A New Lower Bound in the *abc* Conjecture

Curtis Bright
University of Windsor

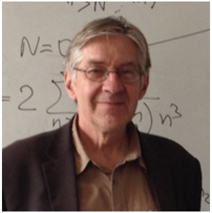
June 5, 2023

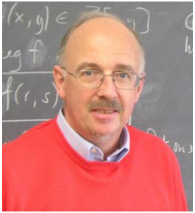
CanaDAM 2023

Number Theory and Algebraic Connections

Introduction

The *abc* conjecture (Oesterlé and Masser, 1985) has been called "The most important unsolved problem in Diophantine analysis".





If true, it would enable the resolution of many Diophantine equations—equations to be solved over the integers. For example, the *abc* conjecture implies Fermat's last theorem.

The *abc* conjecture

Three natural numbers a, b, c are said to be an *abc triple* if they do not share a common factor and

$$a + b = c.$$

The *abc* conjecture says that an *abc* triple cannot be very *smooth* (divisible by only small primes) when c is large.

typical triple:	$3^{10} \cdot 109 + 1 = 2 \cdot 11 \cdot 292561$
exceptional triple:	$3^{10} \cdot 109 + 2 = 23^5$

How to measure smoothness

The *radical* of a number is the product of the distinct primes in its prime factorization:

$$\text{rad}(2^8 \cdot 3^4 \cdot 5^2 \cdot 7) = 2 \cdot 3 \cdot 5 \cdot 7.$$

The *abc* conjecture is that *abc* triples have relatively large radical in the sense that for every $\epsilon > 0$

$$c < \text{rad}(abc)^{1+\epsilon}$$

with finitely many exceptions. For $\epsilon = 0$ the conjecture is false.

The most exceptional triples known

We construct infinitely many *abc* triples with

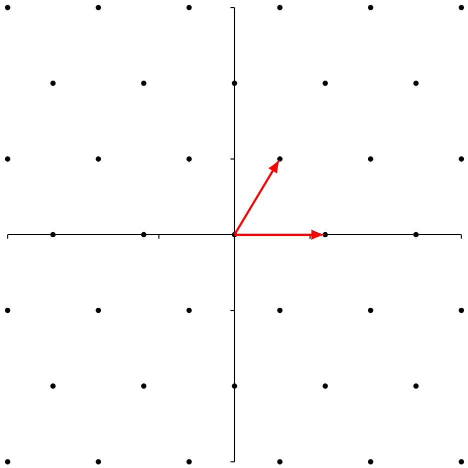
$$\exp\left(\frac{6.563\sqrt{\log c}}{\log\log c}\right)\operatorname{rad}(abc) < c,$$

thereby providing a lower bound on the best possible form of the conjecture.

We improve on the work of van Frankenhuysen, who in 1999 showed the existence of *abc* triples with 6.068 in place of 6.563.

Lattices

The *lattice* spanned by vectors $\boldsymbol{b}_1 = [3,5]$ and $\boldsymbol{b}_2 = [6,0]$:



The odd prime number lattice

Consider the lattice L_n generated by the rows $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ of

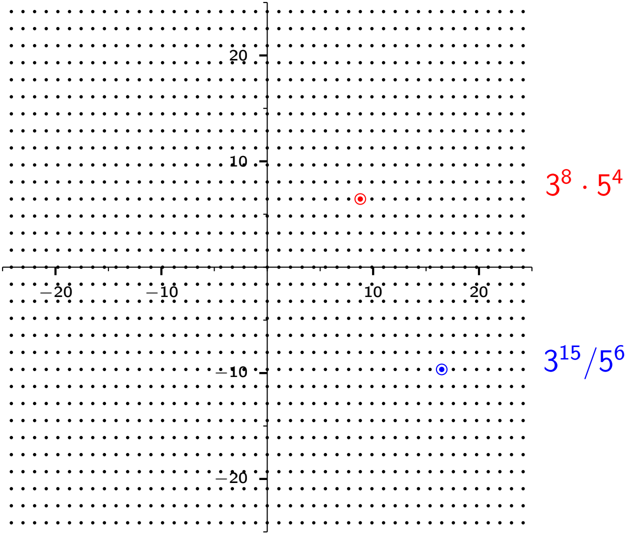
$$\begin{bmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \boldsymbol{b}_3 \\ \vdots \\ \boldsymbol{b}_n \end{bmatrix} = \begin{bmatrix} \log 3 & & & & \\ & \log 5 & & & \\ & & \log 7 & & \\ & & & \ddots & \\ & & & & \log p_n \end{bmatrix}$$

where p_i denotes the ith odd prime number.

