Congruente getallen

Frans Oort

Kaleidoscoop voordracht
Utrecht, 10 februari 2009

Inleiding

In deze voordracht bestuderen we het probleem van de Congruente Getallen, dat in een 10-de eeuws Arabisch manuscript voorkomt, dat in de 13de eeuw door Fibonacci bestudeerd werd, dat Fermat waarschijnlijk motiveerde om zijn grote vermoeden FLT te formuleren (pas in 1995 door Andrew Wiles opgelost). Dit probleem is vele malen bestudeerd, veel deelresultaten zijn bewezen, maar 10 eeuwen later is het in essentie nog steeds niet opgelost. Voor twee definities van het begrip "Congruent Getal" zie § 1.

Lang was dit een geïsoleerd probleem. Pas in de 20-ste eeuw werd dit probleem gekoppeld aan een rijke theorie: de elliptische krommen. En er werd bewezen dat het probleem opgelost kan worden als we een veel algemener vermoeden kunnen bewijzen: het vermoeden van Birch en Swinnerton-Dyer. Wil je $ 1,000,000 verdienen? los dat probleem op: een van de Clay Mathematics Institute Millenium problems.

We zullen het probleem opsplitsen, preciseren in 3 vragen, zie § 2. Het is verrassend dat sommige van die vragen heel eenvoudig en elementair te beantwoorden zijn. Maar ook dat de belangrijkste vraag tot op heden onopgelost is.

De §§ 1 - 6 geven de inhoud van de voordracht, pp. 2 - 13. Andere paragrafen zijn opgenomen voor verder uitleg en toelichting voor de lezer met verdere interesse. Methoden zijn elementair, behalve in § 10; daar wordt de 20-ste eeuwse benadering van het probleem gegeven; daar kan ik niet alle definities en details geven, maar er zijn genoeg verwijzingen om te vinden hoe die theorie in elkaar zit. Het onderwerp "elliptische krommen" is veelzijdig en centraal in de meetkunde en in de getaltheorie. Er zijn heel veel mooie en nuttige bewijzen mee gevonden.

Van de onderstaande vraagstukken kunt U een oplossing van één van de drie inleveren (meer mag ook, maar dat hoeft niet).

(0.1) Vraagstuk 1. Kies $N = 30$. Geef twee verschillende presentaties van het feit dat dit een CG is. (Controleer het antwoord. U mag ook twee verschilende realisaties geven.)

(0.2) Vraagstuk 2. Een variatie op (3.2).
a) Voor elke $j \in \mathbb{Z}_{>0}$ schrijf: $v_j := (j+2)^2 - j^2$. M.a.w. de rij $\mathcal{V}_2 = \{v_j \mid j \in \mathbb{Z}_{>0}\} = \{8, 12, \cdots\}$, is de rij van verschillen in de rij van kwadraten die 2 plaatsen van elkaar af staan. *Bewijs dat er in deze rij oneindig veel kwadraten voorkomen.*

b) Kies $k \in \mathbb{Z}_{>1}$. Schrijf: $w_j := (j+k)^2 + j^2$. *Bewijs dat er in de rij* $\mathcal{V}_k = \{w_j \mid j \in \mathbb{Z}_{>0}\}$ *oneindig veel kwadraten voorkomen.*
c) Geef een voorbeeld van twee kwadraten die 7 plaatsen van elkaar afstaan zodat hun verschil een kwadraat is.

(0.3) Vraagstuk 3. In dit vraag stuk nemen we aan dat het vermoeden (5.2) juist is (Pas Op ! tot op heden nog onbewezen). *Gebruik Stelling* (5.1)*, neem de juistheid van dit vermoeden aan en bewijs:*
a) $N = 1$ *is niet een* CG.
b) $N = 2$ *is niet een* CG. *WS*
c) $N = 3$ *is niet een* CG.
d) Een getal $N \in \mathbb{Z}_{>0}$ *met* $N \equiv 6 \pmod 8$ *is wel een* CG. (Hint: bewijs eerst dat als $d \in \mathbb{Z}_{>0}$ en $N = d^2 \cdot M$ dan is $M \equiv 6 \pmod 8$.)
(Opmerking: de conclusies in (a), (b) en (c) zijn waar, ook zonder aanname van het vermoeden; de conclusie onder (d) is bij mijn weten onbewezen voor veel waarden van $N \in \mathbb{Z}_{>0}$ met $N \equiv 6 \pmod 8$.)

(0.4) Vraagstuk 4. Voor een oneven priemgetal p definiëren we het pCG T_p door: $n = 2$, $m = p$,

$$mn(m^2 - n^2) = 2 \cdot p \cdot (p-2) \cdot (p+2) = D^2 \cdot T_p.$$

a) Bewijs: *als* $p > 2$ *en* $q > p + 2$ *priemgetallen zijn dan is* $T_p \neq T_q$.
b) Bewijs *dat er oneindig veel* pGCen *zijn.*
c) Bewijs: *als* p *en* q *verschilende oneven priemgetallen zijn dan is* $T_p \neq T_q$.

1 Definitie: Congruent Getal

We geven de definitie van een congruent getal. Eerst geven we de definitie die historisch de eerste was. Daarna geven we een eenvoudiger definitie die we waarschijnlijk beter begrijpen. We laten zien dat de twee definities equivalent zijn.

(1.1) Een voorbeeld. Kies $N = 5$. Rond 1220 vroeg Johann Panormitanus di Palermo aan Leonardo di Pisa (Fibonacci) of er een positief rationaal getal δ bestaat zodanig dat $\delta^2 \pm 5$ allebei kwadraten zijn; zie [13], page 460. Fibonacci vond: voor $\delta = \frac{41}{12}$ geldt

$$\delta^2 - N = \frac{1681}{144} - 5 = \frac{961}{144} = (\frac{31}{12})^2 \quad \text{en} \quad \delta^2 + N = \frac{1681}{144} + 5 = \frac{2401}{144} = (\frac{49}{12})^2.$$

Met andere woorden: het drietal

$$\delta^2 - N, \quad \delta^2, \quad \delta^2 + N$$

vormt een rekenkundige rij van 3 kwadraten in $\mathbb{Q}$ (en we zullen zeggen dat $N = 5$ een congruent getal is, zie Definitie I). Dit was voor Fibonacci het begin voor zijn boek "Liber Quadratorum" (1225).

Dit voorbeeld komt ook voor in een eerder, anoniem Arabische manuscript uit de 10-de eeuw (in totaal geeft dat manuscript 30 congruente getallen), zie [1], zie pp. 256/257, maar ook in en artikel van Abu Jafar Muhammad ibn al-Hasan Al-Khazin, zie [31], page 83, zie [3].

(1.2) Definitie I. Een positief geheel getal N heet een *congruent getal* als er bestaat een $\delta \in \mathbb{Q}$ zodanig dat

$$\delta^2 - N, \quad \delta^2, \quad \delta^2 + N$$

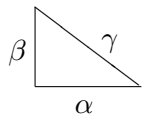
kwadraten zijn in $\mathbb{Q}$. We zullen schrijven CG = congruent getal, en CGP = het probleem van het vinden van congruente getallen / bepalen of een gegeven getal congruent is.

Opmerking. Deze terminologie, ingevoerd door Fibonacci, lijkt vreemd. Het bedoelt uit te drukken dat de drie getallen een rekenkundige rij vormen. Als de twee opeenvolgende verschillen gelijk zijn dan noemt Fibonacci dit in Latijns *congruum*, vandaar de naamgeving; zie [16], pp. 53/54, page 54, regel 13.

De vraag welke positieve gehele getallen congruent zijn is eeuwen lang bestudeerd. Dit is het onderwerp van deze voordracht. Zijn er nog meer congruente getallen? Probeer maar eens (1.7); de oplossing staat in (11.4).

Een meetkundige beschouwing helpt de algebraïsche definitie te verduidelijken.

(1.3) Definitie II. Een positief geheel getal N heet een *congruent getal* als er een rechthoekige driehoek bestaat met lengtes van zijden in $\mathbb{Q}_{>0}$ en met oppervlak gelijk aan $N \in \mathbb{Z}$. Noem de lengtes van de zijden $\alpha, \beta, \gamma \in \mathbb{Q}$; met behulp van de stelling van Pythagoras zien we:



$\alpha \cdot \beta/2 = N$,
$\alpha^2 + \beta^2 = \gamma^2$;
een voorbeeld is: $\alpha = 9/6, \quad \beta = 40/6, \quad \gamma = 41/6, \quad N = 5.$

(1.4) Lemma. *Deze beide definities zijn equivalent.*
Bewijs. Zij gegeven N en δ als in Definitie I. Schrijf $\delta^2 - N = \xi^2$ en $\delta^2 + N = \lambda^2$ met $\xi, \lambda \in \mathbb{Q}_{>0}$. Schrijf

$$\gamma := 2\delta, \quad \text{en} \quad \alpha := \lambda + \xi, \quad \beta := \lambda - \xi.$$

Dan is

$$\alpha \cdot \beta = \lambda^2 - \xi^2 = 2N$$

en

$$\alpha^2 + \beta^2 = \lambda^2 + 2\lambda\xi + \xi^2 + \lambda^2 - 2\lambda\xi + \xi^2 = 2\lambda^2 + 2\xi^2 = 4\delta^2 = \gamma^2.$$

We hebben geconstrueerd:

$$\delta \quad \mapsto \quad (\delta, \lambda, \xi) \quad \longmapsto \quad (\alpha, \beta, \gamma).$$

We zien dat Definitie I als gevolg heeft Definitie II.

Omgekeerd, onderstel gegeven $\alpha, \beta, \gamma \in \mathbb{Q}$ en $N \in \mathbb{Z}$ zoals in Definitie II. Definieëer $\delta := \gamma/2$. Dan is

$$\delta^2 \pm N = \frac{1}{4}(\gamma^2 \pm 2\alpha\beta) = (\frac{1}{2}(\alpha \pm \beta))^2.$$

Dus voldoen δ en N aan Definitie I. We hebben geconstrueerd:

$$(\alpha, \beta, \gamma) \quad \longmapsto \quad (\delta, \lambda, \xi) \quad \mapsto \quad \delta.$$

We zien dat de twee definities aan elkaar gelijk zijn. QED

(1.5) Nog een voorbeeld: $N = 6$ is een congruent getal. Inderdaad: $\delta = 5/2$ voldoet aan:

$$\delta^2 - N = \frac{25}{4} - 6 = (\frac{1}{2})^2, \quad \text{en} \quad \delta^2 + N = \frac{25}{4} + 6 = (\frac{7}{2})^2.$$

Maar er geldt ook:

$$\text{de keuze } \Delta = \tfrac{1201}{140} \text{ laat zien dat } N = 6 \text{ een congruent getal is.}$$

Inderdaad:

$$49^2 + 1200^2 = 1201^2, \quad \text{en} \quad 2{\cdot}N = \frac{1200}{140}{\cdot}\frac{49}{140}; \quad \text{dus} \quad \delta^2 + N = \frac{1249}{140} \quad \text{en} \quad \delta^2 - N = \frac{1151}{140}.$$

Hoe vinden we een dergelijk voorbeeld? We zullen dit laten zien, zie (6.1).

(1.6) Terminologie. Als $N \in \mathbb{Z}_{>0}$ gegeven is, en $\delta \in \mathbb{Q}_{>0}$ laat zien dat dit een CG is, zoals in Definitie I, dan zeggen we dat dit een *realisatie* van dit CG is.

Als $N \in \mathbb{Z}_{>0}$ gegeven is, en $(\alpha, \beta, \gamma) \in (\mathbb{Q}_{>0})^3$ laat zien dat N een CG is, zoals in Definitie II, dan zeggen we dat dit een *presentatie* van dit CG is.
(Deze terminologie is niet standaard, maar ik introduceer die hier om gemakkelijker over deze onderwerpen te kunnen praten.)

Als $(\alpha, \beta, \gamma) \in (\mathbb{Q}_{>0})^3$ laat zien dat N een CG is, dan laat $(\beta, \alpha, \gamma) \in (\mathbb{Q}_{>0})^3$ ook zien dat N een CG is. De rol van α en β in Definitie II lijkt symmetrisch. Echter, we zullen in § 3 zien dat we wel degelijk onderscheid kunnen maken, en we zullen voor een volgorde $\alpha - - - - \beta$ kiezen zodra we Pythagoreïsche Drietallen beschrijven, en gebruik maken van het onderscheid even-oneven voor gehele getallen.

(1.7) Voorbeeld/Opgave. *Is $N = 13$ een congruent getal?*
(Hier zie je dat het vaak niet eenvoudig is om een dergelijke vraag te beantwoorden. Een oplossing staat in (11.4).)

(1.8) Zij gegeven $N, d \in \mathbb{Z}_{>0}$. Merk op dat N een CG is dan en slechts dan als $d^2{\cdot}N$ een CG getal is (schrijf een bewijs uit in de terminologie van Definitie I en van Definitie II).

(1.9) Definitie. We zeggen dat $N \in \mathbb{Z}> 0$ "*kwadraatvrij*" is als 1 het grootste kwadraat van een geheel getal is dat M deelt;

$$d \in \mathbb{Z}_{>0}, \quad d^2 \mid N \quad \Longrightarrow \quad d = 1.$$

(1.10) Opmerking. Zie § 8 voor details over factorontbinding in $\mathbb{Z}$. Ga na dat N kwadraatvrij is dan en slechts dan voor elk priemgetal p het getal M niet deelbaar is door p^2:

$$N \quad \text{is kwadraatvrij} \quad \Longleftrightarrow \quad (\text{voor elk priemgetal } \ p: \quad p^2 \quad \text{deelt niet} \quad N).$$

Een kwadraatvrij CG heet een *primitief congruent getal*, afgekort pCG. We kennen alle CGen als we alle pCGen kennen.

