Priemgetallen

Frans Oort

Communiceren in de Wiskunde (WISB 106)
Utrecht, 11 november 2012

$\cdots$ *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

Inleiding

In deze voordracht bestuderen we *priemgetallen*. We zijn vooral geïnteresseerd in de vraag "hoeveel priemgetallen zijn er, en waar liggen ze"? Die vraag zullen we toch eerst precies moeten 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 $\pi(y) = 1$ voor $2 \leq y < 3$, etc. Kunnen we iets zinnigs zeggen over deze grillige functie? Zie het artikel [26], 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 vin 1849 aan zijn vriend Encke schreef. Ook werd dit vermoed door Legendre (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: *zonder álle priemgetallen te berekenen kunnen we wel degelijk iets zeggen of er ergens* (boven een

bepaalde grens, in een gegeven interval) *priemgetallen liggen* (die we misschien niet precies kennen, maar wel het bestaan ervan bewijzen). In § 8 citeren we dat resultaat (zonder dat we een bewijs geven); bovendien blijken er heel bruikbare zwakkere vormen van die stelling te bestaan die 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 je 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: en 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), 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 [17]. 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 - 5.

- In § 4 geef ik een paar opgaven. Die kun je maken en inleveren. Je kunt die vraagstukken maken zonder veel voorkennis, maar je zult wel iets slims moeten doen.

- Probeer voorbeelden door te rekenen, en kijk of je zo tot 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).

- Deze syllabus bevat veel meer materiaal dan ik kan behandelen. Bewaar een exemplaar, en raadpleeg zo af en toe de tekst gedurende jouw studie, en kijk of je dan meer inzicht gekregen hebt, in de structuur, en in de verbluffende schoonheid en elegantie van dit materiaal.

- 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 je er af en toe over kunt nadenken en vooral voelen wat je erbij ervaart; zie §§ 6 - 7.

- Een vreemde §: in 10 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.

- Een toepassing (van groot belang: RSA),
  een moderne ontwikkeling (het ABC vermoeden),
  iets van onderliggende theorie,
  en een lijst met een paar open problemen

  (grote wiskundigen komen daar nog niet uit ... wat is de onderliggende theorie die het probleem oplost en verklaart?) geef ik in §§ 11 - 14.

Leesadvies. De boeken [5], [11] zijn romans; zeer de moeite waard om te lezen.
Om een indruk te krijgen van het gebied van de elementaire getaltheorie, van elementaire methodes en van resultaten, lees: [12], [3], [4]. Zie ook [19].
Voor basis-kennis over algebra zie [27].
Op het internet is veel informatie te vinden. In deze syllabus staan verwijzingen. Die kun je 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.
Rekenadvies. Probeer van allerlei verschijnselen die besproken worden een aantal gevallen door te rekenen; in de syllabus vind je allerlei suggesties daarvoor.

1 Een paar vragen

(1.1) Vraag 1. *Is de verzameling van alle priemgetallen eindig of oneindig?*
[Hoe begin je 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 probeer je? Nadenken? Of voorbeelden maken?]
Zie (5.1).

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 (5.3).

(1.4) Vraag 4. 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*?
[Je ziet dat voor een beetje grote i het getal F_i groot is; kun je hier aan rekenen? of wil je eerst nadenken? of wat ga je anders doen om dit te begrijpen?]
Zie § 6 en (14.5).

(1.5) Vraag 5. 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 je voor elke i het i-de priemgetal p_i kunt berekenen?*
[Is die vraag wel goed gesteld?]
Zie (5.4); zie § 8.

(1.6) Vraag 6. 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 concludeer je dan? Of hoe pak je dit op een andere manier aan?]
Zie: *het vermoeden van Goldbach* (14.2).

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*?

(1.7) Vraag 7. Bestaat er een priemgetal met 2013 cijfers?
[Waar te beginnen? Kan ik een getal van 2013 cijfers opschrijven, en proberen of dit een priemgetal is? Is de kans erg groot dat ik door een willekeurige keuze te maken ik toevallig een priemgetal op schrijf?]
Zie (5.8). Zie (8.3).