There is an isomorphism between the points of L_n and the positive rationals with $\{p_1, \ldots, p_n\}$-smooth prime factorization:

$$\sum_{i=1}^{n} e_i \boldsymbol{b}_i \leftrightarrow \prod_{i=1}^{n} p_i^{e_i}.$$

The lattice–number isomorphism

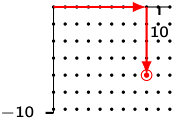


L_2

The height lemma

The ℓ_1 *norm* (Manhattan norm) of a vector is the sum of the absolute value of its components.

The *logarithmic height* h of a positive rational b/c is $\log \max\{b, c\}$.



$$\|\boldsymbol{x}\|_1 = 8\log 3 + 4\log 5$$

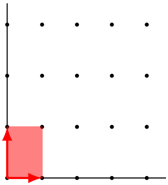
$$h(3^8/5^4) = 8\log 3$$

In general, if b/c is the rational associated to $\boldsymbol{x}$ then

$$\|\boldsymbol{x}\|_1 \geq h(b/c).$$

Lattice volume

The *volume* (or determinant) of a lattice is the volume of the parallelepiped generated by its basis vectors.



$$\det(L_2) = \log 3 \cdot \log 5$$

The volume of L_n is the product of the diagonal basis entries:

$$\det(L_n) = \prod_{i=1}^{n} \log p_i$$

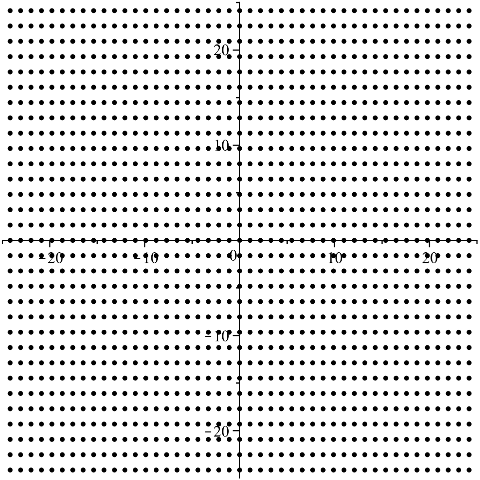
A special sublattice

The *kernel sublattice* $L_{n,m}$ consists of the points of L_n whose corresponding $\{p_1, \ldots, p_n\}$-smooth rational b/c get sent to 1 under the *reduce mod* 2^m mapping.

That is,

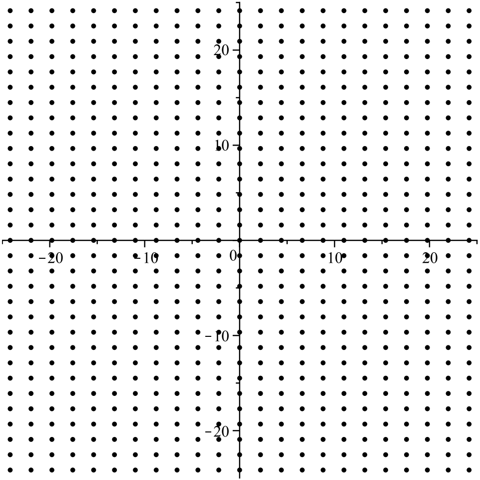
$$L_{n,m} \coloneqq \left\{ \sum_{i=1}^{n} e_i \boldsymbol{b}_i : \prod_{i=1}^{n} p_i^{e_i} \equiv 1 \pmod{2^m} \right\}.$$

What does $L_{2,m}$ look like?



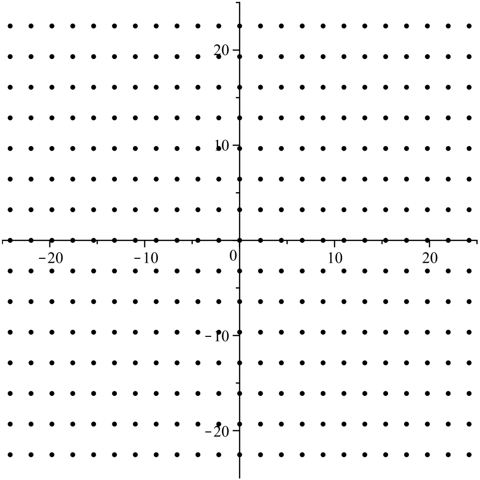
$L_{2,1}$

What does $L_{2,m}$ look like?



