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 de paragraaf over elliptische krommen; 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

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

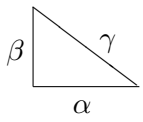
kwadraten zijn in $\mathbb{Q}$. We zullen schrijven CG = congruent getal, en CGP = het probleem van het vinden van congruente getallen / bepalen of een gegeven getal congruent is.

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 (7.4).

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 (7.4).)

(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;

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

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 (7.1).

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 § 7 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 $\mathrm{ggd}(x, y)$ 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.

(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 $\mathrm{ggd}(x, y) = 1$. Afkorting: pPD.

Merk op: als $\mathrm{ggd}(x, y) = 1$ en $x^2+y^2 = z^2$ dan volgt ook $\mathrm{ggd}(y, z) = 1$ en $\mathrm{ggd}(z, x) = 1$, 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 $x := 2\ell + 1$, $y := j$, $z := j + 1$, 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* $\gcd(m, n) = 1$ *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

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?

(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

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

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 $ji(j^2 - i^2) = d^2 N'$ 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:

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

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? 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).

7 Voorbeelden

(7.1) 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.

(7.2) 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:

(7.3) 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.

(7.4) 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.

(7.5) 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