieuw priemgetal met $P \equiv 1 \pmod 4$. QED

We stellen de vraag of priemgetallen $\equiv 1 \pmod 4$ al of niet vaker voorkomen dan priemgetallen $\equiv 3 \pmod 4$, zie (1.11). Deze vraag heeft geleid tot een stroom van interessante observaties en nieuwe onderzoekingen. We lichten een tipje van de sluier op.

(13.19) Schrijf $\pi_{4,1}(x)$ voor het aantal priemgetallen $p \equiv 1 \pmod 4$ met $p \leq x$; analoog $\pi_{4,3}(x)$ voor het aantal priemgetallen $p \equiv 3 \pmod 4$ met $p \leq x$. Voor kleine x kunnen proberen die beide getallen te berekenen; welk getal lijkt steeds groter? Wat bewezen kan worden (niet heel eenvoudig):

$$\lim_{x\to\infty} \frac{\pi_{4,1}(x)}{\pi_{4,3}(x)} = 1;$$

dit is een bijzonder geval van een veel algemenere stelling "Chebotarev's density theorem" (buiten het bestek van ons college) , zie
`http://en.wikipedia.org/wiki/Chebotarev%27s_density_theorem`

(13.20) In een brief in 1835 schrijft Chebyshev aan Fuss dat het lijkt alsof $\pi_{4,3}(x) > \pi_{4,1}(x)$ voor elke x (en dat was ons wellicht al opgevallen, als we een aantal gevallen hadden doorgerekend). Dit heet nu de "Chebyshev's bias" ("bias": vooroordeel). Het bleek een pracht idee, dat weliswaar niet juist bleek, maar dat toch fascinerende wiskunde opleverde. Zie
`http://arxiv.org/pdf/1210.6946v1.pdf`

Littlewood bewees in 1914:

$$\pi_{4,3}(x) - \pi_{4,1}(x) \textit{ wisselt oneindig vaak van teken } x \to \infty.$$

Zie [51]. Nauwkeurige resultaten staan in [73]. In het prachtige artikel [31] over dit mooie onderwerp zien we dat Chebyshev "bijna gelijk had": voor "veel" waarden van x is $\pi_{4,3}(x) > \pi_{4,1}(x)$.

We zien een voorbeeld dat een "eenvoudige vraag", nieuwsgierigheid, kan leiden tot bespiegelingen en diepe resultaten (zoals zo vaak in de wiskunde). Ook zien we dat berekeningen, zelfs bij een groot wiskundige als Chebyshev, tot verkeerde verwachtingen kan leiden.

(13.21) Priemgetallen modulo 3. We gaan zien dat eenvoudig te bewijzen is:
(13.21)(2). *Er zijn oneindig veel priemgetallen* $p \equiv 2 \pmod 3$.
Geef zelf een bewijs. Hint: $(P_1 \times \cdots \times P_t)^2 + 2$.

Iets moeilijker is:
(13.21)(1)*. *Er zijn oneindig veel priemgetallen* $p \equiv 1 \pmod 3$.
We geven een schets van een bewijs; daarbij gebruiken we methoden die niet helemaal elementair zijn.

Feit.*

$$\begin{aligned} &\textit{voor } p \equiv 1 \pmod 3 \textit{ is } -3 \bmod p \in \mathbb{Z}/p \textit{ wel een kwadraat.} \\ &\textit{voor } p \equiv 2 \pmod 3 \textit{ is } -3 \bmod p \in \mathbb{Z}/p \textit{ niet een kwadraat.} \end{aligned}$$

We geven niet een bewijs. Maak voorbeelden om te zien of dit werkt in die gevallen. (Een bewijs volgt uit de zogenaamde kwadratische reciprociteitswet, die we niet behandelen.)

Gevolg. *Zij* $B \in 2\mathbb{Z}_{>0}$ *een even positief geheel getal dat niet deelbaar is door* 3.

$$p \textit{ is priem en } p \mid B^2 + 3 \quad \Longrightarrow \quad p \equiv 1 \pmod 3$$

en p is oneven.
Inderdaad, omdat B even is, is B^2+3 oneven, en dus is $p \neq 2$. Omdat B niet deelbaar is door 3 volgt dat $p \neq 3$. Uit $p \mid B^2+3$ volgt dat $-3 \bmod p \in \mathbb{Z}/p$ een kwadraat is; hieruit volgt $p \equiv 1 \pmod 3$. QED

Bewijs van (13.21)(1). We zien dat $7 \equiv 1 \pmod 3$. Laat $\{P_1, \cdots, P_t\}$ een niet-lege verzameling priemgetallen zijn met $P_i \equiv 1 \pmod 3$ voor alle i. Schrijf

$$B := 2 \times P_1 \times \cdots \times P_t \quad \text{en} \quad M := B^2 + 3.$$

Een priemdeler Q van M is oneven, niet deelbaar door 3 en $Q \equiv 2 \pmod 3$ zoals we zien uit het bovenstaande gevolg. Ook zien we $Q \notin \{P_1, \cdots, P_t\}$. QED

(13.22) Opgave. Vind $a \in \mathbb{Z}$ met $a^2 \equiv -3 \pmod{37}$. Zie (18.33).

(13.23) Opgave. Voor welk(e) priemgetal(len) geldt:

$$15^2 \equiv -3 \pmod p \ ?$$

Zie (18.34).

(13.24) Een voorbeeld van het rekenen modulo n. We laten zien dat 641 een deler is van F_5. We zien:

$$641 = 640 + 1 = 5{\cdot}2^7 + 1 = 625 + 16 = 5^4 + 2^4.$$

Dit geeft

$$5{\cdot}2^7 \equiv -1 \pmod{641}, \text{ dus } 5^4{\cdot}2^{4\times 7} \equiv +1 \pmod{641};$$

daarom

$$-2^4{\cdot}2^{28} \equiv 5^4{\cdot}2^2 8 \equiv +1 \pmod{641}; \text{ dus } F_5 \equiv 0 \pmod{641}.$$

QED

14 Appendix C: Groepen, ringen en lichamen

Ter herinnering. Deze § geeft een samenvatting van een paar feiten die we gebruiken, maar dit is niet een volledig dictaat over deze theorie. Voor verwijzingen zie het begin van § 13. De essentie van deze begrippen kwam veelvuldig voor in de wiskunde. Van een goede formalisering en van een abstract definiëren van deze begrippen kwam de theorie pas in de periode, ruwweg, 1890 - 1930 in focus (maar nog na 1960 hoorde ik een wiskundige vragen: "is dit een concrete of een abstracte groep?")

We zullen de begrippen "groep", "ring" en "lichaam" veelvuldig tegen komen. Dit zijn abstract algebraïsche begrippen. Deze stroomlijnen argumenten, en maken vaak ingewikkelde situaties transparant. Het formaliseren van deze begrippen heeft in de wiskunde een enorme ontwikkeling gebracht.

(14.1) We beginnen met een paar voorbeelden, en zullen daarna dan de abstracte definitie geven.

(14.1)**(1)** In de verzameling $\mathbb{Z} = \{\cdots, -1, 0, 1, 2, \cdots\}$ van de gehele getallen kunen we:

optellen; voor $a, b \in \mathbb{Z}$ is $a + b \in \mathbb{Z}$ gedefinieerd; bovendien geldt (associatieve wet): $a + (b + c) = (a + b) + c$, m.a.w. de volgorde van optellen doet er niet toe;

er is een element $0 \in \mathbb{Z}$ waarvoor geldt $a + 0 = a = 0 + a$ voor alle $a \in \mathbb{Z}$;

tegengestelde: voor elke $a \in \mathbb{Z}$ is er een $-a \in \mathbb{Z}$ met $a + (-a) = 0 = (-a) + a$.

(14.1)**(2)** Het vorige voorbeeld beschrijft een oneindige groep. Hier is een voorbeeld van een eindige groep. Beschouw de verzameling

$$\mathbb{Z}/5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

bestaande uit 5 elementen. Hierin kunnen we optellen "modulo 5"; bij voorbeeld $\overline{3} + \overline{4} = \overline{2}$. Met deze optelling krijgen we dezelfde eigenschappen als boven (associativiteit, nul-element, tegengestelde). Zie (13.10).

(14.1)**(3)** In de vorige voorbeelden werd de "operatie" in de groep additief geschreven. maar soms is een multiplicatieve schrijfwijze meer voor de hand liggend. Beschouw de verzameling

$$(\mathbb{Z}/5)^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}.$$

Hierin kunen we "vermenigvuldigen modulo 5. We krijgen analoge eigenschappen als boven (associativiteit, een-element, inverse). Bijvoorbeeld $\overline{2} \times \overline{3} = \overline{1}$, en we schrijven $\overline{3}^{-1} = \overline{2}$.

(14.1)**(4)** In alle voorgaande voorbeelden was de groeps-wet commutatief; dat wil zeggen $a + b = b + a$, respectievelijk $a \times b = b \times a$. Maar we kunnen ook voor beelden beschouwen waar de groeps-wet niet commutatief is. Beschouw de verzameling S_3 van all permutaties van 3 symbolen; laten we die symbolen $1, 2, 3$ noemen. Een permutatie is een handeling die deze symbolen op een (mogelijk andere) manier opschrijft. We kunnen een permutatie definiëren als een bijectieve afbeelding $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$.

Bij voorbeeld schrijven we $\sigma(12)$ voor de permutatie die 1 en 2 verwisselt en 3 op zijn plaats laat. We schrijven $(12)1 = 2$, $(21)2 = 1$ en $(12)3 = 3$ (we zien de permutatie als een soort "functie-symbool", opererend van links). Idem voor de permutatie (13). De groeps-wet is achter elkaar uitvoeren van de permutaties. We zien:

$$(12)(13)1 = 3, (12)(13)2 = 1, (12)(13)3 = 2,$$

en

$$(13)(12)1 = 2, (13)(12)2 = 3, (13)(12)3 = 1.$$

Uitleg van de berekening $(12)(13)1 = 3$. We zien dat eerst (13) werkt, en onder die werking gaat 1 in 3 over. Dan krijgen we: $(12)(13)1 = (12)3 = 3$. Ga alle andere identiteiten hierboven op deze manier na. We kunnen inzien dat met deze groeps-wet en met een-element de identieke permutatie (alles blijft op zijn plaats) aan de regels voldaan is. Echter

$$(12)(13) \neq (13)(12);$$

inderdaad, we zien dat deze twee permutaties verschillend zijn. Deze groepen van permutaties hebben heel veel toepassingen.

(14.1)**(5)** Beschouw twee symbolen a en b. Zij G de verzameling van alle woorden in de letters a en b waarin de combinatie aa en bb niet voorkomen. Het lege woord noteren we als e. We maken een groeps-wet in G, genoteerd als $*$, door woorden achter elkaar te zetten, maar zodra aa voorkomt schrappen we dat, zodra bb voorkomt schrappen we dat. Dit geeft b.v. $a * a = e$, $b * b = e$, $aba * ab = a$, etc. Ga associativiteit na. Voor elk element is er een inverse, bv. de inverse van $ababab$ is $bababa$, want

$$(ababab) * (bababa) = (ababa) * (ababa) = (abab) * (baba) =$$

$$= (aba) * (aba) = (ab) * (ba) = (a) * (a) = e.$$

We krijgen weer een verzameling met een groeps-wet. Die groepswet is niet-commutatief: $ba \neq ab$. Deze groep is niet-commutatief en niet eindig. Overigens: zulke groepen zullen in onze cursus niet voorkomen, maakt U zich geen zorgen hierover.

Als we zo door deze voorbeelden heen werken, dan voelen we aan dat een begrip dat deze situaties systematiseert de verwarring die we bij deze steeds ingewikkelder voorbeelden zien kan

(14.2) Definitie. Een groep is een viertal $(G, *, e, i)$ bestaand uit: een niet-lege verzameling G een "groeps-wet" die aan elke $x, y \in G$ een element $x * y \in G$ toevoegt, een element $e \in G$, en een afbeelding $i : G \to G$, zodat voldaan is aan:
(ass) voor alle $x, y, z \in G$ geldt $x * (y * z) = (x * y) * z$;
(eenh) voor elke $x \in G$ geldt $x * e = e * x$;
(inv) voor elke $x \in G$ is er een $i(x) \in G$ met $i(x) * x = e = x * i(x)$.

Met deze abstracte definitie in de hand, ga de voorbeelden hierboven nog een keer na.

We spreken vaak van "de groep G" als we bedoelen een viertal $(G, *, e, i)$ waar de andere symbolen een duidelijke betekenis hebben.We spreken b.v. van de groep $\mathbb{Z}$ van de gehele getallen, en laten de symbolen $+$, $e = 0$ en $a \mapsto i(a)$ weg.

We gebruiken de additieve schrijfwijze niet voor een niet-commutatieve groep. Maar verder worden zowel additieve schrijfwijze als de multiplicatieve schrijfwijze voor eenzelfde object gebruikt (en dat is juist de kracht van deze theorie).

We zegen dat een groep G *abels* is als de groeps-wet commutatief is. (Hier eren we de grote Noorse wiskundige Niels Henrik Abel.)

(14.3) Definitie. We zeggen dat twee groepen G en H *isomorf* zijn als er een bijectieve afbeelding $\varphi : G \to H$ met $\varphi(e_G) = e_H$, en $\varphi(x * y) = \varphi(x) * \varphi(y)$.

Voor een groep G en een deelverzameling $M \subset G$ zeggen we dat M een *ondergroep* is van G als M het eenheidselement van G bevat, voor elke $x \in M$ ligt ook x^{-1} in M en voor alle $x, y \in M$ ligt ook $x * y$ in M. In dit geval is M, met de geïnduceerde structuur een groep.

(14.4) Een voorbeeld. We laten zien dat $\mathbb{Z}/4$ en $(\mathbb{Z}/5)^*$ isomorf zijn (is dat niet verwarrend .. ?). Schijf

$$\mathbb{Z}/4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}, \quad (\mathbb{Z}/5)^* = \{\tilde{1}, \tilde{2}, \tilde{3}, \tilde{4}\};$$

in de eerste groep: optellen modulo 4; in de tweede groep: vermenigvuldigen modulo 5. Geef φ door:

$$\varphi(\overline{1}) = \tilde{2}, \quad \varphi(\overline{2}) = \tilde{2}^2 = \tilde{4}, \quad \varphi(\overline{3}) = \tilde{2}^3 = \tilde{3}, \quad \varphi(\overline{0}) = \tilde{1}.$$

Ga na dat dit een isomorfisme geeft. Is er nog een ander isomorfisme tussen deze twee groepen?

(14.5) Definitie. Zij G een groep (multiplicatief geschreven). We zeggen dat G *cyclisch* is als er een element $g \in G$ is (een "voortbrenger") zodat dat voor elke $x \in G$ er een $i \in \mathbb{Z}$ is met $x = g^i$ (additieve schrijfwijze: $x = ig$).
Voorbeeld. De additieve groep $\mathbb{Z}$ is cyclisch. Voor elke $n \in \mathbb{Z}$ is $\mathbb{Z}/n$ cyclisch. Ga na: de groep $(\mathbb{Z}/8)^*$ is niet cyclisch. De groep $(\mathbb{Z}/17)^*$ is cyclisch (vind een voortbrenger; let op: multiplicatieve schrijfwijze).

(14.6) Zij G een groep, multiplicatief geschreven, en $x \in G$. We zeggen dat n de *orde* is van x, notatie $\text{orde}(x) = n$ als $n \in \mathbb{Z}_{>0}$, en $x^n = 1$ en voor $1 \leq i < n$ geldt $x^i \neq e$. M.a.w. de orde is de kleinste exponent j nodig om $x^j = e$ te krijgen. Als er een dergelijke exponent niet bestaat dan schrijven we $\text{orde}(x) = \infty$.
Opmerking. Als $x \in G$ en de orde van x is oneindig dan is de ondergroep $\{\cdots, x^{-2}, x^{-1}, e, x, \cdots, x^i, \cdots\}$ isomorf met $\mathbb{Z}$ (additief geschreven). Als $x \in G$ en de orde van x is gelijk aan $n \in \mathbb{Z}_{>0}$ dan is $\{e, x^1, \cdots, x^{n-1}\}$ een ondergroep en die is isomorf met $\mathbb{Z}/n$.
Opmerking. Als G een groep is, dan geven we met $\#(G)$ het aantal elementen in G aan (oneindig of eindig). Dit wordt de orde van G genoemd. Raak niet in verwarring door "de orde van een groep" en "de orde van een element in een groep".

(14.7) Stelling (Lagrange). *Zij G een eindige groep en zij $x \in G$. Dan is*

$$\textit{de orde } \text{orde}(x) \textit{ van } x \textit{ een deler van } \#G, \textit{ de orde van } G.$$

Voor een bewijs: geef het zelf, of raadpleeg de literatuur.

(14.8) Lemma. *Zij G een eindige* abelse *groep.*
(1) *Voor $x, y \in G$ is* $\text{orde}(xy)$ *een deler van* $\text{kgv}(\text{orde}(x), \text{orde}(y))$.
(2) *Voor $x, y \in G$ met* $\text{ggd}(\text{orde}(x), \text{orde}(y)) = 1$ *geldt* $\text{orde}(xy) = \textit{orde}(x) \times \text{orde}(y)$.
(3) *Schrijf m voor het grootste getal dat voorkomt als orde van een element in G:*

$$m := \max_{x \in G} \text{orde}(x).$$

(Dit getal wordt wel de exponent van de abelse groep G genoemd.) *Dan geldt: voor elke $y \in G$ is* $\text{orde}(y)$ *een deler van m.*
Opmerking. Alle onderdelen van dit lemma zijn onjuist voor sommige niet-abelse groepen. Bij voorbeeld in de groep S_3 van permutaties van 3 symbolen zijn de ordes van elementen 1,

2 en 3. We zien dat 2 niet een deler is van het maximum van deze getallen. Het product xy met orde$(x) = 2$ en orde$(y) = 3$ heeft orde$(xy) = 2$.

Zie ook (14.9).

Geef zelf een bewijs van (14.8)(1) en van (14.8)(2).

Bewijs van (14.8)(3). Onderstel orde$(z) = m$, waar m de exponent is van de eindige abelse groep G, en zij $x \in G$, met orde$(x) = a$. Als a niet een deler van m zou zijn, dan is er een priemgetal p, en $i, j \in \mathbb{Z}_{\geq 0}$ waar p^i een deler is van m, en p^{i+1} niet een deler van m en p^j een deler van a en $j > i$. Dan heeft $u := z^{p^i}$ orde gelijk aan m/p^i en merk op dat p niet een deler is van m/p^i. Beschouw ook $v := x^{a/p^j}$; we zien dat orde$(v) = p^j$. Uit (2) volgt dat

$$\text{orde}(u{\cdot}v) = \frac{m}{p^i} \times p^j = m \times p^{j-i} > m.$$

Dit is een tegenspraak met het feit dat m de grootste orde is die voorkomt in G. We concluderen dat voor elke $x \in G$ de orde van dat element een deler is van m. QED

Voor een eindige (niet noodzakelijk commutatieve) groep G definiëren we de exponent van G het kleinste positieve getal $m \in \mathbb{Z}_{>0}$ zodanig dat voor elke $x \in G$ er geldt $x^m = e$.

(14.9) Opgave. Beschouw de volgende lineaire afbeeldingen $S, U : \mathbb{R}^2 \to \mathbb{R}^2$ gegeven door

$$S(1,0) = (0,1), \quad S(0,1) = (-1,0), \qquad U(1,0) = (0,-1), \quad U(0,1) = (1,-1).$$

Beschouw de groep van lineaire afbeeldingen voortgebracht door S en U onder compositie van afbeeldingen (achter elkaar uitvoeren van afbeeldingen, vermenigvulidgen van matrices). Bewijs:

$$S^2 = -1, \quad \text{orde}(S) = 4, \quad U^3 = 1, \quad \text{orde}(U) = 3, \quad \text{orde}(SU) = \infty.$$

(We zien dat (14.8)(3) onjuist is als we de eis "G is abels" laten vallen.)