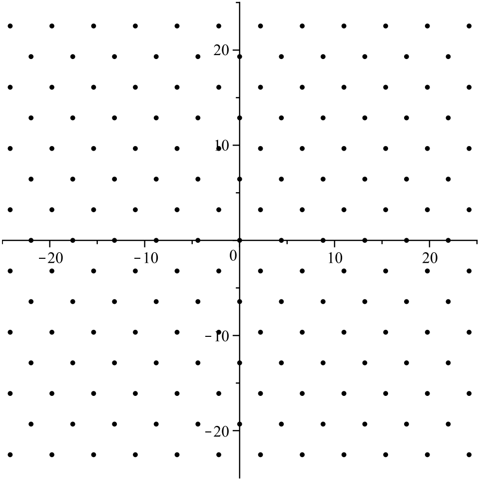
$L_{2,2}$

What does $L_{2,m}$ look like?



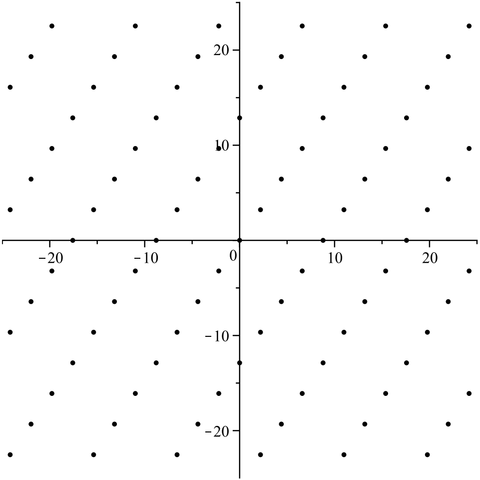
$L_{2,3}$

What does $L_{2,m}$ look like?



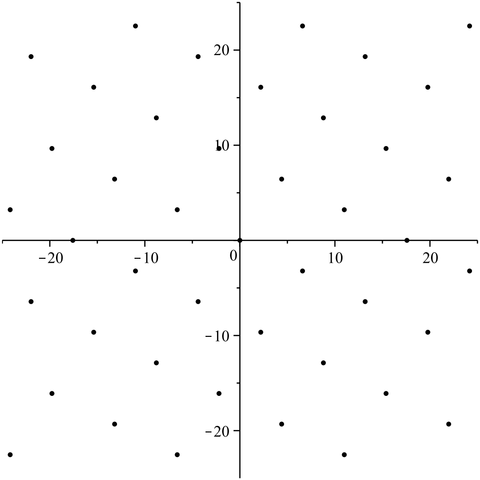
$L_{2,4}$

What does $L_{2,m}$ look like?



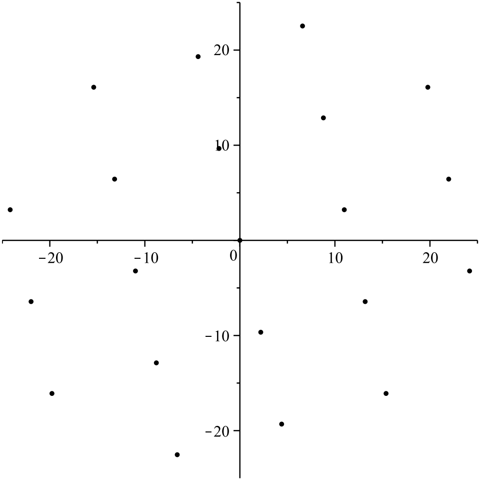
$L_{2,5}$

What does $L_{2,m}$ look like?



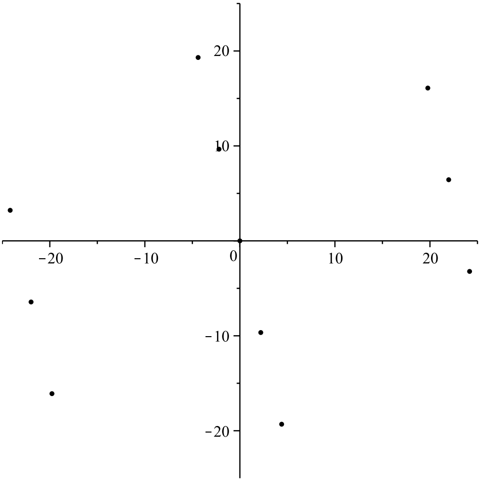
$L_{2,6}$

What does $L_{2,m}$ look like?



