# De stelling van Granville

**Hendrik Lenstra**
(aantekeningen: Jeanine Daems)

In deze voordracht wordt de (niet gepubliceerde) stelling van Granville geformuleerd, er wordt aangegeven hoe deze stelling nuttig kan zijn voor het zoeken naar ABC-hits en de stelling wordt bewezen.

Het probleem is als volgt: gegeven een getal $N$, zo groot als je maar wilt, vind *alle* ABC-hits tot $N$.

Voorbeeld: Bekijk de diophantische vergelijking $x^2+y^3 = z^7$, waarbij we zoeken naar gehele getallen $x$, $y$ en $z$ waarvoor geldt dat $\text{ggd}(x, y) = 1$. (Doordat we eisen dat de ggd van $x$ en $y$ groter dan 1 is, worden triviale oplossingen als $8^2 + 4^3 = 2^7$, waar in feite $64 \cdot 1 + 64 \cdot 1 = 64 \cdot 2$ staat, uitgesloten.)

Merk op dat voor deze vergelijking de som van de inverse exponenten kleiner dan 1 is: $\frac{1}{2} + \frac{1}{3} + \frac{1}{7} = \frac{41}{42} < 1$. Beschouw de diophantische vergelijking $x^2 + y^3 = z^7$. Stel dat we een oplossing $x$, $y$, $z$ gevonden hebben. Als we dan $a = x^2$, $b = y^3$ en $c = z^7$ nemen, dan volgt dat $a + b = c$ en $\text{rad}(abc) = \text{rad}(x^2 \cdot y^3 \cdot z^7) = \text{rad}(xyz) < c^{\frac{1}{2}+\frac{1}{3}+\frac{1}{7}} = c^{\frac{41}{42}} < c$. We weten dus dat $\text{rad}(abc)^{\frac{42}{41}} < c$, dus elke oplossing van de betreffende vergelijking geeft ons een ABC-hit en volgens het ABC-vermoeden verwachten we nu dat er maar eindig veel oplossingen $x$, $y$, $z$ zijn.

Het klassieke argument om aannemelijk te maken waarom we verwachten dat het aantal oplossingen van een dergelijke vergelijking eindig is, luidt als volgt. Laat $a$, $b$ en $c$ gehele, onderling ondeelbare getallen zijn met $a+b = c$ en $c \leq N$. Het aantal dergelijke drietallen is ongeveer $C \cdot N^2$, voor een zekere constante $C$. Wat is de kans dat een random getal $\leq N$ een kwadraat is? Die kans is ongeveer

$$\text{prob}(a \text{ is een kwadraat}) \sim \frac{\sqrt{N}}{N} = N^{\frac{1}{2}-1}.$$

Op dezelfde manier vinden we

$$\text{prob}(b \text{ is een derde macht}) \sim \frac{\sqrt[3]{N}}{N} = N^{\frac{1}{3}-1} \text{ en}$$

$$\text{prob}(c \text{ is een zevende macht}) \sim \frac{N^{\frac{1}{7}}}{N} = N^{\frac{1}{7}-1}.$$

Als we aannemen dat deze drie kansen onafhankelijk zijn, dan vinden we dat

$$\text{prob}(a \text{ is een kwadraat, } b \text{ is een derde macht en } c \text{ is een zevende macht}) \sim$$

$$\frac{N^{\frac{1}{2}}}{N} \cdot \frac{N^{\frac{1}{3}}}{N} \cdot \frac{N^{\frac{1}{7}}}{N} = \frac{1}{N^2} \cdot \frac{1}{N^{\frac{1}{42}}}.$$

We komen ongeveer $N^2$ van dergelijke drietallen tegen, dus het verwachte aantal successen met $c \leq N$ is ongeveer $\frac{1}{N^{\frac{1}{42}}}$. Dit aantal gaat naar 0 als $N$ naar oneindig gaat, dus we verwachten dat de vergelijking maar eindig veel oplossingen heeft. Dit argument gaat op voor alle diophantische vergelijkingen $x^p + y^q = z^r$ met $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$.

Schaefer, Poonen en Stoll hebben bewezen dat alle oplossing van onze vergelijking zijn:

$$\begin{aligned} x &= 2213459, \quad y = 1414, \quad z = 65 \\ x &= 15312283, \quad y = 9262, \quad z = 113. \end{aligned}$$

Wat is nu de rol van de stelling van Granville in dit verhaal? We kunnen ons afvragen of eenzelfde soort los argument gebruikt zou kunnen worden om het ABC-vermoeden aannemelijk te maken.