(14.10) Torsie. Voor een abelse groep A en een getal $n \in \mathbb{Z}_{>0}$ schrijven we

$$A[n] := \{x \in A \mid x^n = e\}.$$

Voor een abelse groep A schrijven we

$$\text{Tors}(A) := \{x \mid \text{orde}(x) < \infty\}.$$

(14.11) Lemma. (1) *Voor een abelse groep A geldt dat* Tors$(A) \subset A$ *een ondergroep is.*
(2) *Voor een abelse groep A en $n \in \mathbb{Z}_{>0}$ is $A[n] \subset A$ een ondergroep.*

(14.12) Opmerking/Opgave. In beide conclusies van het lemma is het gegeven "A is abels" nodig; geef tegenvoorbeelden in niet-commutatieve gevallen.

(14.13) Definitie. Een *ring* is een verzameling R met operaties $+, -, \times$ en elementen $0, 1 \in \mathbb{Z}$ zodanig dat:
$\{R, 0, +, -\}$ is een commutatief (additief geschreven) groep,
$\times$ is een operatie $R \times R \to R$ met $((x \times y) \times z) = (x \times (y \times z))$ voor alle $x, y, z \in R$,
voor alle $x \in R$ geldt $1 \times x = x = x \times 1$, en

$x \times (y+z) = x \times y + y \times z$ en $(x+y) \times z = x \times z + y \times z$ voor alle $x, y, z \in R$.
Opmerking. Vaak wordt in plaats van $x \times y$ geschreven xy.
Ga na dat $\mathbb{Z}$ een (commutatieve) ring is.

Opmerkingen. We laten toe dat de vermenigvuldiging niet commutatief is.
Voorbeeld. De verzameling van 2×2 matrices met elementen in $\mathbb{Z}$ is een niet-commutatieve ring (ga na).
We laten toe dat $-1 = +1$. Bij voorbeeld $\mathbb{Z}/2$ is een ring waarin dit geldt.
We laten toe dat $1 = 0$. Als dat het geval is dan is $R = \{0\}$ (ga na).
We zullen de ringen $\mathbb{Z}, \quad \mathbb{Z}/n, \quad \mathbb{Z}[\sqrt{-1}]$ veelvuldig tegenkomen.

(14.14) Definitie. Een *delingsring* is een ring waarin elk element ongelijk aan nul een inverse heeft en waarin $0 \neq 1$.
We zullen dergelijke ringen niet tegenkomen.
Een voorbeeld. $R = \mathbb{Z}\cdot 1 \times \mathbb{Z}\cdot i \times \mathbb{Z}\cdot j \times \mathbb{Z}\cdot k$ met $i^2 = -1 = j^2 = k^2$ en $ij = k, \quad jk = i, \quad ki = j, \quad ik = -j, \quad ji = -k, \quad kj = -1$ (is het duidelijk hoe $+, -, \times, 0, 1$ in deze ring eruit zien? (Elementen van deze ring worden quaternionen genoemd, of Hamilton quaternionen).
Een delingsring wordt ook wel een "scheef lichaam" genoemd; deze verkeerde terminologie is verlaten, omdat een scheef lichaam geen lichaam hoeft te zijn, grammaticaal een vreemde constructie.

(14.15) Definitie. Een *lichaam* is een commutatieve ring waarin elk element ongelijk aan nul een inverse heeft en waarin $1 \neq 0$.
Voorbeelden. We kennen $K = \mathbb{Q}, \quad \mathbb{R}, \quad \mathbb{C}$.
Opgave! Zij p een priemgetal. Bewijs dat $\mathbb{Z}/p$ een lichaam is.
Opgave! Zij $n \in \mathbb{Z}$, niet een priemgetal. Bewijs dat $\mathbb{Z}/n$ niet een lichaam is.
Zie (14.21).
Er zijn nog veel meer voorbeelden.
Belangrijke opmerking. Zij K een lichaam en schrijf $K^* := K - \{0\}$. De vermenigvuldiging in K maakt K^* tot een (multiplicatief geschreven) groep. Geef een bewijs.

Het kan voorkomen dat een lichaam eindig is. De voorbeelden $\mathbb{Z}/p$ voor een priemgetal p kennen we. Eindige lichamen zijn volledig geclassificeerd. Ze spelen een grote rol (ook in het dagelijkse leven, b.v. in de cryptografie), maar vooral ook in de wiskunde.

(14.16) Stelling ("de kleine steling van Fermat"). *Voor een priemgetal p en $a \in \mathbb{Z}$ geldt:*

$$a^p - a \equiv 0 \pmod{p}.$$

We geven twee bewijzen. Allereerst:
Opgave. *Voor een priemgetal p en $i \in \mathbb{Z}$ met $0 < i < p$ is de binomiaal coëfficient $\binom{p}{i}$ deelbaar door p.*
Opmerking. Voor $m \in \mathbb{Z}_{>0}$ schrijven we $m! = 1 \times \cdots \times m$ en $0! = 1$.
Voor $n \in \mathbb{Z}_{>0}$ en $0 \leq i \leq n$ wordt gedefinieerd:

$$\binom{n}{i} = \frac{n!}{i! \times (n-i)!}.$$

We weten dat

$$(X+Y)^n = \sum_{i=0}^{i=n} \binom{n}{i} X^{n-i} Y^i,$$

het "binomium van Newton". http://nl.wikipedia.org/wiki/Binomiaalco%C3%ABffici%C3%ABnt

(14.16)(1) **Eerste bewijs van** (14.16). Voor $a = 0$ is de uitspraak juist. Nu verder met inductie: neem aan dat voor $a \geq 0$ de stelling juist is;

$$(a+1)^p - (a+1) = a^p - a + \sum_{i=1}^{i=p-1} \binom{p}{i} a^i.$$

Uit de inductie-aanname en uit de voorgaande opgave volgt

$$(a+1)^p - (a+1) \equiv 0 \pmod{p},$$

en deze inductie-stap geeft een bewijs van de stelling. QED

(14.16)(2) **Tweede bewijs.** De stelling is juist voor elke a die deelbaar is door p; neem aan dat a niet deelbaar is door p. Dan is $a \bmod p \in (\mathbb{Z}/p)^*$. Uit de stelling van Lagrange, zie (14.7) volgt

$$(a \bmod p)^{p-1} = a \bmod p$$

in de eindige groep $(\mathbb{Z}/p)^*$ die $p-1$ elementen heeft. We zien dat $a^{p-1} - 1$ deelbaar is door p (als a niet deelbaar is door p). Voor alle $a \in \mathbb{Z}$ geldt dat $a(a^{p-1} - 1)$ deelbaar is door p. QED

(14.17) Opgave. Neem de verzameling van alle priemgetallen die een Mersenne getal delen. Beschrijf deze verzameling. Zie (18.35).

(14.18) Zij R een commutatieve ring. Een polynoom met coëfficiënten in R is een uitdrukking $G = \sum a_i T^i$. Deze verzameling wordt aangegeven met $R[T]$. De optelling is coëfficiëntsgewijs, en de vermenigvuldiging gebruikt $T^i T^j = T^{i+j}$ en de vermenigvuldiging in R.

Voor een polynoom $G = \sum a_i T^i$ schrijven we G' voor de afgeleide, gegeven door $G' := \sum i a_i T^{i-1}$.

Dit is een zuiver formele definitie; dut heeft niets met "limieten" te maken. Maar voor een polynoom-functie $G : \mathbb{R} \to \mathbb{R}$ kunnen we de (formele) afgeleide gebruiken, en de afgeleide zoals in de reële analyse, en de resultaten zijn dezelfde; vandaar.
Ga na: als R een ring is, en $G \in R[T]$ en $a \in R$ zo dat $(T-a)^2$ een deler is van G, dan is $G(a) = 0$ en $G'(a) = 0$.

(14.19) Lemma. *Zij R een ring zonder nuldelers, en $G \in R[T]$ een polynoom. Het aantal nulpunten van G in R hooguit gelijk aan de graad van G.*
Opmerking. Als bovendien gegeven is dat voor elke $a \in R$ met $G(a) = 0$ er geldt $G'(a) \neq 0$ en alle nulpunten van G liggen in K dan is het aantal nulpunten van G in R precies gelijk aan de graad van G.
Geef zelf een bewijs van het lemma en van de opmerking.

(14.20) Een voorbeeld. *We laten zien dat het gegeven "R heeft geen nuldelers" nodig is.* Zij $R = \mathbb{Z}/91$. Zij $G = T^3 - 1 \in R[T]$. We zien dat $G' = 3T^2$. Bewijs: $3 \bmod 91 \in R$ is een eenheid (hint: wat is $((-30) \times 3) \pmod{91}$?). Bewijs: als $b \in R$ met $G'(b) = 0$ dan is $b = 0$ (en dus hebben G en G' niet een gemeenschappelijk nulpunt in R want $G(0) \neq 0$). Laat zien dat het aantal nulpunten van G in R groter is dan 3 (de graad van G).

(14.21) Eindige lichamen. Voor elke $n \in \mathbb{Z}_{>1}$ schrijven we

$$\mathbb{Z}/n = \{a \bmod n \mid 0 \leq a < n\}.$$

Dit is een ring.
Stelling. *$\mathbb{Z}/n$ is een lichaam dan en slechts dan als $n = p$, een priemgetal.*
Bewijs. Als $ab = n$ met $1 < a < n$ en $1 < b < n$ dan geldt

$$(a \pmod n) \times (b \pmod n) = n \pmod n = 0, \text{ en } a \pmod n \neq 0, \quad b \pmod n \neq 0.$$

Als $R = \mathbb{Z}/n$ een lichaam zou zijn, en $a \pmod n \neq 0$ dan is er een $x \in R$ met $x \times a \pmod n = 1$. Er zou komen

$$x \times a \pmod n \times b \pmod n = 1 \times b \pmod n = \times b \pmod n \neq 0,$$

en

$$x \times (a \pmod n \times b \pmod n) = x \times 0 = 0,$$

een tegenspraak (we bewijzen en gebruiken: een lichaam heeft geen nuldelers).

Anderzijds veronderstel dat $0 < a < n = p$, waar p een priemgetal is. Dan geldt $\text{ggd}(a, p) = 1$. Dus zijn er $y, z \in \mathbb{Z}$ met $ya + zp = 1$, zie (13.6). Dan geldt $(y \pmod p) \times (a \pmod p) = 1$. Conclusie: elk element $0 \neq \overline{a} \in \mathbb{Z}/p$ heeft een inverse. Dit laat zien dat $\mathbb{Z}/p$ een lichaam is.

(14.22) Dit geeft voorbeelden, $\mathbb{Z}/p$ van een eindig lichaam. Er zijn nog veel meer eindige lichamen, geclassificeerd, een mooie theorie, we gaan er niet verder op in.

Een eigenschap. Als K een eindig lichaam is, dan is er een priemgetal p en inclusie van lichamen $\mathbb{Z}/p \hookrightarrow K$, en $\#(K)$ is een veelvoud van p.
Bewijs: beschouw $1, 1+1, 1+1+1, \cdots$ in K; de kleinste $k > 0$ waarvoor $k \cdot 1 = 0$ in K is een priemgetal (gebruik dat K geen nuldelers heeft); in dat geval is $\mathbb{Z}/p$ als additieve groep een ondergroep van K; uit de stelling van Lagrange volgt dat p een deler is van $\#(K)$.
Opmerking: er geldt zelfs dat er een priemgetal p en een $n \in \mathbb{Z}_{>0}$ is met $\#(K) = p^n$.
Zie literatuur, of zie:
`http://en.wikipedia.org/wiki/Finite_field`

(14.23) Zij R een commutatieve ring. We zeggen dat $a \in R$ een *eenheid* is in R als er een $b \in R$ is met $ab = 1$ (d.w.z. als a een inverse heeft in R. We schrijven R^* voor de verzameling van de eenheden in R.
Laat zien dat R^* een (multiplicatief geschreven) groep is.

Voor $n \in \mathbb{Z}_{>0}$ geldt:

$$(\mathbb{Z}/n)^* = \{a \bmod n \mid 0 < a < n, \quad \text{ggd}(a, n) = 1\};$$

bewijs dit.

(14.24) Opgave. Bepaal de structuur van de groep $(\mathbb{Z}/n)^*$ voor alle $n \in \{5, 6, 8, 9, 10, 13\}$.

(14.25) Definitie/opmerking/opgave. (1) Voor $n \in \mathbb{Z}_{>0}$ definiëren we

$$\varphi(n) = \#((\mathbb{Z}/n)^*);$$

de afbeelding $\varphi : \mathbb{Z}_{>0} \to \mathbb{Z}$ wordt de Euler-φ-functie genoemd.
(2) Ga na: $\varphi(p) = p - 1$, en ook: $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.
(3) Ga na: als $a, b \in \mathbb{Z}_{>0}$ en $\text{ggd}(a,b) = 1$ dan geldt $\varphi(ab) = \varphi(a)\cdot\varphi(b)$.
(4) Bereken $\varphi(144)$, en $\varphi(2343)$.

(14.26) Stelling. *Zij K een eindig lichaam. De (multiplicatieve) groep K^* is cyclisch.*
Opmerking. We bewijzen de stelling, maar het bewijs geeft niet aan hoe je een voortbrenger construeert.
Bewijs. Zij $N = \#(K^*)$; als $\#(K) = q$ dan is $N = q - 1$ (want alle elementen ongelijk aan nul in K hebben een inverse in K, liggen daarom in K^*).

Beschouw de (multiplicatief geschreven) groep K^*. We schrijven m voor het maximum van de ordes van elementen van deze groep. We hebben gezien dat orde(x) een deler is van m voor alle $x \in K^*$, zie (14.8).3. Hieruit volgt dat elke $x \in K^*$ een nulpunt is van het polynoom $f = T^m - 1$. Uit (14.19) volgt dat het aantal nulpunten van f hooguit m is. Maar het aantal nulpunten is gelijk aan $\#(K^*) = N = q - 1$. Conclusie: $m = N$. We zien dat er in K^* een element van orde $q - 1$ is. Daaruit volgt dat K^* cyclisch is. QED

Notatie. We schrijven wel $\mathbb{F}_p$ voor het lichaam met p elementen; we zien dat de $(\mathbb{F}_p, +) = (\mathbb{Z}/p, +)$.

(14.27) Uitgewerkt voorbeeld. Neem $p = 11$. We bepalen de structuur van de groep $(\mathbb{F}_{11})^*$; we weten al dat die groep cyclisch is (d.w.z. de groep wordt voortgebracht door één element). In dit voorbeeld zien we dat.

We weten $\#((\mathbb{F}_{11})^*) = 10$; de delers 2 en 5 van 10 geven $2^2 \not\equiv 1 \pmod{11}$ en $2^5 \not\equiv 1 \pmod{11}$; conclusie: 2 mod 11 brengt $(\mathbb{F}_{11})^*$ voort,

$$j \longmapsto 2^j \bmod 11 \quad \text{geeft} \quad (\mathbb{Z}/10, +) \quad \xrightarrow{\sim} \quad ((\mathbb{F}_{11})^*, \times).$$

j	$2^j \bmod 11$	orde
0	1	1
1	2	10
2	4	5
3	8	10
4	5	5
5	10	2
6	9	5
7	7	10
8	3	5
9	6	10

We zien dat er precies 4 elementen zijn die als voortbrenger kunnen optreden van $(\mathbb{F}_{11})^*$. Dat konden we ook al concluderen, haast zonder rekenen: dat aantal is het aantal elementen dat $\mathbb{Z}/10$ voortbrengt, en dat aantal is gelijk aan $\varphi(10) = \varphi(2)\cdot\varphi(5) = 4$. Het bepalen van de orde van een k mod 11 geeft wat rekenwerk, maar bepalen van de orde van een j mod 10 is eenvoudig.

(14.28) Vraagstuk. (1) Bewijs dat $(\mathbb{Z}/64)^* \cong (\mathbb{Z}/2) \times (\mathbb{Z}/16)$.
(2) Bewijs dat $(\mathbb{Z}/121)^*$ een cyclische groep is (van orde $\varphi(121) = 110$). Zie (14.31)

(14.29) Voorbeelden/vraagstukken. (1) Ga na dat 3 mod 17 een voortbrenger is van $(\mathbb{Z}/17)^*$.
(2) Bepaal de orde van $(k \bmod 41) \in (\mathbb{Z}/41)^*$ voor alle $k \in \{2, 3, 4, 5, 6\}$.
Voorbeeld van een berekening. We zien $2^5 = 32$, en dus is $2^{10} \equiv -1 \pmod{41}$; ook is $2^4 \not\equiv -1 \pmod{41}$; conclusie orde$(2 \bmod 41) = 20$ voor $(2 \bmod 41) \in (\mathbb{F}_{41})^*$). Merk op $3^4 = 81$ en bereken de orde van 3 mod 41.
(3) Bepaal de verzameling van alle elementen die kunnen optreden als een voortbrenger van $(\mathbb{Z}/41)^*$. Zie (14.30).

(14.30) Oplossing van (14.29)(3). We zien dat orde$(k \bmod 41) < 40$ voor alle $k \in \{2, 3, 4, 5\}$ en orde$(6 \bmod 41) = 40$. Dus is 6 mod 41 een voortbrenger, en

$$(\mathbb{Z}/40, +) \xrightarrow{\sim} ((\mathbb{F}_{41})^*, \times) \quad j \longmapsto 6^j \bmod 41$$

geeft een isomorfisme. Voor alle j met $1 \leq j < 40$ en $\text{ggd}(j, 40) = 1$ is daarom $6^j \bmod 41$ een voortbrenger. Dit geeft $\varphi(40) = \varphi(5) \cdot \varphi(8) = 4 \cdot 4 = 16$ elementen die als voortbrenger van $(\mathbb{F}_{41})^*$ kunnen optreden:

$$\{1 \leq j < 40 \mid \text{ggd}(j, 40)\} \cong \{6^j \bmod 41 \mid j = 1, \ \ 3, \ \ 7, \ \ 9, \cdots, 37, \ \ 39\}.$$

Voorbeelden van die beelden $(6^j \bmod 41) \in (\mathbb{F}_{41})^*$:

$$j = 1 : \ \ 6; \quad j = 3 : \ \ 6^3 \equiv 11 \pmod{41} \ ;$$

$$j = 7 : \ \ d^7 \equiv 29 \pmod{41}; \ \ \cdots \ \ ; j = 39 : \ \ d^{39} \equiv 8 \pmod{41};$$

zo kunnen alle elementen die een voortbrenger zijn van $(\mathbb{Z}/41)^*$ berekend worden.
Zie [8], tabel op pag. 357 voor een voortbrenger van $(\mathbb{F}_p)^*$ voor $p < 1000$.

(14.31) Oplossing van (14.28)(1). Ga na: $3^8 \equiv 33 \pmod{64}$ en $3^{16} \equiv 1 \pmod{64}$. Laat zien dat de natuurlijke afbeelding

$$< 63 \bmod 64 > \times < 3 \bmod 64 > \xrightarrow{\sim} (\mathbb{Z}/64)^*$$

een isomorfisme is.
Oplossing van (14.28)(2). Ga na: $3^{10} = 19049 = 488 \times 121 + 1$ en $(1+11)^{11} \equiv 1 \pmod{121}$. Concludeer dat de orde van 33 mod 131 gelijk is aan 10×11.

(14.32) Opmerking. Voor $n \in \mathbb{Z}_{>0}$ waarvan we de factorizatie weten is de structuur van $(\mathbb{Z}/n)^*$ gemakkelijk te bepalen door middel van:
voor $n > 1$ is $(\mathbb{Z}/2^n)^* \equiv (\mathbb{Z}/2) \times (\mathbb{Z}/2^{n-2})$, en
voor $n > 0$ en een priemgetal $p \neq 2$ is $(\mathbb{Z}/p^n)^*$ cyclisch (van orde $p^n - p^{n-1}$).

(14.33) Een analogie. Zij K een lichaam. De ring $K[T]$ van polynomen in één variabele met coëfficienten in K heeft eigenschappen die lijken op eigenschappen van $\mathbb{Z}$; bij voorbeeld geldt unieke factorizatie in beide ringen. We proberen in deze ringen stellingen te formuleren. Soms zien we dat analoge beweringen in beide ringen waar zijn. Ook kunnen we proberen voor een vermoeden in de ene ring een analoge uitspraak in de andere ring te beschouwen. Een dergelijke analogie kan een leidraad zijn in welke richting we moeten zoeken. We geven drie voorbeelden, waar de stelling / het vermoeden in $\mathbb{Z}$ moeilijk is, maar de analoge uitspraak in $K[T]$ gemakkelijk te bewijzen is.