(1.8) Vraag 8. Kun je 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 (5.9).

(We kunnen nog veel meer van dergelijk vragen stellen, maar het is al voldoende om over deze 8 vragen na te denken om een gevoel te ontwikkelen voor dit vak.)

2 Definities, notaties en een paar eigenschappen

(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: $a \mid b$.

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 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 (12.8).
De eigenschap $\text{ggd}(m, n) = 1$ wordt wel verwoord als "m en n zijn onderling priem".

(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 heb je 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.)

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 (6.1).

4 Een paar vraagstukken en suggesties

Van de onderstaande vraagstukken kunt je een oplossing van één van de drie inleveren.

(4.1) Vraagstuk 1. *Bewijs dat de verzameling van priemgetallen met de eigenschap*

$$p \equiv 3 \pmod 4$$

oneindig is.

Opmerking. Ook kan bewezen worden dat er oneindig veel priemgetallen zij met de eigenschap $p \equiv 1 \pmod 4$; zie (13.4).

(4.2) Vraagstuk 2. *Zij $n \in \mathbb{Z}_{>0}$. Bewijs: er is een $a \in \mathbb{Z}_{>0}$ zodanig dat er in de rekenkundige rij*

$$\{a, a + n, a + 2n, \cdots\} = \{a + in \mid i \in \mathbb{Z}_{>0}\}$$

er oneindig veel priemgetallen voorkomen.

Opmerking. Een stelling van Dirichlet zegt dat voor elke $a, n \in \mathbb{Z}_{>0}$ met $\text{ggd}(a, n) = 1$ er in de rekenkundige rij $\{a + in \mid i \in \mathbb{Z}_{>0}\}$ oneindig veel priemgetallen voorkomen; bewijs de voorgaande opgave zonder gebruik te maken van deze (diepe) stelling.

(4.3) Vraagstuk 3. *Bewijs dat er oneindig veel getallen $N \in \mathbb{Z}_{>0}$ bestaan zodanig dat N niet het verschil is tussen twee priemgetallen.*

5 Een paar antwoorden

(5.1) 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

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

Neem voor p_i het grootste priemgetal 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

$$p_{i+1} \geq M+N+2; \quad \text{dus } p_{i+1} - p_1 \geq (M+N+2) - (M+2) = N.$$

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 33 komt veel eerder dan het getal

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

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

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

Zie `http://en.wikipedia.org/wiki/Prime_gaps` Zie ook [8], pag. 10. Zie ook de laatste pagina van deze syllabus.

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 § 8, dat er geldt $\pi(x) < Bx/(\log(x))$ 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 (14.4).

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

(5.2) Tweelingen. Een antwoord op (1.3)(2)? Er zijn heel veel priemtweelingen bekend. We denken dat er oneindig veel zijn, zie (14.3). 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.

(5.3) Drielingen. Een antwoord op (1.3)(3).
In een rij $\{n, n+2, n+4\}$ is 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 wel 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`
Vermoeden. *Het aantal priem-tripletten is oneindig (?).* (Er is geen bewijs maar we kunnen ook niet bewijzen dat het aantal priem-tripletten eindig is.)

(5.4) 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?

(5.5) 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:

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

(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 [13].

(5.6) 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 [14], 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`

(5.7) 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 $x < 3{\cdot}10^{13}$.

(5.8) Bestaat er een priemgetal met precies 2013 cijfers? Zou er een tabel bestaan waar we dit in 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 § 8, 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 (8.3), (8.7).

(5.9) 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, 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.) Langt 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 [18]. Nadenken en abstract denken triomferen weer over berekeningen.
Zie `http://en.wikipedia.org/wiki/Catalan%27s_conjecture`.

6 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 (13.6).

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`

(6.1) 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).

(6.2) Opgave Als $2^m + 1$ een priemgetal is, dan is er een i met $m = 2^i$.
[De vraag naar primaliteit van getallen van de vorm 2^a waar a een oneven deler groter dan 1 heeft is niet zo interessant....]

(6.3) 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 [7], 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 ?).

