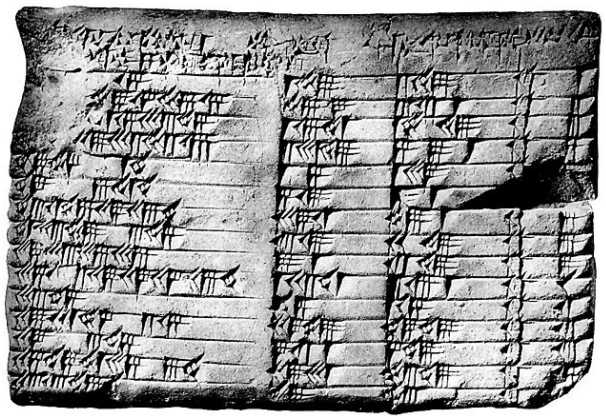
De kromme van Diophantus

Bachelorseminarium, 1 Maart 2023

Jan Vonk

Babylon (18e eeuw v.Chr.)



Plimpton 322

Tabel gehele oplossingen van $x^2 + y^2 = z^2$:

$$\begin{array}{ccccc} 3^2 & + & 4^2 & = & 5^2 \\ 5^2 & + & 12^2 & = & 13^2 \\ 8^2 & + & 15^2 & = & 17^2 \\ 7^2 & + & 24^2 & = & 25^2 \\ & & \dots & & \end{array}$$

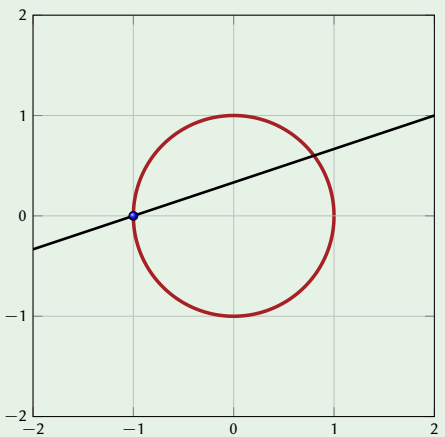
Alle coprieme oplossingen (x, y, z) komen van coprieme paren gehelen $(m, n) \in \mathbb{Z}^2$ via

$$(x, y, z) = \left(m^2 - n^2, 2mn, m^2 + n^2\right)$$

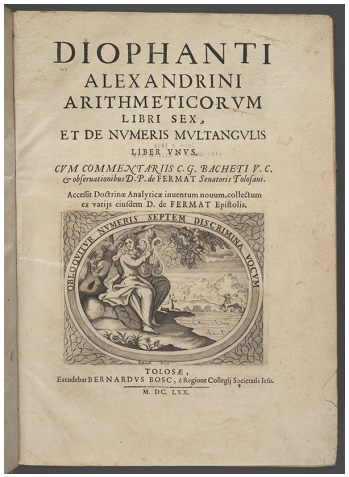
Reden hiervoor is als volgt:

- Oplossingen zijn veelvouden van rationale (X, Y) op
$$X^2 + Y^2 = 1.$$
- Rationale punten $\leftrightarrow$ rationale rechten door $(-1, 0)$; d.w.z. $mY = nX + n$, heeft snijpunt

$$(X, Y) = \left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2}\right)$$



Alexandria (Diophantus, 3e eeuw)


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& observationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrinæ Analyticæ inventum novum, collectum
ex variis ejusdem D. de FERMAT Epistolis.
TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.

In de Arithmetika van Diophantus staat Probleem 24 van Boek IV:

κδ.

Δοθέντα ἀριθμὸν διελεῖν εἰς δύο ἀριθμούς, καὶ ποιεῖν τὸν ὑπ' αὐτῶν κύβον παρὰ πλευράν.