Een idee hiervoor komt van Barry Mazur. Definieer $\mathrm{pow}(n)$ voor $n \in \mathbb{Z}_{>0}$ als volgt:

$$\mathrm{pow}(n) = \frac{\log(n)}{\log(\mathrm{rad}(n))} \text{ voor } n \in \mathbb{Z}_{>1} \text{ en } \mathrm{pow}(1) = \infty,$$

dus $n = \mathrm{rad}(n)^{\mathrm{pow}(n)}$ voor alle $n \in \mathbb{Z}_{>0}$. Als $n$ een $k$-de macht is, dan geldt dat $\mathrm{pow}(n) \geq k$.

Zij $a$, $b$ en $c$ gehele getallen met $a + b = c$, dan geldt dus $\mathrm{rad}(a)^{\mathrm{pow}(a)} + \mathrm{rad}(b)^{\mathrm{pow}(b)} = \mathrm{rad}(c)^{\mathrm{pow}(c)}$.

**Vermoeden van Mazur = Stelling van Granville.** Zij $\alpha \in \mathbb{R}, \alpha \geq 1$. Dan geldt

$$\#\{n \leq N : \mathrm{pow}(n) \geq \alpha\} = N^{\frac{1}{\alpha}+o(1)} \ (N \to \infty).$$

Met andere woorden:

$$\lim_{N\to\infty} \left( \frac{\log(\#\{n \leq N : \mathrm{pow}(n) \geq \alpha\})}{\log(N)} \right) = \frac{1}{\alpha}.$$

Als $\mathrm{pow}(n) \geq \alpha$, dan geldt $\mathrm{rad}(n)^\alpha \leq \mathrm{rad}(n)^{\mathrm{pow}(n)} = n \leq N$. Een verscherping van de bovengrens zegt ook dat

$$\lim_{N\to\infty} \left( \frac{\log(\#\{n \leq N : \mathrm{rad}(n) \leq N^{\frac{1}{\alpha}}\})}{\log(N)} \right) = \frac{1}{\alpha}.$$

**Bewijs van de stelling van Granville.**
Het bewijs valt uiteen in twee delen: de ondergrens en de bovengrens.
**Ondergrens.**
Als $\alpha \in \mathbb{Z}_{\geq 1}$, dan weten we dat $\#\{n \leq N : \mathrm{pow}(n) \geq \alpha\} \geq \lfloor \sqrt[\alpha]{N} \rfloor$, want elke $\alpha$-de macht $m$ heeft $\mathrm{pow}(m) \geq \alpha$. Neem vanaf nu aan dat $\alpha \notin \mathbb{Z}_{\geq 1}$. Kies

nu $a, b \in \mathbb{Z}_{\geq 1}$ met $a < \alpha < b$, en beschouw de gehele getallen $n = t^a u^b$ met $t, u \in \mathbb{Z}_{>0}$, waarbij $t$ kwadraatvrij is. Dan geldt dat $\text{rad}(n) \leq tu$.

*Voorbeeld:* Zij $\alpha = \frac{5}{3}$, neem $a = 1$, $b = 2$. We zoeken $n = tu^2$ waarvoor geldt dat

- $\text{rad}(n)^{\frac{5}{3}} \leq n$
- $n \leq N$

Hoe kunnen we dat bereiken? Aan de eerste eis wordt voldaan als $(tu)^{\frac{5}{3}} \leq tu^2 = n$, dus als $t \leq u^{\frac{1}{2}}$ (dus dan geldt $tu^2 \leq u^{2\frac{1}{2}}$). Aan de tweede eis wordt voldaan als $tu^2 \leq N$; omdat volgens de eerste eis moet gelden dat $tu^2 \leq u^{2\frac{1}{2}}$ is het voldoende als $u \leq N^{\frac{2}{5}}$. Dan geldt:

$$\#\{n \leq N : \text{pow}(n) \geq \frac{5}{3}\} \geq \sum_{0<u\leq N^{\frac{2}{5}}, u\in\mathbb{Z}} \#\{t \leq u^{\frac{1}{2}} \text{kwadraatvrij}\}.$$