7 Mersenne (priem)getallen

We introduceren de Mersenne getallen:

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

en vragen ons af of daar priemgetallen onder voorkomen.

(7.1) Opgave.

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

(7.2) Merk op dat de omkering niet geldt:

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

Inderdaad: $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$.

(7.3) Opgave. Laat p een priemgetal zijn zodanig dat $q = 2p + 1$ ook een priemgetal is; Het priemgetal p heet dan een Sophie Germain priemgetal; zie (14.7). Bewijs dat in dit geval q een deler is van M_p.

Er zijn Mersenne priemgetallen bekend. Momenteel weten we van 47 priemgetallen p dat M_p een (Mersenne) priemgetal is. Zie
`http://en.wikipedia.org/wiki/Mersenne_prime`

Vroeger kwam de interesse voor zulke 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. 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.

(7.4) (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: $p = 2, 3, 5, 7, 13, 17, \cdots$.

We laten één implicatie in de stelling zien (de implicatie die reeds door Euclides bewezen werd:

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

Schrijf $\sigma(N)$ voor de som van de delers d met $1 \leq d \leq N$. Ga na:

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

QED$\Rightarrow$

(7.5) Opgave. *Bewijs deze stelling.*

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

8 De Priemgetalstelling PNT

(Voor de notatie $\log(x)$ zie (2.3).)
We bespreken in deze § 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).

(8.1) 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:

(8.2) 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 [3]; het bewijs is werkelijk elementair en eenvoudig. Er zijn veel scherpere varianten. Zie ook [26].

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

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

(8.3) Een voorbeeld. Omdat

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

volgt:

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

Dus bestaat er een priemgetal met 2013 cijfers.

(8.4) 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

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

(8.5) 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.

(8.6) 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`

(8.7) 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 201 cijfers heeft. We zien dat de schattingen 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 denk je?); dat is iets moeilijker te bewijzen; ik denk dat het exacte aantal niet met abstracte methodes te bepalen is.

9 ABC

Deze § gaat over een "eenvoudig" vermoeden, dat waarschijnlijk nu opgelost is. Dit zou wel eens een revolutie in de getaltheorie kunnen betekenen. Het probleem is zo eenvoudig te formuleren. Als het waar is dan zijn de gevolgen enorm. Waarschijnlijk geven de methodes ontwikkeld door Shinichi Moichizuki een nieuwe, succesvolle aanpak.

(9.1) 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`
We beginnen met een heel eenvoudige vorm van het vermoeden (mogelijk te sterk geformuleerd als we α "te klein" nemen):

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

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

(9.3) 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

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

tegenspreken. Is $(\mathrm{ABC})_2$ 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.

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

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

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).

(9.4) 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 gehele getallen ongelijk aan 0"; de uitspraak $(\mathrm{FLT})_n$ is waar voor alle $n > 3$: de beslissende stap in het bewijs werd gezet door Andrew Wiles, 1995, een van de meest spectaculaire resultaten in de wiskunde van de laatste jaren).
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 $c > 0$ en $n > 3{\cdot}\alpha$. QED

We zien dat de juistheid van dit vermoeden, in deze sterke vorm (9.2), waar α berekend kan worden, vérstrekkende gevolgen zou hebben.

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

Equivalente formulering. *Voor elke $\alpha \in \mathbb{R}$ met $\alpha > 1$ is er een constante $\gamma = \gamma(\alpha) \in \mathbb{R}$ zodanig dat voor elke drietal (A, B, C) dat aan $(*)$ voldoet geldt:*

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

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

Equivalente formulering. *Er bestaat een $\alpha \in \mathbb{R}$ waarvoor $(\mathrm{ABC})_{\alpha}$ juist is.*

(9.6) Nieuwe ontwikkelingen. Formuleringen van het ABC-vermoeden, en van gerelateerde vermoedens zijn te vinden in [23]. In de vorm (9.5) wordt een bewijs van dit vermoeden (en van al die andere vermoedens) gegeven door Shinichi Moichizuki (Kyoto, Japan) in ongeveer 500 pagina's manuscript (4 delen) gebaseerd bovendien op 10 eerdere artikelen van dezelfde auteur, 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.

