H.E. Reijngoud

Kwaliteit van ABC-drietallen

Bachelorscriptie, 11 juni 2010

Scriptiebegeleider: Dr. B. de Smit

Mathematisch Instituut, Universiteit Leiden

Inhoudsopgave

1 Het ABC-vermoeden

In 1985 is het ABC-vermoeden bedacht door de wiskundigen David Masser en Joseph Oesterlé. Het vermoeden is een vrij eenvoudig probleem, waar geen diepe wiskunde voor nodig is om het te begrijpen. Het vermoeden bewijzen echter is een heel ander verhaal. Daar gaan wij ons in deze scriptie dan ook niet aan wagen.
Voordat we verder kunnen gaan, moeten we eerst enkele begrippen introduceren.

Definitie 1. Het radicaal $r(n)$ van een positief geheel getal n is gedefinieerd als het product van de priemdelers van n;

$$r(n) = \prod_{\substack{p|n \\ p \text{ priem}}} p. \tag{1}$$

Dus $r(54) = r(2 \cdot 3^3) = 2 \cdot 3 = 6$ en $r(38) = r(2 \cdot 19) = 2 \cdot 19 = 38$.

Definitie 2. Een ABC-drietal is een drietal $a, b, c \in \mathbb{Z}_{>0}$ zodanig dat:

i. $a + b = c$;

ii. $ggd(a, b, c) = 1$;

iii. $r(abc) < c$.

Definitie 3. De kwaliteit q van een ABC-drietal wordt gegeven door:

$$q = \frac{\log c}{\log r(abc)}. \tag{2}$$

De kwaliteit van een ABC-drietal is dus altijd groter gelijk 1. Alle ABC-drietallen onder de 100 zijn te vinden in tabel 1, samen met hun radicaal en kwaliteit.

a	b	c	$r(abc)$	$q = \frac{\log(c)}{\log(r(abc))}$
1	8	9	6	1,2263
5	27	32	30	1,0190
1	48	49	42	1,0412
1	63	64	42	1,1127
1	80	81	30	1,2920
32	49	81	42	1,1757

Stelling 4. *Er zijn oneindig veel ABC-drietallen.*

Bewijs. Stel $n \in \mathbb{Z}_{\geq 1}$. Neem $a = 1$, $b = 9^n - 1$ en $c = 9^n$. Dan heeft a geen priemfactoren, c heeft alleen 3 als priemfactor en b heeft als deler $8 = 2^3$. Dus $r(b) \leq \frac{b}{4}$. Nu geldt

$$r(abc) \leq r(a)r(b)r(c) \leq \frac{3b}{4} < c. \tag{3}$$

En dus is $(1, 9^n - 1, 9^n)$ een ABC-drietal voor elk natuurlijk getal n. □

Het ABC-vermoeden luidt nu:

Vermoeden 5. *Voor alle $\alpha > 1$ bestaan er slechts eindig veel ABC-drietallen met $q \geq \alpha$.*

Als een sterke versie van dit vermoeden waar is, dan kunnen we dit gebruiken om, bijvoorbeeld, "De laatste stelling van Fermat"te bewijzen. Er is nu al wel een bewijs van deze stelling, maar dit is zeer complex en maar voor enkelen begrijpelijk.

Stelling 6. *Stel er bestaan geen ABC-drietallen met een kwaliteit $q \geq 2$. Dan geldt voor $n > 2 \in \mathbb{Z}$, dat er geen positieve x, y en z bestaan zodat $x^n + y^n = z^n$.*

Bewijs. Stel er bestaan getalen x, y en z zodanig dat $x^n + y^n = z^n$. Dan is dit een ABC-drietal met $a = x^n$, $b = y^n$ en $c = z^n$. Hiervoor geldt $r(a) = r(x)$, $r(b) = r(y)$ en $r(c) = r(z)$ en dus $r(abc) \leq r(xyz) \leq xyz \leq z^3$.

$$q = \frac{\log(c)}{\log(r(abc))} \geq \frac{\log(z^n)}{\log(z^3)} = \frac{n\log(z)}{3\log(z)} = \frac{n}{3}. \tag{4}$$

Als we nu aannemen dat er geen ABC-drietallen bekend zijn met een kwaliteit $q \geq 2$, dan volgt dat $n \leq 6$. Maar voor $n = 3, 4, 5$ zijn er al relatief eenvoudige bewijzen voor de stelling van Fermat. [6] □

2 ABC-drietallen maken

Als we de kwaliteit uitrekenen voor het drietal $(1, 9^n - 1, 9^n)$ zien we dat de ondergrens van de kwaliteit steeds lager wordt als we n groter nemen.

$$\begin{aligned}
q &= \frac{\log(c)}{\log(r(abc))} && (5)\\
&\geq \frac{\log(c)}{\log(\frac{3b}{4})} && (6)\\
&= \frac{n\log 9}{\log(\frac{3}{4}) + \log(b)} && (7)\\
&> \frac{n\log 9}{\log(\frac{3}{4}) + \log(c)} && (8)\\
&= \frac{2n\log 3}{2n\log 3 + \log(\frac{3}{4})} && (9)\\
&= 1 + \frac{\log\frac{4}{3}}{2n\log 3} && (10)\\
&> 1 + \frac{1}{8n}. && (11)
\end{aligned}$$

Als het ABC-vermoeden waar is, kunnen we op geen enkele manier een rijtje ABC-drietallen maken waarvoor de kwaliteit niet-dalend is. We gaan dus op zoek naar een methode om oneindig veel drietallen te maken, maar waarvan de kwaliteit zo langzaam mogelijk naar 1 zal gaan.