Vraag is "verdeel een gegeven getal N in twee getallen wiens product een kubus min zijn ribbe is". Het boek behandelt $N = 6$, door een rationale oplossing te vinden van

$$E \ : \ y(6-y) = x^3 - x.$$

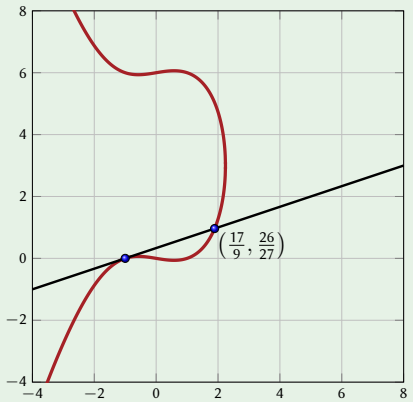
Diophantus veronderstelt dat $x = 3y - 1$. Substitutie geeft $27y^3 - 26y^2 = 0$, met dubbele wortel $y = 0$ en enkelvoudige wortel $y = 26/27$, dus

$$6 = 26/27 + 136/27.$$

Diophantus beschrijft de raaklijn aan $(-1, 0)$. Deze rechte snijdt de kromme E opnieuw in het (rationale) punt

$$(x, y) = \left(\frac{17}{9}, \frac{26}{27}\right).$$

Vandaag beschouwen we dit als toepassing van "groepenwet".



Methode van bestijging

De methode van Diophantus om oplossingen te vermeerderen werd formeel gemaakt in de moderne beschrijving van de groepenwet op elliptische krommen en Jacobianen van krommen door Poincaré (1901). Hij schrijft:

PROPRIÉTÉS ARITHMÉTIQUES DES COURBES ALGÉBRIQUES. 171

On peut se proposer de choisir les arguments

$$(2) \qquad \alpha, \quad \alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_q,$$

de telle façon que la formule (1) comprenne tous les points rationnels de la cubique. Les $q+1$ points rationnels qui ont les arguments (2) formeront alors ce que nous appellerons un *système de points rationnels fondamentaux*.

Il est clair que l'on peut choisir d'une infinité de manières le système des points rationnels fondamentaux. On devra tout d'abord dans ce choix s'arranger de telle façon que le nombre $q+1$ des points fondamentaux soit aussi petit que possible. Cette valeur minima de ce nombre $q+1$ sera ce que j'appellerai le *rang* de la cubique; c'est évidemment un élément très important de la classification des cubiques rationnelles.

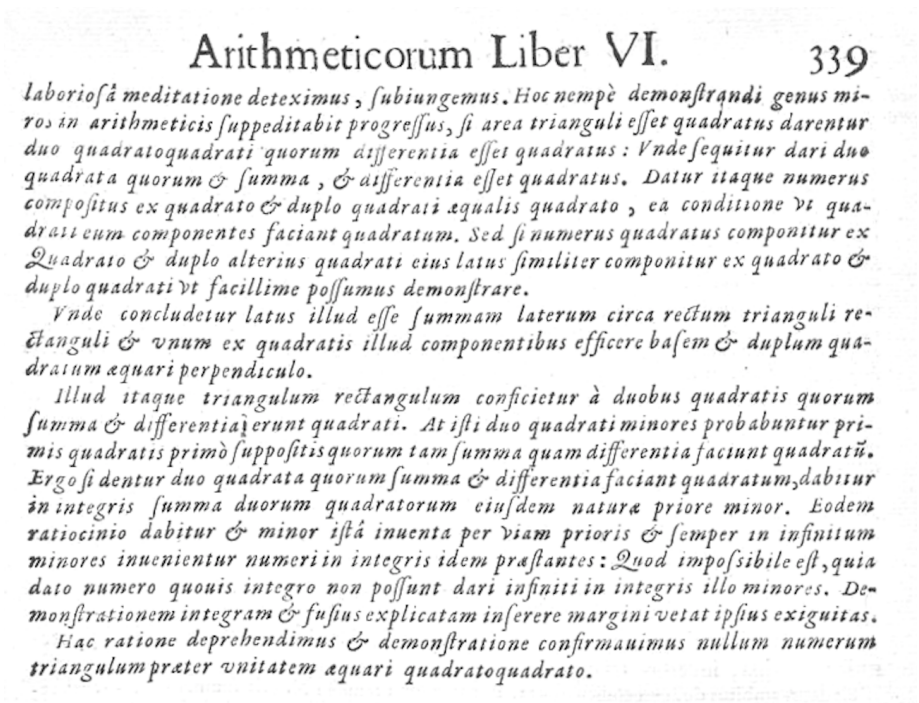
Hoeveel fundamentele oplossingen zijn er nodig om *alle* oplossingen op deze manier te kunnen verkrijgen? Poincaré noemt dit de “rang”.