2 Vragen

Weke getallen zijn een CG? hoe kunnen we zien dat iets een CG is? We zullen zien dat we gemakkelijk een aantal CGen kunnen construeren. Maar hoe beslissen we voor een gegeven getal of het een CG is? Laten we beginnen met een voorbeeld:

(2.1) Kies $\boxed{N = 1}$. Is dit een congruent getal? Deze vraag werd tenminste 7 eeuwen bestudeerd, en foute bewijzen werden gegeven, zie [13], page 462, [11], page 20. Fibonacci zei dat hij een bewijs had dat dit niet een CG is; we betwijfelen of hij werkelijk een bewijs had. Pas het genie Fermat wist deze vraag te beantwoorden: $N = 1$ is niet een CG. We zullen zien dat dit probleem een catalysator was in wiskundig onderzoek. Zie (11.1).

Ik ken geen methode om een getal te kiezen waarvan we eenvoudig kunnen laten zien dat het niet een CG *is.*
Om het probleem van het vinden van de CGen e preciseren formuleer ik 3 vragen:

(2.2) Vraag A. *Kunnen we een lijst maken waarin alle* pCGen *staan?*

(2.3) Vraag B. *Is er een effectieve manier om te beslissen of een gegeven getal congruent is?*
Hiermee bedoelen we: is er een formule die voor elk gegeven geheel getal N de hoeveel tijd (of de hoeveel rekenkundige stappen) geeft zodanig dat het beslissen of N een CG getal is gedaan kan worden binnen die tijd.

(2.4) Vraag C. *Hoeveel presentaties heeft een* CG ?
Notatie. Een $((\alpha, \beta, \gamma), N)$ zoals in Definitie II heet een "presentatie" van het CG N. Equivalent: we kunnen ook vragen naar de realisaties van een CG, zie Definitie I.

Stop. Alvorens verder te lezen, laat de vragen goed tot U doordringen, probeer te begrijpen dat dit inderdaad goede formulering zijn van het CGP, en probeer in te schatten welke vraag een moeilijk/gemakkelijk antwoord heeft.

Hier is een overzicht van wat gaan doen:

We zullen zien dat Vraag A niet moeilijk is, en dat die lijst oneindig lang is. Zie § 4. Lost dit ons probleem op? Onderstel dat we willen weten of $N = 1$ een CG getal is. We inspecteren de lijst. Na lang zoeken hebben we nog steeds dit getal niet gevonden. Wat zegt dat? Nog niets. En we zullen zien dat voor een relatief klein getal (bv. $N = 157$, of $N = 263$) we heel ver moeten gaan in die lijst om inderdaad dat getal te vinden. Voorbeelden staan o.a. in § 11 op de laatste twee pagina's van deze syllabus.

We zullen zien dat Vraag B echt moeilijk is. Die vraag is nog steeds onopgelost, maar dat we wel een vermoeden hebben wat een goed antwoord op deze vraag B zou kunnen zijn. Zie § 5.

We zullen zien dat Vraag C elementair en eenvoudig te beantwoorden is: voor elk CG is het aantal onderling verschillende presentaties oneindig. Zie § 6.

3 Pythagoreïsche Drietallen

Om een antwoord op Vraag A te geven behandelen we een heel oude techniek: het bepalen van alle Pythagoreïsche Drietallen.

We bestuderen vergelijkingen van de vorm $X^n + Y^n = Z^n$ en oplossingen daarvan in de gehele getallen. Het vermoeden van Fermat zegt dat zulke oplossingen $(z, y, x) \in \mathbb{Z}^3$ voor $n \geq 3$ alleen maar bestaan met $xyz = 0$ (dat worden wel de "triviale oplossingen" genoemd). In deze paragraaf houden we ons bezig met het geval $n = 2$.

We zullen zien dat er dan oneindig veel oplossingen bestaan, en we zullen ze allemaal classificeren. We zullen een dergelijk drietal $(x, y, z) \in (\mathbb{Z}_{>0})^3$, een oplossing van $X^2+Y^2 = Z^2$, een Pythagoreïsch Drietal noemen; afgekort: PD.

Hier begint eigenlijk de geschiedenis van ons onderwerp. Op een oud Babylonisch klei-tablet gedateerd tussen 1800 en 1650 vóór Christus zijn een aantal van dergelijke oplossingen vermeld; zie het klei-tablet Plimpton 322, [26], [17]. Het is aannemelijk dat zulke drietallen en rol speelden in oude beschavingen.

Soms wordt vermeld dat het drietal $(3, 4, 5)$ gebruikt werd om rechte hoeken te construeren bij het bouwen van de Egyptische piramides. Ik ken geen historische of archeologische gegevens om deze veronderstelling te onderbouwen.

Uit de stelling van Pythagoras volgt dat (x, y, z) een dergelijk drietal is, deze getallen kunnen opteden als lengtes van een rechthoekige driehoek; vandaar de naamgeving.

De classificatie van alle Pythagoreïsche driehoeken is een van de oudste stellingen van de wiskunde. Euclides beschreef dit in zijn "Elementen", Boek X, Propositie 28a, ongeveer 23 eeuwen geleden.

Voor $x, y \in \mathbb{Z}_{>0}$ schrijven we $\text{ggd}(x, y)$ voor de *grootste gemene deler* van die twee getallen, dat will zeggen het grootste getal $d \in \mathbb{Z}_{>0}$ dat x en y deelt. Zie (8.7) voor een definitie van dit begrip.

(3.1) Definitie: Pythagoreïsche drietallen. Een drietal positieve gehele getallen $(x, y, z) \in (\mathbb{Z}_{>0})^3$ heet een *Pythagoreïsch drietal* als $x^2 + y^2 = z^2$. We zullen dit begrip aangeven met PD.
Primitief PD. We zeggen dat een PD (x, y, z) *primitief* is als $\text{ggd}(x, y) = 1$. Afkorting: pPD.

Merk op: als $\text{ggd}(x, y) = 1$ en $x^2+y^2 = z^2$ dan volgt ook $\text{ggd}(y, z) = 1$ en $\text{ggd}(z, x) = 1$, ga na!

Enkele voorbeelden: $(3, 4, 5)$, $(6, 8, 10)$, $(5, 12, 13)$, $(9, 40, 41)$ zijn PDen. Het tweede voorbeeld is niet primitief, de andere wel.

(3.2) *We laten zien dat er oneindig veel onderling verschillende* pPD *zijn.* We gebruiken alleen maar heel elementaire middelen. Beschouw

$$1, 4, 9, 16, \cdots, j^2, \cdots,$$

en de onderlinge verschillen

$$3, 5, 7, \cdots, (j+1)^2 - j^2 = 2j+1, \cdots \ .$$

We zien dat alle oneven getallen groter dan 2 *voorkomen.* Dus komen alle oneven kwadraten groter dan 1 voor. Kies j zodanig dat $2j+1$ een kwadraat is; schrijf $2j+1 = (2\ell+1)^2$. Dus $j = 2\ell^2 + 2\ell$. Kies $x := 2\ell+1, \quad y := j, \quad z := j+1$, en inderdaad:

$$z^2 - y^2 = (z-y)(z+y) = 1 \cdot (4\ell^2 + 4\ell + 1) = (2\ell+1)^2 = x^2.$$

Voor elke $\ell \in \mathbb{Z}_{>0}$ krijgen we zo een PD. Omdat $z = y+1$ is dit een ook en pPD. Voorbeelden:

$$3^2 = 5^2 - 4^2, 5^2 = 13^2 - 12^2, \cdots, (2\ell+1)^2 = (2\ell^2+2\ell+1)^2 - (2\ell^2+2\ell)^2, \cdots \ .$$

We zien dat er oneindig veel onderling verschillende pPDen bestaan.

Zijn we nu tevreden en kunnen we de rest van de paragraaf overslaan? Nee, een wiskundige probeert een classificatie van álle oplossingen te geven. Zoals we zullen zien, zal ons dat later goed van pas komen.

We geven een stelling die alle PDen classificeert. We zullen drie verschillende bewijzen geven van de stelling die deze classificatie geeft.

(3.3) Lemma. *Als (x, y, z) een primitief* PD *is, dan is z oneven, en van x en y is er precies één even, en één oneven.*
Bewijs. Als een geheel getal $u \in \mathbb{Z}$ even is, dan is u^2 deelbaar door 4. Als u oneven is dan geldt $u^2 \equiv 1 \pmod 4$; d.w.z. u^2 kan geschreven worden als $u^2 = q \cdot 4 + 1$; inderdaad, als $u = 2k+1$ dan is $u^2 = 4k^2 + 4k + 1 = (k^2+k) \cdot 4 + 1$.

Als x en y beide even zouden zijn, dan is het drietal niet primitief. Als x en y beide oneven zouden zijn dan geldt $x^2 + y^2 \equiv 2 \pmod 4$; dus is $x^2 + y^2$ niet een kwadraat in dit geval. Blijft over: van x en y is er precies één even, en één oneven; in dat geval is z oneven. QED

Afspraak: Als (x, y, z) een pPD is, dan nemen we aan dat x oneven is en y even (zo niet, dan verwisselen we x en y).

Merk op:

$$(m^2 - n^2)^2 \quad + (2m \cdot n)^2 \quad = \quad (m^2 + n^2)^2.$$

Voor elke keuze van $m, n \in \mathbb{Z}$ met $m > n > 0$ krijgen we op deze manier een PD.

(3.4) Opmerking. *Als $m, n \in \mathbb{Z}_{>0}$ met $m > n$, en* ggd$(m, n) = 1$ *en $m+n$ oneven dan is $(m^2 - n^2, 2mn, m^2 + n^2)$ primitief.*
Bewijs. Uit "$m+n$ is oneven" volgt dat $m^2 - n^2 = (m+n)(m-n)$ oneven is; dus is 2 niet een gemeenschappelijk factor van $m^2 - n^2$ en $2mn$. Stel $p > 2$ is een priemdeler van $m^2 - n^2$ en van $2mn$; dan is het ook een deler van $m^2 + n^2$; dan is het ook een priemdeler van m^2, dus van m, ook een priemdeler van n^2 dus van n, tegenspraak. QED

We laten zien dat we op deze manier ze alle Pythagoreïsche Drietallen krijgen:

(3.5) Stelling (Euclides). *Als* (x, y, z) *een primitief* PD *is met* x *oneven, dan zijn er getallen* $m, n \in \mathbb{Z}_{>0}$ *met* $m > n$, *en* $\gcd(m, n) = 1$ *en* $m + n$ *oneven zodat*

$$x = m^2 - n^2, \quad y = 2m{\cdot}n, \quad z = m^2 + n^2.$$

We zien dat de stelling alle primitieve PDen geeft; hieruit kunnen alle Pythagoreïsche drietallen bepaald worden.
Kijk naar deze tabel, bij voorbeeld naar de laatste kolom; is er iets dat opvalt aan deze getallen?

(3.6) Een paar voorbeelden:

n	m	x	y	z
1	2	3	4	5
1	4	15	8	17
2	3	5	12	13
1	6	35	12	37
2	5	21	20	29
3	4	7	24	25
1	8	63	16	65
2	7	45	28	53
4	5	9	40	41
1	10	99	20	101
2	9	77	36	85
3	8	55	48	73
4	7	33	56	65
5	6	11	60	61
1	12	143	24	145
2	11	117	44	125
3	10	91	60	109
4	9	65	72	97
5	8	39	80	89
6	7	13	84	85
etc.	etc.	etc.	etc.	etc.

Welke priemgetallen treden op als delers van z?
Komt een waarde voor z meerdere malen voor in deze tabel?

We verwijzen naar § 9 voor 3 verschillende bewijzen van Stelling (3.5).

(3.7) In (3.2) zagen we een methode om oneindig veel pPDen te construeren:

$$x^2 = 2\ell + 1, \quad y = j, \quad z = j + 1, \qquad j = 2\ell^2 + 2\ell.$$

In de notatie van Steling (3.5) hebben we daar verkregen: $m = \ell + 1$, en $n = \ell$, en $j = 2mn$. Dit geeft deze pPDen een plaats in de classificatie zoals gegeven in Stelling (3.5). We zien dat we lang niet all oplossingen op deze manier verkregen hebben.

(3.8) Amusant vraagstuk. We maken precies wat we bedoelen met "lang niet alle oplossingen". *Voor* $M \in \mathbb{Z}$ *zij* T_M *het aantal* pPDen *zoals geconstrueerd in* (3.7) *met* $m+n = 2\ell+1 \leq M$. *Zij* N_M *het aantal* pPDen *zoals geconstuerd* (3.5) *met* $m+n \leq M$. *Laat zien dat de fractie* T_M/N_M *als limiet* 0 *heeft voor* $M \to \infty$:

$$\lim_{M\to\infty} \frac{T_M}{N_M} = 0.$$

4 Vraag A

We gaan nu de theorie van de PDen gebruiken, zoals beschreven in §3, in het bijzonder in Stelling (3.5). Als $\alpha^2 + \beta^2 = \gamma^2$ een driehoek beschrijft met oppervlak $\alpha\beta/2$ dan is voor elke $\rho > 0$ een driehoek $(\rho\alpha)^2 + (\rho\beta)^2 = (\rho\gamma)^2$, met oppervlak $\rho^2\alpha\beta/2$. Als N een CG is en $D \in \mathbb{Z}_{>0}$ dan is D^2N en omgekeerd. Daarom is het voldoende om alleen maar kwadaraatvrije congruente getallen te beschouwen: pCG.