(14.33)(1) Het ABC-vermoeden in $\mathbb{Z}$ en in $R = K[T]$.
Veronderstel dat $\mathbb{Q} \subset K$ (anders gezegd: we nemen aan dat K karakteristiek nul heeft). Voor een polynoom $f \in K[T]$ schrijven we $\mathrm{Rad}(f)$ voor het radicaal (ook wel genoemd de conductor) van F: het product van alle irreducibele factoren van f.
Stelling (Mason). *Laat $A, B, C \in K[T]$ met*

$$A + B = C, \quad \mathrm{ggd}(A, B) = 1.$$

Dan geldt

$$\max\{\mathrm{graad}(A).\mathrm{graad}(B), \mathrm{graad}(C)\} \leq \mathrm{graad}(\mathrm{Rad}(ABC)) - 1.$$

Dit zegt dat het aantal priemfactoren van ABC niet te klein kan zijn, in analogie met het ABC vermoeden in $\mathbb{Z}$.
Zie `http://www.fen.bilkent.edu.tr/~franz/ag05/ag-02.pdf`
Het bewijs van deze stelling is niet moeilijk.

(14.33)(2) Het FLT-vermoeden in $\mathbb{Z}$ en in $k[T]$.
Zij $k = \mathbb{C}$ (of, algemener, een lichaam dat algebraïsch gesloten is met $\mathbb{Q} \subset k$).
Stelling (FLT in $k[T]$). *Zij $n \in \mathbb{Z}_{\geq 3}$. Neem $F, G, H \in k[T]$ met*

$$F^n + G^n = H^n \quad \mathrm{ggd}(F, G) = 1.$$

Dan geldt $F, G, H \in k$.
Probeer deze stelling af te leiden uit de vorige stelling.
Zie `http://www.fen.bilkent.edu.tr/~franz/ag05/ag-02.pdf`

(14.33)(3). De PNT in $\mathbb{Z}$ en een analogon in $R = K[T]$.
Laat K een eindig lichaam zijn met q elementen, Schrijf K_n voor het lichaam (dat K bevat) met q^n elementen. Het is bekend at een dergelijk lichaam bestaan en uniek is op isomorfie na. We zeggen dat een polynoom $f \in K'[T]$ monisch is als de coëfficient van de hoogste graads term gelijk aan 1 is. Het aantal monische, irreducibele elementen van graad i in $K_n[T]$ noemen we N_i.
Stelling.

$$N_i \quad \sim \quad \frac{q^i}{i}, \quad i \to \infty.$$

Onder de substitutie $x = q^i$ is de rechterhand gelijk aan $i/^q\log(i)$, en we zien een analogie.
Zie: *Analogue for irreducible polynomials over a finite field* in
`http://en.wikipedia.org/wiki/Prime_number_theorem`
Niet besproken: de Riemann hypothese in het algemeen, en in functielichamen over eindige lichamen.

15 Appendix D: De gehele getallen van Gauss

(15.1) We bespreken een ring die eigenschappen heeft die heel veel lijkt op die van de ring $\mathbb{Z}$. We geven een toepassing van de factorontbinding in deze ring. In deze § zal de notatie i niet gebruikt worden als index, maar als $i = \sqrt{-1}$. We schrijven:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\};\ \text{de ring van gehele getallen van Gauss.}$$

In deze verzameling is optellen, aftrekken, 0 en 1 gedefinieerd. Verder gebruiken we $i^2 = -1$ om de vermenigvuldiging te krijgen. We gebruiken het woord "priemgetal" voor een element $p \in \mathbb{Z}$ dat in die ring een priemgetal is. In de ring $\mathbb{Z}[i]$ zijn de elementen $1, i, -1, -i$ eenheden (elementen die een inverse in $\mathbb{Z}[i]$ hebben). We gebruiken in deze § het woord *priemelement* voor een element $\alpha \in \mathbb{Z}[i]$ dat niet een eenheid is, niet 0 is en niet een ontbinding toelaat $\alpha = zt$ waar z en t geen eenheden zijn.
Voorbeelden. $2 = 2 + 0{\cdot}i$ is niet een priemelement, want $2 = (1+i)(1-i) = i(1-i)^2$.
We zullen zien dat het priemgetal 3 wel een priemelement (in $\mathbb{Z}[i]$) is (ga na).
Merk op dat $5 = (2+i)(2-i)$. We zien dat 5 wel een priemgetal is (in $\mathbb{Z}$), maar niet een priemelement (in $\mathbb{Z}[i]$).
Probeer zelf na te gaan welke priemgetallen wel en welke niet een priemelement zijn.

(15.2) Stelling. *In de ring $\mathbb{Z}[i]$ geldt eenduidigheid van ontbinding in priemelementen, of volgorde, en op eenheden na.*
Voor een bewijs verwijzen we naar de literatuur.

(15.3) Stelling (Gauss). *Elk priemgetal p met $p \equiv 1 \pmod 4$ kan geschreven worden als*

$$p = a^2 + b^2, \quad a, b \in \mathbb{Z}_{>0}.$$

Opmerking. Die schrijfwijze is uniek op verwisselen van a en b na (geef zelf een bewijs).
Bewijs van (15.3). Stap 1. *Er is een getal $d \in \mathbb{Z}$ met $d^2 \equiv -1 \pmod 4$.*

Inderdaad, $(\mathbb{Z}/p)^*$ is een multiplicatieve, cyclische groep van orde $p-1$, en 4 is een deler van $p-1$; dus is er een element $(d \bmod 4) \in (\mathbb{Z}/p)^*$ van precies orde 4.
(Expliciet: zij $p = 2r+1$; laat zien dat $d := r! = 1 \times 2 \times \cdots \times r$ de eigenschap $d^2 \equiv -1 \pmod 4$ heeft; geef een bewijs.)
Stap 2. *Neem d als in Stap 1. Voor elke $y \in \mathbb{Z}$ geldt $(dy)^2 + y^2 \equiv 0 \pmod p$.* Allicht.
Merk op: als omgekeerd $x^2 - y^2 \equiv 0 \pmod p$ en p deelt niet xy dan geldt

$$(\frac{x \bmod p}{y \bmod p})^2 = -1 \in \mathbb{Z}/p.$$

Stap 3. *Er bestaan $a, b \in \mathbb{Z}$ met*

$$0 < a < \sqrt{p}, \quad 0 < b < \sqrt{p}, \quad a^2 + b^2 = p.$$

Kies een $\delta \in \mathbb{Z}$ niet deelbaar door p (en straks nemen we $\delta = d$). Schrijf $t = [\sqrt{p}]$ (het grootste gehele getal met $t^2 < p$. Beschouw

$$\{x - \delta{\cdot}y \mid 0 \le x \le t, \quad 0 \le y \le t\}.$$

Merk op dat hier een verzameling met $(t+1) \times (t+1)$ gehele getallen geven wordt. Omdat $(t+1)^2 > p$ zijn er tenminste twee verschillende paren (x_1, y_1), (x_2, y_2) (gebruik het "laden principe" of te wel het "duivenhok principe") die dezelfde waarde mod p geven:

$$x_1 - \delta{\cdot}y_1 \equiv x_2 - \delta{\cdot}y_2 \pmod p.$$

Kies

$$\delta := d, \quad a :=\mid x_1 - x_2 \mid, \quad b :=\mid y_1 - y_2 \mid; \quad \text{dan geldt} \quad a \equiv db \pmod{p}.$$

Omdat die paren verschillend waren geldt $a \neq 0$ (en dan volgt $b \neq 0$) of omgekeerd $b \neq 0$ (en dan volgt $a \neq 0$). We zien $0 < a < \sqrt{p}$ en $0 < b < \sqrt{p}$. Omdat $\delta = d$ en $a \equiv db \pmod{p}$ volgt $a^2 + b^2 \equiv 0 \pmod{p}$ (zie Stap 2). Omdat $0 < a^2 + b^2 < 2(\sqrt{p})^2 = 2p$ volgt $a^2 + b^2 = p$. QED

(15.4) Stelling. *De priemelementen (op eenheden na) in $\mathbb{Z}[i]$ zijn:*

(2) $1 + i$*;*

(3) *elk priemgetal $p \in \mathbb{Z}$ met $p \equiv 3 \pmod{4}$;*

(1) *elk element $a + bi$ zo dat $a^2 + b^2 = p$ een priemgetal is, met $p \equiv 1 \pmod{4}$.*

Een bewijs is niet zo moeilijk (raadpleeg de literatuur of geef zelf een bewijs). Gebruik vooral de afbeelding $a + bi \mapsto N(a + bi) = a^2 + b^2$.

(15.5) Nog een **bewijs** van (15.3). In dit bewijs gebruiken we (15.2). Inductie aanname: de uitspraak is reeds bewezen voor alle $q < p$ met $q \equiv 1 \pmod{4}$. We nemen $d \in \mathbb{Z}$ met $1 < d < p/2$ en $d^2 \equiv -1 \pmod{p}$. We kiezen $y = 1$ en $x = d$. Dan geldt $x^2 + y^2 \equiv 0 \pmod{p}$; schrijf $x^2 + y^2 = ep$. Als een priemgetal $r \equiv 3 \pmod{4}$ een deler zou zijn van e dan is r een deler van x en van y; dit bewijzen we als volgt: uit (15.4) volgt dat r een priemelement in $\mathbb{Z}[i]$ is; we zien dat r een deler is van $(x + iy)(x - iy)$; dus is r een deler van tenminste een van deze factoren; uit $r(a+ib) = x \pm iy$ volgt dat r en deler is van x en een deler van y (delers in $\mathbb{Z}$). Uit deze tegenspraak volgt dat een priemgetal s dat e deelt of gelijk is aan 2 of $s \equiv 1 \pmod{4}$. We geven een definitie van $e_+, e_- \in \mathbb{Z}[i]$.
Voor een priemgetal s dat e niet deelt schrijven we $e_+(s) = 1 = e_-(s)$.
Als 2^t een deler is van e en 2^{t+1} is niet een deler is van e dan schrijven we

$$e_+(2) = (1 - i)^t = e_-(2).$$

Als s^t een deler is van e en s^{t+1} is niet een deler is van e met $s \equiv 1 \pmod{4}$ en $t > 0$, dan weten we dat $s < p$; volgens de inductie aanname kunnen we kiezen $u + vi$ een deler van $d + i$, dan is $u - vi$ een deler van $d - i$, en $u^2 + v^2 = s$; we schrijven

$$e_+(s) = (u + vi)^t, \quad e_-(s) = (u - vi)^t.$$

We nemen $e_+ = \prod_s \ e_+(s)$ en $e_- = \prod_s \ e_-(s)$. We zien:

$$N(e_+) = e = N(e_-), \quad \text{en} \quad a' + b'i := di + 1/e_+; \quad a :=\mid a' \mid, \quad b =\mid b' \mid$$

geeft $a^2 + b^2 = N(a + bi) = N(d + i)/Ne_+) = p$. Conclusie:

$$0 < a < p/2, \quad 0 < b < p/2, \quad a^2 + b^2 = p.$$

QED

(15.6) Een voorbeeld. Neem $p = 29$. Dan is $d = 12$, want $12^2 = 144 = 5{\cdot}29 - 1$. Hier is $e = 5 = (2 + i)(2 - i)$. Er geldt

$$12 + i = (2 + i)(5 - 2i); \quad a = 2, \quad b = 5 \text{ geeft } 2^2 + 5^2 = 29.$$

Nog een voorbeeld: $p = 89$, $d = 34$. Dan is $d^2 + 1 = 1757 = 13 \times 89$; $N(d + i) = ep$ met $e = 13$. Wat zijn a en b in dit geval?

(15.7) Opgave. Neem $p = 41$, vind d met $1 < d < p/2$ en $d^2 \equiv -1 \pmod{41}$. Vind all paren (x, y) met $0 < x < p/2$, en $0 < y < p/2$, en $x^2 + y^2$ deelbaar door p; voor elk van die paren schrijf $x^2 + y^2 = e(x, y) \times p$; welke $e(x, y)$ komen voor? Zie (15.8).

(15.8) Oplossing van (15.7). Er zijn $(41-1)/10$ van zulke paren (op verwisselen van x en y na): $(1, 9), e = 2$, $(2, 18), e = 8$, $(3, 14), e = 5$, $(4, 5), e = 1$, $(6, 13), e = 5$, $(7, 19), e = 10$, $(8, 10), e = 4$, $(11, 17), e = 10$, $(12, 15), e = 9$, $(16, 20), e = 16$. (Merk op: $e = 1$ komt precies éénmaal voor; de priemdelers van e zijn 3, dan en slechts dan als x en y allebei deelbaar door 3, en verder zijn 2 en 5 delers van de andere e; kunnen we dit verklaren?)

(15.9) Pythagoreïsche drietallen.
Definitie. Een drietal $(a, b, c) \in (\mathbb{Z}_{>0})^3$ positieve gehele getallen heet een *Pythagoreïsch drietal* (afgekort PD) als $a^2 + b^2 = c^2$.

Als bovendien geldt $\text{ggd}(a, b) = 1$ dan spreken van een *primitief Pythagoreïsch drietal* (afgekort pPD); in dat geval is ook $\text{ggd}(b), c = 1$ en $\text{ggd}(c, a) = 1$ (ga na).
Opgave. Als (a, b, c) een pPD is dan geldt óf a is even en b is oneven óf b is even en a is oneven

Merk op: als $m, n \in \mathbb{Z}$ dan geldt $(m - n)^2 + (2mn)^2 = (m + n)^2$ (ga na). We laten zien (classificatie) dat omgekeerd alle pPD-en zo verkregen kunnen worden:

(15.10) Stelling. *Veronderstel (a, b, c) is een* pPD *met a is even en b is oneven. Dan bestaan er gehele getallen $m > n > 0$ met* $\text{ggd}(m, n) = 1$ *en $m + n$ oneven zodanig dat:*

$$a = m - n, \quad b = 2mn, \quad c = m + n.$$

Opgave. Geef een PD (niet primitief) dat niet van de vorm $(m^2 - n^2, 2mn, m^2 + n^2)$ is.
Opmerking. Er zijn veel onderling verschillende bewijzen. We geven hier een bewijs dat eigenschappen van $\mathbb{Z}[i]$ gebruikt.
Bewijs van de stelling. We gebruiken de resultaten vermeld in (15.2). We zien:

$$a^2 + b^2 = (a + bi) \times (a - bi) = c^2.$$

Stap 1. *Een priemelement $\alpha = x + yi$ dat wel $a + bi$ deelt, deelt niet $a - bi$.*

Stel α deelt zowel $a + bi$ als $a - bi$. Dan deelt het ook $a + bi + a - bi = 2a$ en ook $a + bi - (a - bi) = 2bi$. Zij p hét priemgetal dat deelbaar is door α (er is precies één zo'n priemgetal voor elk priemelement α, ga na). Dan deelt p het gehele getal $2a$ en ook het gehele getal $2b$. Omdat $\text{ggd}(a, b) = 1$ impliceert dit $p = 2$. Als $1 + i$ een deler is van $a + bi$ dan zou volgen dat $2 = N(1 + i)$ een deler is van $N(a + bi) = a^2 + b^2 = c^2$; hieruit zou volgen dat 2 een deler is van c, en dat is een tegenspraak met het feit dat a even is en $\text{ggd}(c, a) = 1$. Dit bewijst Stap 1.
Stap 2. *En bestaan $m \in \mathbb{Z}_{>0}$ en $n \in \mathbb{Z}_{>0}$ zodanig dat $a + bi = (m + ni)^2$.*

Merk op dat voor elk priemelement α dat $a+bi$ deelt er een getal $t \in \mathbb{Z}$ is met: $\alpha^{2t} \mid a+bi$ en α^{2t+1} deelt niet $a+bi$. Inderdaad, een dergelijke α deelt c en niet $a-bi$ dus is de maximale macht van α die $a+bi$ deelt ook de maximale macht die c^2 deelt, dus even. Uit de eenduidige factorontbinding in $\mathbb{Z}[i]$ volgt dat $a+bi =$ (eenheid) $\times$ (kwadraat); schrijf $a+bi = e(m+ni)^2$ met e een eenheid en $m > 0$ ($m = 0$ zou een tegenspraak geven, als m negatief is, dan vermenigvuldigen we met -1 en nemen -1 op in e):

$$a+bi \quad = \quad e \times (m+ni)^2 = e\cdot((m^2+n^2)+(2mn)i).$$

We zien dat $e \neq -1$. Als we zouden hebben dat $e = +i$ of $e = -i$ dan krijgen we $a+bi = 2mnie + (m^2+n^2)e$, met als conclusie dat $a = 2mnie$; tegenspraak met het feit dat a oneven is. We zien $e = 1$.
Stap 3: Einde van het bewijs.

We zien dat $a = m^2 - n^2 > 0$; dus is $m > n > 1$; verder is $b = 2mn$. Uit $\text{ggd}(a,b) = 1$ volgt $\text{ggd}(m,n) = 1$. Uit het feit dat a even is volgt dat m en n niet beiden oneven zijn; ook m en n niet beiden even kan niet vanwege $\text{ggd}(m,n) = 1$; dus volgt dat $m+n$ oneven is. QED

16 Appendix E: Berekeningen kunnen verkeerde verwachtingen suggereren

In deze paragraaf geven we een paar voorbeelden dat een (eindig) aantal berekeningen een verkeerde indruk kan geven. Soms stellen wiskundigen een vraag en ze proberen in een aantal gevallen door een berekening te zien wat het antwoord zou kunnen zijn (dat kan een goede benadering zijn). We hebben gezien hoe soms het vermoeden daardoor gesuggereerd onjuist bleek te zijn. Soms wordt zelfs bewezen dat de verwachtte conclusie oneindig vaak fout blijkt te zijn. We zien gevallen waar een abstract bewijs gegeven wordt dat het vermoeden onjuist is, zelfs oneindig vaak onjuist is, maar dat de berekening die dit aangetoond zou hebben ver buiten ons bereik ligt (b.v. veel meer cijfers moet gebruiken dan er elementaire deeltjes in ons heelal zouden zijn).

(16.1) In § 4 hebben we gezien dat de som

$$\sum_{p<N} \frac{1}{p},$$

de som genomen over alle priemgetallen met $p < N$, heel langzaam groeit voor $N \to \infty$. Het doen van een heel groot aantal berekeningen, eeuwen lang, zou wel eens een verkeerde suggestie kunnen wekken. Maar we weten dat Euler al lang geleden bewees dat de som

$$\sum_{p} \frac{1}{p} \quad \text{divergeert, onbegrensd is.}$$

(16.2) De Chebyshev's bias. Berekeningen die Chebyshev deed in 1835 gaven hem de indruk dat er (onder elke bovengrens) meer priemgetallen $p \equiv 3 \pmod 4$ zijn dan priemgetallen $q \equiv 1 \pmod 4$; zie (13.19). We zien weer hoe (zelfs veel) berekeningen een indruk geven hoe een verschijnsel zich gedraagt. Maar we weten nu ook (dankzij Littlewood) dat $\pi_{4,3}(x) - \pi_{4,1}(x)$ oneindig vaak van teken wisselt. Zelfs in de handen van een grootheid als Chebyshev gaf een (eindige) berekening een verkeerde suggestie.

(16.3) Hermite berekende in 1895 het volgende getal:

$$e^{\pi \times \sqrt{163}}.$$

Toen hij aan de berekening begon wist hij al dat dit niet een geheel getal is. Een benadering van dit getal is:

$$e^{\pi \times \sqrt{163}} \approx 262537412640768743.99999999999925007 \cdots.$$

Als we niets vermoedend aan een berekening zouden beginnen, en zoveel negens achter de komma zien (het zijn er twaalf), dan zouden we al gauw willen concluderen dat we met een geheel getal te maken hebben. Zie "The French paper of Hermite (1859) 'Sur la thorie des equations modulaires' is available freely at Google books, it begins at page 29"; ook te vinden via google: <hermite 163>. Voor een uitleg hoe je op het idee komt om juist dit getal te berekenen, zie [76], A4 op pagina 192

(16.4) Li en pi. In de PNT, gedeeltelijk besproken in § 10, worden afschattingen gedaan voor de functie $\pi(x)$ die het aantal priemgetallen onder x telt. We gebruikten de benadering $x/\log(x)$. Er is een heel ander benadering, gegeven door de functie $\mathrm{Li}(x)$:

$$\mathrm{Li}(x) = \int_2^x \frac{1}{t} dt;$$

zie b.v.
`http://en.wikipedia.org/wiki/Prime_number_theorem`
voor details. Dit zou een betere benadering is voor $\pi(x)$ geven. Voor "kleine" waarden van x geldt

$$\mathrm{Li}(x) > \pi(x),$$

en wiskundigen als Gauss en Riemann dachten dat deze ongelijkheid zou gelden voor alle x. Echter, Littlewood bewees in 1914 dat

- er wel degelijke getallen x zijn met $\mathrm{Li}(x) < \pi(x)$,
- maar de eerste keer dat dit gebeurt wel eens in de buurt van 10^{316} zou kunnen liggen,
- en dat $\mathrm{Li}(x) - \pi(x)$ oneindig vaak wisselt van teken voor $x \to \infty$.