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

10 Heuristiek

Deze § bevat geen wiskunde, maar heeft wel heel veel met wiskunde te maken .....

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 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.

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.)

(10.1) 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.)

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

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

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

(10.5) Opgave. Pas deze heuristiek toe, en krijg een gevoel voor (14.4)(1).

De methode van deze § 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 (14.3). 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 §, hoe discutabel dan ook, levert ons een merkwaardig goed gevoel*wat "er waar zou moeten zijn", in welke richting we soms moeten zoeken.*

11 Cryptografie: RSA

Doel van een crypto-systeem: een methode maken waarmee je een bericht kunt versleutelen, zodat derden het niet kunnen ontcijferen, maar, dankzij een sleutel, de door jou gewenste ontvanger (met behulp van een sleutel) wel het bericht kan ontcijferen.

De huidige maatschappij is ondenkbaar zonder crypto-systemen (elke keer als je met plastic geld uit de muur haalt .... etc.).

In de loop van de geschiedenis zijn er vele systemen ontwikkeld. Zie [22] voor een prachtige beschrijving van de historische ontwikkelingen hierin, en van de verschillende systemen die in de loop van de geschiedenis gebruikt zijn.

We vermelden éń systeem: RSA Public Key System; de naam komt van de ontdekkers: Ron Rivest, Adi Shamir en Len Adleman.
Zie `http://nl.wikipedia.org/wiki/RSA_28cryptografie29`
Het grote voordeel van dit systeem is dat het versleutelen (Encrypten) van een bericht publiekelijk bekend is, terwijl het decoderen (Decyphering) heel moeilijk is als je de sleutel niet kent (een systeem dat aan die voorwaarden voordoet was niet eerder bekend). Zij M de verzameling van boodschappen (denk aan een groot aantal letters of cijfers per bericht). We zoeken

$$E : M \to M \text{ en } D : M \to M, \text{ met } DE = 1_M, \quad ED = 1_M;$$

met andere woorden, D en E zijn bijectieve afbeeldingen. De afzender zet een boodschap $x \in M$ om in een gecodeerde boodschap $E(x)$, en verstuurt die. De bonafide ontvanger weet hoe te ontcijferen en verkrijgt: $D(E(x)) = x$, maar de malafide persoon die dit onderschept wordt verondersteld D niet te kennen, en ook niet gemakkelijk te kunnen vinden.

Maar, goede vraag, als je weet hoe je versleuteld, dan maak je toch een lijst van alle berichten, en zoekt in die lijst op welke het is.
(1) Als je een naam weet, dan kun je vrij eenvoudig een telefoonnummer in het telefoonboek opzoeken, maar omgekeerd als het telefoonnummer weet, dan is het vinden van de bijbehorende naam niet eenvoudig.

Met moderne zoekmethoden is dit misschien te ondervangen. Maar:
(2) De gebruikte systemen zijn zo groot, dat alleen al het aantal mogelijke berichten veel groter is dan het geschatte aantal elementaire deeltjes in het heelal. Er is dus geen sprake van dat je een dergelijk lijst aan kunt leggen, niet digitaal, zeker niet als hard-copy.

Principe van het RSA systeem: kies

$$e, d, p, q \in \mathbb{Z}_{>0}, \quad pq = n,$$

gehele getallen, waarvan p en q priem zijn en

$$\text{ggd}(e, (p-1)(q-1)) = 1, \quad de \equiv 1 \pmod{n};$$

n en e *worden bekend gemaakt*,
p, q en d *blijven geheim.*

Versleutelen. We kiezen voor M de verzameling $\mathbb{Z}/n = \{0, 1, \cdots, n-1\}$. Een boodschap $x \in M$ wordt gecodeerd als

$$E(x) = y \in M \text{ met } y \equiv x^e \pmod{n};$$

met andere woorden: bereken x^e en pas deling door n toe, waar $0 \leq y < n$ de rest is. Iedereen kan e en n kennen, dus iedereen kan coderen.
Feit, decoderen. Als

$$de \equiv 1 \pmod{n} \text{ dan geldt } (x^e)^d \equiv x \pmod{n}.$$

Conclusie.

$$D(y) = x \text{ met } y^d \equiv x \pmod{n}$$

ontcijfert de boodschap (N.B. d is geheim). Ga na dat dit inderdaad werkt: gebruik § 13.

