AM2520-H: De Laatste Stelling van Fermat

week 1.9, maandag

K. P. Hart

Faculteit EWI
TU Delft

Delft, 26 oktober 2020

Outline

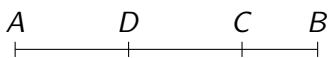
De Elementen, Boek X, Propositie 19

Lemma 1

Bepaal twee vierkante getallen zó dat hun som ook een vierkant is.

Bewijs.

Neem twee getallen AB en AC beide even of beide oneven; dan is hun verschil AC even, halveer dit bij D.



Neem aan dat AB en BC gelijkvormige vlakke getallen zijn, bijvoorbeeld vierkant.
Het product van AB en BC tezamen met het kwadraat van CD is het kwadraat van BD.
Aangezien AB en BC gelijkvormig zijn is hun product een kwadraat. □

De Elementen, Boek X, Propositie 19

Vlakke getallen zijn niet priem, product van twee andere dus.

Twee van zulke getallen zijn gelijkvormig als ze te schrijven zijn als $k \cdot l$ en $m \cdot n$ met $k : l = m : n$.

Als nu $d = \text{ggd}(k, l)$ en $e = \text{ggd}(m, n)$ dan geldt $k/d = m/e = a$ en $l/d = n/e = b$. En dus $k \cdot l \cdot m \cdot n = d^2 e^2 a^2 b^2$.

Schrijf overigens $BD^2 = (BC + CD)^2$ maar uit dan zie je de gelijkheid wel.

Wat moderner

Neem twee positive gehele getallen a en b (met $a > b$) en schrijf

$$x = 2ab$$
$$y = a^2 - b^2$$
$$z = a^2 + b^2$$

Dan geldt $x^2 + y^2 = z^2$.

Alle paren (a, b) met $\text{ggd}(a, b) = 1$ leveren de 'primitieve' drietallen; die met x, y en z relatief priem.

De rest met een extra parameter k.

Het beroemde citaat

Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superadere 10. Tet igitur 2. adiicitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 5. maior 7. & satisfacient quæstioni.

IN QVÆSTIONEM VII.

CONDITIONIS appositæ eadem ratio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Casores iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum fit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 — 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 1 Q. ille sit 2 N. — 4. ipse igitur quadratus erit 4 Q. + 16. — 16 N. hæc æquabuntur vnitatibus 16 — 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferatur similia, fient 5 Q. æquales 16 N. & fit 1 N. 3 Erit igitur alter quadratorum $\frac{9}{25}$. alter verò $\frac{16}{25}$ & vtriusque summa est $\frac{25}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oportet quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. — 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. — 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. — 16 N. æquatur vnitatibus 16. & fit 1 N. 7 erit

H iii

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Het is niet mogelijk een derdemacht in twee derdemachten te verdelen, of een vierdemacht in twee vierdemachten, of in het algemeen, een macht hoger dan de tweede in twee gelijkaardige machten. Ik heb hier een waarlijk wonderlijk bewijs voor gevonden, waar deze marge te nauw voor is om het te kunnen bevatten.

Het geval $n = 4$

Stelling

Als het drietal (x, y, z) aan $x^4 + y^4 = z^2$ voldoet, dan is er een ander drietal (u, v, w) dat aan $u^4 + v^4 = w^2$ voldoet en met $w < z$.

Bewijs.

We mogen aannemen dat $\text{ggd}(x, y, z) = 1$.
Neem twee positive gehele getallen a en b (met $a > b$) zó dat

$$\begin{aligned} x^2 &= 2ab \\ y^2 &= a^2 - b^2 \\ z &= a^2 + b^2 \end{aligned}$$

Herhaal dit voor de middelste vergelijking: $b^2 + y^2 = a^2$.

□

Het geval $n = 4$

Bewijs, voortgezet.

Neem twee positive gehele getallen c en d zó dat

$$b = 2cd, \qquad y = c^2 - d^2, \qquad a = c^2 + d^2$$

Dan geldt dus $x^2 = 2ab = 4cd(c^2 + d^2)$.
Wegens $\text{ggd}(c, d, c^2 + d^2) = 1$ volgt dat c, d en $c^2 + d^2$ kwadraten zijn:

$$c = u^2, \qquad d = v^2, \qquad c^2 + d^2 = w^2$$

en dus $u^4 + v^4 = w^2$ en $w^2 < w^4 = (c^2 + d^2)^2 + 4c^2d^2 = a^2 + b^2 = z$. □

Andere gevallen

- $n = 3$ Euler (1770, twee bewijzen)
- $n = 5$ Dirichlet (1825), Legendre (1828)
- $n = 14$ Dirichlet (1832)
- $n = 7$ Lamé (1839)
- $n = p$ als $2p + 1$ priem: Sophie Germain ($\sim$1820) bewees als $x^p + y^p = z^p$ dan $p \mid xyz$.