We maken een lijst van alle PDen (x, y, z); voor elk zo'n drietal kiezen we de grootste $D \in \mathbb{Z}_{>0}$ zodat D^2 een deler is van $xy/2$. Dan is

$$\alpha := x/D, \quad \beta := y/D, \quad \gamma := z/D \quad \text{een presentatie van het pCG} \quad N := \alpha\beta/2 = xy/(2D^2).$$

(4.1) Conclusie (een positief antwoord op vraag **A**). *Er is een (oneindige) lijst waar alle* pCGen *in voorkomen.*

n	m	x	y	z	D	N	
1	2	3	4	5	1	6	
1	4	15	8	17	2	15	
2	3	5	12	13	1	30	
1	6	35	12	37	1	210	$x = m^2 - n^2$
2	5	21	20	29	1	210	$y = 2mn$
3	4	7	24	25	2	21	$z = m^2 + n^2$
1	8	63	16	65	6	14	
2	7	45	28	53	3	70	
4	5	9	40	41	6	5	
1	10	99	20	101	3	110	$ND^2 = (m^2 - n^2)mn$
2	9	77	36	85	3	154	
3	8	55	48	73	2	330	
4	7	33	56	65	2	231	
5	6	11	60	61	1	330	
1	12	143	24	145	2	429	
2	11	117	44	125	3	286	
3	10	91	60	109	1	2730	
4	9	65	72	97	6	65	
5	8	39	80	89	2	390	
6	7	13	84	85	1	546	
etc.	etc.	etc.	etc.	etc.	etc.	etc.	

We beginnen met n en m in de linker kolommen zodanig dat

$$0 < n < m, \quad \gcd(m, n) = 1, \quad m + n \quad \textit{is oneven.}$$

Kies voor D^2, het grootste kwadraat dat $ab/2 = (m^2 - n^2)\cdot m\cdot n$ deelt. schrijf

$$\alpha = a/D, \quad \beta = b/D, \quad \gamma = c/D \quad and \quad N = \alpha\beta/2 = (m^2 - n^2)\cdot m\cdot n/D^2;$$

dit is een pCG.

Omgekeerd als N voldoet aan de eigenschappen in Definitie II. Kies het kleinste positieve getal $d \in \mathbb{Q}_{>0}$ met:

$$x := d\cdot\alpha, \quad y := d\cdot\beta, x := d\cdot\gamma \in \mathbb{Z}_{>0}.$$

Dan is (x, y, z) en pPD. We zien dat elk pCG inderdaad voorkomt in de bovenstaande lijst.

Merk op dat het CGP voor N vertaald is in het vinden van $m > n$ en D zodat

$$N\cdot D^2 = m\cdot n\cdot(m^2 - n^2).$$

We zullen ook zeggen dat $((m, n), D, N)$ een presentatie is van het pCG N. Dit bewijst de conclusie. QED

(4.2) Opmerking *Er zijn oneindig veel* pCGen.
Bewijs. Voor elk priemgetal p kiezen we $m, n \in \mathbb{Z}$ met $m + n = p$; dit geeft een pCG door:

$$m\cdot n\cdot(m^2 - n^2) = D^2\cdot N.$$

Voor $i, j \in \mathbb{Z}$ met $i + j < p$ en $ji(j^2 - i^2) = d^2N'$ zien we dat $N \neq N'$ (want N is wel, en N' is niet door p deelbaar). Bij elk nieuw priemgetal $p = m + n$ komen er weer nieuwe pCGen die nog niet eerder voorkwamen in de lijst zoals boven. QED

5 Vraag B: een vermoeden

Het is verrassend te zien dat een antwoord op vraag **B** nog steeds onbekend is. Dat betekent dat in veel gevallen we ad hoc methodes moeten toepassen om te beslissen of en een gegeven getal N congruent is. Abstracte methodes zijn ontwikkeld, en op die manier zijn sommige gevallen opgelost. Sommige gevallen zijn beslist door middel van zeer snelle rekentechnieken.

In 1983 formuleerde Tunnel een vermoeden dat precies formuleert van welke getallen we *verwachten* dat ze een CG zijn. Het vermoeden is verrassend. Dit is niet iets wat je zou concluderen als je een (lange) lijst maakt van CGen en die consulteert. De wiskunde achter dit vermoeden is diep en is gebaseerd op een van de meest interessante en onopgeloste problemen van de 20-ste eeuw. Hier is het vermoeden van Tunnell.

Zij $N \in \mathbb{Z}_{>0}$ kwadraatvrij. Onderstel allereerst dat N *oneven* is. Definiëer

$$L(N) := \#\left(\{(x, y, z) \in \mathbb{Z}^3 \mid N = 2x^2 + y^2 + 32z^2\}\right)$$

en schrijf

$$R(N) := \frac{1}{2}\#\left(\{(x, y, z) \in \mathbb{Z}^3 \mid N = 2x^2 + y^2 + 8z^2\}\right).$$

Voor $N \in \mathbb{Z}_{>0}$ kwadraatvrij en N *even* schrijven we

$$L(N) := \#\left(\{(x,y,z) \in \mathbb{Z} \mid \frac{N}{2} = 4x^2 + y^2 + 32z^2\}\right)$$

en

$$R(N) := \frac{1}{2}\#\left(\{(x,y,z) \in \mathbb{Z} \mid \frac{N}{2} = 4x^2 + y^2 + 8z^2\}\right).$$

Zie [22], pag. 221.

Bij gegeven N is het meestal eenvoudig om $L(N)$ en $R(N)$ te berekenen.

(5.1) Stelling (Coates and Wiles). *Zij N een* pCG. *Dan is $L(N) = R(N)$.*
(Dit berust op diepe kennis. We geven geen bewijs.) Zie [10].

(5.2) Vermoeden (Tunnell). *Zij N een kwadraatvrij positief geheel getal. Als $L(N) = R(N)$ dan (?) is N een* pCG.
(De uitleg hoe je aan een dergelijk vermoeden komt is moeilijk. We gaan hier verder niet op in.) Zie [35], zie [22], IV.4.

Een toepassing. Kies $N = 1$. We zien: $L(N) = 2$ en $R(N) = 1$; ja, want in beide gevallen zijn de enige oplossingen $x = 0,\ y = \pm 1,\ z = 0$. De stelling impliceert dat $N = 1$ niet een CG is. Merk op dat deze stelling van Coates and Wiles een bewijs geeft van dit feit, eeuwen eerder reeds op een meer elementaire manier bewezen door Fermat.

Een toepassing. Kies $N = 157$. Laat zien dat $L(N) = 0 = R(N)$. Als het vermoeden juist zou zijn, dan kunnen we concluderen dat $N = 157$ een CG is. Dit is ook juist, zoals een berekening van D. Zagier aantoonde, zie [22], pag. 5.

Merk op dat het criterium zoals Tunnell dat voorstelt inderdaad effectief is. Bij gegeven N hoeven we alleen maar drietallen (x,y,z) te beschouwen met $\mid x \mid < \sqrt{N}/2, \quad \mid y \mid \leq \sqrt{N}$ and $\mid z \mid < \sqrt{N/8}$. Heel weinig berekeningen zijn nodig, and dat aantal kan expliciet begrensd worden in termen van N.
Conclusie. Als het vermoeden van Tunnell juist is, dan heeft Vraag **B** een bevestigend antwoord.

(5.3) P. Monsky bewees dat voor elk *priemgetal* N met $N \equiv 5 \pmod 8$ of $N \equiv 7 \pmod 8$ een CG is; zie [25]. Dit geeft een bewijs dat gevallen als $N = 13$ en $N = 157$ inderdaad CGen zijn, zonder berekeningen uit te voeren, maar door zuiver denkwerk.

Dit bewijst dat er oneindig veel CGen bestaan: gebruik het bewijs van Monsky, en gebruik de stelling van Dirichlet die zegt dat in de rekenkundige rij $\{5 + 8i \mid i \in \mathbb{Z}_{>0}\}$ er oneindig veel priemgetallen zijn. Maar er is ook een elementair bewijs voor het bestaan van oneindig veel pCGen, zie (0.4).

Een van de meest belangrijke vermoedens in de moderne wiskunde is die uitgesproken door Birch en Swinnerton-Dyer, zie [7]. Dit is een van de Clay Mathematics Institute Millenium problems, waarvoor \$ 1,000,000 is uitgeloofd voor een oplossing. Zie
http://www.claymath.org/millennium/

http://planetmath.org/encyclopedia/BirchAndSwinnertonDyerConjecture.html
http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/BSD.pdf
Als dat vermoeden waar is, dan volgt het vermoeden van Tunnell, en dus zou een positief antwoord op vraag **B** volgen. Dit is typerend voor de moderne wiskunde. Bij het bestuderen van een vraag, formuleren we een veel algemenere vraag of mogelijk theorie, die de wiskundige structuur achter die vraag formuleert. We zien dat dit vaak tot onverwachte ontwikkelingen leidt.

(5.4) Opmerking. We kunnen Vraag B preciseren:
Vraag B'. *Is er een effectieve grens op een presentatie om te beslissen of voor een gegeven getal N al of niet een presentatie bestaat die bewijst dat N al of niet congruent is?*
Bij mijn weten is dit onopgelost, en bestaat er ook geen vermoeden die dit precies maakt. Het vermoeden (5.2) zou een effectieve manier geven om te beslissen of een gegeven N congruent is. Maar daaruit volgt nog niet hoe we effectief een presentatie van een congruent getal maken. We zien aan voorbeelden als $N = 157$ of $N = 997$ dat deze getallen wel congruent zijn, maar dat presentaties heel groot zijn. Is er een grens (uitgedrukt in N) op de grootte (bv. van z of van D) van een eventuele presentatie?

6 Vraag C: een mysterieus mechanisme

We gaan Vraag **C** beantwoorden. We beginnen met een voorbeeld, dat een speciaal geval zal zijn van algemenere formules later.

(6.1) We weten dat $3^2 + 4^2 = 5^2$; dus is $(3, 4, 5)$ een PD, en we zien dat $xy/2 = 3{\cdot}4/2 = 6$ een CG is (en we nemen $D = 1$).

Kies $A = 49, B = 1200, C = 1201$. Merk op: $49^2 = 2401$. Dan geldt

$$1201^2 = 1200^2 + 2.1200 + 1 = 1200^2 + 49^2.$$

Kies $E = 70$. Dan is $AB/(2E^2) = 49 \times 1200/(7^2 \times 10^2 \times 2) = 6$. We hebben een nieuwe presentatie van het congruente getal $N = 6$ geproduceerd. Merk op dat $D = 1 < E = 70$.

Hier is nog een voorbeeld. We weten dat $((n = 4, m = 5), D = 2, 5)$ een presentatie is van het congruente getal 5. We zien dat $(V = 720, U = 1681, E = 747348)$,

$$720 \times 1681 \times (1681 - 720) \times (1681 + 720) = 5 \times 747348^2,$$

en we hebben een andere presentatie van $N = 5$. merk op dat $D = 2 < E = 747348$.

(6.2) Een mysterieus mechanisme. Deze voorbeelden zijn bijzondere gevallen van de volgende algemene formules.

Veronderstel $m > n$ zijn als in (3.5); kies D zodat $N = m{\cdot}n{\cdot}(m^2 - n^2)/D^2$ een pCG is, dat wil zeggen dat $((m, n), D, N)$ een presentatie is van N:

$$m{\cdot}n{\cdot}(m^2 - n^2) \quad = D^2 \cdot N, \quad xy = 2ND^2.$$

Kies

$$U := z^2 = (m^2 + n^2)^2, \quad V = 2xy = 2(m^2 - n^2)2mn.$$

Dan geldt:

$$U \cdot V \cdot (U-V) \cdot (U+V) = z^2 \cdot 2xy \cdot (y^2+y^2-2xy) \cdot (x^2+y^2+2xy) =$$
$$= 2xy \cdot z^2 \cdot (x-y)^2 \cdot (x+y)^2 =$$
$$= \{2 \cdot z \cdot D \cdot (x-y) \cdot (x+y)\}^2 \cdot N.$$

Conclusie. Als we beginnen met een presentatie $((m,n),D,N)$ dan geven deze formules een nieuwe presentatie van N door middel van

$$U = c^2, \quad V = 2ab, \quad E = |\{2 \cdot z \cdot D \cdot (x-y) \cdot (x+y)\}|.$$

Merk op dat $D < E$.

(6.3) Gevolg (een antwoord op Vraag C). *Voor elk congruent getal is het aantal presentaties oneindig.*
Inderdaad, deze formules construeren uit elke presentatie een nieuwe presentatie met veel grotere getallen $D < E$. Dit proces kan oneindig vaak herhaald worden, en steeds krijgen we nieuwe presentaties. QED

Opmerking. We moeten in het algemeen wel erg ver in de lijst gaan om op deze manier weer een nieuwe presentatie te vinden. Daarom was dit verschijnsel ons nog niet opgevallen.