Methode van afdaling

Fermat (1670) bewees dat er geen niet-triviale oplossing zijn van

$$x^4 - y^4 = z^2.$$

Dit impliceert de befaamde Laatste Stelling van Fermat voor exponent 4.



Arithmeticorum Liber VI. 339

laborioſâ meditatione deteximus, ſubiungemus. Hoc nempè demonſtrandi genus mirosin arithmeticis ſuppeditabit progreſſus, ſi area trianguli eſſet quadratus darentur duo quadratoquadrati quorum differentia eſſet quadratus: Vnde ſequitur dari duo quadrata quorum & ſumma, & differentia eſſet quadratus. Datur itaque numerus compoſitus ex quadrato & duplo quadrati æqualis quadrato, ea conditione vt quadrati eum componentes faciant quadratum. Sed ſi numerus quadratus componitur ex Quadrato & duplo alterius quadrati eius latus ſimiliter componitur ex quadrato & duplo quadrati vt facillime poſſumus demonſtrare.

Vnde concludetur latus illud eſſe ſummam laterum circa rectum trianguli rectanguli & vnum ex quadratis illud componentibus efficere baſem & duplum quadratum æquari perpendiculo.

Illud itaque triangulum rectangulum conficietur à duobus quadratis quorum ſumma & differentia erunt quadrati. At iſti duo quadrati minores probabuntur primis quadratis primò ſuppoſitis quorum tam ſumma quam differentia faciunt quadratũ. Ergo ſi dentur duo quadrata quorum ſumma & differentia faciant quadratum, dabitur in integris ſumma duorum quadratorum eiuſdem naturæ priore minor. Eodem ratiocinio dabitur & minor iſtâ inuenta per viam prioris & ſemper in infinitum minores inuenientur numeri in integris idem præſtantes: Quod impoſsibile eſt, quia dato numero quouis integro non poſſunt dari infiniti in integris illo minores. Demonſtrationem integram & fuſius explicatam inſerere margini vetat ipſius exiguitas.

Hac ratione deprehendimus & demonſtratione confirmauimus nullum numerum triangulum præter vnitatem æquari quadratoquadrato.

Stap 1. Stel dat (x, y, z) een niet-triviale coprieme oplossing is. Dan

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

Beide factoren zijn kwadraten:

$$\begin{cases} x^2 - y^2 &= s^2 \\ x^2 + y^2 &= t^2. \end{cases}$$

Nu zijn s, t oneven en y even, dus

$$\left(\frac{t \pm s}{2}\right)\left(\frac{t \mp s}{4}\right) = \left(\frac{y}{2}\right)^2.$$

Beide factoren zijn kwadraten:

$$\begin{cases} \pm s &= u^2 - 2v^2 \\ t &= u^2 + 2v^2 \end{cases} \quad \text{met } u^4 + 4v^4 = x^2$$

Stap 2. Merk op dat de relatie

$$u^4 + 4v^4 = x^2$$

impliceert dat $(u^2, 2v^2, x)$ een Pythagoreaans drietal is, dus zijn er coprieme $m, n > 0$ met

$$\begin{cases} u^2 &= m^2 - n^2 \\ 2v^2 &= 2mn \\ x &= m^2 + n^2 \end{cases}$$

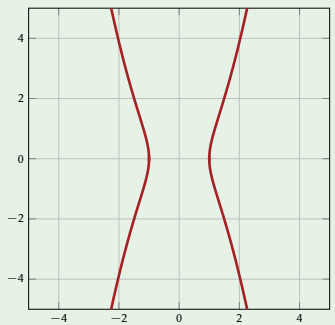
Omdat $v^2 = mn$ en m, n copriem, hebben we $(m, n) = (a^2, b^2)$ en vinden we een **kleinere** oplossing van de oorspronkelijke vergelijking

$$a^4 - b^4 = u^2.$$

Indien een niet-triviale oplossing bestaat, dalen we zo af ad infinitum, dat is absurd.