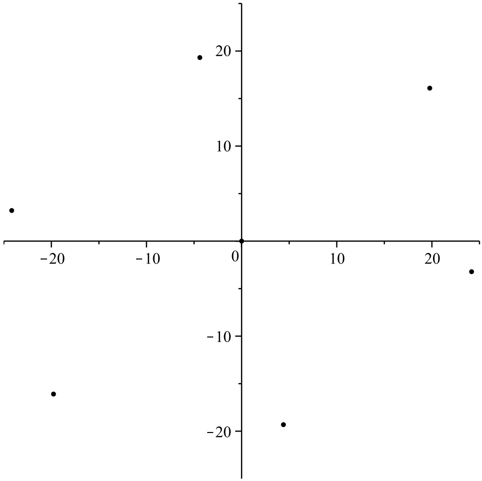
$L_{2,7}$

What does $L_{2,m}$ look like?



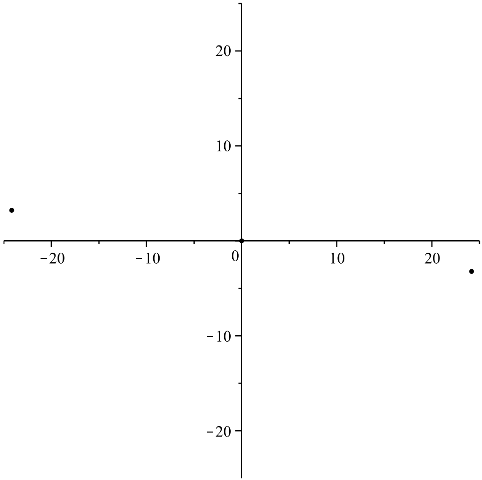
$L_{2,8}$

What does $L_{2,m}$ look like?



$L_{2,9}$

What does $L_{2,m}$ look like?



$L_{2,10}$

Kernel vectors → good triples

We just saw $(-22\log 3, 2\log 5) \in L_{2,10}$, i.e.,

$$3^{-22} \cdot 5^2 \equiv 1 \pmod{2^{10}}$$

which can be rewritten as

$$2^{10}k + 5^2 = 3^{22}$$

for an integer k. This *abc* triple satisfies

$$\begin{aligned} c &= 3^{22} & \operatorname{rad}(abc) &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 173 \cdot 12653, \\ &\approx 3.1 \cdot 10^{10} & &\approx 4.6 \cdot 10^{8}, \end{aligned}$$

so $\operatorname{rad}(abc)$ is small (about 1.5% of c).

Arbitrarily large $c/\text{rad}(abc)$

Let b/c be the smooth rational corresponding to a vector in $L_{n,m}$. By construction of the kernel sublattice,

$$b/c \equiv 1 \pmod{2^m}.$$

For simplicity suppose $c > b$, so we have the *abc* triple

$$2^m k + b = c$$

for some positive integer $k = a/2^m \leq c/2^m$. Examining the prime factorizations of a, b, c:

$$\text{rad}(abc) \leq 2k\,\text{rad}(bc) \leq \frac{c}{2^{m-1}} \prod_{i=1}^{n} p_i.$$

Thus $c/\text{rad}(abc) \to \infty$ as $m \to \infty$.

The existence of a short vector

Hermite's constant is the smallest γ_n such that a lattice of rank n always contains a nonzero vector $\boldsymbol{x}$ with small Euclidean norm in the sense that

$$\|\boldsymbol{x}\|^2 \leq \gamma_n \det(L)^{2/n}.$$

Hermite (1850) showed $\gamma_n \leq \sqrt{4/3}^{n-1}$ but it is now known that γ_n grows linearly in n. Kabatiansky and Levenshtein (1978) showed $\gamma_n \leq n/9.795$.

Hermite's constant in Manhattan

The ℓ_1 Hermite constant is the smallest δ_n such that a lattice of full rank n always contains a nonzero vector $\boldsymbol{x}$

$$\|\boldsymbol{x}\|_1 \leq \delta_n \det(L)^{1/n}.$$

Since $\|\boldsymbol{x}\|_1 \leq \sqrt{n}\|\boldsymbol{x}\|_2$, we have $\delta_n \leq \sqrt{n\gamma_n} = O(n)$.

Let δ be a constant so $\delta_n \leq n/\delta$ for sufficiently large n. A result of Rankin (1948) implies we can take $\delta = 3.659$.