We zien hoe misleidend het doorrekenen van eindig veel gevallen kan zijn voor een gedrag dat in oneindig veel gevallen bestudeerd wordt.

(16.5) Het vermoeden van Mertens. We zeggen dat $k \in \mathbb{Z}_{>0}$ *kwadraatvrij* is als voor elke $d \in \mathbb{Z}_{>1}$ het getal d^2 niet een deler is van k.
We zeggen dat $k \in \mathbb{Z}_{>0}$ *niet kwadraatvrij* is als er een $d \in \mathbb{Z}_{>1}$ zo dat d^2 een deler is van k.

De Möbiusfunctie. Voor elke $k \in \mathbb{Z}_{>0}$ definiëren we $\mu(k) \in \{-1, 0, +1\}$ als volgt:

- $\mu(k) = -1$ als n kwadraatvrij is en het aantal priemfactoren in de ontbinding van k is *oneven*;
- $\mu(k) = 0$ als k niet kwadraatvrij is;
- $\mu(k) = +1$ als k kwadraatvrij is en het aantal priemfactoren in de ontbinding van k is *even*.

Zie `http://nl.wikipedia.org/wiki/M%C3%B6biusfunctie`

We schrijven

$$M(n) = \sum_{k=1}^{k=n} \mu(k).$$

Suggestie. Bereken $\mu(k)$ voor alle $1 \leq k \leq 50$, en bereken $M(n)$ voor alle $1 \leq n \leq 50$. Valt er iets op?

Het vermoeden van Mertens, 1897.

$$\mid M(n) \mid < \sqrt{n} \qquad \forall\ n > 1 \quad (??); \quad \text{zie [57].}$$

Dit lijkt toch redelijk? Onze berekening voor kleine n geeft de suggestie dat $\mid M(n) \mid$ nauwelijks groeit. En als we even nadenken dan kunnen we dat ook heel goed "begrijpen": de priemgetallen 2 en 3 komen eerst (bijdrage -1, en $\mu(4) = 0$, en pas bij $\mu(6) = +1$ komt er een positieve bijdrage. (Vage praat.)

Lange tijd was dit vermoeden onbewezen, niet weerlegd. Berekeningen gaven alleen maar bevestigingen en geen tegenvoorbeelden.

Bovendien werd aangetoond dat het vermoeden van Mertens, indien juist, het vermoeden van Riemann zou bewijzen. We begrijpen het grote belang dat dit vermoeden kon hebben.

In 1985 bewezen Andrew Odłyzko en Herman te Riele dat het vermoeden van Mertens onjuist is, zie [59]. Dat is een imposant resultaat; het bewijs gebruikt zowel abstracte methoden als heel diepe berekeningen. En we kunnen nu ook begrijpen waarom we met een "beetje rekenen" hier niet opkwamen:

- er is een $n < e^{1.95 \times 10^{40}}$ met $\mid M(n) \mid > \sqrt{n}$,
- voor $n < 10^{14}$ geldt $\mid M(n) \mid < \sqrt{n}$,
- maar een preciese waarde waarvoor het Mertens vermoeden onjuist is, is niet gevonden.

Zie `http://nl.wikipedia.org/wiki/Vermoeden_van_Mertens`
Ik vind dit een prachtig voorbeeld hoe misleidend een eindig aantal berekeningen kan zijn.

Het is mogelijk dat $M(n)/\sqrt{n}$ een groei-gedrag vertoont dat lijkt op $\log(\log(n))$. Hierover zijn echter, voor zover ik weet, geen heuristische argumenten beschikbaar.

Postscript. Er is niets op tegen om gevoel te krijgen voor een situatie, voor een wiskundige vraag, door een (groot aantal) gevallen door te rekenen. Daar is niets mis mee, zo lang we maar beseffen dat het doorrekenen van een *eindig* aantal gevallen helemaal niets hoeft te zeggen hoe *oneindig* veel gevallen zich gedragen.

17 Appendix F: Enkele wiskundigen

http://en.wikipedia.org/wiki/Timeline-of-mathematics#1s-millennium-BC
http://nl.wikipedia.org/wiki/Lijst-van-wiskundigen
http://www-history.mcs.st-and.ac.uk/history/BiogIndex.html

Pythagoras (Pythagoras van Samos),
geboren tussen 580 en 572 vChr. – gestorven tussen 500 vCHr. en 490 vChr.

Aristoteles (Griekenland, 384 v. Chr.-322 v. Chr.)

Euclides van Alexandrië (Ptolemaïsch Egypte, circa 365 v. Chr.-275 v. Chr.)

Archimedes (Archimedes van Syracuse), (Syracuse, 287 v. Chr.-212 v. Chr.)

Diophantus (Diophantus van Alexandrië),
(Ptolemaïsch Egypte, geboren tussen 200 and 214 - gestorven tussen 284 en 298)
Wanneer hij leefde is niet erg duidelijk, het moet ergens tussen de 1e eeuw v.Chr. en de 4e eeuw na Chr. geweest zijn. Als meest waarschijnlijke datum geldt het midden van de 3e eeuw. Hij zou 84 jaar oud geworden zijn.

Abu Ja'far Muhammad ibn Musa Al-Khwarizmi (Irak, geboren ± 780 - gestorven ±850)

Abu Jafar Muhammad ibn al-Hasan Al-Khazin (Iran, ± 900-± 971)

Abu Mahmud Hamid ibn al-Khidr Al-Khujandi (Perzië, ± 940-1000)

Abu Ali al-Husain ibn Abdallah ibn Sina (Avicenna) (Uzbekistan, 980-1037)

Leonardo di Pisa (Leonardo Pisano Fibonacci, of gewoon Fibonacci),
(Italië, geboren tussen 1170 en 1180 - gestorven 1250)

Nicolaus Copernicus (Polen, 1473-1543)

Simon Stevin (Nederland, 1548-1620)

Pietro Antonio Cataldi (Italië, 1548-1626)

Pietro Antonio Cataldi (Italië, 1552-1626)

Johannes Kepler (Duitsland, 1571-1630)

Marin Mersenne (Frankrijk, 1588-1648)

René Descartes (Frankrijk, 1596-1650)

Claude Gaspar Bachet de Mziriac (Frankrijk, 1581-1638)

Pierre de Fermat (Frankrijk, 1601 (of 1607/08)-1665)

Christiaan Huygens (Nederland, 1629-1695)

Isaac Newton (Groot-Brittannië, 1643-1727)

Gottfried Wilhelm von Leibniz (Duitsland, 1646-1716)

Daniel Bernoulli (Zwitserland, 1700-1782),
Jakob Bernoulli (Zwitserland, 1654-1705),
Johann Bernoulli (Zwitserland, 1667-1748),
Nikolaus I Bernoulli (Zwitserland, 1687-1759)

Christian Goldbach (Duitsland, 1690-1764)

Leonhard Euler (Zwitserland, Rusland, 1707-1783)

Joseph-Louis Lagrange (Frankrijk, 1736-1813)

Adrien-Marie Legendre (Frankrijk, 1752-1833)

Marie-Sophie Germain (Frankrijk, 1776-1831) ("Monsieur LeBlanc")

"In describing the honourable mission I charged him with, M. Pernety informed me that he made my name known to you. This leads me to confess that I am not as completely unknown to you as you might believe, but that fearing the ridicule attached to a female scientist, I have previously taken the name of M. LeBlanc in communicating to you those notes that, no doubt, do not deserve the indulgence with which you have responded." Letter to Gauss (1807)
Zie ook `http://todayinsci.com/G/Germain_Sophie/GermainSophie-Quotations.htm`

Carl Friedrich Gauss (Duitsland, 1777-1855)

Jean Victor Poncelet (Frankrijk, 1788 - 1867)

Augustin Louis Cauchy (Frankrijk, 1789-1857)

Niels Henrik Abel (Noorwegen, 1801-1829)

Johann Peter Gustav Lejeune Dirichlet (Duitsland, 1805-1859)

Ernst Eduard Kummer (Duitsland, 1810-1893)

Évariste Galois (Frankrijk, 1811-1832)

Eugène Charles Catalan (België, 1814-1894)

Karl Weierstrass (Duitsland, 1815-1897)

Alphonse de Polignac (Frankrijk, 1817-1890)

Pafnuty Lvovich Chebyshev (Rusland, 1821-1894)

(Georg Friedrich) Bernhard Riemann (Duitsland, 1826-1866)

Max Noether (Duitsland, 1844-1921)

Georg Ferdinand Cantor (Duitsland, 1845-1918)

Felix Klein (Duitsland, 1849-1925)

Sofia Vasilyevna Kovalevskaya (Rusland, 1850-1891)

Hendrik Lorentz (Nederland, 1853-1928)

Thomas Joannes Stieltjes Jr (1856-1884)

Henri Poincaré (Frankrijk, 1854-1912)

Thomas Jan Stieltjes (Nederland, 1856-1894)

David Hilbert (Duitsland, 1862-1943)

Jacques Salomon Hadamard (Frankrijk, 1865-1963)

Charles-Jean de La Vallée Poussin (België, 1866-1962)

Godfrey Harold "G. H" Hardy (Groot-Brittannië, 1877-1947)

Luitzen Egbertus Jan Brouwer (Nederland, 1881-1966)

Emmy Noether (Duitsland, 1882-1935)

Hermann Weyl (Duitsland, USA, 1885-1955)

Srinivasa Aiyangar Ramanujan (India, Groot-Brittannië, 1887-1920)

Dirk Jan Struik (Nederland, USA, 1894-2000)

Maurits Cornelius Escher (Nederlands kunstenaar, 1898-1972)

Oscar Zariski (Wit-Rusland, USA, 1899-1986)

Bartel Leendert van der Waerden (Nederland, 1903-1996)

Hans Freudenthal (Duitsland, Nederland, 1905-1990)

Derrick Henry "Dick"Lehmer (USA, 1905-1991)

André Weil (Frankrijk, 1906-1998)

Edward Maitland Wright (Groot-Brittannië, 1906-2005)

Lothar Collatz (Duitsland, 1910-1990)

Alan Mathison Turing (Groot-Brittannië, 1912-1954)

Paul Erdös (Polen, 1913-1996)

Richard Phillips Feynman (USA 1918-1988)

Kurt Gödel (Duitsland, 1906-1978)

John Torrence Tate (USA, 1925-)

Jean-Pierre Serre (Frankrijk, 1926-)

Yutaka Taniyama (Japan, 1927-1958)

Henry Peter Francis Swinnerton-Dyer (Groot-Brittannië, 1927-)

Alexander Grothendieck (Duitsland, Frankrijk, 1928-)

Goro Shimura (Japan, 1930-)

Roger Penrose (Groot-Brittannië, 1931-)

Bryan John Birch (Groot-Brittannië, 1931-)

Robert Phelan Langlands (Canada, USA, 1936-)

John Horton Conway (Groot-Brittannië, USA, 1937-)

Yuri Ivanovitch Manin (Rusland, 1937-)

Barry Charles Mazur (USA, 1937-)

David Bryant Mumford (Groot-Brittannië, USA, 1937-)

Robert Tijdeman (Nederland, 1943-)

Gerhard Frey (Duitsland, 1944-)

Andrew M. Odlyzko (USA)

Herman Johannes Joseph te Riele (Nederland, 1947-)

Yuri Matiyasevich (Rusland, 1947-)

Kenneth Alan (Ken) Ribet (USA, 1948-)

Don Zagier (U.S.A., Duitsland, 1951-)

Yoichi Miyaoka (Japan)

Victor Kolyvagin (Rusland)

Matthias Flach (Duitsland, Groot-Brittannië, USA)

Andrew Wiles (Groot-Brittannië, 1953-)

Gerd Faltings (Duitsland, 1954-)

Joseph H. Silverman (USA, 1955-)

Richard Taylor (Groot-Brittannië, USA, 1962-)

Zie ook: Greatest mathematicians of all time
`http://fabpedigree.com/james/mathmen.htm`

18 Een paar vraagstukken

Elk van de onderstaande opgaven is te maken zonder kennis van moeilijke wiskunde-stellingen. Probeer deze opgaven te maken zonder de oplossingen te raadplegen.

(18.1) Opgave. In deze opgave staan 3 foute beweringen;
a) $4^3 = 8 \times 8$;
b) $3 + 4 = 8$;
c) $3^4 \equiv 1 \pmod 8$;
d) $3 \times 4 = 8 + 8^{-3} \times 8^4/2$.
Hoe kan dat? Zie (18.41). (Naar een Opgave van Gardner.)

(18.2) Opgave. Er zijn drie dozen met snoepjes, één doos bevat snoepje van type A, één doos bevat snoepjes van type B, en één doos bevat zowel snoepjes van type A als van type B. Er zijn drie deksels met etiketten A, B, respectievelijk A+B, maar op elk van de dozen zit een verkeerde deksel. Je kunt het verschil tussen A en B niet zien. Hoeveel snoepjes moet je minimaal proeven, en uit welke doos, om te weten welke deksel op welke doos hoort?

Op hoeveel manieren kun je de drie deksels verkeerd plaatsen?
Zie (18.42). Ik ken deze Opgave uit de film "La habitación de Fermat"(Fermat's room), maar waarschijnlijk komt dit raadsel al ergens eerder voor.

(18.3) Opgave.
I know an old man in Tralee
Whose age is his wife's age plus three.
Now he rightly declares,
That the sum of their squares
Is a square; so how old could he be?
Wat is de leeftijd van die man?
Zie (18.43).

(18.4) Opgave. Bewijs dat er in (18.3) maar één oplossing mogelijk is. Zie (18.44).

(18.5) Convexe verzamelingen. Een verzameling $V \subset \mathbb{R}^2$ heet *convex* als voor elk tweetal verschillende punten $P, Q \in V$ het lijnstuk met eindpunten P en Q bevat is in V.

Een lijn, een lijnstuk, een driehoek in $\mathbb{R}^2$ zijn convex.

Ga na: een vierhoek in $\mathbb{R}^2$ is convex dan en slechts dan als elk van de hoeken minder dan 180 graden is.

(18.6) Opgave. (1) Gegeven zijn 5 punten in $\mathbb{R}^2$, waarvan er geen drie op één rechte liggen. Bewijs dat er 4 van deze punten gekozen kunnen worden zodanig dat de vierhoek met deze punten als hoekpunten convex is.
(2) Ga na hoeveel convexe 4-hoeken er zo gekozen kunnen worden (afhankelijk van de ligging van die punten).
Zie (18.45).

(18.7) Opmerking: het "Happy End Problem" (Ester Klein, 1933). We kunnen ons afvragen hoeveel punten $f(n) = N$ we minimaal nodig hebben (geen drie op een rechte) om zeker te weten dat er een convexe n-hoek geconstrueerd kan worden uit deze punten. We zien direct dat $f(3) = 3$, en uit de vorige opgave zien we dat $f(4) = 5$.
Eenvoudige opgave. Bewijs dat $f(5) > 6$ (m.a.w. construeer een 6-tal punten waaruit geen enkel 5-tal een convexe vijfhoek geeft).
Moeilijke opgave. Bewijs dat $f(5) = 9$.
Voor een verdere discussie, zie:

`http://en.wikipedia.org/wiki/Happy_Ending_problem`
`http://mathworld.wolfram.com/HappyEndProblem.html`
`http://neeldhara.com/ramblings/notes/cgt-01`
`http://planetmath.org/happyendingproblem`
`http://pythagoras.nu/pyth/pdf/artikel_50285_20-24.pdf`

(18.8) De definitie van een graaf; Ramsey theorie. Een *graaf* bestaat uit hoekpunten en zijden. Elke zijde is een lijnstuk, en de twee uiteinden zijn gehecht aan een hoekpunt; het is toegestaan dat er een "lus" (Engels:"loop") is, dat wil zeggen een zijde waar begin- en eindpunt gelijk zijn; het is toegestaan dat er meerdere zijden tussen twee hoekpunten zijn. Grafen worden vaak gebruikt om combinatorische problemen inzichtelijk te maken. We zien een graaf als een abstract concept; soms kun je een graaf visualiseren als een ruimtelijke figuur; niet elke graaf is in te bedden in een vlak. Vaak worden eindige grafen bestudeerd (het aantal hoekpunten en het aantal zijden is eindig).

Een *eindige volledige graaf*, notatie K_n bestaat uit n hoekpunten, en de zijden zijn precies alle verbindingen tussen alle paren van twee verschillende hoekpunten.
De volledige 3-graaf: een driehoek.
De volledige 4-graaf: een tetraëder.

In Ramsey theorie wordt bestudeerd welke disjuncte complete deel-grafen voorkomen in een volledige graaf.
Zie § 33 van [26]. Zie `http://en.wikipedia.org/wiki/Ramsey_theory`

(18.9) Opmerking. We kunnen eenvoudig inzien dat niet elke graaf in het vlak $\mathbb{R}^2$ ingebed kan worden zonder dat zijden elkaar kruisen. Heel eenvoudigste voorbeeld:
Neem een graaf bestaande uit de hoekpunten G, W, E, A, B, C in $\mathbb{R}^2$. We proberen van elk van G, W, E een leiding te leggen naar elk van de huizen A, B, C zonder dat leidingen elkaar kruisen. Opgave: dat is niet mogelijk. (Dit is de volledige graaf K_3.)

(18.10) Opgave $R(3,3)$. We nemen een volledige n-graaf, en kleuren elke zijde óf rood (R) óf blauw (B), en we vragen ons af of er in deze K_n een volledige rode K_3 (een rode driehoek) of een volledige blauwe K_3 (een blauwe driehoek) geforceerd voorkomt.
(a) Laat zien dat in een K_5 (een volledige 5-graaf) de zijden zo te kleuren zijn dat er geen rode en ook geen blauwe driehoek in voorkomt.
(b) Laat zien dat voor elke $n \geq 6$ er in een volledige n-graaf met rode en blauwe zijden er tenminste één rode of tenminste één blauwe driehoek voorkomt.
Opmerking. Het resultaat hier gevraagd wordt genoteerd als: $R(3,3) = 6$, waarmee we willen zeggen dat als we twee kleuren gebruiken (het aantal cijfers in $R(\cdots)$), dat we driehoeken zoeken (de getallen 3 en 3), en dat de minimale n die tenminste een dergelijke driehoek forceert

gelijk is aan $n = 6$ in dit geval.
Zie (18.46).

(18.11) Opgave $R(3, 4) = 9$**. (a)** Geef een volledige 8-graaf, waarvan de zijden of rood of blauw zijn, zodanig dat er geen rode driehoek, en geen blauw tetraëder voorkomt in deze K_8. **(b)** Bewijs dat in een K_9 waarvan de zijden rood of blauw zijn er of een rode driehoek of een blauw tetraëder voorkomt.
(Kortom: $R(3, 4) = 9$.)
Zie (18.47)

(18.12) Opmerking. Er gelden de volgende resultaten: $R(3; 5) = 14$, $R(3; 6) = 18$, $R(3; 7) = 23$, $R(3; 8) = 28, R(3; 9) = 36$. (Probeer hier maar iets van te bewijzen.) Voor nog veel meer resultaten, zie
`http://en.wikipedia.org/wiki/Ramsey%27s_theorem`
`http://mathworld.wolfram.com/RamseyNumber.html`

(18.13) Een Ramsey-spel. Hier is een voorstel voor een spel, een variatie op "Boter, Kaas en Eieren":
twee spelers nemen een vel papier en tekenen daarop daarop 6 punten; de ene speler heeft een rood potlood, de ander een blauw; besloten wordt wie er begint; om beurten wordt een "zet gedaan", en die bestaat uit het trekken van een (mogelijk gebogen) lijnstuk tussen twee van die punten die niet reeds verbonden zijn; dat lijnstuk gaat niet door een van de andere vier punten; dat lijnstuk mag wel andere lijnstukken, die reeds getrokken zijn, snijden; het is duidelijk dat na hoogstens 15 zetten alle mogelijke zijden getekend zijn; winnaar is diegene die het eerste een driehoek van de eigen kleur volmaakt.
Opmerkingen.