(6.4) Een andere formule. Uitgaande van een presentatie $(N,(a,b,c),D)$ vonden we een nieuwe presentatie voor hetzelfde CG. We vertalen dit met behulp van Lemma (1.4) in een formule die uit een realisatie een nieuwe vindt. Onderstel gegeven $N \in \mathbb{Z}_{>0}$ en

$$\delta \in \mathbb{Q}_{>0}, \quad \lambda, \xi \in \mathbb{Q}_{>0}: \quad \delta^2 + N = \lambda^2, \quad \delta^2 - N = \xi^2.$$

Definiëer:

$$\Delta = \frac{\delta^4 + N^2}{2\delta\lambda\xi}.$$

Dit geeft een realisatie van N, want:

$$\Delta \pm N = \frac{(\delta^4 \pm 2N\delta^2 - N^2)^2}{(2\delta\lambda\xi)^2}.$$

Ga na dat dit inderdaad juist is.

(6.5) Een voorbeeld. Voor $N = 6$ is er een realisatie:

$$\delta = \frac{5}{2}, \quad \delta^2 + 6 = \frac{7}{2}, \quad \delta^2 - 5 = \frac{1}{2}.$$

Voor

$$\Delta = \frac{1201}{140} \quad \text{geldt} \quad \Delta^2 + 6 = (\frac{1249}{140}), \quad \Delta^2 - 6 = (\frac{1151}{140}).$$

Controleer die op twee manieren: eerst via realisaties een nieuwe PD construeren, daarna via de formule in (6.4) opnieuw deze resultaten berekenen.

(6.6) Een voorbeeld. Voor $N = 5$ is er een realisatie:

$$\delta = \frac{41}{12}, \quad \delta^2 + 5 = \frac{49}{12}, \quad \delta^2 - 5 = \frac{31}{12}.$$

Bewijs:

$$\Delta = \frac{3344161}{24 \times 41 \times 49 \times 31}$$

is ook een realisatie van $N = 5$.
(Hint: probeer $4728001/(24 \times 41 \times 49 \times 31)$ en $113279/(24 \times 41 \times 49 \times 31)$.

(6.7) Hoe kunnen we deze vreemde formules vinden? We komen daarop terug in § 10. Maar laten we nu vast zeggen dat het principe gebaseerd is op een meetkundige interpretatie van het begrip CG. De methode voor het vinden van een dergelijk methode staat eigenlijk al bij Diophantus. Het vinden van de formules hierboven, lag volledig binnen het bereik van bij voorbeeld Diophantus. Maar we zien deze pas door de meetkundige interpretatie, die in de 20-ste eeuw duidelijk werd. We komen hier nog uitvoerig op terug, zie (6.2), zie § 10.

7 Een paar historische opmerkingen.

(7.1) Het probleem van de PDen is klassiek, en volledig begrepen. Zie § 3.

(7.2) We bestuderen het probleem, het vinden van "congruente getallen", dat voor de eerste keer te vinden is in een anoniem Arabisch manuscript geschreven voor 972. Fibonacci bestudeerde in 1225 dit probleem. Verschillende gevallen werden bestuderd door Fermat. Het is mogelijk dat Fermat, gestimuleerd door zijn oplossing van het geval $N = 2$, zijn FLT (Fermat's Last Theorem) formuleerde.

Veel onderzoek is verricht. Veel gevallen zijn nu beslist. **Maar, dit probleem uit de 10-de eeuw, is in wezen in de 20-eeuw nog steeds onopgelost.** We geven hier en in de voordracht een uittreksel uit [27].

(7.3) In de "Arithmetica" van Diophantus vinden we in V.9.III.22, zie ook II.9.II.20, een probleem geformuleerd als het van oplossingen van de twee vergelijkingen $s^2 + w = u^2$ en $s^2 - w = v^2$ in 4 variabelen. Diophantus merkt ook het verband op met rechthoekige driehoeken. We zouden dus kunnen zeggen dat het probleem van de congruente getallen, CGP, afkomstig is van Diophantus. De vraag naar oplossingen in de gehele getallen leidt tot het probleem van de congruente getallen. Maar Diophantus komt niet expliciet met de vraag welke oplossingen tot een bepaalde waarde van w leiden. Daarom ben ik geneigd om te stellen dat het CGP voor de eerste keer in de geschiedenis genoemd wordt in de 10-de eeuwse Arabische wiskunde: het lijkt dat in het anonieme Arabische manuscript er voor het eerst een keuze $N = w \in \mathbb{Z}$ bestudeerd wordt en bovendien worden Pythagoreïsche drietallen gebruikt om voorbeelden van CGen te construeren

Is dit probleem afkomstig uit het oude India? Ik kan daar geen aanwijzingen voor vinden in [12], of in [29].

Het voorbeeld $N = 5$ komt voor in het Arabische manuscript (in totaal geeft dat manuscript 30 congruente getallen), zie [1], zie pp. 256/257, maar ook in en artikel van Abu Jafar Muhammad ibn al-Hasan Al-Khazin, zie [31], page 83, zie [3]. Beide manuscripten zijn

beschreven in de 10-de eeuw. Of het voorbeeld $N = 5$ een congruent getal is werd rond 1220 door Johann Panormitanus di Palermo aan Leonardo di Pisa (Fibonacci) gevraagd, zie [13], page 460. Fibonacci vond dezelfde oplossing als hierboven; dit was voor hem een begin voor zijn boek "Liber Quadratorum" (1225). Het is waarschijnlijk dat Fibonacci de eerder vermelde Arabsiche manuscripten niet kende.

Merk op dat werk van Diophantus reeds bekend was in die tijd in de Arabische wiskunde, bij voorbeeld zie [3], page 136. Maar we weten niet of de auteur van het anonieme manuscript de *Arithmetica* van Diophantus kende ; zie [13], pp. 459/460, en zie [31], pp. 9/10. We weten dat Al-Khazin werk van Diophantus kende, maar in dezelfde vorm als wat we nu tot onze beschikking hebben?

(7.4) Over methodes in het anonieme Arabische manuscript merkt Woepcke op in [1] on page 252: "C'est en effet la meilleure méthode possible ... les divers moyens particuliers qui permettent dans certains cas de reconnaître immédiatement si un nombre donné est ou n'est pas nombre congruent." We kunnen de vraag stellen wat de "best mogelijk methode" is (het kan best zin dat er later betere gevonden worden). Maar mijn bezwaar richt zich vooral op "reconnaître immédiatement ... ou n'est ...": elk eindig deel van de lijst geeft niet een beslissing of $N = 1$ een CG is; voor oneindig veel getallen is het nu nog steeds niet bekend of ze een CG zijn; zo "onmiddellijk" is die methode dus niet.

Pierre de Fermat bewijst dat $N = 1$ en $N = 2$ niet CGen zijn. Verder lijkt het waarschijnlijk dat dit hem inspireerde tot het vermoeden FLT.

Later zijn er heel veel deelresultaten bereikt, zijn er heel veel artikelen over dit probleem geschreven. Ik zal hiervan geen overzicht geven. Het blijkt dat je met elementaire methoden wel wat gevallen aankunt, maar dat een oplossing van het echte probleem buiten bereik blijft. Methoden uit de 20-ste eeuw wierpen een nieuw licht op deze vragen. Een interpretatie via "elliptische krommen" geeft toegang tot het probleem, zie § 10. Daaruit komt een "eenvoudig" antwoord op Vraag C.

Uit een lijst van CGen is het niet zo gemakkelijk te zien wat een effectief criterium zou kunnen zijn. Probeer het zelf maar eens: neem de resultaten die van alle getallen kleiner dan 1000 vermelden welke de CGen zijn, en probeer daaruit een criterium te formuleren.

Het verband met elliptische krommen en speciaal met het vermoeden van Birch en Swinnerton-Dyer werpt een heel ander licht op de zaak, zie [7] en [22], IV.4. Voor het eerst in de geschiedenis is het probleem van de CGen niet meer een geïsoleerde vraag. Deze moderne methoden zijn niet elementair. Bovendien, verder dan een vermoeden zijn we nog niet gekomen.

8 Appendix I: ontbinden in factoren

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

(8.1) 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 betaat 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:

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

(8.2) 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

(8.3) 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.

(8.4) 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.

(8.5) 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.

(8.6) 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

(8.7) 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 $c \not| \, a$.
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

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

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

(8.8) 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 (8.6) 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 (8.3). 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 (8.3)

9 Appendix II: Bewijzen van (3.5)

In deze paragraaf geven we 3 verschillende bewijzen van Stelling (3.5), gebruikmakend van:
elementaire getaltheorie,
meetkunde, en
algebraïsche getaltheorie.

(9.1) Opmerking. *Als $m, n \in \mathbb{Z}_{>0}$ met $m > n$, en $\gcd(m, n) = 1$ en $m + n$ oneven dan is $(m^2 - n^2, 2mn, m^2 + n^2)$ primitief.*
Bewijs. Uit "$m + n$ is oneven" volgt dat $m^2 - n^2 = (m + n)(m - n)$ oneven is; dus is 2 niet een gemeenschappelijk factor van $m^2 - n^2$ en $2mn$. Stel $p > 2$ is een priemdeler van $m^2 - n^2$ en van $2mn$; dan is het ook een deler van $m^2 + n^2$; dan is het ook een priemdeler van m^2, dus van m, ook een priemdeler van n^2 dus van n, tegenspraak. QED

(9.2) Bewijs I van (3.5)**: Elementaire getaltheorie.**
Zie bv. zie bv. [19], Chapter XIII.
Stel $x^2 + y^2 = z^2$ met x oneven. Dan geldt

$$(\frac{y}{2})^2 \quad = \quad \frac{z + x}{2} \cdot \frac{z - x}{2}.$$

Uit de gegevens volgt dat $y/2, \ \ (z + x)/2, \ \ (z - x)/2 \in \mathbb{Z}_{>0}$. Ga na dat ook

$$\gcd(\frac{z + x}{2} \ , \ \frac{z - x}{2}) = 1.$$

Als p een priemgetal is dat $y/2$ deelt en $u \in \mathbb{Z}_{>0}$ zo dat p^u deelt $b/2$ en p^{u+1} deelt niet $b/2$ is p een deler van $(z + x)/2$ óf van $(z - x)/2$ (en niet van allebei); in het eerste geval is p^{2u}

precies de macht van p die $(z+x)/2$ deelt. We concluderen: zowel $(z+x)/2$ als $(z-x)/2$ is een kwadraat van een positief geheel getal. We schrijven

$$m^2 := \frac{z+x}{2} \quad \text{en} \quad n^2 := \frac{z-x}{2}.$$

Ga na dat $\text{ggd}(m,n) = 1$, en dat $m+n$ oneven is. Conclusie:

$$\{(a,b,c) \mid \text{pPD}, \quad 2|b\} \xleftrightarrow{\sim} \{(m,n) \mid 0 < n < m, \quad \text{ggd}(m,n) = 1, \quad m+n \ \text{ oneven}\}.$$

Dit is het eerste bewijs van de stelling (3.5).

Schrijf alle stappen zorgvuldig uit.

(9.3) Bewijs II van (3.5)**: Meetkunde.**
Zij (x,y,z) een PD (niet noodzakelijk primitief); we schrijven

$$u := \frac{x}{z}, \quad \text{en} \quad v := \frac{y}{z},$$

en we zien dat geldt

$$u^2 + v^2 = 1;$$

met ander woorden, het "punt"(u,v) ligt op de cirkel C gegeven door deze vergelijking. We vragen ons omgekeerd af, welke punten op deze cirkel hebben coördinaten in $\mathbb{Q}$? De meetkunde laat ons zien hoe we dat kunnen beslissen. Neem een punt of de cirkel, we kiezen $R := (-1,0)$, en laat het een punt $S_t := (0,t)$ lopen over de V-as. (Later zullen we bovendien veronderstellen dat $0 < t < 1$.) Verbind de punten R en S_t; dat geeft een lijn met de vergelijking

$$L_t : \quad V = t(U+1)$$

(ga na); snijdt deze lijn L_t met de cirkel C; dat geeft twee snijpunten (allicht), en wel:

$$L_t \bigcap C \quad = \quad \{R, P_t\} \quad \text{met} \quad P_t = (u = \frac{1-t^2}{1+t^2}, \quad v = \frac{2t}{1+t^2})$$

(ga na). Omgekeerd kunnen uit een punt $P \in C$ met $P \neq R$ de verbindingslijn L bepalen, en we krijgen: als $P = (u,v)$, met $u^2 + v^2 = 1$, dan is

$$t = \frac{v}{u+1}, \quad P = P_t.$$

We zien

$$t \in \mathbb{Q} \quad \Longleftrightarrow \quad P_t \in (\mathbb{Q} \times \mathbb{Q}) \cap C.$$

Bovendien zien we: $0 < t < 1 \Longleftrightarrow P_t \in \mathbb{Q}_{>0} \times \mathbb{Q}_{>0}$ (ga na; kun je dat "meetkundig inzien"?). We schrijven deze transformaties uit:

$$(x,y,z) \quad \mapsto \quad (u = \frac{x}{z}, \quad v = \frac{y}{z}) \quad \mapsto \quad t := \frac{u}{v+1} = \frac{y}{x+z},$$

en

$$0 < t = \frac{N}{M} \mapsto (u = \frac{1-t^2}{1+t^2}, \quad v = \frac{2t}{1+t^2}) \quad \mapsto (x = M^2 - N^2, y = 2MN, z = M^2 + N^2).$$

We zien dat

$$\{t \in \mathbb{Q} \mid 0 < t < 1\} \overset{\sim}{\longleftrightarrow} \{P = (u, v) \in C \mid x, y \in \mathbb{Q}_{>0}\}$$

(ga na).