Waarom is dit veilig? Het bepalen of een getal van bij voorbeeld 100 cijfers maar ongeveer 40 seconden op een grote computer (met de goede algoritmen). Factoriseren van een getal van een dergelijk getal kostte een aantal jaren geleden zoiets als 10^9 jaar. Tegenwoordig kan dat veel sneller, en worden grotere getallen gekozen

Het is moeilijk om d te vinden zonder de factorizatie $pq = n$ te kennen Zo lang factoriseren van het (grote) getal n practisch niet mogelijk is, is deze code geheim.

Dit onderwerp is in volle ontwikkeling, interessant van wiskundig oogpunt, zeker wat betreft het ontwikkelen van nieuwe algoritmen, en de vraag hoe efficiënt factoriseren theoretisch is. Maar natuurlijk is de practische kant van de zaak van groot belang. Bijna alle communicatie die geheim moet blijven voor (malafide) derden verloopt via een systeem zoals hier beschreven; zodra een code gebroken wordt, is er weer behoefte aan een verfijning die beter bestand is daartegen.

12 Appendix I: ontbinden in priemfactoren

Hier vermelden we een paar feiten die we in de tekst gebruiken.

(12.1) Definitie. We werken in de verzameling $\mathbb{Z}$ van alle gehele getallen. De notatie $d \mid a$ wordt gebruikt voor: d deelt a; dat wil zeggen, er bestaat een b met $d{\cdot}b = a$. Een getal $p \in \mathbb{Z}_{>1}$ heet een priemgetal als 1 en p de enige positieve delers van p zijn:

$$d \in \mathbb{Z}_{>1}, \quad d \mid p \quad \Longrightarrow \quad d = p.$$

(12.2) Opmerking. Elk getal $a \in \mathbb{Z}_{>1}$ is deelbaar door een priemgetal.
Bewijs. Merk op dat de bewering juist is voor $a = 2$. Neem aan dat de bewering juist is voor alle a' met $1 < a' < a$ (inductie-aanname). Als a een priemgetal is dan zijn we klaar. Als A niet een priemgetal is, dan heeft a een deler d heeft met $1 < d < a$. Schrijf $a = d{\cdot}a'$. De inductie veronderstelling bewijst dat er een priemgetal p is dat a' deelt. Dan is p ook een deler van a. QED

(12.3) Stelling. *Voor elk getal $a \in \mathbb{Z}_{>1}$ is er een ontbinding $a = p_1 \times \cdots \times p_t$ in priemfactoren.*
Hiermee wordt bedoeld: voor elke $n \in \mathbb{Z}$ met $n \notin \{-1, 0, +1\}$ bestaan er priemgetallen $p_1, \cdots, p_s$ met $n = \pm p_1 \times \cdots \times p_s$. Bovendien als $p_1 \times \cdots \times p_s = \ell_1 \times \cdots \times \ell_t$ waar alle factoren priemgetallen zijn, dan is $s = t$ en na eventueel omnummeren geldt $p_1 = \ell_1, \quad \cdots \quad , p_s = \ell_s$.

We hoeven alleen maar factorizatie voor positieve gehele getallen te beschouwen. We kunnen (formeel) ook staande houden dat 1 een dergelijk factorizatie heeft, door te postuleren dat het lege product de waarde 1 heeft.

We ontwikkelen een methode om dit te bewijzen.

(12.4) Opmerking. Vroeger, bv. in de tijd van Euler werd ook $a = 1$ als priemgetal gezien. Nu hebben we een iets andere definitie, die $a = 1$ uitsluit als priemgetal.