- Omdat $R(3, 3) = 6$ eindigt het spel met een winnaar.
- In plaats van 6 punten kunnen we ook met meer punten beginnen, en het spel verloopt precies zo.

(18.14) Een opgave over het Ramsey-spel. Bewijs dat de speler die begint in het het Ramsey $3 - 3-$spel, zie (18.13), winst kan forceren. Zie (18.48).

(18.15) Nog een Ramsey-spel. Idem als boven, eveneens met twee spelers, maar nu beginnen we met ≥ 18 punten, en winnaar is diegene die het eerst een tetraëder van de eigen kleur afmaakt; het spel eindigt omdat $R(4, 4) = 18$ (Greenwood en Gleason, 1955).

(18.16) Opgave $R(3, 3, 3) = 17$.
(< 17) Bewijs dat de volledige K_{16} een kleuring van de zijden met drie kleuren toelaat, zodat er geen monochrome driehoeken zijn.
(≥ 18) Bewijs dat in de volledige K_{17} elke kleuring van de zijden met drie kleuren er een monochrome driehoek is.
Zie `http://en.wikipedia.org/wiki/Ramsey's_theorem`voor bewijzen.

(18.17) Een Ramsey $3-3-3$−spel. (Dit lijkt wel leuk, maar ook niet erg practisch uitvoerbaar.) Drie spelers zetten 17 punten op een vel papier; zij kunnen de zijden drie verschillende kleuren geven. Verder zijn de spelregels als in (18.13). Winnaar is diegene die het eerst een monochrome driehoek volmaakt.

Waarschijnlijk moeten we nog de volgende spelregel opnemen. Elke speler die aan zet is, en die niet een monochrome driehoek kan maken is verplicht eventuele mogelijkheden van andere spelers om direct te winnen (twee zijden van één kleur, en de derde zijde is nog open) eerst te blokkeren door een van die driehoek(en) af te maken.

Ik weet niet welk van de spelers in dit spel winst kan forceren.

(18.18) Opgave. Zij $n \in \mathbb{Z}_{>0}$. Bewijs dat er een $a \in \mathbb{Z}_{>0}$ bestaat zodanig dat er in de rekenkundige rij

$$\{a, a+n, a+2n, \cdots\} = \{a+in \mid i \in \mathbb{Z}_{>0}\}$$

er oneindige veel priemgetallen zijn. Zie (18.49)

(18.19) Een diepe stelling van Dirichlet.* Een stelling van Dirichlet zegt: voor alle $a, n \in \mathbb{Z}_{>0}$ met $\gcd(a,n) = 1$ is er in de rekenkundige rij

$$\{a, a+n, a+2n, \cdots\} = \{a+in \mid i \in \mathbb{Z}_{>0}\}$$

oneindig veel priemgetallen. Die stelling is niet eenvoudig te bewijzen. Curieus: de opgave (18.18) (waarvan de uitspraak wezenlijk zwakker is dan die van de stelling van Dirichlet, is dat duidelijk?) is heel eenvoudig en elementair te bewijzen, en wel zonder gebruik te maken van deze stelling van Dirichlet.

(18.20) Opgave. Een boeken-wurm. Johan is student Arabisch, en hij heeft een prachtig Arabisch boek in 5 delen gekocht. Thuis gekomen zet hij deze 5 boeken op de plank, natuurlijk zoals het hoort. Hij kijkt ernaar als hij de ruggen van de 5 boeken ziet, deel 1 rechts, daarnaast deel 2, en tenslotte deel 5 helemaal links. Behalve de kaften heeft elk deel 200 pagina 's (de titel pagina en de lege pagina's meegeteld). Maar, er zit tussen het kaft en de eerste pagina van deel 1 een Boekenwurm. En die knaagt rechtdoor, tot hij aangeland is tussen het kaft en de laatste pagina van deel 5.
– Hoeveel gaten zitten er in de kaften?
– Hoeveel bladzijden hebben een gat?
(We zeggen hier pagina voor een kant van een bladzijde; een bladzijde hier is een vel papier; elk boek hierboven heeft 200 pagina's, en dus 100 bladzijden in onze terminologie. Elk boek heeft een voor-kaft en een achter-kaft.)
Zie (18.50)

(18.21) Opgave. Bepaal het laatste cijfer van 7^{511} in decimale schrijfwijze.
Zie (18.51)

(18.22) Opgave. Is dit een kwadraat ? Is het getal 87618160696635058683 het kwadraat van een geheel getal?

[Nadenken is vaak beter dan het gebruik van een rekenmachine.]
Zie (18.52)

(18.23) Opgave. Is dit een een kwadraat ? Is het getal 3339590081146975295 het kwadraat van een geheel getal?

[Nadenken is vaak beter dan het gebruik van een rekenmachine.]

Zie (18.53)

(18.24) Opgave. Is dit een kwadraat ? Is het getal $C = 1156553944297325629695$ het kwadraat van een geheel getal?

[Nadenken is vaak beter dan het gebruik van een rekenmachine.]

Zie (18.54)

(18.25) Opgave. Wat zijn de rationale punten op deze kromme ? Beschrijf alle $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ zodanig dat

$$(E) \qquad y^2 = x^3 - 4x^2 + 5x - 2.$$

Zie (18.55)

(18.26) Opgave. Wat zijn de gehele oplossingen? Bewijs dat er niet een paar $(x, y) \in \mathbb{Z}^2$ bestaat zodanig dat

$$x^3 + y^4 = 2613527.$$

Zie (18.56)

(18.27) Opgave. Een pad in de 4-dimensionale ruimte. In de 3-dimensionale ruimte $\mathbb{R}^3$ zijn gegeven:

een boloppervlak S door de vergelijking $X^2 + Y^2 + Z^2 = 1$,

een punt P binnen de bol: $P = (0, 0, 0)$,

en een punt Q buiten de bol: $Q = (2, 0, 0)$.

We bedden de ruimte in in een 4-dimensionale ruimte $\mathbb{R}^4$ door een punt $Z = (x, y, z)$ af te beelden op $Z' = (x, y, z, 0)$.

Geef een pad in de 4-dimensionale ruimte dat begint in P', het oppervlak S' niet snijdt, en eindigt in het punt Q'.

[Een pad van A naar B in een ruimte R: een continue afbeelding van het interval $[0, 1]$ naar R, die 0 op A en 1 op B afbeeldt: in de tijd die loopt van 0 naar 1 "loop" je van A naar B zonder sprongen te maken.]

Zie (18.57)

(18.28) Opgave. Deelbaar door 7. Bewijs dat het getal $2222^{5555} + 5555^{2222}$ deelbaar is door 7.

`http://www.vierkantvoorwiskunde.nl/Opgaves/db.html`

Zie (18.58)

(18.29) Opgave. Deze opgave komt uit [27], Ch.6, Problem 6.4. We hebben 27 blokken van afmeting $1 \times 2 \times 4$. Kunnen we die stapelen tot een kubus met afmeting $6 \times 6 \times 6$? Zie (18.61).

Oplossingen van een paar vraagstukken.

(18.30) Een antwoord op (4.4). We stapelen blokken (van lengte 1) zo dat het eerste blok half over het tweede heen steekt, het tweede blok 1/4 over het derde blok, en zo verder: het i-de blok steekt $1/(2i)$ over het $(i+1)$-de blok. We zien dat voor elke $i \geq 1$ de eerste i blokken

$$\frac{1}{2} + 2\frac{1}{4} + \cdots + i\frac{1}{2i}$$

naar buiten steken. Conclusie: bij deze stapeling is er een (labiel) evenwicht. We kunnen een stabiel evenwicht krijgen door het eerste blok iets minder van 1/2 te laten uitsteken, of door de keuze van een $\delta \in \mathbb{R}$ met $0 < \delta < 1$ en elke i-de blok $\delta/(2i)$ te laten uitsteken. Divergentie van de harmonische reeks laat zien dat we willekeurig ver over de rand van de tafel uit kunnen steken (maar dat we wel heel veel blokken nodig hebben willen we aardig ver komen).

(18.31) Een antwoord op (4.5). In de eerste seconde heeft de kever 1/100 van de draad afgelegd. In de tweede seconde 1/200 deel van de draad, en in de i-de seconde $(1/100) \times (1/i)$ deel van de draad. We zien dat na a seconden het deel van de draad door de kever afgelegd gelijk is aan

$$\frac{1}{100} \times \left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{a} \right).$$

Vanwege divergentie van de harmonische reeks weten we dat de kever het eind haalt. Een zeer ruwe schatting geeft dat na 2^{4k-1} de kever $k/100$-ste deel van de draad heeft afgelopen. Na 2^{399} seconden is de kever zeker over de rand verdwenen; dat is ongeveer 1.3×10^{120} seconden, veel langer dan de leeftijd van het heelal.

(18.32) Oplossing van (5.2). Zij $n \in \mathbb{Z}_{>1}$ een *oneven* positief geheel getal. Dan geldt

$$T^n + 1 = (T+1) \times \sum_{i=0}^{i=n-1} (-1)^i T^i.$$

Als $m = n \times a$ met $n \in \mathbb{Z}_{>1}$ een *oneven* positief geheel getal dan zien we dat

$$2^m + 1 = (2^a)^n + 1 = (2^a + 1) \times B$$

met B geheel en groter dan 1; conclusie: in dat geval is $2^m + 1$ niet een priemgetal.

(18.33) Een oplossing van (13.22). We zien dat $16^2 = 256 = 7 \times 37 - 3$; ook geldt daarom: $21^2 \equiv -3 \pmod{37}$ (Is dat duidelijk zonder rekenen?).

(18.34) Een oplossing van (13.23). Uit

$$15^2 + 3 = 225 + 3 = 228 = 4 \times 3 \times 19$$

volgt dat alleen 2, 3 en 19 deze eigenschap hebben.

(18.35) Een oplossing van (14.17). Het is duidelijk dat 2 niet een deler is van een getal van de vorm $M_n = 2^n - 1$. Bewering: elke priemgetal $p > 2$ is wel deler van een Mersenne getal. Bewijs: uit de stelling van Lagrange, zie (14.7), volgt

$$(2 \bmod p)^{p-1} = 1 \bmod p \text{ in } (\mathbb{Z}/p)^*, \quad p > 2.$$

We zien dat $p > 2$ een deler is van M_{p-1}.

(18.36) Oplossing van (4.10). Voor $N = 100$ komt er:

$$\sum_{p<100} 1/p \approx 1.802817201 \quad \text{en} \quad \log(\log(N)) + B + \frac{1}{(\log(N))^2} \approx 1.8362.$$

(18.37) Oplossing van (6.1). Als $n = ab$ met $a, b \in \mathbb{Z}_{>1}$ dan geldt:

$$X^{ab} - 1 = (X^a)^b - 1 = (X^a - 1) \times \sum_{i=0}^{i=b-1} (-1)^i \, (X^a)^i.$$

Voor $a > 1$ en $b > 1$ zien we dat $2^{ab} - 1$ niet een priemgetal is.

(18.38) Oplossing van (7.5). Let goed op de formulering van de vraag. Het antwoord is "nee".

Motivatie: we weten dat die deelnemer een leeftijd heeft tussen de 50 en 110. Binnen die grenzen zien we dat $66, 70, 81$ en 94 een kwadraat als som van de delers heeft. Omdat er meer dan één mogelijkheid is kunnen we niet met zekerheid zeggen wat die leeftijd is,

(18.39) Oplossing van (7.6). Die uitspraak is onjuist: voor $N = 5 \times 7 \times 11$ geldt $\sigma(N) = 6 \times 8 \times 12 = 2^6 \cdot 3^2$.

(18.40) Oplossing van (7.10). Opmerking vooraf: als M_n een priemgetal is, dan is $\sigma(M_n) = 2^n - 1 + 1 = 2^n$.

We nemen aan dat er oneindig veel Mersenne priemgetallen zijn. Kies $k \in \mathbb{Z}_{>0}$. De priemgetallen p die een Mersenne priemgetal M_p geven verdelen zich over de restklassen modulo k; dus is er een $0 < a < k$ zodanig dat

$$\mathcal{P} = \{p \mid M_p \text{ is priem}, \quad p \equiv a \pmod{k}\}$$

een *oneindige* verzameling is. We schrijven die verzameling als

$$\mathcal{P} = \{P_j \mid j \in \mathbb{Z}_{>0}\} = \{P_1, \cdots, P_{k-1}\} \cup \{P_j \mid j \geq k\}.$$

We zien dat de getallen

$$N_j := M_{P_1} \times \cdots \times M_{P_{k-1}} \times M_{P_j}, \quad j \geq k$$

een oneindige verzameling vormen, en elk van die getallen heeft de eigenschap dat

$$\sigma(N_j) = 2^{P_1 + \cdots + P_{k-1} + P_j}$$

een k-de macht is.

(18.41) Oplossing van (18.1). We zien dat (a), (c) en (d) goed zijn. De uitspraak in de eerste zin, en in (b) zijn onjuist; er staan twee foute beweringen in die opgave: de opgave is juist.

(18.42) Oplossing van (18.2). Één snoepje proeven uit de doos met (de verkeerde) deksel A+B. Ga na dat je zo inderdaad kunt beslissen hoe de deksels goed geplaatst moeten worden. Ga ook na dat één snoepje proeven uit een van de andere dozen er geen zekerheid is dat je weet welke deksel op welke doos hoort.

Er zijn twee manieren om alle deksels verkeerd te plaatsen (en drie manieren om precies twee deksels verkeerd te plaatsen).

(18.43) Oplossing van (18.3). Een oplossing is: de vrouw is 60, de man is 63; inderdaad is $60^2 + 63^2 = 87^2$ (voor motivatie zie (18.44)).

(18.44) Oplossing van (18.4). Er zijn meerdere oplossingen van de diophantische vergelijking (oplossing in gehele getallen) $A^2 + (A+3)^2 = C^2$. Bijvoorbeeld: schrijf $A = 3a$; de volgende a hebben de eigenschap dat $a^2 + (a+1)^2$ een kwadraat is:
$a = 3$ en $3^2 + 4^2 = 5^2$;
$a = 20$ en $20^2 + 21^2 = 29^2$;
$a = 119$ en $119^2 + 120^2 = 169^2$;
$a = 696$ en $696^2 + 697^2 = 985^2$;
$a = 4059$ en $4059^2 + 4060^2 = 5741^2$;
ook $a = 23660$ en $a = 137903$ voldoen, etc.;
we kunnen bewijzen: er zijn oneindig veel $a \in \mathbb{Z}_{>0}$ zo dat $a^2 + (a+1)^2$ een kwadraat is.
Hoe kunnen we bewijzen dat er maar één oplossing van (18.3) is?

Claim. Als $A \in \mathbb{Z}_{>0}$ en $A^2 + (A+3)^2 = C^2$ dan zijn A en C deelbaar door 3.
Bewijs. We zien dat $A \equiv \pm 1 \pmod 3$ zou geven $C^2 \equiv 2 \pmod 3$; tegenspraak.

Om $A^2 + (A+3)^2 = C^2$ op te lossen is het voldoende om op te lossen $a^2 + (a+1)^2 = c^2$, met $A = 3a$, en $C = 3c$. Omdat $A + 3$ de leeftijd van een "old man" is, concluderen we dat $15 < a < 40$. Maak een lijst van alle mogelijkheden en concludeer dat $a = 3$ en $a = 20$ de enige oplossingen zijn met $a < 40$; we zien dat de oplossing $(**)$ hierboven de enige oplossing van (18.3) is met $30 < A < 110$ $(10 < a < 37)$.

(18.45) Oplossing van (18.6). Eerst een constructie. We schrijven $V^c \subset \mathbb{R}^2$ voor de kleinste convexe verzameling die een verzameling $V \subset \mathbb{R}^2$ bevat; die bestaat: neem de verzameling $\Gamma(V)$ van alle convexe verzamelingen die V bevat; merk op $\Gamma(V) \neq \emptyset$ (want $\mathbb{R}^2 \in \Gamma(V)$); de doorsnede

$$V^c := \cap_{C \in \Gamma(V)} \ C$$

is convex (ga na), en voldoet aan de eisen. De verzameling V^c wordt het *convexe omhulsel* van V genoemd,

Beschrijf V^c voor een eindige verzameling V.
(1) Zij V^c het convexe omhulsel van $V := \{P_1, \cdots, P_5\}$. We zien dat er 3 mogelijkheden zijn:
(d) V^c is een driehoek, en er zijn twee inwendige punten in V^c;
(vier) V^c is een convexe vierhoek, en er is 1 inwendig punt;
(vijf) V^c is een convexe vijfhoek.

(1) + (2) In het geval (vijf) geeft elk 4-tal van deze punten een convexe vierhoek; in dit geval is het aantal convexe vierhoeken dat zo geconstrueerd kan worden gelijk aan 5.

In het geval (vier) zien we al één convexe vierhoek, zeg P_1, P_2, P_3, P_4; trek diagonalen in die vierhoek; als $Q = P_5$ gelegen is in de driehoek gevormd door P_1 en $[P_2, P_3]$, dan is $[P_2, P_3, P_4, P_5]$ convex: elke diagonaal geeft een extra convexe vierhoek; in dit geval is het totale aantal convexe vierhoeken gelijk aan 3.

In het geval (d) hebben we een driehoek, zeg $[P_1, P_2, P_3]$, met twee inwendige punten. De lijn door P_4 en P_5 heeft twee punten aan de ene kant, en één punt, zeg P_3, aan de andere kant; dan is $[P_1, P_2, P_4, P_5]$ de enige convexe vierhoek die in dit geval geconstrueerd kan worden.

(18.46) Een oplossing van (18.10) **(a)** Neem $P_1, \cdots, P_5$, en geef de zijden $< P_1P_2 >, \cdots, < P_4P_5 >, < P_5P_1 >$ een rode kleur, en alle ander zijden in deze complete 5-graaf een blauwe kleur. Het is duidelijk dat er geen rode driehoek voorkomt. Twee blauwe zijden die een hoekpunt gemeen hebben de andere hoekpunten verbonden door een rode zijde (ga na). Dit bewijst onderdeel (a).
(b) Neem een van de hoekpunten van een K_6 met rode en/of blauw gekleurde zijden; noem dat hoekpunt Q. In Q komen 5 gekleurde zijden aan, en tenminste 3 daarvan hebben dezelfde kleur. Veronderstel dat $< QP_1 >, < QP_2 >, < QP_3 >$ rood zijn; als tenminste een van de zijden $< P_1P_2 >, < P_2P_3 >, < P_3P_1 >$ rood is, dan is er een rode driehoek; als geen van deze zijden rood is, dan zijn ze alle drie blauw, en er is een blauwe driehoek.

(18.47) Oplossing van (18.11) **(a)** Maak een dergelijk voorbeeld, of zie bv.
`http://andrescaicedo.files.wordpress.com/2006/12/bsugrad2011.pdf`
(b) we onderscheiden een aantal gevallen:
(1) *Er is een hoekpunt Q in K_9 waar tenminste 4 rode zijden aangehecht zijn*; laat de andere uiteinden van die rode zijden P_1, P_2, P_3, P_4 zijn. Als een van de verbindingszijden $< P_iP_j >$ met $1 \leq i < j \leq 4$ rood is, dan komt er een rode driehoek. Als geen van die verbindingszijden rood is dan komt er een blauw tetraëder.
2) *Alle hoekpunten hebben precies 3 rode zijden aangehecht.* Dat kan niet: dan zouden er precies 9×3 uiteinden van een rode zijde zijn, maar dat aantal is even.
3) *Veronderstel dat* (1) *en* (2) *niet waar zijn.* Dan is er een hoekpunt T waar hooguit 2 rode zijden aangehecht zijn, dus minstens 6 blauwe zijden: $< TP_i >$ met $1 \leq i \leq 6$ zijn blauw. In de K_6 opgespannen door deze 6 punten geldt $R(3,3) = 6$, m.a.w. daarin is er of een rode driehoek (en we zijn klaar), of er is een blauwe driehoek, die samen met R een blauw tetraëder geeft. Einde bewijs.