Om een beeld te krijgen van hoe groot de kwaliteit is die we zouden willen bereiken en hoe moeilijk dit waarschijnlijk is, hebben we de volgende tabel opgenomen:

kwaliteit groter dan	aantal tot nu toe gevonden	laatste gevonden$^{(*)}$
1.6	3	Brzezinski, 4 januari 1994
1.5	13	Dokchitser, 8 april 2003
1.4	229	Rubin,23 april 2010

((*)voor recent gevonden drietallen kijk op http://www.math.leidenuniv.nl/ desmit/abc/)
Het drietal met de hoogste kwaliteit die tot nu toe bekend is, is $2 + 3^{10} \cdot 109 = 23^5$. Dit drietal heeft kwaliteit $q = 1.6299$ en is gevonden door de Franse wiskundige Eric Reyssat in 1987.

3 Twee priemen

Geïnspireerd door het drietal van Reyssat gaan we eerst proberen een 'makkelijk' drietal te maken. Met makkelijk bedoelen we hier een drietal met weinig verschillende priemdelers. We bekijken het geval dat $r(bc) = 6$.

Stelling 7. *Er bestaat een $\delta > 0$ zodanig dat er oneindig veel ABC-drietallen (a, b, c) bestaan met $r(bc) = 6$ en*

$$q \geq 1 + \frac{\log(\log c) - \delta}{\log c}. \tag{12}$$

Het bewijs van deze stelling zullen we aan het einde van paragraaf 4 geven. Hier geven we een een schets van de methode.

Stel (a, b, c) is een ABC-drietal met $r(bc) = 6$. Dan is $\frac{b}{c} = 2^x 3^y$ met $x, y \in \mathbb{Z}, xy < 0$.

Het maximaliseren van $q = \frac{\log(c)}{\log(r(abc))}$ is natuurlijk hetzelfde als $\frac{\log(r(abc))}{\log(c)}$ minimaliseren.

Merk op:

$$\frac{\log(r(abc))}{\log(c)} = \frac{\log(r(a))}{\log(c)} + \frac{\log(r(bc))}{\log(c)} \leq \frac{\log(a)}{\log(c)} + \frac{\log 6}{\log(c)}. \tag{13}$$

De term $\frac{\log 6}{\log(c)}$ is klein. We willen dus $\frac{\log(a)}{\log(c)}$ minimaliseren. Omdat $a = c - b$, willen we dus bereiken dat $b \approx c$. En dus $\frac{b}{c} \approx 1$ en $\log(\frac{b}{c}) \approx 0$, oftewel $x \log 2 + y \log 3 \approx 0$. Voor het oplossen van dit soort problemen bestaan erg mooie technieken. Eén van die technieken is het vertalen van het vinden van een paar (x, y), naar het vinden van een korte vector in een rooster. De paren (x, y) maken op natuurlijke wijze een rooster, namelijk het rooster $\mathbb{Z}^2$ (x en y mogen namelijk alleen gehele getallen zijn).

In dit rooster willen we een norm, zodat we over afstand en lengte kunnen praten. Maar niet de standaard norm, want dan zou $(0, 1)$ een kortste vector zijn, en $2 + 1 = 3$ is geen ABC-drietal.

De kwadratische vorm welke wij nemen is:

$$Q(x, y) = (x \log 2)^2 + (y \log 3)^2 + N(x \log 2 + y \log 3)^2 \tag{14}$$

met $N \in \mathbb{Z}_{>0}$, deze zullen wij later bepalen.

Merk op dat $Q(x, y) = 0$ dan en slechts dan als $x = 0$ én $y = 0$. Als $Q(x, y)$ klein is, dus als we een korte vector hebben, dan zijn alle 3 de termen klein. Als N groot is, moet $x \log 2 + y \log 3$ heel klein zijn. Enerzijds willen we nu dus N heel groot maken, zodat $x \log 2$ en $y \log 3$ opgeteld bijna 0 zijn (en dus a klein en de kwaliteit hoger).

Met 2 priemen hebben we het geluk dat er altijd een kortste vector te vinden is, maar het zal wel steeds moeilijker worden.

Deze ideeën zullen we gaan gebruiken in de volgende sectie.

4 Minkowski

Neem V een eindig dimensionale vectorruimte over $\mathbb{R}$. Een kwadratische vorm op V is een afbeelding

$$Q : V \longrightarrow \mathbb{R} \tag{15}$$

met

(i) $Q(\lambda v) = \lambda^2 Q(v), \forall \lambda \in \mathbb{R}, \forall v \in V$,

(ii) $Q(v) = 0 \Leftrightarrow v = 0$,

(iii) $\langle , \rangle : V \times V \longrightarrow R$
$\langle v, w \rangle \mapsto \frac{1}{2}(Q(v + w) - Q(v) - Q(w))$is bilineair.

Merk op dat $\langle , \rangle$ een inproduct is en $\langle v, v \rangle = Q(v)$.