Hier hebben we gebruikt dat $t$ kwadraatvrij is, want als $t$ deelbaar zou zijn door een kwadraat $> 1$, dan zouden we aan de rechterkant getallen $n = tu^2$ dubbel kunnen tellen. Merk op dat $\#\{t \leq u^{\frac{1}{2}} \text{kwadraatvrij}\} \sim cu^{\frac{1}{2}}$ voor een constante $c$. We vinden dus:

$$\#\{n \leq N : \text{pow}(n) \geq \frac{5}{3}\} \sim c \int_1^{N^{\frac{2}{5}}} u^{\frac{1}{2}} du \sim c' u^{\frac{3}{2}}|_1^{N^{\frac{2}{5}}} \approx c' N^{\frac{3}{5}} = c' N^{\frac{1}{\alpha}}.$$

Ditzelfde gebeurt voor elke $\alpha$, dus hiermee is de ondergrens bewezen.

**Bovengrens.**
In dit bewijs gebruiken we Rankins truc. Er geldt dat

$$\#\{n \leq N : \text{rad}(n) \leq N^{\frac{1}{\alpha}}\} \leq \sum_{n=1}^{\infty} \left( \frac{N^{\frac{1}{\alpha}}}{\text{rad}(n)} \cdot \frac{N}{n} \right).$$

Het is duidelijk dat deze afschatting correct is, maar de som divergeert. Kies nu $\varepsilon \in \mathbb{R}, \varepsilon > 0$. Dan geldt dat

$$\#\{n \leq N : \text{rad}(n) \leq N^{\frac{1}{\alpha}}\} \leq \sum_{n=1}^{\infty} \left( \frac{N^{\frac{1}{\alpha}}}{\text{rad}(n)} \right)^{1+\varepsilon} \cdot \left( \frac{N}{n} \right)^{\varepsilon} = N^{\frac{1}{\alpha}(1+\varepsilon)+\varepsilon} \cdot f(\varepsilon).$$

Hierbij is

$$f(\varepsilon) = \sum_{n=1}^{\infty} \left( \frac{1}{\text{rad}(n)} \right)^{1+\varepsilon} \frac{1}{n^{\varepsilon}} = \prod_{p \text{ priem}} \left( 1 + \frac{1}{p^{1+\varepsilon}} \left( \frac{1}{p^{\varepsilon}} + \frac{1}{p^{2\varepsilon}} + \frac{1}{p^{3\varepsilon}} + \ldots \right) \right).$$

We willen laten zien dat $f(\varepsilon)$ eindig is. We weten echter dat

$$\frac{1}{p^{\varepsilon}} + \frac{1}{p^{2\varepsilon}} + \frac{1}{p^{3\varepsilon}} + \ldots = \frac{1}{p^{\varepsilon} - 1} \leq \frac{1}{2^{\varepsilon} - 1}.$$

We kunnen $f(\varepsilon)$ dus afschatten door

$$f(\varepsilon) \leq \prod_{p \text{ priem}} (1 + \frac{1}{p^{1+\varepsilon}} \cdot \frac{1}{2^{\varepsilon} - 1}).$$

Omdat

$$\sum_{p\ priem} \frac{1}{p^{1+\varepsilon}} \cdot \frac{1}{2^{\varepsilon} - 1} = \frac{1}{2^{\varepsilon} - 1} \sum_{p \text{ priem}} \frac{1}{p^{1+\varepsilon}}$$

convergeert, volgt nu dat $f(\varepsilon)$ eindig is.

Er geldt dus dat

$$\frac{\log(\#\{n \leq N : \text{rad}(n) \leq N^{\frac{1}{\alpha}}\})}{\log(N)} \leq \frac{1}{\alpha}(1 + \varepsilon) + \varepsilon + \frac{\log(f(\varepsilon))}{\log(N)}.$$

Dus

$$\limsup_{N \to \infty} \frac{\log(\#\{n \leq N : \text{rad}(n) \leq N^{\frac{1}{\alpha}}\})}{\log(N)} \leq \frac{1}{\alpha}(1 + \varepsilon) + \varepsilon.$$

Laat nu $\varepsilon \to 0$, dan vinden we dat

$$\limsup_{N \to \infty} \frac{\log(\{n \leq N : \text{rad}(n) \leq N^{\frac{1}{\alpha}}\})}{\log(N)} \leq \frac{1}{\alpha}.$$

Dit is precies wat we wilden bewijzen.