We gebruiken deze formules om het bewijs af te maken. Als $(u, v) \in C$ dan ook $(v, u) \in C$. Als (x, y, z) een PD is, dan geldt ook $y^2 + x^2 = z^2$. Deze dubbelzinnigheid, en het mechanisme om uit $(u, v) \in C(\mathbb{Q})$ een pPD te construeren analyseren we teneinde het bewijs af te maken.

Waarschuwing. De breuk $t = 1/3$ geeft $(x = 8, y = 6, z = 10)$; we zien dat $t = N/M$ met $\text{ggd}(M, N) = 1$ niet garandeert dat $(x = M^2 - N^2, y = 2MN, z = M^2 + N^2)$ een pPD is. Als we $(x = 8, y = 6, z = 10)$ vereenvoudigen tot $(4, 3, 5)$ dan krijgen we een pPD, maar met $x = 4$ even. Nemen we echter $0 < t = n/m < 1$ met $\text{ggd}(m, n) = 1$ en $m + n$ oneven dan is het bijbehorende PD $(x = m^2 - m^2, y = 2mn, z = m^2 + n^2)$. We zien hoe we uit de meetkunde weer terugkeren tot de getaltheorie:

Onder de correspondentie

$$t = \frac{u}{v+1} = \frac{y}{x+z} \quad \text{krijgen we} \quad t' := \frac{1-t}{1+t} = \frac{v}{u+1} = \frac{x}{y+z}$$

(ga na); merk op: $t \mapsto t'$ correspondeert precies met het verwisselen van x en y, met het verwisselen van u en v. Als $0 < t = N/M < 1$ met $\text{ggd}(M, N) = 1$ en $M + N$ even (dus M en N oneven) dan heeft $t' = (1 - t)(1 + t) = (M - N)/(M + N) = n/m$ met $\text{ggd}(m, n) = 1$ de eigenschap dat $0 < t' < 1$ en $m + n$ is oneven. In deze situatie is $M + N$ oneven dan en slechts dan als $m + n$ even is (ga na). We zien: bij gegeven $t \in \mathbb{Q}$ met $0 < t < 1$ geeft P_t een pPD met x oneven óf $t' := (1 - t)/(1 + t)$ heeft deze eigenschap.

QED Stelling (3.5)

Opmerking: via de meetkunde zien we direct dat er oneindig veel PD zijn (want er zijn oneindig veel t met $t \in \mathbb{Q}$ en $0 < t < 1$. Het bewijs zou gegeven kunnen worden met de formules hierboven zonder meetkundige motivatie of achtergrond.

Zoals zo vaak: de meetkunde suggereert een prachtig algebraïsch bewijs.

(9.4) Bewijs III van (3.5)**: Algebraïsche getaltheorie.***
We geven een bewijs, waarin we methoden gebruiken die niet helemaal elementair zijn. In dit bewijs gebruiken we enkele begrippen uit de algebra. We merken eerst op dat $a^2 + b^2 = c^2$ in $\mathbb{C}$ gefactoriseerd kan worden als:

$$(a + b{\cdot}\sqrt{-1})(a - b{\cdot}\sqrt{-1}) = c^2.$$

We gaan nu eigenschappen onderzoeken van getallen zoals die aan de linkerkant voorkomen.

(9.5) We zulen het begrip "ring" gebruiken. Een voorbeeld daarvan is $\mathbb{Z}$. In en ring is er een element 0, een element 1, een commutatieve optelling en een vermenigvuldiging (die in alle voorbeelden die we gebruiken ook commutatief zal zijn). Voor deze operaties gelden gebruikelijke axioma's, zoals $(a + b) + c = a + (b + c)$, en $a(b + c) = ab + ac$, en $a + 0 = a$ en $b{\cdot}1 = b$ etc. Merk op dat in het algemeen er niet van elk element een inverse in $\mathbb{Z}$ bestaat. De verzameling $\mathbb{Q}$ van rationale getallen is ook een voorbeeld van een ring; daarin geldt dat elk element ongelijk aan nul een inverse heeft (en een dergelijk systeem heet een lichaam).

(9.6) De gehele getallen van Gauss.* Beschouw:

$$R = \mathbb{Z}[\sqrt{-1}] := \{x + y{\cdot}i \mid x, y \in \mathbb{Z}\},$$

waar het symbool i gebruikt wordt als $i = \sqrt{-1}$. In deze verzameling kunnen we optellen, aftrekken en vermenigvuldigen, waar de regel $i^2 = -1$ gebruikt wordt. Het getal $0 = 0 + 0{\cdot}i$ treedt als "nul" op, en het getal $1 = 1 + 0{\cdot}i$ treedt als "een" op. Met deze operaties is dit een ring, die wel de "*Ring van gehele getallen van Gauss*" genoemd wordt. Deling is niet in alle gevallen mogelijk, b.v. is $i/2$ niet een element van $R = \mathbb{Z}[\sqrt{-1}]$. We bepalen eerst de elementen die wel een inverse hebben in deze ring: de verzameling $\{1, +i, -1, -i\}$ is de verzameling van de "eenheden", d.w.z. de elementen die een inverse hebben. Hoe bewijzen we zoiets? Neem

$$N : R = \mathbb{Z}[\sqrt{-1}] \longrightarrow \mathbb{Z}, \quad N(x + y{\cdot}i) := x^2 + y^2,$$

de "norm-afbeelding". Het is duidelijk dat deze verwisselt met $\times$. Als $u, z \in R$ met $u{\cdot}z = 1$ dan geldt $N(u){\cdot}N(z) = 1$. Ga na:

$$N(z) = 1 \quad \Longleftrightarrow \quad z \in \{1, +i, -1, -i\}.$$

We zeggen dat een element $z \in R$ *irreducibel* is, als z niet een eenheid is, en als $z = u{\cdot}v$ impliceert dat óf u óf v een eenheid is. Enkele voorbeelden: $1 + i$ is irreducibel, alhoewel $1 + i = i{\cdot}(1 - i)$. We zien dat $13 = (2 + 3i)(2 - 3i)$, en concludeer dat $13 \in R$ niet ireducibel in R is. Is $7 \in R$ irreducibel? Is $1 - 5i \in R$ irreducibel?

(9.7) De getallen -3 en $+3$ zijn irreducibel in $\mathbb{Z}$; we hebben de gewoonte aangenomen om alleen positieve irreducibele elementen in $\mathbb{Z}$ priemgetallen te noemen. Merk op dat $1 \in \mathbb{Z}$ niet een priemgetal is, niet irreducibel is (vroeger, ten tijde van Euler deed men dat wel). Een waarschuwing; beschouw $5 \in \mathbb{Z} \subset \mathbb{Z}[\sqrt{-1}] \subset \mathbb{C}$; we zien: 5 is irreducibel in $\mathbb{Z}$, reducibel in $\mathbb{Z}[\sqrt{-1}]$ en een eenheid in $\mathbb{C}$.

We gaan irreducibele elementen in R zoeken. Maar eerst een

(9.8) 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:

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

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.

(9.9) Feit. * *Neem de ring $R = \mathbb{Z}[\sqrt{-1}]$ van gehele getallen van Gauss. In deze ring geldt de eenduidigheid van ontbinding in irreducibele factoren op eenheden na, de eenheden zijn:*

$$\{1, +i, -1, -i\}.$$

De irreducibele elementen van deze ring zijn:

2: *Het element* $1+i \in \mathbb{Z}[i]$ *is een irreducibel element.*
N.B. merk op: $2 = -i \cdot (1+i)^2$.

3 mod 4**:** *Als* $p \in \mathbb{Z}$ *een priemgetal is met* $p \equiv 3 \pmod 4$ *dan is* p *irreducibel in* $\mathbb{Z}[i]$.

1 mod 4**:** *Als* $p \in \mathbb{Z}$ *een priemgetal is met* $p \equiv 1 \pmod 4$ *dan zijn er* $x, y \in \mathbb{Z}$ *met* $x^2+y^2 = p$,
dan is $(x+yi)(x-yi) = p$, *en* p *is reducibel in* $\mathbb{Z}[i]$.
Als $x, y \in \mathbb{Z}$ *met* $x^2+y^2 = p$, *waar* p *een priemgetal is in* $\mathbb{Z}$ *met* $p > 2$,
dan is met $p \equiv 1 \pmod 4$ *en* $x+yi$ *is irreducibel in* $\mathbb{Z}[i]$.

Het feit dat $\mathbb{Z}[i]$ een ontbindingsring is, is in bijna elk boek over algebra te vinden, zie bv. [30], pag. 297.

(9.10) Als in een ring eenduidigheid van factorontbinding heerst, dan wordt een irreducibel element ook wel een priemelement genoemd. Maar wees voorzichtig, $13 \in \mathbb{Z}$ is een priemgetal, 13 is een irreducibel element van $\mathbb{Z}$, maar is niet een irreducibel element van $R = \mathbb{Z}[\sqrt{-1}]$.

(9.11) Het feit dat een oneven priemgetal p met $p \equiv 1 \pmod 4$ te schrijven is als som van 2 kwadraten (en dan ook reducibel is in $\mathbb{Z}[\sqrt{-1}]$) werd door Fermat bewezen. Euler was de eerste die een bewijs ervan publiceerde. Er zijn allerlei bewijzen van deze stelling, zie bv. [32], Section 47; [8], 12.2; [19], 20.2 en 20.3.

(9.12) Opmerking. Probeer maar eens "statistiek" te bedrijven, neem een grens (bv $n_0 = 200$) en tel het aantal priemgetallen $p < n_0$ die 1 mod 4 zijn, en die 3 mod 4 zijn. Het valt al gauw op dat ruwweg de helft in de eerste en ruwweg de helft in de tweede categorie valt. Inderdaad, dat is een stelling: voor $n_0 \to$ bestaan die fracties, en ze zijn beide gelijk aan $1/2$, namelijk

$$\lim_{n_0 \to \infty} \frac{\#\{p < n_0 \mid p \text{ is priem}, \ p \equiv 1 \pmod 4\}}{\#\{p < n_0 \mid p \text{ is priem}\}} = \frac{1}{2}.$$

Dit is niet elementair.

(9.13) We nemen aan dat het bovengenoemde feit (9.9) bewezen is, en we geven het derde bewijs van (3.5).
We laten eerst zien:

Als (x, y, z) *een primitief PD is,*
en p *is een priemgetal dat* z *deelt, dan geldt:* $p \equiv 1 \pmod 4$.

We hebben al gezien dat voor een pPD de bijbehorende z oneven is, dus 2 is niet een deler van z. Veronderstel dat $p \equiv 3 \pmod 4$ een deler is van z. In R weten we dat die $p \in R$ irreducibel is, en we hebben de factorizatie

$$(x + y \cdot i)(x - y \cdot i) = z^2.$$

Merk op dat daaruit volgt dat deze p een deler is van $x + y \cdot i$ (en ook van $x - y \cdot i$). Hieruit concluderen we dat p een deler is van x en van y (ga na), tegenspraak met het feit dat (x, y, z) een primitieve PD is. We concluderen dat *alleen priemgetallen met* $p \equiv 1 \pmod 4$ *kunnen optreden als priemdelers van* z in en pPD. [Was dat al opgevallen aan de tabel?]

Zij p een priemgetal met $p \equiv 1 \pmod 4$. Dan bestaan er $a, b \in \mathbb{Z}$ zodanig dat

$$(a + b{\cdot}i)(a - b{\cdot}i) = p \quad \text{in} \quad R = \mathbb{Z}[i];$$

dat volgt uit het bovengenoemde feit; deze ontbinding is eenduidig op eenheden in R na, dat betekent dat de getallen x, y eenduidig zijn op teken en op volgorde na. Bij voorbeeld: $i{\cdot}(a + bi) = -b + ai$.

Stel (x, y, z) is een pPD, en laat

$$z = \prod_j \ p_j$$

een ontbinding in priemgetallen in $\mathbb{Z}$ zijn (een priemgetal kan meerdere malen voorkomen), en schrijf

$$z^2 = x^2 + y^2 = (x + y{\cdot}i)(x - y{\cdot}i).$$

Als p een priemgetal is dat z deelt, dan is $p \equiv 1 \pmod 4$, en we kunnen schrijven $p = (a + bi)(a - bi)$; deze beide factoren zijn onderling ondeelbaar in $\mathbb{Z}[i]$, en precies één ervan is een deler van $(x + y{\cdot}i)$ en de andere is een deler van $(x - y{\cdot}i)$. Door het kiezen van de goede tekens en de goede volgorde kunnen we schrijven

$$p_j \ = \ (a_j + b_j{\cdot}i)(a_j - b_j{\cdot}i), \quad a_j, b_j \in \mathbb{Z}$$

zo dat:

$$(x + y{\cdot}i) = \prod_j \ (a_j + b_j{\cdot}i)^2,$$

en

$$(x - y{\cdot}i) = \prod_j \ (a_j - b_j{\cdot}i)^2.$$

Uitvermenigvuldigen geeft een keuze voor m en n:

$$\prod_j \ (a_j + b_j{\cdot}i) =: m + n{\cdot}i.$$

Uit

$$(x + y{\cdot}i) = (m + n{\cdot}i)^2 = (m^2 - n^2) + 2mni$$

volgt wat we willen bewijzen. QED (3.5)

(9.14) Omgekeerd kunnen we PDen construeren met behulp van de gehele getallen van Gauss. Kies priemgetallen p_j, met $1 \leq j \leq t$, die alle $p \equiv 1 \pmod 4$ zijn. Schrijf elk van deze als $p_j \ = \ (a_j + b_j{\cdot}i)(a_j - b_j{\cdot}i)$, maar kies de tekens zo dat bij gelijke priemgetallen deze tekens gelijk zijn. We definiëren dan x en y met behulp van $(x + y{\cdot}i) = \prod_{j=1}^{t} \ (a_j + b_j{\cdot}i)^2$, en we krijgen een pPD. Op deze manier worden alle primitieve PD geconstrueerd. Hiermede eindigt het derde bewijs van Stelling (3.5).