(18.48) Een oplossing van (18.14). Zeg dat R begint en B de andere speler is. We nummeren de hoekpunten naar aanleiding van de eerste zetten (de nummering doet er niet toe, het is meer een notatie om ons bewijs op te schrijven). Er zijn twee mogelijkheden:
(I) De zet $B1$ heeft een hoekpunt met de zet $R1$ gemeen.
(II) De zet $B1$ heeft niet een hoekpunt met de zet $R1$ gemeen.
Notatie: Ri is de i-de zet van R, etc. We schrijven K voor keus, en F voor een geforceerde zet.

(I) $R1 =< 12 >$, $K:$ $B1 =< 23 >$,
$K:$ $R2 =< 14 >$, $F:$ $B2 =< 24 >$,
$F:$ $R3 =< 34 >$, $F:$ $B3 =< 13 >$,
$K:$ $R4 =< 15 >$, en B heeft geen verweer tegen de dreigingen $< 25 >$ en $< 45 >$.

(I) $R1 =< 12 >$, $K:$ $B1 =< 34 >$,
$K:$ $R2 =< 14 >$, $F:$ $B2 =< 24 >$,
$F:$ $R3 =< 23 >$, $F:$ $B3 =< 13 >$,
$K:$ $R4 =< 15 >$, en B heeft geen verweer tegen de dreigingen $< 25 >$ en $< 45 >$.

(18.49) Oplossing van (18.18). Beschouw alle $x \in \mathbb{Z}$ met $0 < x < n$, en beschouw alle

$$x \bmod n \in \mathbb{Z}/n.$$

Zij $\mathcal{P}$ de verzameling van alle priemgetallen en kijk naar de afbeelding

$$\mathcal{P} \longrightarrow \mathbb{Z}/n \qquad p \mapsto p \bmod n.$$

Merk op dat veelvouden van n niet een priemgetal zijn; we zien dat de oneindige verzameling $\mathcal{P}$ maar eindig veel beelden heeft in $\mathbb{Z}/n - \{0\}$. Voor tenminste één $x = a$ komen er oneindig veel priemgetallen terecht op $p \bmod n = a \bmod n$. Dit is de gevraagde a. (Merk op dat we niet bewijzen, wat wel waar is, dat élke a met $\text{ggd}(a, n) = 1$ gekozen kan worden.)

(18.50) Oplossing van (18.20): **de boeken-wurm.** Arabische boeken beginnen op de meest rechtse pagina, en gaan door (precies andersom als "onze boeken") tot de laatste pagina, de meest linkse als je het boek openslaat. De wurm begint tussen (Arabische voor-)kaft en pagina 1 van deel 1, en eindigt tussen (Arabische achter-)kaft en pagina 200 van deel 5. Daarbij zijn er 300 bladzijden doorgeknaagd, de bladzijden van deel 1, en de bladzijden van deel 5 blijven heel. Daarbij zijn er 8 kaften doorgeknaagd.
Opmerking. De analoge Opgave voor een boek in 5 delen met "onze" manier van pagineren geeft hetzelfde antwoord; mee eens?

(18.51) Oplossing laatste cijfer (18.21). Merk op dat $7^3 = 343$, $7^4 = 2401$ en $511 \equiv 3 \pmod 4$. Dus $7^{511} \equiv 7^3 \pmod{10}$ en we zien $7^{511} \equiv 3 \pmod{10}$.

(18.52) Oplossing is dit een kwadraat (18.22): **niet een kwadraat.** Kwadraten van gehele getallen geschreven als 10-talig cijfer, eindigen op een 0, 1, 4, 5, 6 of 9. We zien dat een getal dat eindigt op een 3 niet een kwadraat is.
Mijn rekenmachine geeft $\sqrt{87618160696635058683} = 9360457291$. Is dat antwoord goed? Nadenken is vaak beter dan het gebruik van een rekenmachine.

(18.53) Oplossing van (18.23): **niet een kwadraat.** We zien dat

$$3339590081146975295 \equiv 6 \pmod 9.$$

Daarom is dit getal wel deelbaar door 3, maar niet deelbaar door 9. In de priemfactorontbinding van dit getal komt 3^1 voor, en niet 3^2; dus is dit getal niet een kwadraat.

Andere oplossing: laat zien dat het getal wel door 5, maar niet door 25 deelbaar is.
Mijn rekenmachine geeft $\sqrt{3339590081146975295} = 1827454536$. Is dat antwoord goed? Nadenken is vaak beter dan het gebruik van een rekenmachine.

(18.54) Oplossing van (18.24): **niet een kwadraat.** We zien dat

$$1156553944297325629695 \equiv 2 \pmod{11}.$$

De kwadraten modulo 11 zijn $0, 1, 3, 4, 5, 9$. Dit is daarom niet een kwadraat.

Merk op dat $C \equiv 5 \pmod{10}$ en $C \equiv 0 \pmod 9$.

Andere oplossing: laat zien dat het getal wel door 5, maar niet door 25 deelbaar is.
Mijn rekenmachine geeft $\sqrt{1156553944297325629695} = 34008145264$. Is dat antwoord goed? Nadenken is vaak beter dan het gebruik van een rekenmachine.

(18.55) Oplossing rationale punten op een kromme (18.25). (We gebruiken dat dit een singuliere kromme geeft.) Het antwoord is:

$$\{(1,0)\} \cup \{(x = \alpha^2 + 2,\ y = \alpha(\alpha^2 + 1)) \mid \alpha \in \mathbb{Q}\}.$$

Bewijs. Voor elk punt $P = (x, y) \neq (1, 0)$ kiezen we de lijn die P verbindt met $S := (1, 0)$; merk op: als $(x, y) \neq S$ voldoet aan (E) dan is $x \neq 1$. Die lijn wordt gegeven door de vergelijking

$$(L) = (L_\alpha) \qquad y = \alpha \cdot (x - 1).$$

Merk op dat

$$x^3 - 4x^2 + 5x - 2 = (x - 1)^2(x - 2).$$

Substitutie van (L) in (E) geeft:

$$(\alpha \cdot (x - 1))^2 = (x - 1)^2(x - 2).$$

Uit $\alpha^2 = x - 2$ volgt $x = \alpha^2 + 2$. Met (L) geeft dit $y = \alpha(\alpha^2 + 1)$. We zien dat elk van de gevraagde punten ongelijk aan S een eenduidig bepaalde α geeft, en dat elke $\alpha \in \mathbb{Q}$ de lijn $(L) = (L_\alpha)$ geeft, die behalve het S ook het punt $(x = \alpha^2 + 2,\ y = \alpha(\alpha^2 + 1))$ geeft.

(18.56) Oplossing gehele getallen (18.26). Merk op dat $261352 \equiv 7 \pmod{13}$.
We bewijzen dat er niet een oplossing bestaat in $(\mathbb{F}_{13})^2$.

De derde-machten in $\mathbb{F}_{13}$ zijn de restklassen van $0, \pm 1, \pm 8$ in $\mathbb{F}_{13}$.

De vierde-machten in $\mathbb{F}_{13}$ zijn de restklassen van $0, 1, 3, 9$ in $\mathbb{F}_{13}$.

We zien dat de restklasse van 7 niet van de vorm $\overline{x}^3 + \overline{y}^4$ geschreven kan worden met $\overline{x}, \overline{y} \in \mathbb{F}_{13}$.
Dus is er geen oplossing in $(\mathbb{F}_{13})^2$. Dus is er geen oplossing in $\mathbb{Z}^2$.

(18.57) Oplossing van (18.27): **een pad.** Als ik de vraag gesteld had over een cirkel in een vlak $\mathbb{R}^2$ in de 3-dimensionale ruimte $\mathbb{R}^3$, en een pad van een punt A binnen die cirkel naar een punt B buiten de cirkel, dan ziet iedereen wat je moet doen. Van 0 tot 1/3 naar boven, dan van 1/3 tot 2/3 horizontaal lopen tot je boven B bent, dan van 2/3 tot 1 naar beneden lopen tot je in B bent.

Imiteer dit tot een oplossing van ons vraagstuk volgt: van 0 tot 1/3 lopen van $P' = (0, 0, 0, 0)$ naar $(0, 0, 0, 1)$, van 1/3 tot 2/3 van $(0, 0, 0, 1)$ naar $(2, 0, 0, 1)$ (ga na dat bij de vierde coödinaat constant $= 1$ dit pad S' niet snijdt), van 2/3 tot 1 van $(2, 0, 0, 1)$ naar $(2, 0, 0, 0)$.

(18.58) Oplossing: deelbaar door 7: (18.28). Voor voor elk priemgetal p en elke $a \in \mathbb{Z}$ niet deelbaar door p geldt $a^{p-1} \equiv \pmod{p}$. Ga na:

$$2222 = 317 \times 7 + 3, \quad 5555 = 925 \times 6 + 5, \quad 5555 = 793 \times 7 + 4, \quad 2222 = 370 \times 6 + 2.$$

Daarom:

$$2222 \equiv 3 \pmod{7}, \quad 5555 \equiv 5 \pmod{6}, \quad \text{dus} \quad 2222^{5555} \equiv 3^5 \pmod{7};$$

omdat $3^5 \equiv 5 \pmod{7}$ geeft dit $2222^{5555} \equiv 5 \pmod{7}$;

$$5555 \equiv 4 \pmod{7}, \quad 2222 \equiv 2 \pmod{6}, \quad \text{dus} \quad 5555^{2222} \equiv 4^2 \pmod{7};$$

omdat $4^2 \equiv 2 \pmod{7}$ geeft dit $5555^{2222} \equiv 2 \pmod{7}$;.
Hieruit volgt het resultaat.

(18.59) Oplossing van (13.13). Merk op dat voor elke $t \in \mathbb{Z}_{>0}$ geldt dat $10^t \equiv 1 \pmod 9$. Dus geldt dat $n \equiv s(n) \pmod 9$. Herhaal dit proces: $n \equiv s^j(n) \pmod 9$ voor alle n en alle j. Hieruit volgt het criterium.

(18.60) Oplossing van (13.14). Omdat $10 \equiv -1 \pmod{11}$ geldt $n \equiv a(n) \pmod{11}$. Herhaald toepassen hiervan geeft het resultaat.

(18.61) Oplossing van (18.29). Het antwoord is: nee, uit deze 27 blokken van afmeting $1 \times 2 \times 4$ kunnen we niet een $6 \times 6 \times 6$ kubus maken.
Bewijs (uit [27]). We nemen een $6 \times 6 \times 6$ kubus K in gedachten en geven elke van de 6^3 deel-blokken van afmeting $1 \times 1 \times 1$ de kleur Z of W. Dat doen we als volgt. Verdeel de kubus K in $3 \times 3 \times 3$ kleinere kubussen k_i, elk van afmeting $2 \times 2 \times 2$. Alle $1 \times 1 \times 1$ blokje in een dergelijke deel-kubus k_i krijgen dezelfde kleur; bovendien kiezen we die kleuren zo dat aangrenzende k_i-kubussen verschillend van kleur zijn. Bv.:

Z		Z			Z			Z		Z
	Z		&	Z		Z	&		Z	
Z		Z			Z			Z		Z

Hier staat links de bovenste laag van 9 k_i's, midden de middelste laag, en rechts de onderste laag. We zien dat 14 k_i's de ene en 13 de andere kleur hebben. De kleuren zijn ongelijk verdeeld over de 27×8 blokjes van afmeting $1 \times 1 \times 1$.

Nu denken we ons in dat de 27 blokken gestapeld zouden kunnen worden tot een kubus K. We zien (ga na) dat van elk $1 \times 2 \times 4$ blok k_i dan precies 4 van de $1 \times 1 \times 1$ deel-blokken de ene en 4 de ander kleur krijgen. De kleuren zouden gelijk verdeeld zijn over de 27×8 blokjes van afmeting $1 \times 1 \times 1$; tegenspraak.

(18.62) Opgave (M. Kontsevic & D. Zagier). Voor $\alpha, \beta \in \mathbb{R}$ construeren we een rij getallen $\{x_i \mid i \in \mathbb{Z}_{>0}\}$ door:

$$x_1 = \alpha, \quad x_2 = \beta, \quad x_3 = \mid x_2 \mid - x_1, \quad \cdots, \quad x_{i+2} = \mid x_{i+1} \mid - x_i, \cdots.$$

(Een symmetrische manier om deze voorwaarde te geven: $\forall i, \quad x_{i-1} + x_{i+1} = \mid x_i \mid$, en we kunnen net zo goed de rij $\{x_i \mid i \in \mathbb{Z}\}$ beschouwen.)
Bewijs dat er bestaat een $N \in \mathbb{Z}_{>0}$ (onafhankelijk van α en β), zodanig dat

$$\forall \alpha, \quad \beta, \quad i > 0 \quad \text{geldt:} \quad x_i = x_{i+N}.$$

Met andere woorden: *die rij is periodiek*, en de periode hangt niet af van de keuze van α en β.
(Er is geen oplossing te vinden in deze syllabus, maar in de cursus zal ik een oplossing bespreken. Graag hoor ik hoe iemand er aan begint, en wat voor bewijs er uit komt.) Opmerking: voor $\alpha = 0 = \beta$ komt er $x_i = 0$ voor alle i; voor elke keus $(\alpha, \beta) \neq (0, 0)$ blijkt de minimale periode niet af te hangen van de keuze van (α, β).
In het artikel [63] staan oplossingen van dit vraagstuk.

19 Open problemen

Waarschuwing. De onderstaande problemen zijn zo eenvoudig te formuleren, maar veel wiskundigen hebben er reeds hun tanden in gezet. Besteed er niet de rest van uw leven aan om een van deze problemen op te lossen (maar het haalt wel de voorpagina van de grote kranten in de hele wereld als u er één van oplost ....).

Wiskundigen hebben het gevoel dat we nog steeds niet de goede techniek, de goede context gevonden hebben om onderstaande problemen aan te pakken. Vaak blijkt dat een andere visie op een probleem, vooral een verband met een ander probleem of een ander techniek de doorbraak geeft die nodig is. Soms zien we ook dat een beter begrijpen van bestaande methoden een oplossing kan brengen, zoals in (8.12), het vermoeden van Catalan, en in (19.3), het ternaire Goldbach probleem.

Een voorbeeld: de laatste stelling van Fermat, die ik hier niet bespreek, behalve even in 11, (11.6) en (13.9), was een geïsoleerd open probleem (vanaf ongeveer 1637); in 1985 gaf een suggestie van Gerhard Frey een mogelijk verband met een reeds ver uitgebouwde theorie (die van de modulaire vormen) en met een (moeilijk) openstaand probleem (het vermoeden van Shimura-Taniyama-Weil). Andrew Wiles kende het Fermat probleem, en kende die theorie van modulaire vormen (waarvan men dacht dat het los van elkaar staande problemen waren). Toen dat verband eenmaal gelegd was begon hij aan een bewijs, met als grote triomf (van hem, maar ook van de moderne wiskunde) dat beide vermoedens opgelost werden.

Voor alle vragen die hier volgen is geprobeerd goede theorie te vinden, zijn er "heuristische" methoden ontwikkeld om tot een idee te komen wat het antwoord zou moeten zijn, en is er (ontzettend) veel rekenwerk verricht, meestal met een slimme combinatie van abstracte argumenten, algoritmen en vele uren computer-rekentijd.

(19.1) Oneven perfecte getallen. Nogmaals: een getal $n \in \mathbb{Z}_{>0}$ heet perfect als $2n$ de som is van alle positieve delers van n. Voorbeeld: $2.6 = 1+2+3+6$; ga na dat 28 een perfect getal is. Zie verder § 6.

Betaat er een oneven *perfect getal*?

Er is veel literatuur over, er zijn veel deelresultaten. De bovengrens waaronder geen oneven perfecte getallen bestaan verschuift voortdurend, en is momenteel heel groot (bij voorbeeld: we weten dat als er een oneven perfect getal bestaat, dit getal meer dan 300 cijfers heeft). Ga dit niet met de hand uitproberen (tenzij je niets beters te doen hebt).
Zie `http://mathworld.wolfram.com/OddPerfectNumber.html`

Verwachting. *Er bestaan geen oneven perfecte getallen.*

(Maar waarom dit waar zou zijn? er is veel aan gerekend, er zijn deelresultaten, maar ik zie nog geen structuur achter de vraag.) (Zouden we iets opgeschoten als we deze vraag kunnen beantwoorden? Dat hangt er van af, alleen een antwoord is misschein niet zo zinvol, maar de methode, de techniek, de theorie om zo ver te komen zou heel interessant kunnen zijn.)

(19.2) Het vermoeden van Goldbach. In 1742 schreef Christian Goldbach een brief aan Euler waarin hij een vermoeden uitsprak. (ik denk dat dit de eerste keer is dat echt het woord "conjecture" gebruikt werd in deze zin.) De formulering die we nu kiezen is:

Is elke even getal $N = 2n \geq 4$ te schrijven als som van twee priemgetallen?

Zie `http://en.wikipedia.org/wiki/Goldbach's-conjecture`
Zie `http://en.wikipedia.org/wiki/Prime-number#Open-questions`
Tot en met februari 2011 is het vermoeden van Goldbach bevestigd voor alle $n < 2 \times 10^{17}$.

Verwachting. *Het vermoeden van Goldbach is juist:*
elk even getal $N = 2n \geq 4$ is te schrijven als som van twee priemgetallen.

"The binary Goldbach Conjecture has been numerically verified to $4{\cdot}10^{18}$" (mei 2013), zie
`http://arxiv.org/pdf/1305.3062v1.pdf`

Zie `http://www.math.dartmouth.edu/~euler/correspondence/letters/OO0765.pdf` voor de brief (1742) van Goldbach aan Euler die aanleiding gaf tot het Goldbach probleem. Zie ook
`http://en.wikipedia.org/wiki/Goldbach%27s_conjecture`

(19.3) Het binaire en het ternaire Goldbach probleem. Hier is het probleem, het "ternaire Goldbach probleem":

elke oneven $N \in \mathbb{Z}_{>5}$ is de som van drie priemgetallen.

De verwachting geformuleerd in (19.2) wordt wel het binaire Goldbach probleem genoemd; ook worden wel de terminologie "het 2-priemen en het 3-priemen Goldbach probleem" gebruikt. Ga na:

het binaire Goldbach probleem impliceert dat
elke $N \in \mathbb{Z}_{>5}$ de som is van drie priemgetallen.

(Beschouw $N-2$ of $N-3$.) Er is nu (13-V-2013) een claim dat het ternaire Goldbach probleem opgelost is (H. A. Helfgott):
`http://arxiv.org/pdf/1305.2897v2.pdf`
`http://arxiv.org/abs/1205.5252`
Dat bewijs bestaat uit een enorme rekenpartij, en een lange serie van afschattingen om het algemene probleem terug te brengen tot onder de grens waar het vermoeden numeriek bewezen is.
Zie ook: een vermoeden van Waring
`http://en.wikipedia.org/wiki/Waring%27s_prime_number_conjecture`

Landau dacht (in 1912) dat het ternaire Goldbach probleem "*unangreifbar*" was. Echter, resultaten van Vinogradov, en vele anderen, lieten zien dat boven een grens het probleem opgelost is (maar vroeger waren die grenzen veel te hoog om alles eronder door te rekenen). In het artikel `http://arxiv.org/pdf/1305.2897v2.pdf` wordt die grens aanzienlijk naar beneden gebracht, en in `http://arxiv.org/abs/1205.5252` wordt het ternaire Goldbach probleem tot die grens opgelost. Een fascinerende geschiedenis, met veel deelresultaten: we zien hoe we worstelen met een dergelijk probleem.