Short vectors → better *abc* triples

$$\begin{aligned}
\log c &\leq \|\boldsymbol{x}\|_1 && \text{(height lemma)} \\
&\leq \tfrac{n}{\delta}\big(\det(L_{n,m})\big)^{1/n} && (\ell_1 \text{ Hermite constant}) \\
&= \tfrac{n}{\delta}\big(2^{m-1}\textstyle\prod_{i=1}^{n}\log p_i\big)^{1/n} && (\text{volume of } L_{n,m}) \\
&:= R && (\text{new variable } R)
\end{aligned}$$

Rewriting the rad(abc) bound in terms of R and n:

$$\frac{(\delta R/n)^n}{\prod_{i=1}^{n} p_i \log p_i} \operatorname{rad}(abc) \leq c.$$

The prime number theorem provides the growth rate of the denominator as $n \to \infty$.

The rad(abc) bound asymptotically

$$f(n) \sim g(n) \quad \text{means} \quad \lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$$

Using asymptotic expansions from the prime number theorem,

- $n \sim p_n / \log p_n$
- $\sum_{i=1}^{n} \log p_i \sim n \log p_n - n$
- $\sum_{i=1}^{n} \log \log p_i \sim n \log \log p_n$

the rad(abc) bound becomes

$$n \log\left(\frac{e\delta R}{p_n^2}\right) + \log \operatorname{rad}(abc) < \log c.$$

Optimal choice of R

For more extremal *abc* triples, we want to maximize

$$n \log\left(\frac{e\delta R}{p_n^2}\right)$$

in terms of R. With $R := ep_n^2/\delta$ we have

$$\begin{aligned} n \log\left(\frac{e\delta R}{p_n^2}\right) &\sim \frac{4\sqrt{(\delta/e)R}}{\log R} \\ &\geq \frac{4\sqrt{(\delta/e)\log c}}{\log\log c}. \end{aligned}$$

Putting it together

There are infinitely many *abc* triples satisfying

$$\frac{4\sqrt{(\delta/e)\log c}}{\log\log c} + \log \operatorname{rad}(abc) < \log c.$$

Exponentiating and setting $\delta := 3.659\ldots$

Putting it together

There are infinitely many *abc* triples satisfying

$$\frac{4\sqrt{(\delta/e)\log c}}{\log\log c} + \log \operatorname{rad}(abc) < \log c.$$

Exponentiating and setting $\delta := 3.659\ldots$

$$\exp\left(\frac{4.64\sqrt{\log c}}{\log\log c}\right) \operatorname{rad}(abc) < c.$$

Lattice (improved)

Modify the odd prime number lattice L_n to have basis

$$\begin{bmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \boldsymbol{b}_3 \\ \vdots \\ \boldsymbol{b}_n \\ \boldsymbol{b}_{n+1} \end{bmatrix} = \begin{bmatrix} \log 3 & & & & & \log 3 \\ & \log 5 & & & & \log 5 \\ & & \log 7 & & & \log 7 \\ & & & \ddots & & \vdots \\ & & & & \log p_n & \log p_n \\ & & & & & n^3 \end{bmatrix}$$

The final row $\boldsymbol{b}_{n+1}$ is included to make L_n full-rank. The entry n^3 is chosen to be large enough to ensure the shortest nonzero vector in $L_{n,m}$ will **not** include $\boldsymbol{b}_{n+1}$ (when $m \sim n \log_2 n$).

rad(abc) bound (improved)

The extra column gives better control on the size of b/c and consequently there are infinitely many abc triples satisfying

$$\frac{2^{m-1}}{\prod_{i=1}^{n} p_i} \operatorname{rad}(abc) \leq c,$$

$$2 \log c \leq \frac{n+1}{\delta} \left(2^{m-1} n^3 \prod_{i=1}^{n} \log p_i \right)^{1/(n+1)}.$$

Of all the differences (shown in red), asymptotically only the 2 matters and it improves the constant 4.64 in the exponent by a factor of $\sqrt{2}$.

Conclusion

There are infinitely many *abc* triples with

$$\exp\left(\frac{6.563\sqrt{\log c}}{\log\log c}\right)\operatorname{rad}(abc) < c,$$

thus providing a new lower bound on the best possible form of the *abc* conjecture.

For these triples $c/\operatorname{rad}(abc)$ grows about 64% faster than the previously known most extremal examples.[1]

[1] M. van Frankenhuysen. A lower bound in the *abc* conjecture. *Journal of Number Theory*, 2000.