(12.5) Waarschuwing. We zijn zo gewend dat "ontbinding in irreducibele factorenëenduidig is op eenheden en volgorde na. In $\mathbb{Z}$ geldt dat op $\pm$ na: $6 = 2{\cdot}3 = (-2){\cdot}(-3)$. In het algemeen geldt die eenduidigheid in een willekeurige ring niet. Hier is een voorbeeld: neem de ring

$$T := \mathbb{Z}[\sqrt{-5}] = \{x + y{\cdot}\alpha \mid x, y \in \mathbb{Z}\},$$

met $\alpha^2 = -5$, bij voorbeeld als deelverzameling van $\mathbb{C}$ beschouwd. Merk op dat in T geldt:

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

Het is gemakkelijk in te zien dat de factoren $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5}) \in T$ irreducibel zijn. Ook zien we dat $+1, -1 \in T$ de eenheden zijn. Hier zien we dat er niet sprake is van eenduidige factorontbinding in déze ring T.

Voor we aan een bewijs beginnen gaan we eerst een fundamenteel hulpmiddel invoeren: de *eenduidigheid van factorizatie* in $\mathbb{Z}$.

Merk op dat als voor gehele getallen $d, e \in \mathbb{Z}$ geldt $d{\cdot}e = 1$ dan is óf $e = +1$ óf $e = -1$. We zullen $+1$ en -1 de eenheden van $\mathbb{Z}$ noemen. De enige positieve delers van een priemgetal p zijn 1 en p zelf. Als we schrijven $n = \pm p_1 \times \cdots \times p_s$, waar $p_1, \cdots, p_s$ priemgetallen zijn, dan spreken we van een (priem)factorizatie van het gehele getal n.

(12.6) 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: $j \neq k$ 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

(12.7) De grootste gemene deler. 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 $c \nmid a$.
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 $a,\ b \in \mathbb{Z}$. We definiëren de grootste gemene deler d van a en b als volgt: beschouw

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

merk op dat deze verzameling niet leeg is (ga alle mogelijke gevallen na). Het grootste getal in deze verzameling noteren we als $\text{ggd}(a, b)$, de grootste gemene deler $d = \text{ggd}(a, b)$ van a en b. Merk op: voor $a = 0$ geldt $\text{ggd}(0, b) = b$; voor $a \neq 0$ en $b \neq 0$ geldt $\text{ggd}(a, b) > 0$. Als $\text{ggd}(a, b) = 1$, dan zeggen we dat a en b *onderling ondeelbaar* zijn.

(12.8) 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). Beschouw alle paren gehele getallen (α, β) zodanig dat $\mid \alpha \mid \geq \mid \beta \mid > 0$ en $\mathrm{ggd}(\alpha, \beta) = d$. Als $\beta = d$ dan kunnen we de gevraagde x en y vinden: $0{\cdot}\alpha + 1{\cdot}\beta = d$. We beschouwen nu $\mid a \mid \geq \mid b \mid > d$ en we nemen aan (inductie hypothese) dat de uitspraak waar is voor alle paren (α, β) als boven met $\mid b \mid > \mid \beta \mid \geq d$. Uit (12.6) 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

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 (12.3). 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 priemfactorizatie voor alle $n \in \mathbb{Z}_{>1}$. Nu nog de eenduidigheid.

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). 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.

Kies $s \leq t$ in een factorizatie als boven en neem aan dat eenduidigheid bewezen is in alle gevallen met kleinere s. Uit de aanname volgt 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 de eenduidigheid. QED (12.3)

13 Appendix II: rekenen modulo n

(13.1) Rekenen modulo n. Geef $n \in \mathbb{Z}_{>1}$. Beschouw de verzameling van symbolen

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

In die verzameling gaan we optellen en aftrekken en vermenigvuldigen. Dat doen we door gelijk te stellen $\overline{m} = \overline{m - in}$. We geven een afbeelding

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

Anders gezegd: een $m \in \mathbb{Z}$ schrijven we als $m = dn + r$ met $0 \leq r = r(m) < n$ ("deling 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 $\overline{a-b}$.
Om te benadrukken dat we modulo n rekenen schrijven we wel $\overline{m} = m \bmod n$.
Maak goed onderscheid tussen $(m \bmod n) \in \mathbb{Z}/n$ enerzijds en $a \equiv b \pmod{n}$ anderzijds.