(9.15) Enkele voorbeelden: Neem $z = 65 = 5 \times 13$. De factorizatie

$$65 = \{(1 - 2i)(2 + 3i)\} \ \times \ \{(1 + 2i)(2 - 3i)\} = (8 + i)(8 - i)$$

geeft $(8 + i)^2 = 63 + 16{\cdot}i$, en dit geeft

$$63^2 + 16^2 = 95^2.$$

De factorizatie

$$65 = \{(1-2i)(-2+3i)\} \times \{(1+2i)(-2-3i)\} = (4+7i)(4-7i),$$

en dit geeft

$$33^2 + 56^2 = 65^2.$$

(9.16) We zien dat $z = 25 = 5 \times 5$ alleen maar voorkomt als

$$25 = \{(1+2i)^2\} \times \{(1-2i)^2\}$$

en dit geeft

$$7^2 + 24^2 = 25^2.$$

Weliswaar heeft 25 twee priemfactoren, maar het verdelen van de factoren $(1 \pm 2i)$ kan maar op een manier gebeuren willen we een pPD krijgen.

(9.17) Neem $z = 1885 = 5 \times 13 \times 29$. Laat zien dat de factorizatie

$$(1-2i)(2+3i)(5+2i) = -34 + 27i$$

aanleiding geeft tot

$$27^2 + 34^2 = c,$$

de getallen $m = 34$ en $n = 27$ geven

$$427^2 + 1836^2 = 1885^2.$$

Andere verdelingen laten zien dat deze $z = 1885$ meerdere malen optreedt in een pPD, en wel precies vier keer.

(9.18) Voorbeeld. Neem $z = 29^3$. Uit het bewijs weten we dat dit voorkomt in een PD. Hoe vinden we x en y? Merk op dat $29 = 5^2 + 2^2 = (5+2i)(5-2i)$. We berekenen:

$$(5+2i)^3 = 125 + 3{\cdot}25{\cdot}2{\cdot}i + 3.{\cdot}5{\cdot}4i^2 + 8{\cdot}i^3 = 142 + 65i.$$

We zien:

$$65^2 + 142^2 = 29^3; \qquad (x = 142^2 - 65^2 = 15939, \quad y = 2{\cdot}142{\cdot}65 = 18460, \quad 29^3 = 24389)$$

is een PD.

(9.19) Opgave: Zij $z \in \mathbb{Z}$ een product van priemgetallen die alle $\equiv 1 \pmod 4$ zijn. Onderstel dat er t onderling verschillende priemfactoren in z zijn (een priemfactor kan meerdere keren optreden, maar telt in deze telling maar voor één). Dan komt z precies 2^{t-1} keer voor in de lijst van primitieve PDen.

Recreatie: zie [5], Chapter XIV.

(9.20) Opmerking. Waarom geven we verschillende bewijzen? Allereerst is het instructief om te zien dat dit probleem zich niet in een vakje laat duwen: we kunnen het op veel verschillende manieren benaderen. Gauss gaf in zijn leven 8 verschillende bewijzen van één stelling; we zijn in goed gezelschap.

10 Appendix III: Elliptische krommen

In deze paragraaf geven we een paar aanwijzingen die het vermoeden van Tunnell verklaren, en de oorsprong van het mysterieuze mechanisme aangeven. Begrippen in deze paragraaf zijn niet elementair.

We geven aan welke benadering gekozen kan worden voor het bestuderen van het probleem van de congruente getallen; een uitvoerige beschrijving vinden we in het boek [22].

Het centrale begrip daarin is dat van een "elliptische kromme". We geven geen complete definitie, laat staan een volledige behandeling, wel te vinden in [33], of in [21]. Ook in het bewijs van "Fermat's Laatste Stelling" speelt de theorie van elliptische krommen een cruciale rol. We zullen zien dat deze objecten een brug vormen tussen objecten uit de getaltheorie, en verschijnselen die in de meetkunde verklaard kunnen worden.

(10.1) Neem een veelterm $X^3 + AX + B$ met bij voorbeeld $A, B \in \mathbb{Q}$ zodanig dat deze veelterm 3 verschillende nulpunten heeft in $\mathbb{C}$. De vergelijking

$$Y^2 = X^3 + AX + B$$

definiëert een **elliptische kromme.** Eigenlijk moeten we niet alleen oplossingen in $\mathbb{Q}^2$ en in $\mathbb{C}^2$ beschouwen, maar ook oplossingen in een projectief vlak; dat komt erop neer dat we niet alleen $(x, y) \in \mathbb{C}^2$ beschouwen, maar ook één punt in oneindig (gelegen op elke verticale lijn); dat punt zullen we 0 noemen; in projectieve coördinaten: $(x, y) = (x : y : 1)$ en $0 = (0 : 1 : 0)$. Die verzameling

$$E = \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^3 + Ax + B\} \cup \{0\}$$

heeft heel mooie eigenschappen. Bij voorbeeld: elke lijn in het vlak heeft precies drie snijpunten met deze verzameling (geteld met multipliciteiten). Deze verzameling is een commutatieve groep met als optelling: voor $P, Q \in E$, verbind deze twee punten, neem het derde snijpunt S neem de verticale lijn door S en neem het snijpunt, noem dat $P + Q$:

$$P, Q, P + Q \in E, \quad \{P, Q, S\} \text{ en } \{S, 0, P + Q\} \text{ op een rechte.}$$

In deze constructie moet gepreciseerd worden wat we doen als $P = Q$, in dat geval is de "lijn die P en Q verbindt"de raaklijn aan E in $P = Q$, etc. Het punt $0 \in E$ (het punt in "oneindig") blijkt de eigenschap te hebben, dat de raaklijn daar de kromme E drievoudig snijdt (het punt 0 is een buigpunt van $E \subset \mathbb{P}^2$). Merk op dat voor $P = (x, y)$ geldt dat $-P = (x, -y)$. We zien zo in dat voor $P = (x, y) \in E$ geldt: $2P = 0 \Leftrightarrow y = 0$. De meeste van de axioma's voor een groep zijn gemakkelijk na te gaan, de associativiteit van deze "optelling" geeft enig werk.

We schrijven

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + Ax + B\} \cup \{0\}.$$

Als een lijn de kromme E snijdt in twee punten in $E(\mathbb{Q})$ dan kan die lijn gedefiniëerd worden door een vergelijking met coëfficienten in $\mathbb{Q}$, en het derde snijpunt heeft coördinaten in $\mathbb{Q}$. Zo zien we dat $E(\mathbb{Q})$ een groep is.

Teneinde het probleem welke getallen congruent zijn in verband te brengen met elliptische krommen gaan we terug naar een karakterisering van congruente getallen, die reeds door Fibonacci gegeven werd:

(10.2) Stelling: *Een positief geheel getal $N \in \mathbb{Z}_{>0}$ is een congruent getal dan en slechts dan als er een $x \in \mathbb{Q}_{>0}$ bestaat zo dat*

$$x - N, \quad x, \quad x + N \quad \textit{kwadraten zijn.}$$

Bewijs: Enerzijds hebben we

$$\alpha, \beta, \gamma \in \mathbb{Q}_{>0} \quad \text{met} \quad \alpha^2 + \beta^2 = \gamma^2, \quad \text{en} \quad \alpha \cdot \beta = 2N,$$

anderzijds een x zoals in de stelling. We laten zien dat het ene uit het andere volgt en omgekeerd. We nemen aan dat $0 < \alpha < \beta$.
$\Leftarrow$: Bij gegeven x construeren we:

$$\alpha := \sqrt{x+N} - \sqrt{x-N}, \quad \beta := \sqrt{x+N} + \sqrt{x-N}, \quad \gamma := 2\sqrt{x},$$

en we zien dat:

$$\alpha^2 + \beta^2 = \gamma^2, \quad \alpha \cdot \beta = 2N.$$

$\Rightarrow$: Bij gegeven α, β, γ als boven schrijven we:

$$x := (\frac{\gamma}{2})^2,$$

en we zien

$$\frac{\gamma^2}{4} \pm N = \frac{(\alpha \pm \beta)^2}{4}.$$

□

(10.3) AHA We zien: als

$$\alpha^2 + \beta^2 = \gamma^2, \quad \alpha \cdot \beta = 2N$$

dan geeft

$$x := \frac{\gamma^2}{4}, \quad y := \frac{(\beta^2 - \alpha^2) \cdot \gamma}{8}$$

dat

$$y^2 = x^3 - N^2 x.$$

Opmerking. We zien dat de presentatie (α, β, γ) van een congruent getal N een punt (x, y) op een elliptische kromme geeft, die gegeven wordt door "$Y^2 = X^3 - N^2X$". De formules die $(\alpha, \beta, \gamma) \mapsto (x, y)$ geven lijken niet erg doorzichtig. Maar de meetkunde is "duidelijk": de twee kwadratische vergelijkingen (N vast, α, β, γ "variabel") geven een kromme in een 3-dimensionale ruimte; algebraïsche meetkunde vertelt ons dat dit een kromme van geslacht één is, en die kan gegeven worden als vlakke kromme van graad 3, dat is wat de formules ons ook vertellen; zie ook (10.12).

Opmerking. Uit $\alpha^2 + \beta^2 = \gamma^2, \quad \alpha \cdot \beta = 2N$ kunnen we met behulp van $u := \gamma/2, \quad v := (\beta^2 - \alpha^2)/4$ afleiden:

$$u^4 - N^2 = v^2.$$

We krijgen zo de vergelijking van een vierde graads kromme met een "tacnode"(een keerpunt). Door middel van $x = u^2, \quad y = uv$ gaat deze vergelijking over in $y^2 = x^3 - N^2x$, m.a.w. deze kwadratische transformatie voert de singuliere 4-de graad kromme over in een niet-singuliere derde-graads kromme.

Een belangrijk detail. Zij E_N de elliptische kromme gegeven door $Y^2 = X^3 - N^2X$. Voor een punt $P \in E_N(\mathbb{Q})$, met $P = (x, y)$ (de coördinaten van P zijn rationale getallen) geldt dat de orde van P eindig is, P is een torsie-punt op E_N, desda $y = 0$ (en in dat geval is $x \in \{-N, 0, +N\}$), zie [22], I.2, Proposition 17 op pag. 44.

De vertaling van het probleem over congruente getallen als het bestaan van punten op een elliptische kromme wordt gegeven door:

(10.4) Feit (zie [22], Prop. 1 op pagina 4, en Prop. 19 op pp. 46/47): *Zij $N \in \mathbb{Z}_{>0}$. Beschouw de elliptische kromme E_N gedefiniëerd door de vergelijking*

$$E_N : \quad Y^2 = X \cdot (X - N) \cdot (X + N).$$

Dan is N een congruent getal dan en slecht dan als er bestaan

$$x, y \in \mathbb{Q} \ \ met \ \ y \neq 0 \ \ en \ \ (x, y) \in E_N(\mathbb{Q}).$$

(10.5) Uit de stelling van Mordell, zie [21], pag. 14, Th. 1.5, weten we dat $E_N(\mathbb{Q})$ en abelse groep is die *eindig voortgebracht* is; we kunnen schrijven $E_N(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$, waar $r \in \mathbb{Z}_{\geq 0}$ en T een eindige abelse groep is (waar r en T afhangen van de keuze van de elliptische kromme). Het blijkt dat in dit geval $\#(T) = 4$: deze eindige groep bestaat uit $\{0, (-N, 0), (0, 0), (+N, 0)\}$. De bovenstaande stelling zegt:

$$N \quad \text{is congruent} \quad \Longleftrightarrow \quad r(E_N) > 0.$$

(10.6) We geven een deel van het bewijs van (10.4). We schrijven $\alpha, \beta, \gamma \in \mathbb{Q}$ voor de lengtes van de zijden van een rechthoekige driehoek met oppervlakte $\alpha \cdot \beta/2 = N$, maar we kiezen de volgorde zo dat $\alpha < \beta < \gamma$ (dus $\alpha = a/D$, of $= b/D$ en $\beta = b/D$ of $= a/D$. De "vertaling"die we gaan gebruiken hebben we reeds gezien:

$$\{(\alpha, \beta, \gamma) \in \mathbb{Q}^3 \mid 0 < \alpha < \beta < \gamma, \ \ \alpha^2 + \beta^2 = \gamma^2\} \overset{\sim}{\leftrightarrow}$$

$$\overset{\sim}{\leftrightarrow} \{x \in \mathbb{Q} \mid x > 0, \ \ \text{zo dat} \ \ x, x - N, x + N \ \ \text{elk een kwadraat in } \mathbb{Q}_{>0} \text{ is}\},$$

door middel van:

$$(\alpha, \beta, \gamma) \mapsto (x = \frac{\gamma^2}{4}, y = \pm\frac{(\beta^2 - \alpha^2) \cdot \gamma}{8}),$$

en

$$x \mapsto (\alpha = \sqrt{x + N} - \sqrt{x - N}, \ \ \beta = \sqrt{x + N} + \sqrt{x - N}, \ \ \gamma = 2 \cdot \sqrt{x}).$$

Zo zien we: als N en congruent getal is, dan schrijven we

$$y = \pm\sqrt{x^3 - N^2x},$$

en dan zijn er $x, y \in \mathbb{Q}$ met $y \neq 0$ en $(x, y) \in E_N$. De omkering is niet geheel vanzelfsprekend, we verwijzen naar [22], pp. 46/47.