Als $V = \mathbb{R}^m$ en $Q(x_1 \cdots x_m) = x_1^2 + \cdots + x_m^2 = \|x\|^2$ de standaard norm, dan is $\langle x, y \rangle = \sum_i x_i y_i$ het standaard inproduct.

Een ondergroep $L \subset V$ heet een rooster, als L een stel voortbrengers $e_1, \ldots, e_n$ heeft dat lineair onafhankelijk is over $\mathbb{R}$.

Definitie 8. Laat L een rooster, Q een kwadratische vorm en $\langle , \rangle$ het inproduct dat bij Q hoort. Zij $e_1, e_2, \ldots, e_n$ een basis van L, dan is

$$d(L) := \sqrt{|\det(\langle e_i, e_j \rangle)_{i,j}|} \tag{16}$$

de determinant van het rooster.

Lemma 9. *De determinant $d(L)$ is onafhankelijk van de keuze van de basis $e_1, e_2, \ldots, e_n$.*

Bewijs. Zij $f_1, f_2, \ldots, f_n$ een andere basis van het rooster L en M de basistransformatiematrix van e naar f. De matrix M en ook M^{-1} hebben coëfficienten in $\mathbb{Z}$, want f_i is een roosterpunt en dus een gehele combinatie van de e_j's, en omgekeerd. Dus $\det(M) = \pm 1$.

Nu geldt

$$\sqrt{|\det(\langle f_i, f_j \rangle)_{i,j}|} = \sqrt{|\det(\langle e_i, e_j \rangle)_{i,j} \cdot \det(M)^2|} = \sqrt{|\det(\langle e_i, e_j \rangle)_{i,j}|}. \tag{17}$$

□

Lemma 10. *Laat $N \in \mathbb{R}_{>0}$. Zij $L = \mathbb{Z}^2$, $Q(x,y) = (x \log 2)^2 + (y \log 3)^2 + N(x \log 2 + y \log 3)^2$. Dan $d(L) = (\log 2)(\log 3)\sqrt{1+2N}$.*

Bewijs. Neem $e_1 = (1,0)^T$ en $e_2 = (0,1)^T$. Dan geldt

$$\langle e_1, e_1 \rangle = Q(e_1) = (\log 2)^2(1+N) \tag{18}$$

en

$$\begin{aligned}
\langle e_2, e_1 \rangle &= \langle e_1, e_2 \rangle && (19)\\
&= \frac{1}{2}\left((\log 2)^2 + (\log 3)^2 + N(\log 2 + \log 3)^2\right. && (20)\\
&\quad -((\log 2)^2 + N(\log 2)^2) - ((\log 3)^2 + N(\log 3)^2) && (21)\\
&= N(\log 2)(\log 3).
\end{aligned}$$

(23)

En dus:

$$\begin{aligned}
d(L)^2 &= \begin{vmatrix} \langle e_1, e_1 \rangle & \langle e_2, e_1 \rangle \\ \langle e_1, e_2 \rangle & \langle e_2, e_2 \rangle \end{vmatrix} && (24)\\
&= \begin{vmatrix} (\log 2)^2(1+N) & N(\log 2)(\log 3) \\ N(\log 2)(\log 3) & (\log 3)^2(1+N) \end{vmatrix} && (25)\\
&= (\log 2)^2(\log 3)^2 \cdot (1+N)^2 - N^2(\log 2)^2(\log 3)^2 && (26)\\
&= (\log 2)^2(\log 3)^2(1+2N) && (27)\\
&= ((\log 2)(\log 3)\sqrt{1+2N})^2. && (28)
\end{aligned}$$

□

Lemma 11. *Zij $L \subset \mathbb{R}^n$ een rooster, Q een kwadratische vorm met bijbehorend inproduct $\langle , \rangle$ en $x \in \mathbb{R}^n$ zodanig dat $\forall l \in L : \langle x, l \rangle = 0$. Laat $L' = L \oplus x \cdot \mathbb{Z}$.*
Dan geldt $d(L') = \sqrt{Q(x)} \cdot d(L)$.

Bewijs. Zij $e_1, e_2, \ldots, e_k$ een basis van L. Noem $x = e_0$, dan is $e_0, e_1, \ldots, e_k$ een basis van $L^{'}$.

$$d(L^{'}) = \sqrt{|\det(\langle e_i, e_j\rangle)_{i,j}|} \tag{29}$$

$$= \sqrt{\left|\begin{pmatrix} \langle x,x\rangle & 0 & \cdots & 0 \\ 0 & \langle e_1,e_1\rangle & & * \\ \vdots & & \ddots & \\ 0 & * & & \langle e_k,e_k\rangle \end{pmatrix}\right|} \tag{30}$$

$$= \sqrt{|\langle x,x\rangle \cdot \det(\langle e_i,e_j\rangle)_{i,j\geq 1}|} \tag{31}$$

$$= \sqrt{Q(x)} \cdot d(L). \tag{32}$$

□

Een andere manier om het volume van ons rooster uit te rekenen is nu als volgt:
Bekijk de afbeelding $L = \mathbb{Z}^2 \hookrightarrow \mathbb{R}^3$ welke gegeven wordt door

$$\Phi : (x,y) \mapsto \begin{pmatrix} x\log 2 \\ y\log 3 \\ \sqrt{N}(x\log 2 + y\log 3) \end{pmatrix}. \tag{33}$$

Opmerking: Voor alle $(x,y) \in \mathbb{Z}^2$ geldt $Q(x,y) = ||\Phi(x,y)||^2$, waarbij $||.||$ de standaard norm op $\mathbb{R}^3$ is.