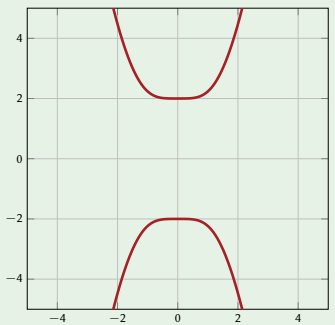
Fermat gebruikt een paar elliptische krommen, gerelateerd door (duale) twee-isogenieën

$$E_1 : x^4 - y^4 = z^2$$
$$E_2 : u^4 + 4v^4 = w^2$$



$$\phi_1 = (z, xy, x^4 + y^4)$$

$$\phi_2 = (w, 2uv, u^4 - 4v^4)$$



Het argument van Fermat toont eigenlijk twee dingen: Ten eerste

$$E_1(\mathbf{Q})/\phi_2(E_2(\mathbf{Q})) \simeq \mathbf{Z}/2\mathbf{Z} \simeq E_2(\mathbf{Q})/\phi_1(E_1(\mathbf{Q})),$$

en ten tweede, met behulp van de methode van afdaling, dat

$$\begin{aligned} E_1(\mathbf{Q}) &= \{(1,0,1),(1,0,-1),(1,1,0),(1,-1,0)\} &&\simeq \mathbf{Z}/4\mathbf{Z} \\ E_2(\mathbf{Q}) &= \{(1,0,1),(1,0,-1),(0,1,2),(0,1,-2)\} &&\simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}. \end{aligned}$$

Mordell–Weil theorem

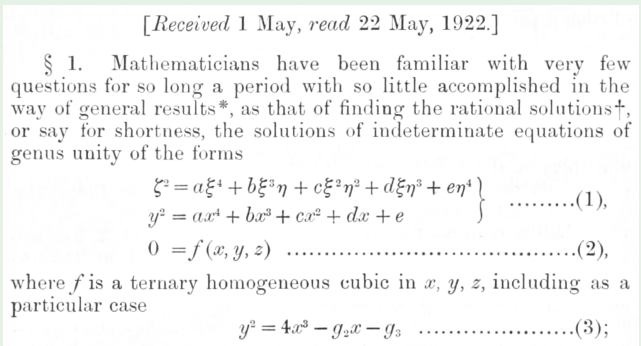
De methode van afdaling leidde Mordell (een eeuw geleden) tot de volgende stelling:

Theorem (Mordell 1922)

Zij $E/\mathbf{Q}$ een elliptische kromme, dan is haar groep van rationale punten $E(\mathbf{Q})$ eindig voortgebracht;

$$E(\mathbf{Q}) \simeq T \times \mathbf{Z}^r$$

waar T = eindige groep (torsie)
r = geheel ≥ 0 (rang)



[*Received* 1 May, *read* 22 May, 1922.]

§ 1. Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results*, as that of finding the rational solutions†, or say for shortness, the solutions of indeterminate equations of genus unity of the forms

$$\left.\begin{aligned}\zeta^2 &= a\xi^4 + b\xi^3\eta + c\xi^2\eta^2 + d\xi\eta^3 + e\eta^4\\ y^2 &= ax^4 + bx^3 + cx^2 + dx + e\end{aligned}\right\} \quad \ldots\ldots\ldots(1),$$

$$0 = f(x, y, z) \quad \ldots\ldots\ldots(2),$$

where f is a ternary homogeneous cubic in x, y, z, including as a particular case

$$y^2 = 4x^3 - g_2x - g_3 \quad \ldots\ldots\ldots(3);$$

1. De krommen van Fermat: Allebei rang $r = 0$ and torsie (respectievelijk)

$$\begin{aligned} T &= \mathbf{Z}/4\mathbf{Z} \\ T &= \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}\,. \end{aligned}$$