(19.4) Priemtweelingen. We spreken van een priemtweeling (p, q) als $q - p = 2$, waar p en q priemgetallen zijn. Er zijn erg veel voorbeelden. Kenmerkend voor het "statistische gedrag" in de verdeling van priemgetallen: soms liggen ze zo dicht bij elkaar als maar mogelijk, soms zijn er dan weer grote gaten in de rij van priemgetallen.

http://en.wikipedia.org/wiki/First-Hardy-Littlewood-conjecture
Vermoeden. *Er zijn oneindig veel Priemtweelingen.*

De verwachting is dat het aantal priemtweelingen $\pi_2(x)$ beneden een grens x gegeven wordt door

$$\pi_2(x) \approx 2 \times 0.66 \times \frac{x}{(\log x)^2}.$$

Zie http://en.wikipedia.org/wiki/Twin-prime
Numerieke resultaten (grote berekeningen) kloppen merkwaardig goed met dit vermoeden.

Een voorbeeld:

$$\pi_2(10^{18}) = 808,675,888,577,436,$$

en

$$2 \times 0.66 \times \frac{10^{18}}{(\log 10^{18})^2} \approx 768,418,024,862,131.$$

De voorspelling geeft ongeveer 95% van het werkelijke aantal. Weer een wonderlijk voorbeeld van het verschijnsel dat we wel degelijk iets kunnen zeggen over priemgetallen, zonder de individuele priemen te kennen.

Grote berekeningen hebben heel grote priemtweelingen geproduceerd:
"On December 25, 2011 PrimeGrid announced that yet another record twin prime had been found. It is $37568016956852^{666669} \pm 1$. The numbers have 200700 decimal digits."

Recente, spectaculaire ontwikkeling: Yitang Zhang bewijst dat in de verzameling van gaten in de rij van priemgetallen er een verdichtingspunt is onder 7×10^7; zie [95]. Met andere woorden: er is een k onder die grens zodanig dat k oneindig veel voorkomt als verschil $p_{i+1} - p_i$. Het vermoeden dat zegt dat er oneindig veel priemtweelingen zouden zijn zegt dat 2 een verdichtinspunt zou zijn (we lijken er dus nog ver vandaan).

Een project: http://michaelnielsen.org/polymath1/index.php?title=Bounded_gaps_between_primes
onderzoekt of de grens die Yitang Zhang geeft omlaag gebracht kan worden. Op 17-VIII-2013 is er een claim dat die bovengrens (voor het bestaan van oneindig veel gaten van die lengte) omlaag gebracht is naar 14950 (??).

(19.5) Gaten in de rij van priemgetallen.
(19.5)(1) Verwachting (het vermoeden van Polignac). *Voor elk even positief getal $m = 2n \in \mathbb{Z}_{>0}$ zijn er oneindig veel paren opeenvolgende priemgetallen (p_i, p_{i+1}) met $p_{i+1} - p_i = m$.* Zie (19.7).
http://en.wikipedia.org/wiki/Twin-prime
http://en.wikipedia.org/wiki/Polignac%27s_conjecture

Echter, er schijnt een tegenspraak te zijn met "het eerste Hardy-Littlewood vermoeden". Welke van de twee is onjuist? (Of misschien wel allebei?)
http://en.wikipedia.org/wiki/First_Hardy%E2%80%93Littlewood_conjecture#First_Hardy.E2.80.93Littlewood_conjecture

(19.5)(2) Vermoeden. Voor elk even positief getal $m = 2n \in \mathbb{Z}_{>0}$ zijn oneindig veel paren priemgetallen (p, q) met $q - p = m$.

Duidelijk: "ja" tegen (19.5)(1) geeft "ja" tegen (19.5)(2);
"nee" tegen (19.5)(2) geeft "nee" tegen (19.5)(1).

(19.6) Het tweede Hardy-Littelwood vermoeden. We denken dat er in het begin van de getallen-rij de dichtheid van de priemgetallen groter is dan verderop (en dat is in een ruwe vorm waar). Dit gevoel werd precies gemaakt:

$$x, y \in \mathbb{Z}_{\geq 2} \stackrel{?}{\Longrightarrow} \pi(x+y) \leq \pi(x) + \pi(y).$$

`http://en.wikipedia.org/wiki/Second_Hardy%E2%80%93Littlewood_conjecture`
`http://mathworld.wolfram.com/Hardy-LittlewoodConjectures.html`

(19.7) Het vermoeden van Polignac. In 1849 schreef het volgende in [66]:

1^{er} *Théorème.* Tout nombre pair est égal á la difference de deux nombres premiers consécutifs d'une infinité de manières (7^e *Théorème du* § II).
2^{e} *Théorème.* Tout nombre impair est égal à une puisance de 2, plus un nombre premier. (Vérifié jusqu'a 3 millions.)

Commentaar/waarschuwing. Het is duidelijk dat het woord "Théorème" zoals gebruikt door Polignac opgevat moet worden als "bewering" (of misschien wel als "vermoeden") en niet in de vorm van een bewezen stelling.

Het is goed mogelijk dat het "1^{er} Théorème" eens bewezen zou kunnen worden. Echter:

(19.8) Opgave. Is het 2^{e} Théorème van Polignac juist? Vind een tegenvoorbeeld. Zie (19.21)

Over gaten tussen tweelingen, triplets etc., zie: [42], [43].

(19.9) Zij er slechts eindig veel Fermat priemgetallen? We schrijven $F_i = 2^{2^i}$ voor $i \in \mathbb{Z}_{\geq 0}$.

Verwachting. *Het aantal Fermat priemgetallen is eindig.*

Zie [44] voor meer informatie.

(19.10) Zijn er oneindig veel Mersenne priemgetallen? We schrijven $M_n = 2^n - 1$ voor $n \in \mathbb{Z}_{>0}$.

Verwachting. *Het aantal Mersenne priemgetallen is oneindig.*

(19.11) Zij er oneindig veel Sophie Germain priemgetallen? We zeggen dat p een Sophie Germain priemgetal is als $q := 2p + 1$ ook een priemgetal is.
Voorbeelden:

$$2,\ 3,\ 5,\ 11,\ 23,\ 29,\ 41,\ 53,\ 83,\ 89,\ 113,\ 131,\ 173,\ 179,\ 191,\ 233,\ \cdots$$

$$\cdots,\ \ 137211941292195 \times 2^{171960} - 1, \cdots,\ \ 18543637900515 \times 2^{666667} - 1,\ \cdots.$$

Zijn er oneindig veel Sophie Germain priemgetallen?

Er zijn er 190 met $p < 10^4$ en 56032 met $p < 10^7$.
Zie `http://en.wikipedia.org/wiki/Sophie-Germain-prime`

Verwachting. *Het aantal Sophie Germain priemgetallen is oneindig.*

(19.12) Is de lengte van een Sophie Germain ketting onbegrensd? Laten we spreken van een (maximale) Sophie Germain ketting $\{Q_1, \cdots, Q_t\}$ als dit allemaal priemgetallen zijn met bovendien de eigenschap dat

$$Q_{i+1} = 2 \cdot Q_i + 1, \quad 1 \leq i < t,$$

met bovendien: $(Q_1 - 1)/2$ en $2Q_t + 1$ zijn niet een priemgetal. Een dergelijke rij heet ook wel een "**Cunningham chain**".
`http://primes.utm.edu/glossary/xpage/CunninghamChain.html`

Voorbeelden:
$S = \{2,\ 5,\ 11,\ 23,\ 47\}$ is een SGk en lengte$(S) = 5$;
$S = \{89,\ 179,\ 359,\ 719,\ 1439,\ 2879\}$ is een SGk en lengte$(S) = 6$;
$S = \{509,\ 1019,\ 2039,\ 4079\}$ is een SGk en lengte$(S) = 4$.
Het niet zo gemakkelijk om een SGk te vinden van lengte 7
(antwoord: begin met 1122659, zie [52], Table 3).

Laat zien:
Als $S = \{Q_1, ...\}$ *met* $Q_1 > 2$, *en* $Q_1 \not\equiv 9 \pmod{10}$ *dan volgt* lengte$(S) < 5$.

Propositie. *We kiezen een priemgetal* $R = R_1 \in \mathbb{Z}_{>2}$ *en we beschouwen* $R = R_1 < R_2 < \cdots$ *inductief geconstrueerd door* $R_{i+1} = 2R_i + 1$. *Dan geldt:*

$$R \quad \textit{deelt} \quad R_{R_1}.$$

Inderdaad, $R_i = 2^{i-1}R + 2^{i-1} - 1$, en de kleine stelling van Fermat zegt dat $2^{R_1 - 1} \equiv 1 \pmod{R}$.

Gevolg. *Voor een* SGk $S = \{Q_1, \cdots, Q_t\}$ *met* $2 < Q_1$ *geldt lengte*$(S) < Q_1$.

Gevolg. *Er is niet een oneindige* SGk.

Verwachtingen. *Er zijn oneindig veel* Sophie Germain *priemgetallen.*
Voor elke $k \in \mathbb{Z}_{>1}$ *zijn er oneindig veel* SG ketens *van lengte* k (en er zijn precieze afschattingen over het aantal van zulke ketens beneden elke gegeven grens).
Zie [52];
`http://primes.utm.edu/glossary/xpage/CunninghamChain.html`
`http://primes.utm.edu/top20/page.php?sort=SophieGermain`
`http://oeis.org/A005602`

Commentaar: Lucas getallen. De definitie van Lucas$(n) = L(n)$:

$$L(0) = 2, \quad L(1) = 1, \quad L_{i+2} = L_i + L_{i+1},\ i \geq 0.$$

Dit geeft de rij

$$2,\ 1,\ 3,\ 4,\ 7,\ 11,\ 18,\ 29,\ 47,\ 76,\ 123, \cdots;$$

zie `http://en.wikipedia.org/wiki/Lucas_number`
zie A000032 op
`http://en.wikipedia.org/wiki/On-Line_Encyclopedia_of_Integer_Sequences`

Laat zien: voor een priemgetal $p > 5$ geldt:

$$p \equiv -1 \pmod{30} \;\&\; 2p+1 \text{ is ook priem} \iff 2p+1 \text{ deelt Lucas}(p).$$

Helpt dit om te beslissen welke SG ketens er zijn met lengte groter dan 5?

(19.13) Een vermoeden van Legendre. Als we voldoende zouden wetgen over het gedrag van gaten in de rij van priemgeetallen, dan zouden we mogelijk kunnen beslissen over de volgende vraag:

Vermoeden (Legendre, 1798). *Voor elke $n \in \mathbb{Z}_{>0}$ is er een priemgetal p zodanig dat:*

$$n^2 < p < (n+1)^2. \qquad (?)$$

Zie [50]. Zie `http://arxiv.org/pdf/1201.1787v3.pdf`
`http://primes.utm.edu/notes/conjectures/`

(19.14) Fibonacci priemgetallen. Kijk naar de Fibonacci rij:

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144, \cdots$$

gegeven door

$$A_0 = 0, \quad A_1 = 1, \quad A_n = A_{n-1} + A_{n-2}.$$

Een priemgetal dat in deze rij voorkomt heet een *Fibonacci priemgetal*; voorbeelden:

$$2,\ 3,\ 5,\ 13,\ 89,\ 233,\ 1597,\ \cdots.$$

Vraag. *Zijn er oneindig veel Fibonacci priemgetallen*?
(Nog onopgelost.)
`http://en.wikipedia.org/wiki/Fibonacci_number`
`http://en.wikipedia.org/wiki/Fibonacci_prime`

(19.15) Opgave. Bewijs dat voor Fibonacci getallen geldt:

$$\text{ggd}(A_n, A_m) = A_{\text{ggd}(n,m)}.$$

Concludeer dat er oneindig veel priemgetallen zijn.

(19.16) Een kwadraat plus een. Beschouw alle priemgetallen van de vorm $p = n^2 + 1$ voor alle $n \in \mathbb{Z}_{>0}$. Is het aantal van priemgetallen van deze vorm eindig of oneindig? Wat zegt de heuritstiek ons? Zie [9], 3.8. Zie (9.6).

(19.17) Collatz: $3x+1$.
We definiëren de functie $C : \mathbb{Z}_{>0} \longrightarrow \mathbb{Z}_{>0}$ door:

$$C(2m) := m, \qquad C(2m+1) = 3(2m+1) + 1$$

(als n *even* is dan geldt $C(n) = n/2$, als n *oneven* is, dan geldt $C(n) = 3n+1$). Begin met een willekeurig getal in $a_1 \in \mathbb{Z}_{>0}$ en maak een rij getallen

$$\{a_1, a_2, \cdots \mid a_{i+1} = C(a_i)\};$$

een dergelijke rij noemen we een *Collatz rij*. Bij voorbeeld:

$$17,\ 52,\ 26,\ 13,\ 40,\ 20,\ 10,\ 5,\ 16,\ 8,\ 4,\ 2,\ 1 \cdots$$

We zien in dit voorbeeld dat de rij eindigt in de cykel $4 \mapsto 2 \mapsto 1 \mapsto 4 \mapsto 2 \mapsto 1 \mapsto 4$ etc..

Het Collatz probleem, of: het $3x+1$ vermoeden:

Elke Collatz rij eindigt met $\{4, 2, 1 \text{ etc}\}$.

Tot op heden is dit niet opgelost, en we begrijpen niet welk mechanisme, welke theorie een mogelijk antwoord zou kunnen geven.

Suggestie: construeer zelf een paar keer een Collatz rij, en constateer de verwondering dat in de gevallen die je construeert die Collatz rij inderdaad zo eindigt. (Of, maak een rij die niet zo eindigt .. ? Als je een tegenvoorbeeld wilt maken, is het misschien verstandig om met een getal te beginnen met meer dan 500 cijfers !?).

Een bespreking van dit probleem, en veel verwijzingen zijn te vinden in:
J. C. Lagarias
The ultimate challenge: the $3x+1$ *problem.* AMS, 2010.
Zie `http://www.math.lsa.umich.edu/~lagarias/`
Zie: `http://arxiv.org/pdf/math/0608208v6.pdf`
`http://www.math.grin.edu/~chamberl/papers/3x-survey-eng.pdf`
`http://en.wikipedia.org/wiki/Collatz-conjecture`

Ga naar `http://www.nitrxgen.net/collatz.php`,
typ een getal in (van hooguit 500 cijfers), en de Collatz rij die zo begint verschijnt.

Hier is een ander voorbeeld. Begin met 27, en na 111 stappen komt het einde $4, 2, 1$;
de Collatz $3x+1$-rij met dit beginpunt is:

$$27, 82, 41, 124, 62, 31, 94, 47, 142, 71, 214, 107, 322, 161, 484, 242, 121, 364,$$
$$182, 91, 274, 137, 412, 206, 103, 310, 155, 466, 233, 700, 350, 175, 526, 263,$$
$$790, 395, 1186, 593, 1780, 890, 445, 1336, 668, 334, 167, 502, 251, 754, 377,$$
$$1132, 566, 283, 850, 425, 1276, 638, 319, 958, 479, 1438, 719, 2158, 1079, 3238,$$
$$1619, 4858, 2429, 7288, 3644, 1822, 911, 2734, 1367, 4102, 2051, 6154,$$
$$3077, 9232, 4616, 2308, 1154, 577, 1732, 866, 433, 1300, 650, 325, 976,$$
$$488, 244, 122, 61, 184, 92, 46, 23, 70, 35, 106, 53, 160, 80, 40, 20, 10, 5, 16, 8, 4, 2, 1$$

Verwachting. *Voor elk begin* $n \in \mathbb{Z}_{>0}$ *eindigt de Collatz rij met* $\{...., 4, 2, 1, \text{etc.}\}$.
Vraag. Is er een formule die voor elk begin-getal a_1 de lengte van de Collatz rij uitrekent tot de eerste keer dat 1 voorkomt?

(19.18) Niet behandeld: het Riemann vermoeden, dat zou me te ver voeren.

Voor nog veel meer vermoedens over priemgetallen, zie: [33]; zie ook:
`http://en.wikipedia.org/wiki/Category:Conjectures-about-prime-numbers`
`http://en.wikipedia.org/wiki/Category:Conjectures_about_prime_numbers`

(19.19) Op het ICM (International Congress of Mathematicians) in 1912 formuleerde Landau vier problemen:

(1) het vermoeden van Goldbach, zie (19.2);
(2) $n^2 < p < (n+1)^2$, zie (19.13);
(3) het vermoeden over de priem-tweelingen, zie (19.4);
(4) er zijn oneindig veel priemgetallen van de vorm $p = n^2 + 1$, zie (19.16).

Toen waren dit (oude) open problemen. Nu nog steeds lijke we ver verwijderd van een bevredigend antwoord voor elk van deze vragen.
Zie [16]; zie pagina 2 of `http://arxiv.org/pdf/1205.0774v1.pdf`
Zie `http://en.wikipedia.org/wiki/Landau%27s_problems`

(19.20) Het woord "vermoeden" (in het Engels "conjecture") wordt in de wiskunde veelvuldig gebruikt. Ik ben daar spaarzaam in. Ik hanteer een onderscheid in vier categoriën:

- een *probleem*: je kunt je best afvragen of iets het bestuderen waard is; als je dat gedaan hebt kan er een suggestie uit komen; die kunnen we formuleren als:
- een *vraag*: een preciese formulering van het probleem, op een manier die wel eens tot de waarheid zou kunnen leiden. Na veel proberen kan er dan een patroon duidelijk worden:
- een *verwachting* ("expectation"): dit lijkt toch wel het goede antwoord te zijn, ik zie niet waarom, maar zo zit het vast en zeker in elkaar. Dit gebruik ik als nog niet aan het volgende voldaan is:
- een *vermoeden* ("conjecture"). Ik gebruik dit woord pas als er tenminste één van de volgende patronen zich voordoet:

  er is een theorie, weliswaar nog niet bewezen, die prachtig in elkaar zit, en die de vraag zou beantwoorden (structurele evidentie) (elegantie);

  er is een analogie: twee wiskundige structuren lijken heel erg op elkaar, in de ene kun je een uitspraak bewijzen, in de andere denk je dan dat de analoge uitspraak ook waar is. Bij een dergelijke analogie is er heel vaak sprake dat dingen op elkaar lijken, zonder dat er sprake is van een logische implicatie. Zie (14.33).

  er is numerieke evidentie: heel veel gevallen zijn doorgerekend; pas op, dit criterium is uiterst subjectief. We zullen zien in § 16 dat "heel veel rekenen" soms onvoldoende is, de verkeerde indruk kan geven.

(19.21) **Een oplossing van** (19.8). Zoals Euler reeds lang geleden bewees: 127 en 959 kunnen niet geschreven worden als de som van een macht van 2 en een priemgetal.

Wat te lezen?
De onderstaande literatuur lijst bevat veel meer dan wat we nodig hebben. Maar ik dacht dat het goed is dat u voldoende verwijzingen heeft om nog heel lang veel pleizier te hebben. Een deel van dit materiaal hier beneden is niet elementair. Hier volgen wat aanwijzingen.

Elementaire getal theorie en algebra.
Om een indruk te krijgen van het gebied van de elementaire getaltheorie, van elementaire methodes en van resultaten kunt u de volgende boeken raadplegen [37], [5], [8]. Zie ook [64]. Voor basis-kennis over algebra zie [83]. Algebra (meer geavanceerd): [87] (een klassieker), [48] (geavanceerd, nogal volledig). Zie ook [13].

Leesadvies, romans.
Er zijn veel boeken waar wiskundigen als hoofdpersoon opgevoerd worden. Ik bedoel niet biografieën, maar fictie. Daar zijn juweeltjes onder. Zie:

[14], een prachtige beschrijving van iemand die het Goldbach vermoeden probeert op te lossen;

[58] geeft een (fictief) dagboek van Sophie Germain: een prachtige beschrijving hoe haar jeugd er uit kan hebben gezien. Een fascinerende beschrijving van de jonge jaren van Sophie Germain; ik vond dit erg mooi;

[36] geeft een fascinerende beschrijving van gedachtengangen van een autistische persoonlijkheid; de hoofdstukken zijn genummerd $2, 3, 5, \cdots$ (en het duurt even voor je dat door hebt); een prachtig boek;

[41], een bestseller; een fictieve beschrijving van een ontmoeting, die echt heeft plaats gevonden, tussen de wiskundige Carl Friedrich (Friederich) Gauss (1777 – 1855) en Alexander von Humboldt (1769 –1859); ik vond dit een vreselijk boek; zie de boekrecensie
`http://www.ams.org/notices/200806/tx080600681p.pdf`;

[32], een vermakelijk boek; voor een boekrecensie zie:
`http://www.nieuwarchief.nl/serie5/deel01/mrt2000/pdf/papegaai.pdf`

[49], een magistrale beschrijving van het universitaire leven in Cambridge, UK, in de eerste helft van de 20-ste eeuw, en van S. Ramanujan die daar komt werken met G. H. Hardy; voor een boekrecensie zie:
`http://www.nytimes.com/2007/09/16/books/review/Freudenberger-t.html`

Op de volgende site vinden we een zeer uitgebreid overzicht van fictie waar wiskundigen in voor komen:
`http://kasmana.people.cofc.edu/MATHFICT/default.html`
Een zeer uitgebreid (misschien wel volledig) overzicht van "Mathematical Fiction". Zeer aanbevolen!