(10.7) We geven een kleine moeilijkheid in het bewijs aan. Neem $N = 5$. We zien dat

$$P = (x = -4, y = 6) \in E_N(\mathbb{Q}),$$

want substitutie van $x = -4$ in $X^3 - 25{\cdot}X = X(X-5)(X+5)$ geeft $(-4){\cdot}(-4-5){\cdot}(4-+5) = 4{\cdot}9$. Echter dit punt P voldoet niet aan de voorwaarde dat $x - N, x, x + N$ kwadraten zijn.

Maar laten we niet de moed verliezen. Trek de raaklijn in dit punt $P \in E_5$ aan die kromme. Omdat de kromme wordt gegeven door de vergelijking

$$F := -Y^2 + X^3 - 25{\cdot}X = 0$$

wordt de raaklijn in een punt $(x, y) = P \in E_5 = E$ aan die kromme. gegeven door de vergelijking

$$\frac{\partial F}{\partial X}(x){\cdot}(X - x) + \frac{\partial F}{\partial Y}(y){\cdot}(Y - y) = 0.$$

De raaklijn in $P = (x = -4, y = 6) \in E_N(\mathbb{Q})$ wordt gegeven door

$$(48 - 25)(X + 4) - 12(Y - 6) = 0;$$

deze lijn, gegeven door $23X - 12Y + 4{\cdot}41 = 0$, snijdt de kromme E_5 in het punt $P = (x = -4, y = 6)$ twee maal (allicht, zo hebben we deze lijn geconstrueerd), en het snijdt de kromme in het punt

$$(\frac{41^2}{4{\cdot}6^2}, \quad -\frac{(40^2 - 9^2){\cdot}41}{8{\cdot}6^3}) = Q \in E_5(\mathbb{Q})$$

(ga na!). Met behulp van dít punt kunnen we een bijbehorend drietal berekenen, en we krijgen dat

$$\alpha = \frac{9}{6}, \quad \beta = \frac{40}{6}, \quad \gamma = \frac{41}{6}$$

(ga na!). We zien dat $Q = 2P$, en met meer theorie beschikbaar, bewijzen we dat elk punt

$$Q = (x, y) \in E_N(\mathbb{Q})$$

dat verkregen wordt als $Q = 2P$ met $P \in E_N(\mathbb{Q})$ bewijst dat N congruent is; zo verloopt de rest van het bewijs van het bovenstaande feit.

(10.8) We zien een subtiel verschil tussen de meetkunde enerzijds en de getaltheorie anderzijds van dit probleem: neem $M, N \in \mathbb{Z}_{>0}$, dan geldt:

$$E_N \quad \cong_{\mathbb{R}} \quad E_M,$$

maar

$$E_N \quad \cong_{\mathbb{Q}} \quad E_M \quad \Longleftrightarrow \quad \exists d \in \mathbb{Q}_{>0} \ \text{ met } \ M = d^2{\cdot}N.$$

Als E_N gegeven wordt door $Y^2 = X^3 - M^2X$, dan geeft de substitutie $X = d^2{\cdot}\xi, \quad Y = d^3{\cdot}\eta$ een vergelijking die bij deling door d^6 een vergelijking geeft die E_M definiëert.

(10.9) **Voorbeeld:** We weten dat $N = 5$ een congruent getal is, door middel van $a = 9, b = 40, c = 41, D = 6$. Zoals we reeds zagen geeft de constructie:

$$(\alpha = \frac{9}{6}, \beta = \frac{40}{6}, \gamma = \frac{41}{6}) \mapsto (x = \frac{41^2}{4 \cdot 6^2}, \quad y = \pm\frac{(40^2 - 9^2) \cdot 41}{8 \cdot 6^3}).$$

Inderdaad is $y^2 = x^3 - 5^2{\cdot}x$ (ga na). Merk op dat

$$x - 5 = (\frac{31}{12})^2, \quad x = (\frac{41}{12})^2, \quad x + 5 = (\frac{49}{12})^2.$$

(10.10) We geven nu met behulp van deze meetkundige benadering een uitleg van het "mysterieuze mechanisme", zie (6.2). We laten zien:

a) Neem $0 < n < m$ als voorheen, die een PD (a, b, c) produceren, en die een congruent getal N produceren met behulp van $(\alpha = a/D,\ \beta = b,\ \gamma = c/D)$ en

$$\frac{a{\cdot}b}{D^2} = \alpha{\cdot}\beta = 2N, \quad m{\cdot}n{\cdot}(m^2 - n^2) = N.$$

Merk op dat

$$\frac{n}{m} = \frac{b}{a+c}.$$

b) Met behulp van deze presentatie van N als congruent getal produceren we

$$P = (x, y) \in E_N(\mathbb{Q})$$

door middel van

$$x = (\frac{\gamma}{2})^2 = \frac{c^2}{4D^2}, \quad y = \pm\frac{(b^2 - a^2)c}{8D^3}$$

zoals we dat deden in (6.2).

c) Voor een punt $P = (x, y) \in E$ construeren we $-2P = Q \in E$, door de raaklijn in P aan E te trekken en het derde snijpunt $Q = \xi, \eta$ te construeren. Voor onze kromme $E = E_N$ geeft dit: de raaklijn wordt gegeven door:

$$(2y)(Y - y) = (3x^2 - N^2)(X - x).$$

Substitutie van

$$Y = \frac{(3x^2 - N^2)(X - x)}{2y} + y \quad \text{in} \quad -Y^2 + X^3 - N^2X$$

geeft een derde graads polynoom in X dat factoriseert als

$$(X - x)^2(X - \xi) \quad \text{met} \quad \xi = (\frac{x^2 + N^2}{2y})^2$$

(ga na !). Merk op dat:

$$\xi \pm N = (\frac{x^2 \pm 2Nx - N^2}{2y})^2.$$

Conclusie: voor het punt $(x, y) \in E = E_N$ wordt

$$-2{\cdot}P =: (\xi, \eta) \in E_N$$

gegeven door

$$(\xi, \eta) = (\ (\frac{x^2 - N^2}{y})^2,\ \frac{x^2 - N^2}{y} \cdot \frac{x^2 + 2Nx - N^2}{2y} \cdot \frac{x^2 - 2Nx - N^2}{2y}).$$

d) We zien dat dit aanleiding geeft tot rationale getallen

$$A = \frac{x^2 - N^2}{y},\ B = \frac{2Nx}{y}, \quad C = \frac{x^2 + N^2}{y}$$

met $A^2 + B^2 = C^2$. We zien dat

$$\frac{B}{A+C} = \frac{\frac{2Nx}{y}}{\frac{x^2+N^2}{y} + \frac{x^2-N^2}{y}} = \frac{2Nx}{2x^2} = \frac{N}{x} = \frac{4N}{\gamma^2} = \frac{2ab}{c^2}.$$

Kies nu $U := 2ab$ en $V := c^2$.

Conclusie: Het "mysterieuze mechanisme"van (6.2) vertaalt zich via (10.3) en (10.4) in de handeling $P \mapsto -2P = Q$: trek de raaklijn in P en neem voor Q het derde snijpunt. Overzicht:

$$\begin{array}{ccc} (m,n,D) & \mapsto & P = (x,y) \in E_N(\mathbb{Q}) \\ \downarrow & & \downarrow \\ (U,V,E) & \mapsto & -2P = Q \in E_N(\mathbb{Q}); \end{array}$$

voor $(m,n,D) \mapsto (U,V,E)$ zie (6.2).

Opmerking/opgave: Neem een presentatie van een congruent getal, en de bijbehorende $P = (x,y)$ als boven; laat zien dat de orde van P (met $y_P \neq 0$) als element van de groep $E_N(\mathbb{Q})$ niet eindig is.

(10.11) Om nog een bewijs van (6.3) te geven, merken we eerst op dat een congruent getal N aanleiding geeft tot een punt op E_N met rationale coördinaten, dat volgt uit de formules boven. Omgekeerd kan bewezen worden dat in de groep van punten op E_N een punt $P = (x,y)$ met rationale coördinaten $x, y \in \mathbb{Q}$ en $y \neq 0$ de orde van P niet eindig is (dat is niet zo eenvoudig, zie [22], pp. 43 - 46: $\#(\text{Torsie}(E_n(\mathbb{Q}))) = 4$). Met behulp daarvan kan een bewijs van (6.3) afgemaakt worden.

(10.12) Hoe komt een mens ooit aan een dergelijk idee? De vergelijkingen $\alpha^2 + \beta^2 = \gamma^2$ en $\alpha \cdot \beta = 2N$ kunnen beschouwd worden als twee kwadratische vergelijkingen in drie onbekenden (zeg, over $\mathbb{C}$) de oplosverzameling is een kromme (in $\mathbb{C}^3$), en algemene theorie vertelt je dat dit een "elliptische kromme" is, de formules geven dan de juiste coördinaten transformatie die deze kromme geven als een vlakke derde graads kromme. Met andere woorden, meetkundig is het bovenstaande "feit" geen verrassing. Dat is de kracht van het combineren van methodes: een probleem uit de getaltheorie wordt meetkundig bekeken (neem alle oplossingen over $\mathbb{C}$), dat vertelt je wat je moet doen, en de (mysterieuze) formules volgen uit de meetkunde !

(10.13) We zien soms presentaties van hetzelfde pCG niet verkregen uit elkaar door het bovenstaande mechanisme. Bij voorbeeld $(n,m) = (1,6)$, $(n,m) = (2,5)$ with $D = 1$ and $(n,m) = (7,8)$ with $D = 2$ geven drie verschillende presentaties voor $N = 210$. Een dergelijk verschijnsel kon pas worden verklaard met de theorie van arithmetiek op elliptische krommen.

(10.14) Een idee? We hebben gezien dat we (6.3) voor een gegeven CG N bewijzen door de operatie $P \mapsto -2P$ op de kromme E_N uit te voeren. Maar waarom $\times -2$? De operatie $P \mapsto 3 \cdot P$, of algemener de operatie $P \mapsto k \cdot P$ voor een of andere $k \in \mathbb{Z}_{>1}$ geeft een afbeelding $\times k : E_N(\mathbb{Q}) \to E_N(\mathbb{Q})$. Omdat een punt $P = (x,y) \in E_N(\mathbb{Q})$ niet van eindige orde is, geeft dit proces voor een vast k de oneindige rij van onderling verschillende punten

$P,\ kP,\ k^2P, \cdots \in E_N(\mathbb{Q})$. Dit correspondeert met een oneindige rij van onderling verschillende presentaties van N, weer een bewijs van (6.3). Het zou interessant zijn om de formules voor een vast gekozen k uit te schrijven, analoog aan de formules voor $k = -2$ zoals in (6.2). Dit lijkt een interessant spel dat gegarandeerd tot succes leidt.

11 Voorbeelden

(11.1) Theorem (Pierre de Fermat). $\boxed{N = 1}$ *is niet een congruent getal.*
See [21], Coroll. 4.20.

$\boxed{N = 1}$ Lang was dit een open probleem. Soms werden verkeerde bewijzen geproduceerd, zie [13], pag. 462, [11], pag. 20. Na vele eeuwen kwam Fermat met een bewijs.

Voor de samenhang tussen werk van Diophantus en het CGP zie § 7

(11.2) FLT **en.** $\boxed{N = 2}$
Pierre de Fermat (1608 – 1665) bewees dat $N = 1$, $N = 2$ en $N = 3$ niet CGen zijn. Uit
Stelling (Fermat). *Als* $x, y, w \in \mathbb{Z}$ *met* $x^4 + y^4 = w^2$ *dan is* $xyw = 0$.
concluderen we:

(11.3) Gevolg (Fermat). $N = 2$ *is niet een congruent getal.*
Bewijs. We nemen aan dat $N = 2$ wel een CG is, en komen tot een tegenspraak. Inderdaad, onderstel dat $\delta = c/d \in \mathbb{Q}$ de eigenschap heeft dat $\delta^2 - 2 = (u/d)^2$ and $\delta^2 + 2 = (v/d)^2$. Schrijf $x = uv$, $y = 2cd$ and $t = c^4 + 4d^4$. Omdat

$$u^2 = c^2 - 2d^2, \quad w^2 = c^2 + 2d^2$$

krijgen we

$$x^4 + y^4 = (uv)^4 + (2cd)^4 = ((c^2 - 2d^2)(c^2 + 2d^2))^2 + 16c^4d^4 = (c^4 + 4d^4)^2 = t^2.$$

Dit is in tegenspraak met de bovenstaande stelling. Dit bewijst het gevolg. QED

Was dit de inspiratie voor Fermat om zijn FLT te formuleren ?

