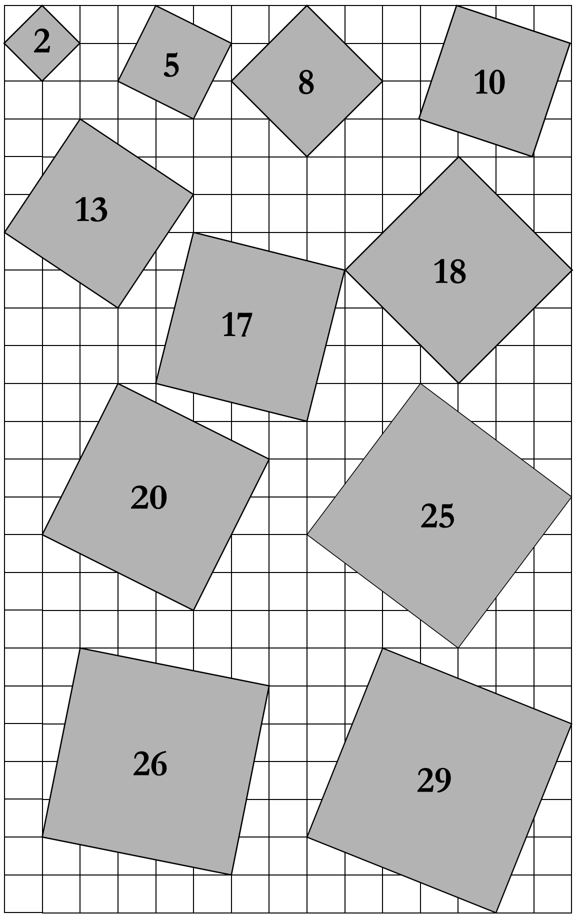
Wat te bewijzen is (47)

Rubriek

Op ruitjespapier is het makkelijk vierkanten tekenen. Dat kan rechttoe rechtaan: 1 bij 1, 2 bij 2, 3 bij 3, enzovoort. Maar er zijn ook scheve vierkanten mogelijk met roosterpunten op de hoeken. Het leren tekenen daarvan is een mooie aanloop naar de stelling van Pythagoras. Immers de oppervlakte van zo'n scheef vierkant blijkt steeds gelijk te zijn aan de som van twee rechte exemplaren. In de Wiskivon-tijd (tussen 1975 en '80) lieten we de leerlingen met elastiekjes scheve vierkanten op een spijkerbord spannen. Een van de opdrachten daarbij was om vierkanten opklimmend in grootte te maken tot en met het vierkant met oppervlakte 20. In de figuur hieronder ben ik, met weglating van de (triviale) rechte vierkanten, daarmee nog wat verder gegaan.



Al doende dringt het besef door dat lang niet alle natuurlijke getallen als oppervlakte van een recht of scheef vierkant te voorschijn komen. De oppervlaktegetallen van de scheve vierkanten in het rooster noem ik in dit stukje 'scheve kwadraten'. Een voor de hand liggende vraag is: welke natuurlijke getallen behoren tot de rij van scheve kwadraten?

65 wel, 67 niet

In de volgende vier-rijen-tabel zijn de kwadraten en de scheve kwadraten onder 65 aangegeven.

1	**5**	**9**	**13**	**17**	21	**25**	**29**	33	**37**	**41**	**45**	**49**	**53**	57	**61**
2	6	**10**	14	**18**	22	**26**	30	**34**	38	42	46	**50**	54	**58**	62
3	7	11	15	19	23	27	31	35	39	43	47	51	55	59	63
4	**8**	12	**16**	**20**	24	28	**32**	**36**	**40**	44	48	**52**	56	60	**64**

Wat opvalt, is dat de derde rij geen enkel kwadraat of scheef kwadraat bevat. Dat blijft zo bij voortzetting van de tabel: 67, 71, 75, ... zijn geen (scheve) kwadraten.
Dit is eenvoudig (ook op school!) te bewijzen. Bedenk eerst dat het kwadraat van een even getal een viervoud is en dat het kwadraat van een oneven getal een viervoud + 1 is.
Het gevolg daarvan is:

(a) $\mathit{even}^2 + \mathit{oneven}^2 = \text{viervoud} + 1$
(b) $\mathit{oneven}^2 + \mathit{oneven}^2 = \text{viervoud} + 2$
(c) $\mathit{even}^2 + \mathit{even}^2 = \text{viervoud}$