Een voorbeeld. Heeft de vergelijking $T^2 = 47440033367001212$ een oplossing in $\mathbb{Z}$? we gaan rekenen moduli 3. Als we een oplossing $t \in \mathbb{Z}$ zouden vinden, dan zou gelden $\overline{t} = \overline{474400333670012} = \overline{2}$ (ga na !). De kwadraten in $\mathbb{Z}/3$ zijn $= \overline{0}$, $\overline{1}$ en niet $\overline{2}$; tegenspraak; de oorspronkelijke vergelijking heeft geen oplossing in $\mathbb{Z}$. QED
Een andere methode. Welke eindcijfers komen voor bij kwadraten in het 10-tallig stelsel?

Bovendien geldt: *voor elk priemgetal p heeft elke $0 \neq \overline{a} \in \mathbb{Z}/p$ een inverse.*
Bewijs. We gebruiken (12.8). Omdat $0 \neq \overline{a}$ geldt $\gcd(a, p) = 1$. Dus bestaan er

$$x, y \in \mathbb{Z} \text{ met } xa + yp = 1; \text{ dit geeft } \overline{xa} = \overline{x} \cdot \overline{a}.$$

QED

We zullen vaak gebruiken:

(13.2) Stelling (de Chinese reststelling). *Voor $m, n \in \mathbb{Z}$ met $\gcd(m, n) = 1$ is er een natuurlijk afbeelding*

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

die een isomorfisme is (een bijectieve afbeelding die $+$ en $\times$ en $-$ in elkaar overvoert).

(13.3) 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 volgt dat 4 een deler is van $\#((\mathbb{F}_p)^*) = p - 1$. QED

(13.4) Gevolg. *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 (13.3) 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

(13.5) Opmerking. Schrijf $\pi_{4,1}(x)$ voor alle priemgetallen $p \equiv 1 \pmod 4$ en $\pi_{4,3}(x)$ voor alle priemgetallen $p \equiv 3 \pmod 4$ met $p \leq x$. Probeer voor kleine x deze aantallen te berekenen. Het zal je opvallen dat ze dicht beijelkaar liggen.

In een brief in 1835 schreef Chebyshev aan Fuss dat het wel leek alsof $\pi_{4,3}(x) > \pi_{4,1}(x)$. Een fascinerende geschiedenis, en veel mooie resultaten daarna. Zie bv.
`http://arxiv.org/pdf/1210.6946v1.pdf`

Wat bewezen kan worden:

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

Dit is een bijzonder geval van een veel algemenere stelling, die ik hier niet behandel. Verder geldt

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

Zie [9]; een prachtig artikel over dit fascinerende onderwerp. Een voorbeeld hoe een "eenvoudige" vraag aanleiding kan geven tot prachtig onderzoek, hoe een verschijnsel dat elementair lijkt verband blijkt te hebben met mooie, diepe verschijnselen (zoals zo vaak in de wiskunde).

(13.6) 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

Rekenen modulo n zal nog uitvoerig behandeld woorden in het college algebra. Het is een eenvoudig, krachtig hulpmiddel in de wiskunde.

14 Appendix III: Een paar 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 jouw 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 je 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.

Een voorbeeld: de laatste stelling van Fermat (die ik hier niet bespreek, behalve even in (9.4)) 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 (als van elkaar losstaande problemen). 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.

(14.1) 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 § 7.

Betaat er een oneven *perfect getal*?

Er is veel literatuur over, er zij 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.)

(14.2) 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 $= 2n \geq 4$ is te schrijven als som van twee priemgetallen.

(14.3) Priemtweelingen. We spreken van een priemtweeling (p, q) als $q - p = 2$. Er zijn erg veel voorbeelden. Dit is 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.

Grote berekeningen hebben sommige 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."

(14.4) Gaten in de rij van priemgetallen.
(14.4)(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 $p_{i+1} - p_i = m$.*
`http://en.wikipedia.org/wiki/Twin_prime`

(14.4)(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 (14.4)(1) geeft "ja" tegen (14.4)(2);
"nee" tegen (14.4)(2) geeft "nee" tegen (14.4)(1).