Nieuwe methoden

Stelling van Kummer, 1850

De vergelijking $x^p + y^p = z^p$ heeft geen geheeltallige oplossingen voor reguliere priemgetallen p.

Kummer: p is regulierals $p \not| B_2$, $p \not| B_4$, $\ldots$, $p \not| B_{p-3}$, met

$$B_{2k} = (-1)^{k-1} \frac{2(2k)!}{(2\pi)^{2k}} \zeta(2k)$$

de Bernoulli getallen.

De eerste paar niet-reguliere priemgetallen zijn 37, 59, 67, 101, 103, 131, 149, $\ldots$

Open probleem: zijn er oneindig veel reguliere priemgetallen?
Vermoeden (Siegel, 1964): de fractie reguliere priemgetallen is $e^{-\frac{1}{2}}$.

Euler, $n = 3$

Een paar stappen uit het bewijs van Euler voor $n = 3$.

Wegens $\text{ggd}(x, y, z) = 1$ is slechts één van de drie getallen even.

Geval 1: z is even, dus $x - y$ en $x + y$ zijn even.
Neem a en b met $x + y = 2a$ en $x - y = 2b$, en dus $x = a + b$ en $y = a - b$.
Dan $z^3 = x^3 + y^3 = a^3 + 3a^b + 3ab^2 + b^3 + a^3 - 3a^2b + 3ab^2 - b^3 = 2a(a^2 + 3b^2)$.

Geval 2: x is even, dus $z + y$ en $z - y$ zijn even.
Neem a en b met $z + y = 2b$ en $z - y = 2a$, en dus $z = b + a$ en $y = b - a$.
Dan $x^3 = z^3 - y^3 = b^3 + 3b^2a + 3b^2a + a^3 - b^3 + 3b^2a - 3ba^2 + a^3 = 2a(a^2 + 3b^2)$.

Euler, $n = 3$

Gevolg: als er een oplossing is voor $n = 3$ dan zijn er a en b waarvoor

$$2a(a^2 + 3b^2)$$

een derdemacht is.

Na wat werk kwam Euler uit op een strikt kleinere oplossing.

Hierin speelde de ontbinding

$$2a(a + b\sqrt{-3})(a - b\sqrt{-3})$$

een grote rol.

Hier werd eigenlijk in de ring $\mathbb{Z}[\sqrt{-3}]$ gewerkt.

Kummer's aanpak

Neem een priemgetal p en $\zeta_p = \exp(\frac{2\pi i}{p})$.
Werk in $\mathbb{Z}[\zeta_p]$, de verzameling van alle getallen van de vorm

$$a_1 + a_2\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}$$

met a_1, a_2, $\ldots$, a_{p-1} geheel.
Sommen en producten elementen van $\mathbb{Z}[\zeta_p]$ zitten weer in $\mathbb{Z}[\zeta_p]$.
(Als bij complexe getallen vervang je bij vermenigvuldigen ζ_p^p telkens door 1.)

Waarom doen we dit? Omdat:

$$z^p - y^p = (z-y)(z-y\zeta_p)\cdots(z-y\zeta_p^{p-1})$$

en ook $x^p + y^p = (x+y)(x+y\zeta_p)\cdots(x+y\zeta_p^{p-1})$

Kummer's aanpak

Idee: de factoren in

$$x^p + y^p = (x + y)(x + y\zeta_p) \cdots (x + y\zeta_p^{p-1})$$

zijn 'relatief priem' in $\mathbb{Z}[\zeta_p]$.
Wegens $x^p + y^p = z^p$ zijn al die factoren zelf $p$demachten.
Bewijs dat dat niet kan bij reguliere p.

Probleem (en de oorsprong van veel wiskunde):
in $\mathbb{Z}[\zeta_p]$ is er niet altijd unieke factorisatie (voor het eerst bij $p = 23$).

Vermoeden van Mordell (1922), Stelling van Faltings (1983)

Stelling

Een algebraische kromme over $\mathbb{Q}$ van genus $g > 1$ heeft slechts eindig veel rationale punten.

Gevolg

Voor $p \geqslant 3$ heeft $x^p + y^p = z^p$ slechts eindig veel oplossingen.

Bewijs van Wiles

Frey (1984), Ribet (1986)

Als $a^p + b^p = c^p$ met $p \geqslant 3$ dan is de elliptische kromme

$$y^2 = x(x - a^p)(x - b^p)$$

niet modulair.

Vermoeden van Taniyama-Shimura (1955)

Elke elliptische kromme is modulair.

Bewijs van Wiles

Wiles (1993), Taylor-Wiles (1994)

Elke semi-stabiele elliptische kromme is modulair.

De kromme van Frey is semi-stabiel, dus klaar.