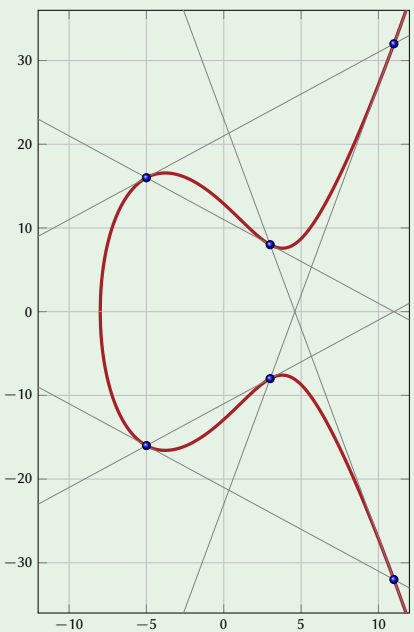
2. De krommen van Diophantus: Gaat over $E_N : y(N-y) = x^3 - x$.

$E_1(\mathbf{Q}) \simeq \mathbf{Z}$	$E_4(\mathbf{Q}) \simeq \mathbf{Z}^2$	$E_7(\mathbf{Q}) \simeq \mathbf{Z}^3$	$E_{10}(\mathbf{Q}) \simeq \mathbf{Z}^3$	$E_{13}(\mathbf{Q}) \simeq \mathbf{Z}^2$
$E_2(\mathbf{Q}) \simeq \mathbf{Z}$	$E_5(\mathbf{Q}) \simeq \mathbf{Z}^3$	$E_8(\mathbf{Q}) \simeq \mathbf{Z}^2$	$E_{11}(\mathbf{Q}) \simeq \mathbf{Z}^3$	$E_{14}(\mathbf{Q}) \simeq \mathbf{Z}^3$
$E_3(\mathbf{Q}) \simeq \mathbf{Z}^2$	$E_6(\mathbf{Q}) \simeq \mathbf{Z}^2$	$E_9(\mathbf{Q}) \simeq \mathbf{Z}^2$	$E_{12}(\mathbf{Q}) \simeq \mathbf{Z}^2$	$E_{15}(\mathbf{Q}) \simeq \mathbf{Z}^2$

Torsie groepen

Wat zijn de mogelijke torsiegroepen T? Bijvoorbeeld, kan er ooit een punt van orde 7 bestaan? Zeker! Het punt $P = (3, 8)$ is van orde 7 op de elliptische kromme

$$E \ : \ y^2 = x^3 - 43x + 166, \qquad (a = 2)$$



Elke E met punt P (niet van orde ≤ 3) heeft *Tate normaalvorm*

$$E : y^2 + uxy + vy = x^3 + vx^2, \qquad P = (0, 0)$$

Uitdrukken dat $7P = 0$ geeft relatie u, v + parametrisatie van **alle** elliptische krommen met een punt van orde 7 als

$$E_a : y^2 - (a^2 - a - 1)xy - (a^3 - a^2)y = x^3 - (a^3 - a^2)x^2$$

Heeft discriminant $\Delta = a^7(a-1)^7(a^3 - 8a^2 + 5a + 1)$.

Terminologie: De *modulaire kromme* $X_1(7)$ is isomorf met $\mathbf{P}^1_a$.
De wortels van Δ zijn de *spitsen* ($\leftrightarrow$ gedegenereerde E_a).

Torsie groepen

Deze methode geeft algemene aanpak! Een elliptische kromme met een punt van orde 11 geeft een rationaal punt op $X_1(11)$, met deze vergelijking

$$X_1(11) \ : \ y^2 + y = x^3 - x^2.$$

Het punt $P := (0, 0)$ is van orde 5, en al haar veelvouden zijn *spitsen*. Een moderne (effectieve) versie van de methode van afdaling kan gebruikt worden om te bewijzen dat

$$X_1(11)(\mathbf{Q}) = \langle P \rangle \simeq \mathbf{Z}/5\,\mathbf{Z}\,.$$

Conclusie: er zijn geen elliptische krommen over $\mathbf{Q}$ met rationaal punt van orde 11.