Een vraag die me bezig houdt: is het toegestaan om in fictie een persoon op te voeren die bestaan heeft, herkenbaar is in de beschrijving, terwijl historische gegevens of karakter eigenschappen duidelijk anders worden weergegeven dan aantoonbaar juist? Sommige mensen vinden dat in fictie alles toegestaan is wat dat betreft. Graag hoor ik uw mening!

Referenties

[1] E. Bach & J. Shallit *Algorithmic number theory. Vol. 1. Efficient algorithms. Foundations of Computing Series.* MIT Press, Cambridge, MA, 1996.

[2] A. Beiler – *Recreations in the theory of numbers: The queen of mathematics untertains.* Dover Publ., pocket, 1964.

[3] E. Bell – *Men of mathematics.* Simon & Schuster. 1937.

[4] F. Beukers – *Getaltheorie voor beginners.* Epsilon Uitgaven, Utrecht 1999.

[5] F. Beukers – *Elementary number theory.* Collegedictaat WISB321, Utrecht 2012.

[6] F. Beukers, F. Luca & F. Oort – *Power values of divisor sums.* Amer. Math. Monthly **119** (2012), pp. 373–380.

[7] A. Booker – *On Mullin's second sequence of primes.*
`http://arxiv.org/pdf/1107.3318v2.pdf`

[8] D. Burton – *Elementary number theory.* Allyn & Bacon, 1980.

[9] C. Caldwell – *An amazing prime heuristic.*
`http://www.utm.edu/staff/caldwell/preprints/Heuristics.pdf`

[10] P. Chebyshev – *Mémoire sur les nombres premiers.* J. de Math. Pures Appl. **17** (1852), 366-390. Also in Mémoires présentés à l'Académie Impériale des sciences de St.-Pétersbourg par divers savants **7** (1854), 15–33. Also in Oeuvres 1 (1899), 49–70.

[11] H. Diamond – *Elementary methods in the study of the distribution of prime numbers.* Bulletin Amer. Math. Soc. **7** (1982), 553–589.

[12] L. Dickson – *History of the theory of numbers.* Volume II: Diophantine analysis. Chelsea publ. Cy. New York, 1952.

[13] R. Dijkgraaf – *Symmetrie,* collegedictaat, een inleiding in de wiskunde; 2001.
`http://www.science.uva.nl/onderwijs/wns/onderwijsCD/symmetrie/symmetrie.pdf`

[14] Apostolos Doxiades – *Oom Petros en het vermoeden van Goldbach.*
Oorspronkelijke Griekse titel: *O Theios Petros kai i Eikasia tou Goldbach* (1992). *Uncle Petros and Goldbach's Conjecture: A Novel of Mathematical Obsession.*
zie: `http://en.wikipedia.org/wiki/Apostolos-Doxiadis`
Lees vooral: `http://www.ams.org/notices/200010/rev-jackson.pdf`
`http://www.authortrek.com/uncle-petros.html`

Voor een andere bespreking van dit boek zie:

`http://www.math.leidenuniv.nl/~naw/serie5/deel02/mrt2001/pdf/goldbach.pdf`

[15] H. Edwards – *Fermat's last theorem. A genetic introduction to algebraic number theory.* Grad. Texts Math. 50, Springer, 1977.

[16] P. Erdös & J. Surányi – *Topics in the Theory of Numbers.* Springer, 2003.

[17] *Leonhard Euler und Christian Goldbach, Briefwechsel, 1729 – 1764.* Boek met correspondentie van Euler; editors A. Juškevič & E. Winter. Berlin 1965.

[18] T. Freiberg – *Products of shifted primes simultaneously taking perfect power values.* Preprint (2010),
http://arxiv.org/abs/1008.1978

[19] G. Frey – *Some aspects of the theory of elliptic curves over number fields.* Expos. Math. 4 (1986), 35-66

[20] G. Frey – *Links between stable elliptic curves and certain Diophantine equations.* Ann. Univ. Sarav. Ser. Math. 1 (1986), 1–40.

[21] G. Frey – *Links between solutions of $A - B = C$ and elliptic curves.* In: Number theory, Ulm 1987 (Ed. H. P. Schlickewei & E. Wirsing). Lect. N. Math. 1380, Springer,1989, pp. 31–62.

[22] A. Fröhlich & M. Taylor – *Algebraic number theory.* Cambridge Std. Advanc. Math. 27, Cambridge Univ. Press, 1991.

[23] Leonardo Pisano Fibonacci – *The book of squares.* An annotated translation into modern English by L. E Sigler. Academic Press, 1987.

[24] M. Gardner – *Mathematical games.* Scientific American, 1977, 101–121.

[25] M. Gardner – *Penrose tiles to trapdoor ciphers.* W. H. Freeman & Cy, New York 1987.

[26] M. Gardner – *The colossal book of mathematics.* W. W. Norton & Co 2001.

[27] M. Gardner – *The colossal book of short puzzles and problems.* W. W. Norton & Co 2005.

[28] C. F. Gauss – *Disquisitiones Arithmeticae.* Geschreven 1798, gepubliceerd in 1801.

[29] C. Gauss, Letter to Encke, 24 Dec. 1849, Werke, vol. 2, Kng. Ges. Wiss., Göttingen, 1863, pp. 444–447.

[30] A. Granville – *Harald Cramér and the distribution of prime numbers.* Scandinavian Actuarial Journal **1** (1995), 12–28.
http://www.dartmouth.edu/~chance/chance-news/for-chance-news/Riemann/cramer.pdf

[31] A. Granville & G. Martin – *Prime number races.* Amer. Math. Monthly **113** (2006), 1–33.

[32] D. Guedj – *Le théorème du perroquet.* Éditions Seuil, 1998.
Nederlandse vertaling: *De stelling van de papegaai, roman over de geschiedenis van de wiskunde.* Ambo, 1999,

[33] R. Guy – *Unsolved problems in number theory.* Springer, 3rd Edition 2004.

[34] J. Hadamard – *Étude sur les propriétés des fonctions entières et en particulier d'une fonction considérée par Riemann.* J. de Math. Pures Appl. **9** (1893), 171–215; reprinted in Oeuvres de Jacques Hadamard, C.N.R.S., Paris, 1968, vol. 1, pp. 103–147.

[35] J. Hadamard - *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques.* Bull. Soc. Math. France **24** (1896), 199-220; reprinted in Oeuvres, vol. 1, pp. 189-210.

[36] M. Haddon – *The curious incident of the dog in the night-time.* Jonathan Cape (UK) Doubleday (US), 2003.
http://en.wikipedia.org/wiki/The-Curious-Incident-of-the-Dog-in-the-Night-Time

[37] G. Hardy & E. Wright – *An introduction to the theory of numbers.* Oxford, Clarendon Press, first edition 1938, fourth edition, 1975, sixth edition 2008. Onlangs is er een nieuwe druk verschenen, met een appendix over elliptische krommen.

[38] T. Heath – *A history of Greek mathematics.* Oxford, Clarendon Press, 1921.

[39] J. Jones – *Formula for the Nth prime number.* Canad. Math. Bull. **18** (1975), 433–434.

[40] J. Jones, D. Sato, H. Wada & D. Wiens – *Diophantine representation of the set of prime numbers.* Amer. Math. Monthly, **83** (1976), 449–464.

[41] D. Kehlmann – *Die Vermessung der Welt.* Rowohlt 2005 (ook vertaald in het Engels, in het Nederlands en...).
Voor een review zie: http://www.ams.org/notices/200806/tx080600681p.pdf

[42] A. Kourbatov – *Tables of record gaps between prime constellations.*
http://xxx.lanl.gov/pdf/1309.4053.pdf

[43] A. Kourbatov – *Maximal gaps between prime k-tuples: a statistical approach.* J. Integer Seq. **16** (2013), Article 13.5.2.
http://xxx.lanl.gov/pdf/1301.2242v3.pdf

[44] M. Krízek, F. Luca & L. Somer -*17 Lectures on Fermat numbers from number theory to geometry.* CMS Books in Mathematics Springer, New York 2002.

[45] S. Lang – *Die abc-Vermutung.* El. Math. **48** (1993), 89–99.

[46] S. Lang – *Algebraic number theory.* Grad. Texts Math. 110, Springer, 1986.

[47] S. Lang - *Undergraduate algebra.* Undergr. Text Math., Springer 1987.

[48] S. Lang – *Algebra.* Addison – Wesley Publ. Cy, 1965. Third edition. Addison-Wesley Publ. Cy, 1993.

[49] D. Leavitt – *The Indian clerk.* Bloomsbury, 2007.

[50] A.-M. Legendre – *Essai sur la théorie des nombres.* Duprat, Paris, 1798.

[51] J.Littlewood – *Sur la distribution des nombres premiers.* Comptes Rendus, **158** (1914), pp. 1869–1872.

[52] G. Löh – *Long chains of nearly doubled primes.* Math. Comp., **53** (1989) 751 – 759.

[53] Yuri I. Manin – *Good proofs are proofs that make us wiser.* Interview by Martin Aigner and Vasco A. Schmidt. The Berlin Intelligencer, 1998, pp. 16–19.

[54] B. Mazur – *Number theory as a gadfly.* Amer. Math. Monthly **98** (1991), 593–610.

[55] P. Mihăilescu – *Primary cyclotomic units and a proof of Catalan's conjecture.* Journ. Reine angew. Math. 572 (2004), 167–195.

[56] A. Mingarelli – *Some conjectures in elementary number theory.* http://arxiv.org/abs/1302.5299

[57] F. Mertens - *Über eine zahlentheoretische Funktion.* Sitzungsberichte der Kaiserlichen Akademie der Wissenschaften, Mathematisch-Naturwissenschaftliche Klasse, Abteilung 2a, **106** (1897), pp. 761–830.

[58] D. Musielak – *Sophie's diary: a historical fiction.* AuthorHouse (April 16, 2004).

[59] A. Odlyzko & H. te Riele - *Disproof of the Mertens conjecture*, Journ. reine angew. Mathematik **357** (1985), 138–160.

[60] J. Oesterlé – *Nouvelles approaches du "théorème"de Fermat.* Sém. Bourbaki **40** (1987/88), Exp. 694. Astérisque 161–162 (1988), 165–186.

[61] F. Oort – *Priemgetallen.* In: Kaleidoscoop van de wiskunde 1. Editors: F. van der Blij, J. P. Hogendijk, F. Oort. Epsilon Uitgaven, 1990; pp.1–32.

[62] F. Oort – *Congruent numbers in the tenth and in the twentieth century.* In: Vrolijk, Arnoud & Jan P. Hogendijk (eds.), O ye Gentlemen: Arabic Studies on Science and Literary Culture, in Honour of Remke Kruk. Leiden [etc.]: Brill, 2007; pp. 77–97.

[63] F. Oort – *Dynamica en periodieke rijen.* Nw. Archief Wiskunde (5) **13** (2012), 110–111.

[64] F. Oort – *Priemgetallen.* Syllabus van een Kaleidoscoop-voordracht, 11 november 2013.
F. Oort – *Prime numbers.* (Syllabus Academia Sinica en National Taiwan University, 17 December 2012.) Notices of the ICCM **1** Number 2 (2013), 60–78.
Zie http://www.staff.science.uu.nl/~oort0109/

[65] A. de Polignac – *Six propositions arithmologiques déduites de crible d'Ératosthène.* Nouv. Ann. Math. **8** (1849), 423–429.

[66] A. de Polignac – *Recherches nouvelles sur les nombres premiers.* Comptes Rendus Paris **29** (1849), pp. 397–401 en 738–739.

[67] G. Pólya - *Heuristic reasoning in the theory of numbers.* Amer. Math. Monthly **66** (1959), 375–384. http://www.jstor.org/stable/pdfplus/2308748.pdf

[68] K. Ribet – *From the Taniyama-Shimura conjecture to Fermat's last theorem.* Ann. Fac. Sc. Univ. Toulouse **11** (1990), 116–139.

[69] K. Ribet – *Wiles proves Taniyama's conjecture; Fermat's last theorem follows.* Notices A.M.S. 40 (1993), 575-576.

[70] H. Riesel – *Prime numbers and computer methods for factorization.* Progress Math. 57, Birkhäuser, 1985.

[71] K. Rosen – *Elementary number theory and its applications.* Addison Wesley, 2000.

[72] J. Rosser & L. Schoenfeld – *Approximate formulas for some functions of prime numbers,* Illinois J. Math., **6** (1962), 64–94.

[73] M. Rubinstein & P. Sarnak - *Chebyshev's bias.* Experiment. Math. **3** (1994), 173–197.

[74] E. Selmer – *The diophantine equation* $ax^3+by^3+cz^3 = 0$. Acta Math. **85** (1951), 203–362. Zie b.v.
`https//www.math.lsu.edu/~verrill/teaching/math7280/selmer-example/selmer-example.pdf`

[75] E. Selmer – *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$. *Completion of the tables.* Acta Math. **92** (1954), 191–197.

[76] J-P. Serre - *Lecture on the Mordell-Weil theorem.* Asp. Math. E 15, Vieweg, 1989.

[77] D. Shanks – *Solved and unsolved problems in number theory.* Chelsea Publ. Cy., 1978.

[78] Simon Singh – *Fermats Last Theorem.* Fourth Estate, 1997.
Simon Singh – *Het laatste raadsel van Fermat.* Arbeiderspers, 1998.

[79] S. Singh – *The code book, the science of secrecy from ancient Egypt to quantum cryptography.* Fourth Estate, 1999.
S. Singh – *Code, de wedloop tussenmakers en brekers van geheime codes en cijferschrift.* De Arbeiderspers, 1999.
http://www.math.leidenuniv.nl/ naw/serie5/deel01/jun2000/pdf/vermeulen.pdf

[80] S. Singh – *Big bang: the origin of the universe.* Fourth Estate, 2004.
http://www.simonsingh.net/Big-Bang-Reviews.html
S. Singh – *De oerknal.* De Arbeiderspers, 2005.

[81] I. Stewart & D. Tall – *Algebraic number theory.* Second edition. Chapman and Hall Mathematics Series. Chapman & Hall, London, 1987.

[82] *De laatste stelling van Fermat*, Syllabus van lezingen gehouden op 6-XI-1993. WG & Universiteit Utrecht.

[83] Syllabus Algebra, ontwikkeld sinds 1964 in Amsterdam en Leiden, nu online, zie
`http://websites.math.leidenuniv.nl/algebra/algebra1.pdf`

[84] C. de la Vallée Poussin - *Recherches analytiques sur la théorie des nombres premiers.* Ann. Soc. Sci. Bruxelles **20** (1896), 183–256.

[85] C. de la Vallée Poussin - *Sur la fonction* $\zeta(s)$ *de Riemann et le nombre des nombres premiers inférieurs à une limite donnée.* Memoires Couronnés de l'Acad. Roy des Sciences, Belgique **59** (1899–1900); reprinted in Colloque sur la Théorie des Nombres (Bruxelles, 1955), Thone, Liège, 1956, pp. 9–66.

[86] P. Vojta – *Diophantine approximations and value distribution theory.* Lect. Notes Math. 1239, Springer, 1987.

[87] B. van der Waerden – *Moderne Algebra.* Eerste uitgave in 1931. Vierde uitgave: Heidelberger Taschenbuch, 2 delen, Springer, 1967.

[88] A. Weil – *Number theory, an approach through history, from Hammurapi to Legendre.* Birkhäuser 1984.

[89] A. Weil – *Prehistory of the zeta-function.* Sympos. Atle Selberg (1987): Number theory, trace formulas and discrete groups (Editors A. Aubert, E. Bombieri nd D. Goldfeld). Acad. Press 1989.

[90] E. Weiss – *Algebraic number theory.* Mc-Graw-Hill Cy, 1963.

[91] A. Wiles – *Modular elliptic curves and Fermat's Last Theorem.* Annals Math. **141** (1995), 443–551.

[92] H. Wilf – *What is an answer?* Amer. Math. Monthly, **89** (1982), 289–292.

[93] D. Zagier – *The first 50 milion prime numbers.*
`http://sage.math.washington.edu/edu/2007/simuw07/misc/zagier-the-first-50-million-prime-numbers.pdf`
Published in *The Mathematical Intelligencer*, Vol. **0**, August 1977.

[94] D. Zagier – *Newmans short proof of the prime number theorem.* Amer. Math. Monthly **104** (1997), 705–708.

[95] Y. Zhang – *Bounded gaps between primes.* To appear: Ann. Math.
`http://annals.math.princeton.edu/articles/7954`

Prof. Dr F. Oort
Mathematisch Instituut
Budapestlaan 6
NL - 3508 TA Utrecht
The Netherlands
email: f.oort@uu.nl
`http://www.staff.science.uu.nl/~oort0109/`

Deze tabel vergelijkt x met $\pi(x)$, en geeft $\pi(x) - \frac{x}{\log x}$, en $\pi(x)/\frac{x}{\log x}$, en de gemiddelde grootte van gaten in de rij van priemgetallen tot die grens.

Overgenomen uit:
`http://en.wikipedia.org/wiki/Prime_number_theorem`

x	$\pi(x)$	$\pi(x) - \frac{x}{\log x}$	$\pi(x)/\frac{x}{\log x}$	$x/\pi(x)$
10	4	-0.3	0.921	2.500
10^2	25	3.3	1.151	4.000
10^3	168	23	1.161	5.952
10^4	1,229	143	1.132	8.137
10^5	9,592	906	1.104	10.425
10^6	78,498	6,116	1.084	12.740
10^7	664,579	44,158	1.071	15.047
10^8	5,761,455	332,774	1.061	17.357
10^9	50,847,534	2,592,592	1.054	19.667
10^{10}	455,052,511	20,758,029	1.048	21.975
10^{11}	4,118,054,813	169,923,159	1.043	24.283
10^{12}	37,607,912,018	1,416,705,193	1.039	26.590
10^{13}	346,065,536,839	11,992,858,452	1.034	28.896
10^{14}	3,204,941,750,802	102,838,308,636	1.033	31.202
10^{15}	29,844,570,422,669	891,604,962,452	1.031	33.507
10^{16}	279,238,341,033,925	7,804,289,844,393	1.029	35.812
10^{17}	2,623,557,157,654,233	68,883,734,693,281	1.027	38.116
10^{18}	24,739,954,287,740,860	612,483,070,893,536	1.025	40.420
10^{19}	234,057,667,276,344,607	5,481,624,169,369,960	1.024	42.725
10^{20}	2,220,819,602,560,918,840	49,347,193,044,659,701	1.023	45.028
10^{21}	21,127,269,486,018,731,928	446,579,871,578,168,707	1.022	47.332
10^{22}	201,467,286,689,315,906,290	4,060,704,006,019,620,994	1.021	49.636
10^{23}	1,925,320,391,606,803,968,923	37,083,513,766,578,631,309	1.020	51.939

Tabel van de 168 priemgetallen tot 1,000:

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113
127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239
241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373
379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503
509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647
653 659 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809
811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953
967 971 977 983 991 997

Enkele gaten in de rij van priemgetallen, overgenomen uit:
`http://www.dms.umontreal.ca/~andrew/PDF/cramer.pdf`

p_n	$p_{n+1} - p_n$
31397	72
370261	112
2010733	148
20831323	210
25056082087	456
2614941710599	652
19581334192423	778

Een paar Sophie Germain priemgetallen:

2,3,5,11,23,29,41,53,83,89,113,131,173,179,191,
233,239,251,281,293,359,419,431,443,491,509,593,
641,653,659,683,719,743,761,809,911,953,1013,1019,
1031,1049,1103,1223,1229,1289,1409,1439,1451,1481,
1499,1511,1559, $\cdots$