(14.5) 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 [15] voor meer informatie.

(14.6) 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.*

(14.7) 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.*

(14.8) 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 $\{a_1, \cdots, a_{i+1} = C(a_i), \ldots\}$; 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 kom, het einde,
de Collatz $3x+1$ 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 n de lengte van de Collatz rij uitrekent tot de eerste keer dat 1 voorkomt?

Niet behandeld: het Riemann vermoeden, dat zou me te ver voeren.

Voor nog veel meer vermoedens over priemgetallen, zie: [10]; zie ook:
`http://en.wikipedia.org/wiki/Category:Conjectures_about_prime_numbers`

Referenties

[1] A. H. Beiler - *Recreations in the theory of numbers: The queen of mathematics entertains.* Dover Publ., pocket, 1964.

[2] E. T. Bell – *Men of mathematics.* Simon & Schuster. 1937.

[3] F. Beukers – *Elementary number theory.* Collegedictaat WISB321, Utrecht 2012.

[4] D. M. Burton - *Elementary number theory.* Allyn & Bacon, 1980.

[5] 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`

[6] A. Fröhlich & M. J. Taylor – *Algebraic number theory.* Cambridge Std. Advanc. Math. 27, Cambridge Univ. Press, 1991.

[7] C. F. Gauss – *Disquisitiones Arithmeticae.* Geschreven 1798, gepubliceerd in 1801.

[8] 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

[9] A. Granville & G. Martin – *Prime number races.* American Mathematical Monthly **113** (2006), 1–33.

[10] R. K. Guy – *Unsolved problems in number theory.* Springer Verlag, 3rd Edition 2004.

[11] 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

[12] G. H. Hardy & E. M. Wright - *An introduction to the theory of numbers.* Oxford, Clarendon Press, fourth edition, 1975.

[13] J. Jones – *Formula for the Nth prime number.* Canad. Math. Bull. **18** (1975), 433434.

[14] J. Jones, D. Sato, H. Wada & D. Wiens – *Diophantine representation of the set of prime numbers.* Amer. Math. Monthly, **83** (1976), 449–464.

[15] M. Krízek, F. Luca& L. Somer -*17 Lectures on Fermat numbers from number theory to geometry.* CMS Books in Mathematics Springer, New York 2002.

[16] S. Lang – *Algebraic number theory.* Grad. Texts Math. 110, Springer Verlag, 1986.

[17] 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.

[18] P. Mihăilescu – *Primary cyclotomic Units and a proof of Catalan's Conjecture.* Journ. Reine angew. Math. 572 (2004), 167–195.

[19] F. Oort – *Priemgetallen.* Kaleidoscoop van de wiskunde 1: van priemgetal tot populatiegenetica. (Ed. F. van der Blij, J. P. Hogendijk, F. Oort). Epsilon Uitgaven, 1990; pp. 1–32

[20] H. Riesel - *Prime numbers and computer methods for factorization.* Progress Math. 57, Birkhäuser, 1985.

[21] D. Shanks – *Solved and unsolved problems in number theory.* Chelsea Publ. Cy., 1978.

[22] S. Singh – *The code book: the evolution of secrecy from Mary, Queen of Scots to quantum cryptography.* Simon Singh Doubleday Books, 1999.

[23] P. Vojta – *Diophantine approximations and value distribution theory.* Lect. Notes Math. 1239, Springer-Verlag, New York, 1987.

[24] A. Weil – *Number theory, an approach through history, from Hammurapi to Legendre.* Birkhäuser 1984.

[25] E. Weiss – *Algebraic number theory.* Mc-Graw-Hill Cy, 1963.

[26] 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`

[27] Syllabus Algebra, ontwikkeld sinds 1964 in Amsterdam en Leiden, nu online, zie
`http://websites.math.leidenuniv.nl/algebra/algebra1.pdf`

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

Prof. Dr F. Oort
Mathematisch Instituut
P.O. Box. 80.010
NL - 3508 TA Utrecht
The Netherlands
email: f.oort@uu.nl