Theorem (Mazur 1977)

Let $E_{\mathbf{Q}}$ be an elliptic curve. The torsion subgroup T of its Mordell–Weil group $E(\mathbf{Q})$ is isomorphic to one of the following groups:

$$T \simeq \begin{cases} \mathbf{Z}/n\mathbf{Z} & 1 \leq n \leq 10,\ n = 12 \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2n\mathbf{Z} & 1 \leq n \leq 4 \end{cases}$$

Mazur bepaalt alle rationale punten op de krommen $X_1(p)$ voor p priem. Op eindig veel uitzonderingen na, hebben deze krommen geslacht $g > 1$, dus is veel moeilijker!

Weten we nu alles?

Nee! **Torsie** kan ook groeien over lichaamsuitbreidingen.

Er geldt $[11]P = 0$ op de kromme

$$E : y^2 + xy = x^3 + x^2 - 2x - 7,$$

waarbij het punt $P = (\alpha, \beta)$ gegeven wordt door

$$\begin{cases} \alpha &= -2\zeta^8 + 2\zeta^7 - \zeta^6 - \zeta^5 + 2\zeta^4 - 2\zeta^3 - 3 \\ \beta &= -12\zeta^9 - \zeta^8 - 4\zeta^7 - 9\zeta^6 + \zeta^5 - 7\zeta^4 - 6\zeta^3 + 3\zeta^2 - 9\zeta - 3 \end{cases}$$

De Galois groep $\mathrm{Gal}(\mathbf{Q}(\zeta_{11})/\mathbf{Q}) = \{\sigma_i : \zeta_{11} \mapsto \zeta_{11}^i\} \simeq \mathbf{F}_{11}^\times$ werkt als $\sigma_{i^3}(P) = [i]P$.

В своем обзоре [(3), § 22] Касселс отмечает:
«Следующая гипотеза вошла уже в фольклор:
Гипотеза. *Для заданного k (и, в частности, для $k = \mathbf{Q}$) порядок групп Φ ограничен*».
В этой заметке доказана справедливость соответствующего утверждения для p-компонент групп Φ:
ТЕОРЕМА 0. *Пусть p — фиксированное простое число. Существует такая константа c (зависящая лишь от p и k), что порядок группы p-кручения k-точек эллиптической кривой, определенной над k, не превосходит c.*

Het werk van Serre, Manin, Mazur, Merel, ... leert ons veel, maar de classificatie van Galois-structuur op de torsie is nog steeds open (Serre uniformiteit, Mazur's Programma B).

Weten we nu alles?

Hoe zit het met de rangen van elliptische krommen over $\mathbf{Q}$? Kunnen we die classificeren?
De grootst gekende rang is ≥ 28 (Elkies 2006) voor de kromme

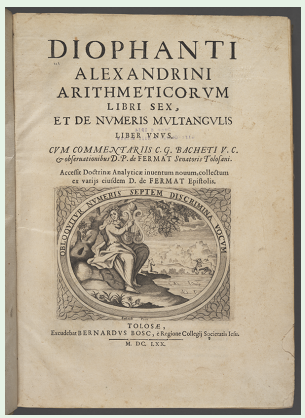
$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x$$
$$+3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

Hoe vaak komt elke rang voor in de oeroude familie elliptische krommen van Diophantus?

$$E_N \ : \ y(N-y) = x^3 - x$$

κδ.

Δοθέντα ἀριθμὸν διελεῖν εἰς δύο ἀριθμούς, καὶ ποιεῖν τὸν ὑπ' αὐτῶν κύβον παρὰ πλευράν.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENT. PRIIS C. G. BACHETI V. C.
& observationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrine Analytice inuentum nouum, collectum
ex variis eiusdem D. de FERMAT Epistolis.
TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.

Methode van afdaling kan geautomatiseerd worden. Voor $N \leq 85000$ vinden we:

r	0	1	2	3	4	5	6	7	8
# N	$< 0.01\%$	$< 0.01\%$	21.96%	41.56%	26.74%	8.33%	1.31%	0.10%	$< 0.01\%$

Is de rang begrensd? Hoe vaak komt elke mogelijkheid voor? ... ?