Een vector die loodrecht op ons rooster $\Phi(L)$ staat is: $\begin{pmatrix} \sqrt{N} \\ \sqrt{N} \\ -1 \end{pmatrix}$. De norm van deze vector is $\sqrt{1+2N}$. Wegens lemma 11;

$$d(L)\cdot\sqrt{1+2N} = \left|\begin{vmatrix} \log 2 & 0 & \sqrt{N} \\ 0 & \log 3 & \sqrt{N} \\ \sqrt{N}\log 2 & \sqrt{N}\log 3 & -1 \end{vmatrix}\right| \tag{34}$$

$$= \left|\begin{vmatrix} \log 2 & 0 & 0 \\ 0 & \log 3 & 0 \\ * & * & -1-2N \end{vmatrix}\right| \tag{35}$$

$$= (\log 2)(\log 3)(1+2N). \tag{36}$$

En dus $d(L) = (\log 2)(\log 3)\sqrt{1+2N}$.

In 1889 heeft Hermann Minkowski de volgende stelling bewezen:

Stelling 12 (Minkowski)**.** *Elk rooster L met positieve rang n bevat een niet-nul element x waarvoor geldt $Q(x) \leq \frac{4}{\pi} \cdot \frac{n}{2}!^{2/n} \cdot d(L)^{2/n} \leq n \cdot d(L)^{2/n}$.*

In ons geval betekent dit het volgende: $L = \mathbb{Z}^2$, dus de rang is 2. En dus is er een $x \in \mathbb{Z}^2/\{0\}$ zodat $Q(x) \leq \frac{4}{\pi} \cdot d(L)$.

Omdat we in een twee-dimensionaal rooster werken, kunnen we vrij eenvoudig zien of we dit resultaat kunnen verbeteren. Volgens [1] is het best mogelijke resultaat de Hermite constate $\gamma_2 = \sqrt{\frac{4}{3}}$. Het is namelijk zo dat $\frac{4}{\pi} \approx 1.27$ en $\sqrt{\frac{4}{3}} \approx 1.15$.

Een bewijs van de stelling van Minkowski kan gevonden worden in [1]. In het bewijs wordt alleen aangetoond dat er zo'n vector bestaat, niet hoe we deze kunnen vinden.

Bewijs. (stelling 7) Neem $L = \mathbb{Z}^2$. Voor elke $N > 54,8$ en $N \in \mathbb{R}$,gaan we een ABC-drietal maken.

$$Q(x,y) = Q_N(x,y) = (x\log(2))^2 + (y\log(3))^2 + N(x\log(2) + y\log(3))^2. \tag{37}$$

met behulp van lemma 10 weten we; $d(L) = (\log(2))(\log(3))\sqrt{1+2N}$. En met behulp van stelling 12 weten we dat er (x,y) bestaan zodat $Q(x,y) < 2d(L) = 2(\log(2))(\log(3))\sqrt{1+2N}$.

Laat (x,y) als in stelling 12. Neem $\mathcal{C}_2 = 6(\log 2)(\log 3)$ dan kunnen we $Q(x,y)$ afschatten met $\mathcal{C}_2\sqrt{N}$.Voor x,y en $t = x\log 2 + y\log 3$ moeten we iets meer werk doen. In het slechtste geval (dus x zo groot mogelijk), geldt dat $Q(x,y) = (x\log 2)^2$, en dus dat $x < \frac{\sqrt{\mathcal{C}_2}}{\log(2)}\sqrt[4]{N}$. Op dezelfde manier krijgen we $y < \frac{\sqrt{\mathcal{C}_2}}{\log 3}\sqrt[4]{N}$ en $t < \frac{\sqrt{\mathcal{C}_2}}{\sqrt[4]{N}}$.
We hebben al afgeschat dat

$$\frac{\sqrt{\mathcal{C}_2}}{\sqrt[4]{N}} > |t| = |x\log 2 + y\log 3| = |\log(\frac{b}{c})| = |\log(1-\frac{a}{c})|. \tag{38}$$

Voor $0 < x < 1$, geldt $|\log(1-x)| = x + \frac{x^2}{2} + \frac{x^3}{3} + O(x^4)$. En dus $x < |\log(1-x)|$. We hebben $0 < \frac{a}{c} < 1$. We mogen dus schrijven $|\log(1-\frac{a}{c})| > \frac{a}{c}$. Hieruit volgt $\frac{c}{a} > \frac{\sqrt[4]{N}}{\sqrt{\mathcal{C}_2}}$ en dus $\log(\frac{c}{a}) > \frac{1}{4}\log N - \frac{1}{2}\log\mathcal{C}_2$.
Nu kunnen we een afschatting gaan maken voor de kwaliteit q. Omdat $ggd(a,b,c) = 1$ geldt $r(abc) = r(a)r(b)r(c)$ en omdat b,c alleen bestaan uit een veelvoud van 2 of van 3 geldt $r(abc) = 6r(a)$. En dus

$$\log r(abc) = \log 6 + \log r(a) \leq \log 6 + \log a. \tag{39}$$

Nu hebben we

$$\begin{aligned} q &= \frac{\log c}{\log r(abc)} && (40)\\ &\geq \frac{\log c}{\log a + \log 6} && (41)\\ &= \frac{1}{1 - \frac{\log c - \log a - \log 6}{\log c}} && (42)\\ &\geq 1 + \frac{\log(c/a) - \log 6}{\log c}. && (43) \end{aligned}$$

De laatste ongelijkheid mogen we gebruiken, omdat voor alle $x < 1$ geldt dat $\frac{1}{1-x} \geq 1 + x$.