Daarom: *een viervoud + 3 kan geen scheef (of recht) kwadraat zijn!*
In de bovenste rij zitten meer grijze vakjes dan in de tweede en vierde rij en dat blijft zo bij uitbreiding van de tabel. Dit volgt uit de regels (a), (b) en (c). Immers combinatie van de eerste n even kwadraten met de eerste n oneven kwadraten geeft n^2 verschillende tweetallen, terwijl combinatie van de eerste n (on)even kwadraten met de eerste n (on)even kwadraten slechts $\frac{1}{2}n(n+1)$ te onderscheiden paren oplevert. Ik merk nog wel op dat verschillende paren niet per se verschillende scheve (of rechte) kwadraten opleveren. Een klassiek voorbeeld daarvan is 65. Daarover merkt Diophantos (derde eeuw na Chr.) in het derde boek van zijn *Arithmetika* op:

> Een eigenschap van 65 is dat het zich op twee verschillende manieren als de som van twee kwadraten laat schrijven: 16 + 49 en 64 + 1 en dit is een gevolg van het feit dat 65 het product is van 13 en 5, die elk gelijk zijn aan de som van twee kwadraten.

Er bestaat nog een kleiner scheef vierkant dat op twee manieren in het rooster past: 50 = 1 + 49 = 25 + 25. Diophantos zou daarvan misschien hebben opgemerkt dat dit een gevolg is van '50 = 10 × 5 en 10 en 5 zijn elk ook scheve kwadraten'.

De bewering van Diophantos

Diophantos licht zijn bewering over het product van twee scheve kwadraten niet verder toe, maar dat betekent niet dat de lezer dit dan maar ('Peijnenburg-effect') voor zoete koek moet slikken. Laat ik daarom eens kijken naar producten van rechte of scheve kwadraten.

- Het product van twee rechte kwadraten is weer een recht kwadraat, dat is flauw.
- Het product van een recht kwadraat en een scheef kwadraat is een scheef kwadraat, immers:

$$a^2 \cdot (b^2 + c^2) = (ab)^2 + (ac)^2$$

Ook niet echt verrassend. Anders is dat met:

- *Het product van twee scheve kwadraten is een scheef of recht kwadraat.*

Dit volgt direct uit een identiteit die in de boeken naar verschillende wiskundigen (Brahmagupta, Fibonacci, Euler, Lagrange) is vernoemd, namelijk:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \qquad (*)$$

Met a, b, c, d positief geheel is het duidelijk dat het product slechts dan een kwadraat oplevert als $ac = bd$.
Een voorbeeld: $(2^2 + 1^2)(2^2 + 4^2) = 10^2$

Het bewijs van de formule is een kwestie van uitwerken van de beide leden en iemand die werkelijk vaardig is in algebra kan het uit zijn hoofd. Als $a \neq b$ en $c \neq d$ vinden we na verwisseling van c en d (of van a en b) een tweede paar kwadraten, waarmee dan Diophantos' opmerking is verklaard.

Kijk maar: neem a, b, c en d achtereenvolgens 1, 2, 2 en 3 en dit leidt enerzijds tot:

$$65 = (2^2 + 1^2)(3^2 + 2^2) = (6 - 2)^2 + (4 + 3)^2$$

en na verwisseling van c en d tot:

$$65 = (2^2 + 1^2)(2^2 + 3^2) = (4 - 3)^2 + (6 + 2)^2$$

Twee opmerkingen.

- In de wereld van de complexe getallen kan de identiteit (*) worden geïnterpreteerd als: $|z| \cdot |w| = |zw|$ waarbij dan $z = a + bi$ en $w = c + di$.
- In de wereld van de matrices is zij een speciaal geval van de regel: $\det P \cdot \det Q = \det(PQ)$, waarbij dan

$$P = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \text{ en } Q = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

Een rol voor rechthoeks- en driehoeksgetallen

Men kan zich afvragen aan welke voorwaarde n moet voldoen, wil respectievelijk $4n + 1$, $4n + 2$ en $4n$ een recht of scheef kwadraat zijn. Het zal blijken dat daarbij naast de kwadraten nog twee getalsoorten een rol spelen, die al eerder in deze rubriek hebben gefigureerd, te weten rechthoeks- en driehoeksgetallen.
De rechthoeksgetallen (in het Engels 'oblong numbers') zijn achtereenvolgens: 2, 2 + 4, 2 + 4 + 6, ... ofwel 1 × 2, 2 × 3, 3 × 4, ...
De driehoeksgetallen zijn halve rechthoeksgetallen, dus 1, 1 + 2, 1 + 2 + 3, 1 + 2 + 3 + 4, ...
Beide rijen kunnen we ook laten beginnen met 0 en dat komt mij in dit stukje beter uit.
Ik begin met $4n$. Een getal van deze vorm kan de som zijn van twee even kwadraten, zeg $4n = (2k)^2 + (2m)^2$.
Er volgt nu onmiddellijk dat $4n$ een recht of scheef kwadraat is, alleen dan als n dat ook is.