We geven nog wat meer voorbeelden. Soms zijn er eenvoudige methoden om te beslissen of een gegeven getal congruent is. Soms denken we of weten al dat een gegeven getal congruent is, maar is er een enorme rekenpartij nodig om een presentatie te vinden. In die gevallen ligt het getal vaak veel te ver in de lijst zoals in A om op die manier een presentatie te vinden; dan moet theorie eerst helpen om de berekening te vereenvoudigen.

(11.4) Oplossing. $\boxed{N = 13}$
Een oplossing: Met $m = 325$ en $n = 36$ komt er

$$m{\cdot}n{\cdot}(m^2 - n^2) = 325{\cdot}36{\cdot}298{\cdot}361 =$$

$$= 13{\cdot}5^2{\cdot}6^2{\cdot}17^2{\cdot}19^2.$$

Conclusie: $N = 13$ is een congruent getal.

We zien dat $\delta = 106921/19380$ de eigenschap heeft dat $\delta^2 - 13 = (80923/19380)^2$ and $\delta^2 + 13 = (127729/19380)^2$. Dat is niet zo eenvoudig te vinden.

$\boxed{N = 23}$
Kies $m = 24336$, en $n = 17689$; dan is $m = 156^2$, $n = 133^2$, $m - n = 6647 = 17^2 \times 23$, en $m + n = 42025 = 205^2$. Dus is 23 een CG.

$\boxed{N = 157}$
Dit "kleine" getal is een CG (voorspeld door Tunnell, bewezen dor Monsky met "zuiver denkwerk", en bewezen door D. Zagier met behulp van een berekening). We zoeken de $\delta = c/d$ zodat $\delta^2 \pm 157$ kwadraten zijn waar d het minst aantal cijfers heeft; dit treedt op met $m = 443624018997429899709925$, and $n = 166136231668185267540804$; zie [22], pag. 5 voor de bijbehorende driehoek.

Dit is een mooi voorbeeld van het "chaotische gedrag" van het getal D in de lijst van CGen; als we te werk gaan zoals in Vraag A, dan krijgen we die lijst, maar het kan voorkomen dat voor een klein getal de bijbehorende D erg groot is. Dit maakt het probleem, in de vorm van Vraag B zo moeilijk. We zullen zien dat $N = 10374$ een kleine presentatie heeft, en $N = 263$ een heel grote.

$\boxed{N = 219}$
Dit is een CG omdat $48 \times 73 \times (73 + 48) \times (73 - 48) = 219 \times (4 \times 5 \times 11)^2$.

Bekijk de rij getallen $3, 11, 19, \cdots, i8 + 3, \cdots, 211$ with $0 \leq i \leq 26$;
dit zijn allemaal kwadraatvrije getallen die niet congruent zijn. Maar $219 = 3 \times 73 = 27 \times 8 + 3$ is een CG, alhoewel 3 en 73 niet CGen zijn. Verder is $N = 171 = 9 \times 29 = 21 \times 8 + 3$ wel een CG.

Bastien bewees dat elk priemgetal van de vorm $i8 + 3$ niet een CG is; zie [4].

Merk op dat $49 \times 48 \times 1 \times 97 = 28^2 \times 291$; dit bewijst dat 291 een CG is; idem voor 299, omdat $36 \times 13 \times 23 \times 49 = 42^2 \times 299$.

We zien het soms onvoorspelbare gedrag van getallen wat betreft het gedrag als wel/niet een CG.

$\boxed{\text{N=263}}$ De keus
$m = 241504696540719988647244439501505 6$
en
$n = 219658997253142085134052135647096 9$
bewijst dat dit een CG is (zoals bewezen door Monsky, voorspeld door Tunnell).

Alle gevallen $1 \leq N \leq 999$, zijn doorgerekend:
http://www.asahi-net.or.jp/ KC2H-MSM/mathland/math10/matb2000.htm
http://www.asahi-net.or.jp/ kc2h-msm/mathland/math10/mail1001.htm
Zie ook [23]. Zie ook de laatste pp. van deze syllabus.

$\boxed{N = 10374}$ Dit is het grootste CG te vinden in het Arabische manuscript [1]. Inderdaad, kies $n = 3$ and $m = 13$ en we krijgen

$$m{\cdot}n{\cdot}(m + n){\cdot}(m - n) = 13 \times 6 \times 19 \times 17 = 10374.$$

Hier zien we een relatief grote N die een kleine presentatie heeft.

Voor elke N met $N \equiv r \pmod 8$, met $r \in \{5, 6, 7\}$, voorspelt het vermoeden van Tunnell dat dit niet een CG. Maar voor andere congruenties is dit niet zo eenvoudig:

$r = 0$ 8 is niet een CG en 24 is een CG;
$r = 1$ 1 is niet een CG en and 41 is een CG;
$r = 2$ 2 is niet een CG en 34 is een CG;
$r = 3$ 3 is niet een CG en 219 is een CG;
$r = 4$ 4 is niet een CG en 28 is een CG.

(11.5) Een paar verwijzingen. Er is de afgelopen 10 eeuwen enorm veel gepubliceerd over het CGP. We geven slechts een paar verwijzingen.

In het tweede deel van Dickson, zie [13], vinden we in Chapter 16 een overzicht van vroege pogingen om het CGP op te lossen. In [18], Problem D27 vinden we een overzicht van bekende oplossingen, en we vinden daar ook recente verwijzingen. In [31] vinden we het verband tussen de *Arithmetica* van Diophantus en Arabische middeleeuwse wiskunde. In [22] vinden we een overzicht van een paar moderne methodes, in het bijzonder de weg naar het vermoeden van Tunnell, zoals geformuleerd in [35].

Voor overzichten zie ook [2] and [11]. In het bijzonder zie [21] voor een heldere uiteenzetting die nodig zijn voor een moderne benadering.

Voor meer gespecialiseerde moderne benaderingen zie [34], [33], [23], [25].

Voor een benadering op elementair niveau, zie [5].

Het CGP, bekend in de oudheid, veel bestudeerd is na zoveel eeuwen nog steeds onopgelost. Net zoals dat bij FLT het geval was: het is nu niet meer een geïsoleerd probleem: sinds 1983 weten we dat dit probleem opgelost is als we het vermoeden van Birch en Swinnerton-Dyer op juist is.

Referenties

[1] Anonymous Arab manuscript (before 972) in the Imperial Library of Paris.
French translation by F. Woepcke: *Recherches sur plusieurs ouvrages de Léonard de Pise.* III: *Traduction d'un fragment anonyme sur la formations des triangles rectangles en nombres entiers, et d'un traité sur je même sujet par Aboū Dja'far Mohammed Ben Alhoçain.* Vol. **14** pp 211 – 227, 241 – 269, 301 – 324, 343 – 356.
Also published: F. Woepcke - Études sur les mathématiques Arabo-Islamiques. Band II. Nachdruck aus den Jahren 1842 – 1974. Herausgegeben von Fust Sezgin. Inst. Geschichte Arabisch-Islamischen Wissensch., Goethe-Universität, Frankfurt am Main, 1986.

[2] R. Alter – *The congruent number problem.* American Mathematical Monthly **87** (1980), 43 – 45.

[3] A. Anbouba – *Un traité d'Abu Ja'fa* [al-Khazin] *sur les trangles rectangle numériques.* Journal for the history orf Arabic sciences. Vol **3** (1979), 134 – 156.

[4] L.Bastien – *Nombres congruents.* Intermédiare des Math. **22** (1915), 231 – 232.

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

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

[7] B. Birch & H. Swinnerton-Dyer – *Notes on elliptic curves II.* Journ. reine angew. Math **218** (1965), 79-108.

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

[9] V. Chandrasekar – *The congruent number problem.* Resonance August 1998, 33 – 45. http://www.ias.ac.in/resonance/Aug1998/pdf/Aug1998p33-45.pdf

[10] J. Coates & A. Wiles – *On the Conjecture of Birch and Swinnerton-Dyer.* Invent. Math. **39** (1977), 223-251.

[11] J. H. Coates – *Congruent number problem.* Quarterly Journal of pure and Applied Mathematics **1** (2005), 14 – 27.

[12] B. Datta & A. N. Singh – *History of Hindu mathematics.* Asia Publ. House, Part I: 1935, Part II: 1938, Single volume edition: 1962.

[13] L. E. Dickson – *History of the theory of numbers.* Volume II: Diophantine analysis. Chelsea publ. Cy. New York, 1952.

[14] N. D. Elkies – *Curves $Dy^2 = x^3 - x$ of odd analytic rank.* Proceedings of ANTS-5, 2002 (C.Fieker and D.R.Kohel, eds.), Lecture Notes in Computer Science 2369, pp. 244-251.

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

[16] Leonardo Pisano Fibonacci – *The book of squares.* An annotated translation into modern English by L. E Sigler. Academic Press, 1987.

[17] D. Fowler & E Robson – *Square root approximations in old Babylonian mathematics.* YBC 7289 in context, Historia Math. **25** (1998), 366-378.

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

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

[20] T. Heath – *A history of Greek mathematics.* Oxford, Clarendon Press, 1921.

[21] A. W. Knapp – *Elliptic curves.* Math. Notes 40, Princeton Univ. Press, 1992.

[22] N. Koblitz – *Introduction to elliptic curves and modular forms.* Grad. Texts Math. 97, Springer - Verlag, 1984.

[23] G. Kramarz – *All congruent numbers less than 2000.* Math. Ann. **273** (1986), 337 – 340.

[24] S. Lang - Algebraic number theory. Grad. Texts Math. 110, Springer Verlag, 1986.

[25] P. Monsky – *Mock Heegner points and congruent numbers.* Math. Zeitschrift **204** (1990), 45-67.

[26] O Neugebauer and A Sachs – *Mathematical Cuneiform Texts.* New Haven, CT., 1945.

[27] 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.

[28] E. Picutti – *Sui numeri congruo-congruenti di Leonardo Pisano.* Physis **23** (1981), 141 – 170.

[29] K. Plofker – *Mathematics in India.* Princeton University Press, 2008.

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

[31] J. Sesiano – *Books IV to VII of Diophantus' Arithmetica.* Sources Hist. Math. Phys. Sciences **3**. Springer – Verlag 1982.

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

[33] J. H. Silverman – *The arithmetic of elliptic curves.* Grad. Texts Math. 106, Springer -Verlag, 1986.

[34] N. M. Stephens – *Congruence properties of congruent numbers.* Bull. London Math. Soc. **7** (1975), 182-184.

[35] J. B. Tunnell – *A classical diophantine problem and modular forms.* Invent. Math. **72** (1983), 323 - 334.

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

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

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

Van: http://www.asahi-net.or.jp/ KC2H-MSM/mathland/math10/matb2000.htm

Congruum g : $1 \leq g \leq 999$
Definition 1.
$k^2g=mn(m^2-n^2)$, k, m, n, g in N (integer > 0)
Definition 2.
$x^2+gy^2=z^2$, $x^2-gy^2=w^2$, x, y, z, w in N (integer > 0), $m=x^2$, $n=gy^2$
Definition 3.
$(x/z^2, y/z^3)$ on elliptic curve $Y^2=X^3-g^2X$, x, y, z in Z (integer), X, Y in Q (rational), $X=mg/n$, $Y=kg^2/n^2$
We are using the same characters x, y, z in the definition 2 and 3, but I think there's no confusion.
There are 361 congruent numbers in the range of $1 \leq g \leq 999$.
g, m, n
5, 5, 4
6, 2, 1
7, 16, 9
13, 325, 36
14, 8, 1
15, 4, 1
21, 4, 3
22, 50, 49
23, 24336, 17689
29, 4901, 4900
30, 3, 2
31, 1600, 81
34, 9, 8
37, 777925, 1764
38, 1250, 289
39, 13, 12,
41, 25, 16,
46, 72, 49,
47, 14561856, 2289169,
53, 1873180325, 1158313156,
55, 125, 44,
61, 12079525, 10227204
62, 39200, 22801,
65, 9, 4,
69, 192, 169,
70, 7, 2,
71, 3600, 121,
77, 2816, 2809,
78, 26, 1,
79, 169000000, 166952241,
85, 85, 36,
86, 338, 49
87, 17956, 169

93, 1444, 75
94, 14112, 529
95, 1445, 76
101, 44715091781, 3975302500
102, 50, 1
103, 8780605285453456, 7551929273974569
109, 2725, 1764
110, 10, 1
111, 37, 12
118, 716311250, 19298449
119, 144, 25
127, 3063173263398676380 16, 305111826865145547009
133, 256036, 143811
134, 2084882, 14161
137, 3425, 3136
138, 24, 1
141, 48, 1
142, 4918336200, 164070481
143, 101124, 1849
145, 29, 20
149, 93125, 56644
151, 115600, 35721
154, 9, 2
157, 443624018997429899709925, 166136231668185267540804
158, 768800, 579121
159, 33124, 11449
161, 16, 7
165, 16, 11
166, 197646962, 96020401
167, 115222229136, 3447686089
173, 2404644000341688241925, 2367961190733987384484
174, 27, 2
181, 3073858021, 1221502500
182, 343, 18
183, 17853541, 456300
190, 10, 9
191, 40472758 8018561600, 384957657745092721
194, 97, 72
197, 1991322221917925, 103880003159716
199, 13933945152400, 27368486201
· · · etc. op die site tot · · ·
995, 320, 121
997, 422137097683075141716864298903634885273173164273488 44
504307265329655015861152197726745537308248325,
376155528445686424185441533115738655613612025371648337903 72
441219001711265289427484319356449229 16
998, 990175074810417659190789298392472344 50, 456840925212009253253860257161127374 89