Stel dat $c = 2^x$, dan kunnen we $\log c$ afschatten met:

$$x\log 2 \leq \frac{\sqrt{\mathcal{C}_2}}{\log 2}\sqrt[4]{N}\log 2 = \sqrt{\mathcal{C}_2}\sqrt[4]{N}. \tag{44}$$

Als $c = 3^y$, dan krijgen we op dezelfde manier dat $\log(c) \leq \sqrt{\mathcal{C}_2}\sqrt[4]{N}$.
Als we dit combineren krijgen we:

$$q \geq 1 + \frac{\frac{1}{4}\log N - \frac{1}{2}\log\mathcal{C}_2 - \log(6)}{\log(c)}. \tag{45}$$

Omdat $\log(\log(c)) \leq \frac{1}{2}\log(\mathcal{C}_2) + \frac{1}{4}\log(N)$, geldt $\frac{1}{4}\log(N) \geq \log(\log(c)) - \frac{1}{2}\log(\mathcal{C}_2)$. En dus

$$q \geq 1 + \frac{\log(\log(c)) - \delta}{\log(c)} \tag{46}$$

met $\delta = \frac{3}{2}\log(2(\log(2))(\log(3))) + \log(6)$.

Als $N > 54,8 > \mathcal{C}_2 \cdot 6^2 = 72(\log(2)(\log(3))$, dus $\frac{1}{4}\log(N) - \frac{1}{2}\log(\mathcal{C}_2) - \log(6) > 0$ en is de kwaliteit q groter dan 1.

Voor elke $N > 54,8$ vinden we nu een ABC-drietal (a_N, b_N, c_N). Dit kunnen niet allemaal dezelfde drietallen zijn, omdat we al eerder hebben gezien dat moet gelden $\sqrt[4]{N} < \frac{\sqrt{\mathcal{C}_2}}{t}$.

Dus er bestaan oneindig veel ABC-drietallen (a, b, c) met $r(bc) = 6$ en

$$q \geq 1 + \frac{\log(\log c) - \delta}{\log c} \tag{47}$$

voor zekere $\delta > 0$. □

Merk op dat een hogere N niet automatisch een ABC-drietal met een hogere kwaliteit oplevert. Stel nu dat we $N = 10000$ nemen. Dan geven de afschattingen dat $x < 19.55$ en $y < 12.34$. Omdat $2^{19} < 3^{12}$ is nu $b = 2^{19} = 524288$, $c = 3^{12} = 531441$ en $a = 7153 = 23 \cdot 311$. We hebben nu dus een ABC-drietal met kwaliteit $q = \frac{\log(3^{12})}{\log(2\cdot 3\cdot 23\cdot 311)} \approx 1.236$. We weten ook al dat $3^5 + 13 = 2^8$ een ABC-drietal is, en wel met $q = \frac{\log(2^8)}{\log(2\cdot 3\cdot 13)} \approx 1.27$. Dit is een 'beter' ABC-drietal dan welke we daarnet gevonden, zodat we dus alle combinaties van x en y moeten uitproberen om het drietal met de hoogste kwaliteit te krijgen.

5 Meer priemen

Stel dat we een ABC-drietal gaan maken waarbij de b en de c uit de eerste n priemgetallen, $p_1, p_2, \ldots, p_n$ mogen bestaan. We willen $y_1, \ldots, y_n, z_1, \ldots, z_n \in \mathbb{Z}_{\geq 0}$ vinden zodanig dat $y_i \neq 0 \Rightarrow z_i = 0$ én $z_i \neq 0 \Rightarrow y_i = 0$. Dan definiëren we $b = p_1^{y_1} \cdots p_n^{y_n}$ en $c = p_1^{z_1} \cdots p_n^{z_n}$. Merk op dat de eis die we aan de y_i's en de z_i's hebben opgelegd ervoor zorgen dat b en c copriem zijn. Bovendien willen we dat $c - b = a$ klein is, dus $\frac{b}{c} = \frac{p_1^{y_1}\cdots p_n^{y_n}}{p_1^{z_1}\cdots p_n^{z_n}}$ zal dicht bij 1 moeten liggen. Definieer nu x_i voor $i = 1, \ldots, n$ door $\frac{b}{c} = p_1^{x_1} \cdots p_n^{x_n}$ met $x_i \in \mathbb{Z}$ (dus $x_i = y_i - z_i$ en als x_i positief is, dan is $p_i^{x_i}$ een deler van b en als p_i negatief is, dan is $p_i^{-x_i}$ een deler van c).