Nu $4n + 2$. Dat kan geen kwadraat zijn, maar wel een scheef kwadraat en dan met oneven kwadraten als componenten. Kortom:

$$4n + 2 = (2k + 1)^2 + (2m + 1)^2$$

met als gevolg:

$$n = k(k + 1) + m(m + 1)$$

Zo wordt direct duidelijk dat $4n + 2$ dan en slechts dan de som van twee kwadraten is, als n de som is van twee rechthoeksgetallen (waarvan er een ook nul kan zijn)
Ik loop het tweede rijtje van de tabel op de vorige bladzijde even langs en vind voor de n-waarden bij de grijze hoekjes achtereenvolgens 0, 2, 2 + 2, 6, 2 + 6, 6 + 6, 2 + 12. Merk op dat 12 op twee manieren de som van twee rechthoeksgetallen is, hetgeen rijmt met de eerder gedane opmerking over het getal 50 (= 4 × 12 + 2).

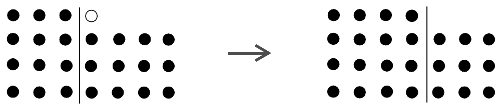
Nu de (scheve) kwadraten van de vorm $4n + 1$. De lezer verwacht misschien dat nu de driehoeksgetallen om de hoek komen kijken, en dat is ook zo. Eerst even proberen.
Daarbij noteer ik de driehoeksgetallen achtereenvolgens als $\Delta_0, \Delta_1, \Delta_2, \ldots$ met $\Delta_k = \frac{1}{2}k(k + 1)$.
Zo geldt bijvoorbeeld:

$$17 = 4 \times (\Delta_1 + \Delta_2) + 1$$
$$37 = 4 \times (\Delta_2 + \Delta_3) + 1$$
$$53 = 4 \times (\Delta_2 + \Delta_4) + 1$$

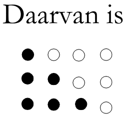
Bij uitbreiding van het aantal voorbeelden begint het vermoeden te rijzen dat $4n + 1$ dan en slechts dan een recht of scheef kwadraat is als n de som van twee driehoeksgetallen is. Het bewijs dat dit echt zo is, vergt meer algebra dan bij de voorgaande gevallen (dus bij $4n$ en $4n + 2$).
Als inleiding neem ik eerst het geval dat *n* zelf een driehoeksgetal Δ_k is (ofwel $\Delta_0 + \Delta_k$).
$4n + 1$ is nu de som van twee opvolgende kwadraten:

$$4 \times \tfrac{1}{2}k(k + 1) + 1 = k^2 + (k + 1)^2$$

Rechthoeks- en driehoeksgetallen danken hun naam aan de bijbehorende stippenpatronen en het is verleidelijk om daar ook nu eens naar te kijken. Daarbij vervang ik vier keer een driehoeksgetal door twee keer een rechthoeksgetal:



Dat is glashelder en als je het mij vraagt, meer inzichtelijk dan het algebraïsch bewijs.
Een tweede bijzonder geval krijg ik door voor n de som van twee opvolgende driehoeksgetallen te nemen. Daarvan is mij bekend dat het een kwadraat is.



$$\tfrac{1}{2}k(k - 1) + \tfrac{1}{2}k(k + 1) = k^2$$

En dan: $4k^2 + 1 = (2k)^2 + 1^2$, ook vertrouwenwekkend.

Als ik nu voor een bewijs voor alle gevallen een weg volg analoog aan die bij $4n+2$ kom ik via

$$4n+1 = (2k)^2 + (2m+1)^2$$

op

$$n = k^2 + m(m+1)$$

Dus moet n de som van een kwadraat en een rechthoeksgetal zijn. Dat dit altijd ook de som van twee driehoeksgetallen is, is echter allerminst direct duidelijk.
Ik maak (het begin van) een opteltabel van vierkants- en rechthoeksgetallen en probeer patronen te vinden:

$m(m+1)$ ↓

k^2 →

+	0	1	4	9	16	25	36
0	0	1	4	9	16	25	36
2	2	3	6	11	18	27	38
6	6	7	10	15	22	31	42
12	12	13	16	21	28	37	48
20	20	21	24	29	36	45	56
30	30	31	34	39	46	55	66
42	42	43	46	51	58	67	78

In de grijze vakken (bij $m = k$ en $m = k-1$) komen driehoeksgetallen te staan. Alweer een goede algebrasom:

$$k^2 + k(k \pm 1) = k(2k \pm 1) = \tfrac{1}{2} \cdot 2k(2k \pm 1)$$

Ook bij deze identiteit kan desgewenst een verhelderend stippenplaatje worden gemaakt, maar dat laat ik met een gerust hart aan de lezer. Nu de getallen in de witte hokjes. Binnen de grenzen van bovenstaande tabel lukt het om die stuk voor stuk als som van twee driehoeksgetallen te schrijven:

+	0	1	4	9	16	25	36
0	0+0	0+1	1+3	3+6	6+10	10+15	15+21
2	1+1	0+3	0+6	1+10	3+15	6+21	10+28
6	3+3	1+6	0+10	0+15	1+21	3+28	6+36
12	6+6	3+10	1+15	0+21	0+28	1+36	3+45
20	10+10	6+15	3+24	1+28	0+36	0+45	1+55
30	15+15	10+21	6+28	3+36	1+45	0+55	0+66
42	21+21	15+28	10+36	6+45	3+55	1+66	0+78

Door steeds het kleinste driehoeksgetal voorop te schrijven, ontvouwen zich mooie patronen. Neem bijvoorbeeld de kolom corresponderend met $k = 5$.
De links geschreven getallen 10, 6, 3, 1, 0, 0, 1 corresponderen met de m-waarden 0, 1, 2, 3, 4, 5, 6. Gelet op de lineair afnemende verschillen is er sprake van een kwadratische functie met nulpunten bij 4 en 5. Hierbij past:

$$m \to \tfrac{1}{2}(m-4)(m-5)$$

De rechts geschreven getallen 15, 21, 28, 36, 55, 66 horen bij hetzelfde rijtje m-waarden en daarbij past de formule:

$$m \to \tfrac{1}{2}(m+5)(m+6)$$

De waarde $k = 5$ is in beide formules terug te vinden en dat brengt mij op het gokje dat de waarde van n in de rij met rangnummer k en de kolom m wel eens gelijk zou kunnen zijn aan:

$$\tfrac{1}{2}(m-k+1)(m-k) + \tfrac{1}{2}(m+k)(m+k+1)$$

Inderdaad is de som van deze driehoeksgetallen gelijk aan $k^2 + m(m+1)$. Omdat k en m positieve getallen zijn, stelt de tweede vorm het getal Δ_{m+k} voor; de eerste vorm staat voor $\Delta_{m\text{-}k}$ of $\Delta_{k\text{-}m\text{-}1}$ al naar gelang $m \ge k$ of $m < k$.
Ik keer nog even terug naar Diophantos. Een alternatieve verklaring voor de twee mogelijke splitsingen van 65 (= 4 × 16 + 1) is dat 16 op twee manieren te schrijven is als de som van twee driehoeksgetallen, namelijk : 1 + 15 = $\Delta_1 + \Delta_5$ en 6 + 10 = $\Delta_3 + \Delta_4$.
Via $m-k = 1$ en $m+k = 5$, komt er $m = 3$ en $k = 2$, dus $2m + 1 = 7$ en $2k = 4$.
Via $k-m-1 = 3$ en $k+m = 4$, komt er $m = 0$ en $k = 4$, dus $2m + 1 = 1$ en $2k = 8$.

Een (andere) stelling van Fermat

Er valt in boeken over getaltheorie heel veel meer te vinden over sommen van twee kwadraten. De belangrijkste stelling bij dit onderwerp staat op naam van Fermat: *elk priemgetal van de vorm $4n+1$, kan op één manier worden geschreven als de som van twee kwadraten.*
Deze stelling geeft een criterium om via de factorontbinding van een natuurlijk getal vast te stellen of dat getal de som is van twee kwadraten of niet.
Immers behalve 2 is ieder priemgetal óf een viervoud + 1 óf een viervoud + 3. Mede in verband met de identiteit (*) moet de de conclusie zijn dat een getal N alleen dan een recht of scheef kwadraat is als de in de ontbinding van N voorkomende machten van priemgetallen van de soort viervoud + 3, een even exponent hebben.

Fermat heeft evenmin als bij wat altijd zijn 'laatste stelling' wordt genoemd, een sluitend bewijs geleverd van zijn bewering over de sommen van twee kwadraten.
Euler was de eerste die wel een correct bewijs publiceerde; dat bewijs vereist niet zoveel voorkennis dat Fermat het niet had kunnen vinden, maar is wel tamelijk lang (zie bijvoorbeeld het fraaie boek van Harold Edward: *Fermat's last theorem, a genetic introduction to algebraic number theory*). Sindsdien zijn veel andere bewijzen van de stelling gegeven. In *Proofs from the Book* (Martin Aigner en Günter Ziegler) zijn een paar heel mooie te vinden. Mijn favoriete bewijs maakt onder andere gebruik van de ring van 'gehele getallen van Gauss' (de getallen $k+m\mathrm{i}$ met k, m geheel). Fermats stelling drukt binnen deze context uit dat de natuurlijke priemgetallen van de vorm $4n+1$ geen priemgetallen van Gauss zijn; immers $a^2+b^2 = (a+b\mathrm{i})(a-b\mathrm{i})$).

Martin Kindt, martin@fi.uu.nl