Als $\frac{b}{c} \approx 1$, dan geldt $\log(\frac{b}{c}) \approx 0$, oftewel $x_1\log(p_1) + \cdots + x_n\log(p_n) \approx 0$.

Neem $L = \mathbb{Z}^n \subset V = \mathbb{R}^n$, met Q gegeven door $Q(x_1, x_2, \ldots, x_n) = Q(\bar{x}) = \sum_i (x_i \log(p_i))^2 + N(\sum_i x_i \log(p_i))^2$, met $N \in \mathbb{R}_0$ nog nader te bepalen.

Om nu het volume $d(L)$ van ons rooster te bepalen bekijken we de volgende afbeelding: $L \hookrightarrow \mathbb{R}^{n+1}$ gegeven door $\bar{x} \mapsto \Big((x_i \log p_i)_{i=1}^n, (\sum x_i \log p_i) \cdot \sqrt{N}\Big)$. De vector loodrecht op ons rooster is dan $(\sqrt{N}, \sqrt{N}, \ldots, \sqrt{N}, -1)^T \cdot \mathbb{R}$. Op dezelfde manier als voor 2 priemen kunnen we nu uitrekenen:

$$d(L) \cdot \sqrt{1 + nN} \quad = \quad |\det \begin{pmatrix} \log(p_1) & 0 & \cdots & 0 & \sqrt{N} \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & \log(p_n) & \sqrt{N} \\ \log(p_1)\sqrt{N} & \cdots & & \log(p_n)\sqrt{N} & -1 \end{pmatrix}| \tag{48}$$

$$= \quad |\det \begin{pmatrix} \log(p_1) & 0 & \cdots & 0 & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & \log(p_n) & 0 \\ * & \cdots & & * & -1-nN \end{pmatrix}| \tag{49}$$

$$= \quad (\prod_i \log p_i)(1+nN). \tag{50}$$

En dus $d(L) = (\prod_i \log p_i)\sqrt{1+nN}$.

Er bestaat wegens stelling 12 een vector met lengte

$$Q(\bar{x}) \leq \frac{4}{\pi} \cdot \frac{n}{2}!^{2/n} \cdot \left((\prod_i \log p_i)\sqrt{1+nN}\right)^{2/n} \leq n \cdot \left((\prod_i \log p_i)\sqrt{1+nN}\right)^{2/n}. \tag{51}$$

We zullen het volgende lemma van Stewart en Tijdeman gaan gebruiken.

Lemma 13. *Zij $p_1 < p_2 < \ldots < p_n$ de eerste n priemgetallen en zij $\delta > 0$. Dan hebben we, voor voldoende grote n;*

i $p_n < n\log(n) + n\log(\log(n)) - (1-\delta)n$;

ii $\sum_{i=1}^{n} \log p_i < n\log(n) + n\log(\log(n)) - (1-\delta)n$;

iii $\sum_{i=1}^{n} (\log\log(p_i)) < n(\log\log(n) + \delta)$.

Bewijs. Zie [2]. □

5.1 Kwaliteit met Minkowski-grens

In deze sectie zullen we een bewijs geven, geïnspireerd op het bewijs van stelling 2 uit [2].

Stelling 14. *Er bestaan oneindig veel ABC-drietallen (a,b,c) met kwaliteit*

$$q > 1 + \frac{2}{\sqrt{\log(c)}\log\log(c)}. \tag{52}$$

Bewijs. We willen N kiezen zodat $d(L) = n^n(\log(n))^{2n}$.
Hiervoor definiëren we $N \in \mathbb{R}$ $(N > -\frac{1}{n})$ door

$$n\log(n) + 2n\log\log(n) = \sum_{i=1}^{n} \log\log(p_i) + \frac{1}{2}(\log(n) + \log(N + \frac{1}{n})). \tag{53}$$

We hebben nu:

$$\begin{aligned} \frac{1}{2}\log(N+\frac{1}{n}) \quad &= \quad n\log(n) && (54)\\ &\quad +n\log\log(n) && (55)\\ &\quad +n\log\log(n) && (56)\\ &\quad -\sum \log\log(p_i) && (57)\\ &\quad -\frac{1}{2}\log(n) && (58) \end{aligned}$$

Zij $\delta > 0$ en n voldoende groot. Wegens lemma 13(iii) geldt dan

$$n \log\log(n) - \sum \log\log(p_i) > \delta n \tag{59}$$

Dus dan hebben we

$$\frac{1}{2}\log(N + \frac{1}{n}) > (n - \frac{1}{2})\log(n) + n(\log\log(n) - \delta) \tag{60}$$

Merk op dat dit een stijgende functie is en zelfs naar ∞ gaat als n groeit.
In het bijzonder geldt nu voor n voldoende groot

$$\frac{1}{2}\log(N + \frac{1}{n}) > 0 \tag{61}$$

en dus $N + \frac{1}{n} > 1$ en dus $N > 0$.

En dan is L gedefiniëerd met Q zodat $d(L) = n^n(\log(n))^{2n}$.

De stelling van Minkowski(stelling 12) vertelt ons dan dat er een $\bar{x} \in L, \bar{x} \neq 0$ is zodat

$$Q(\bar{x}) \leq n \cdot d(L)^{2/n} = n \cdot (n^n \cdot (\log(n))^{2n})^{2/n} = n \cdot (n^2 \cdot (\log(n)^4) = n^3 \cdot (\log(n))^4. \tag{62}$$

Op soortgelijke wijze als voor 2 priemen kunnen we nu een ondergrens voor de kwaliteit q vinden. De getallen b en c bestaan alleen uit machten van de eerste n priemgetallen én ggd(b,c)=1. Definiëer b en c uit $(x_1, \cdots, x_n) \in L$ zodanig dat $p_i^{x_i} | b$ als $x_i > 0$ en $p_i^{x_i} | c$ als $x_i < 0$. We kunnen dus schrijven:

$$\frac{b}{c} = p_1^{x_1} p_2^{x_2} \cdots p_n^{x_n}. \tag{63}$$

En dus

$$\begin{aligned} \log(r(abc)) &= \log(r(a)) + \log(r(bc)) && (64)\\ &\leq \log(r(a)) + \sum_{i=1}^{n} \log(p_i) && (65)\\ &\leq \log(a) + \sum_{i=1}^{n} \log(p_i). && (66) \end{aligned}$$

Nu geldt dus

$$\begin{aligned} q &= \frac{\log(c)}{\log(r(abc))} && (67)\\ &\geq \frac{\log(c)}{\log(a) + \Sigma \log(p_i)} && (68)\\ &= \frac{1}{1 - \frac{\log(c) - \log(a) - \Sigma \log(p_i)}{\log(c)}}. && (69) \end{aligned}$$

Omdat $\log(c) - \log(a) = \log \frac{c}{a}$ én $0 < \frac{log(c) - \log(a) - \Sigma \log(p_i)}{\log(c)} < 1$ geldt:

$$q \geq 1 + \frac{\log(\frac{c}{a}) - \Sigma \log(p_i)}{\log(c)}. \tag{70}$$

Verder weten we dat

$$\frac{a}{c} \leq |\log(1 - \frac{a}{c})| = \log|\frac{b}{c}| = |\Sigma(x_i \log(p_i))| \leq \frac{1}{\sqrt{N}}\sqrt{Q(\bar{x})}. \tag{71}$$

Met de laatste ongelijkheid omdat $Q(\bar{x}) = N(\sum (x_i \log(p_i)))^2 + \sum (x_i \log(p_i))^2$
en $\sum (x_i \log(p_i))^2 > 0$.
Dus

$$\begin{aligned} \log(c) - \log(a) &> \frac{1}{2}\log(N) - \frac{3}{2}\log(n) - 2\log\log(n) && (72) \\ &> n\log(n) + n\log\log(n) - \delta n && (73) \end{aligned}$$

(laatste stap wegens (61)).
Dus $\log(c) - \log(a) - \sum \log(p_i) > (1-\delta)n$, en dus

$$q \geq 1 + \frac{(1-\delta)n}{\log(c)}. \tag{74}$$

We hebben b en c zo gemaakt dat $\log(c) + \log(b) = \sum (|x_i| \log(p_i))$. En dus

$$\begin{aligned} \log(c) &\leq \sum (|x_i| \log(p_i)) && (75) \\ &\leq \sqrt{n} \cdot \sqrt{Q(\bar{x})} && (76) \\ &\leq n^2 (\log(n))^2. && (77) \end{aligned}$$

(Voor de tweede ongelijkheid hebben we gebruik gemaakt van de Cauchy-Schwartz-ongelijkheid met het standaard inproduct op $\mathbb{R}^n$. Het gekregen volgt dan uit: $\Sigma |x_i \log(p_i)|^2 < Q(\bar{x})$.)

Nu is $f : t \mapsto \frac{\sqrt{t}}{\log(t)}$ een stijgende functie voor $t \geq 7.383$ en dus geldt voor $c \geq 1608 = e^{7.383}$: $f(\log(c)) \leq f(n^2(\log(n))^2)$. Dus

$$\frac{\sqrt{\log(c)}}{\log\log(c)} \leq \frac{n\log(n)}{2(\log(n) + \log\log(n))} \leq \frac{n}{2}. \tag{78}$$

Hieruit volgt:

$$\frac{n}{\log(c)} \geq \frac{n}{\sqrt{\log(c)}} \cdot \frac{1}{\sqrt{\log(c)}} \geq \frac{2}{\log\log(c)} \cdot \frac{1}{\sqrt{\log(c)}}. \tag{79}$$

En dus:

$$q > 1 + \frac{2}{\sqrt{\log(c)}\log\log(c)}. \tag{80}$$

□

6 LLL

Stelling 15. *In elk rooster L met positieve rang n is een niet-nul element x te vinden zodat $Q(x) \leq 2^{(n-1)/2} \cdot d(L)^{2/n}$.*

Bewijs. Zie [1] □

Voor 2 vectoren werkt het LLL-algoritme als volgt:
Neem 2 vectoren $b_1 = (x_1, y_1)$ en $b_2 = (x_2, y_2)$, zodat b_2 geen veelvoud is van b_1. Het inproduct $\langle , \rangle$ wordt nu gegeven door:

$$\begin{aligned} \langle b_1, b_1 \rangle &= Q(b_1) && (81) \\ &= Q(x_1, y_1) && (82) \\ &= (x_1 \log 2)^2 + (y_1 \log 3)^2 + N(x_1 \log 2 + y_1 \log 3)^2; && (83) \\ \langle b_1, b_2 \rangle &= \frac{1}{2}\left(Q(b_1 + b_2) - Q(b_1) - Q(b_2)\right). && (84) \end{aligned}$$

Zij m het dichtstbijzijnde gehele getal van $\frac{\langle b_1,b_2\rangle}{\langle b_1,b_1\rangle}$. Vervang nu b_2 door $b_2^* = b_2 - mb_1$. Voor b_2^* geldt nu $|\langle b_1, b_2^*\rangle| \leq \frac{1}{2}\langle b_1, b_1\rangle$. Als nu ook geldt $Q(b_2^*) \geq Q(b_1)$, dan hebben we de korste vector gevonden, namelijk b_1.
Zo niet, doe dan het proces nog een keer met de $b_2 := b_1$ en $b_1 := b_2^*$.
Omdat er slechts eindig veel vectoren korter zijn dan onze eerste b_1 is dit een eindig proces.

Deze methode voor 2 vectoren is niet nieuw. In 1801 gebruikte Gauss dit al bij het rekenwerk aan zijn binaire kwadratische vormen.

Voor de methode met n vectoren, zie [1].

6.1 Kwaliteit met LLL-grens

Als we een ondergrens voor de kwaliteit willen bepalen als we de LLL-grens nemen, dan verschilt deze in het begin erg weinig van de kwaliteit met de Minkowski-grens. Pas bij (71) verandert er wezenlijk iets.

De stelling van LLL geeft ons:

$$\begin{aligned} Q(\bar{x}) &\leq 2^{(n-1)/2} \cdot d(L)^{2/n} && (85)\\ &= 2^{(n-1)/2} \cdot (n^2(\log(n)^2))^{2/n} && (86)\\ &= 2^{(n-1)/2} \cdot n^2 \cdot (\log(n))^4. && (87) \end{aligned}$$

Dan wordt de kwaliteit;

$$q > 1 + \frac{((1-\delta)n}{\log(c)}. \quad (88)$$

En dan krijgen we

$$\begin{aligned} \log(c) &\leq \Sigma(|x_i| \log(p_i)) && (89)\\ &\leq \sqrt{n} \cdot \sqrt{q(\bar{x})} && (90)\\ &\leq 2^{(n-1)/4} \cdot n^{3/2} \cdot (\log(n))^2. && (91) \end{aligned}$$

Met deze afschatting van $\log(c)$ krijgen we nu

$$(\frac{(n-1)}{4-\epsilon}) \log 2 > \log\log(c). \quad (92)$$

Als we dit combineren dan krijgen we als ondergrens voor de kwaliteit

$$q > 1 + \frac{\log\log(c)}{\log(c)}. \quad (93)$$

Merk op dat dit dus nauwelijks beter is dan wanneer we enkel de priemen 2 en 3 zouden gebruiken.

6.2 Gevonden drietallen

De grens voor de kwaliteit die we daarnet gevonden hebben is slechts een ondergrens. De kwaliteit van het drietal is minstens $1 + \frac{\log\log(c)}{\log(c)}$ en zou dus best hoger uit kunnen komen. Laten we nu voor enkele drietallen gaan bekijken hoe de kwaliteit in de praktijk uitvalt.

a	b	c	$\log(c)$	n	q	Minkowski	LLL
2	$3^{10} \cdot 109$	23^5	15.6775	29	1.6299	1.1835	1.1756
11^2	$3^2 \cdot 5^6 \cdot 7^3$	$2^{21} \cdot 23$	17.6916	9	1.6260	1.1655	1.1624
19·1307	$7 \cdot 29^2 \cdot 31^8$	$2^8 \cdot 3^{22} \cdot 5^4$	36.1524	214	1.6235	1.0927	1.0992
283	$5^{11} \cdot 13^2$	$2^8 \cdot 3^8 \cdot 7^3$	20.1718	61	1.5808	1.1482	1.1489
1	$2 \cdot 3^7$	$5^4 \cdot 7$	8.3837	4	1.5679	1.3249	1.2536
7^3	3^{10}	$2^{11} \cdot 29$	10.9919	10	1.5471	1.2516	1.2181

Referenties

[1] H.W. Lenstra Jr, *Lattices*, Algorithmic Number Theory, **volume 44**, (2008), 127-181.

[2] R. Tijdeman, C.L. Oesterlé, *On the Oesterlé-Masser Conjecture*, Monatshefte für Mathematik, **102**, (1986), 251-257.

[3] B. van Dalen, *De geschiedenis van het abc-vermoeden*, http://www.rekenmeemetabc.nl/, (2005).

[4] J. Bosman, *Op zoek naar goede ABC-hits (II)*, http://www.uni-due.de/ ada649b/talks/abc.pdf, (2005)

[5] G. Geuze, *Verslag van het Leraar in onderzoek-project abc-vermoeden*, http://www.nwo.nl/nwohome.nsf/pages/NWOA_78PDCR, (2007).

[6] H.M> Edwards, *Fermat's last theorem. A genetic introduction to algebraic number theory.*, **Graduate Texts in Mathematics, 50**, (1977), sectie 1.5, hoofdstuk 2, sectie 3.3.