Extremal examples in the *abc* conjecture

Curtis Bright

University of Waterloo

March 27, 2014

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 if a, b, c is a large *abc* triple then *abc* cannot be 'very composite'.

Example *abc* triples

- A typical *abc* triple:

$$3^{10} \cdot 109 + 1 = 2 \cdot 11 \cdot 292561$$

- An exceptional *abc* triple:

$$3^{10} \cdot 109 + 2 = 23^5$$

How to measure 'compositeness'

- Define the *radical* of abc to be the product of the primes in abc:

$$\operatorname{rad}(abc) := \prod_{p \mid abc} p$$

- Exceptional abc examples have relatively small radical.

The formal statement

- The *abc* conjecture states that every *abc* triple satisfies

$$c = O\left(\mathrm{rad}(abc)^{1+\epsilon}\right)$$

for every $\epsilon > 0$.

Family of exceptional examples

- Note that $3^{2^m} \equiv 1 \pmod{2^{m+1}}$, so

$$2^{m+1}k + 1 = 3^{2^m}$$

is a family of *abc* triples, where k is a positive integer.

- Here $\mathrm{rad}(abc) \leqslant 2 \cdot 3 \cdot k$, and $k = \frac{c-1}{2^{m+1}} < \frac{c}{2^{m+1}}$, so

$$\frac{2^m}{3}\,\mathrm{rad}(abc) < c.$$

Conjecture is false for $\epsilon = 0$

- Thus there are infinitely many *abc* triples which satisfy

$$N \operatorname{rad}(abc) < c$$

for every $N > 0$.

Better exceptional examples

- We'll use arguments from the geometry of numbers to construct infinitely many *abc* triples which satisfy

$$\exp\left(\frac{6\sqrt{\log c}}{\log\log c}\right)\mathrm{rad}(abc) < c.$$

S-units

- Let S be a set of prime numbers.
- An *S-unit* is defined to be a rational number whose numerator and denominator in lowest terms are only divisible by primes in S.

$$S\text{-units} := \left\{ \pm \prod_{p_i \in S} p_i^{e_i} : e_i \in \mathbb{Z} \right\}$$

- The *height* of an S-unit p/q is $h(p/q) := \max\{|p|, |q|\}$.

The odd prime number lattice

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

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

where p_i denotes the ith odd prime number.

Relationship between L_n and S-units

- There is an isomorphism

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

between the points of L_n and the positive $\{p_1, \ldots, p_n\}$-units.

Lemma 1

- Let $\boldsymbol{x} = \sum_{i=1}^{n} e_i \boldsymbol{b}_i$ and let $\prod_{i=1}^{n} p_i^{e_i} = p/q$ be expressed in lowest terms. Then:

$$\begin{aligned} \|\boldsymbol{x}\|_1 &= \sum_{i=1}^{n} \left| e_i \log p_i \right| \\ &= \sum_{e_i > 0} e_i \log p_i - \sum_{e_i < 0} e_i \log p_i \\ &= \log p + \log q \\ &\geqslant \max\{\log p, \log q\} \\ &= \log h(p/q) \end{aligned}$$

Lemma 2

- The determinant of L_n has a simple form:

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

The kernel sublattice

- Let P be the set of positive $\{p_1, \ldots, p_n\}$-units.
- Consider the homomorphism $\varphi\colon P \to (\mathbb{Z}/2^m\mathbb{Z})^*$ of reduction mod 2^m.
- The subgroup $\ker\varphi$ of P is isomorphic to a sublattice $L_{n,m}$ of L_n:

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

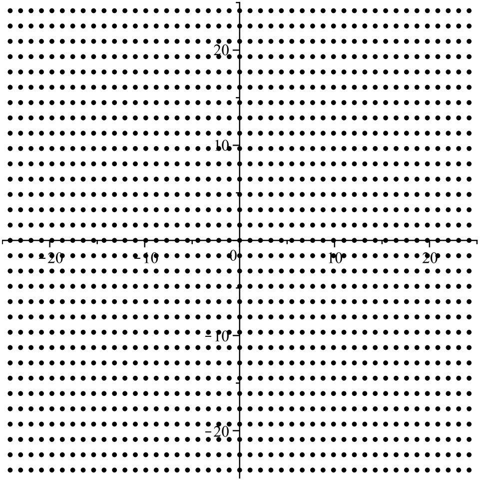
$L_{n,m}$ really is a lattice

- Discrete as it is a subset of L_n.
- Contains the n linearly independent vectors $\mathrm{ord}_{2^m}(p_i)\boldsymbol{b}_i$.
- If $\sum e_i\boldsymbol{b}_i$ and $\sum f_i\boldsymbol{b}_i$ are in $L_{n,m}$, then so is $\sum(e_i \pm f_i)\boldsymbol{b}_i$:

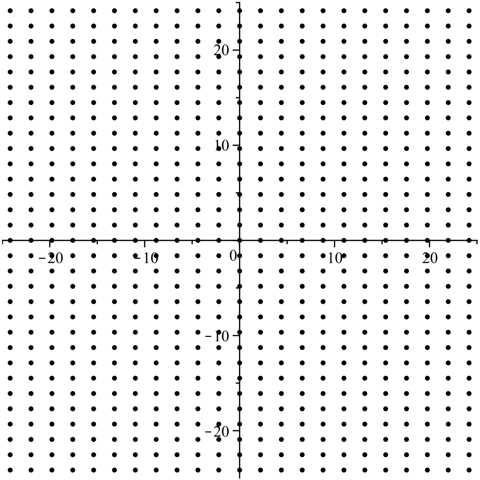
$$\prod p_i^{e_i \pm f_i} \equiv \prod p_i^{e_i} \cdot \prod p_i^{\pm f_i} \equiv 1 \pmod{2^m}$$

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

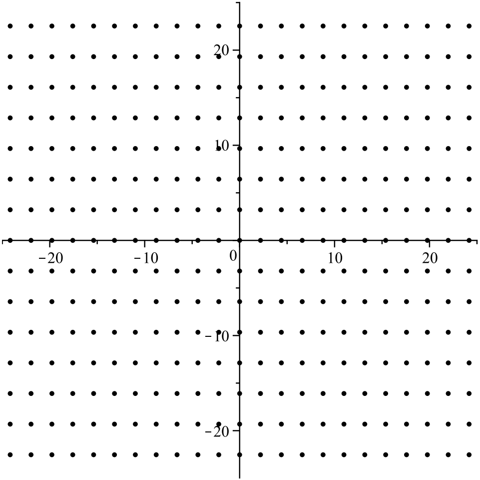
- For $m = 1$, reducing an S-unit mod 2^m necessarily gives 1, since all primes in $S = \{p_1, \ldots, p_n\}$ are odd.
  - Thus $L_{n,1}$ is the full lattice L_n.
- When $n = 2$, we can plot $L_{n,m}$ in the plane...



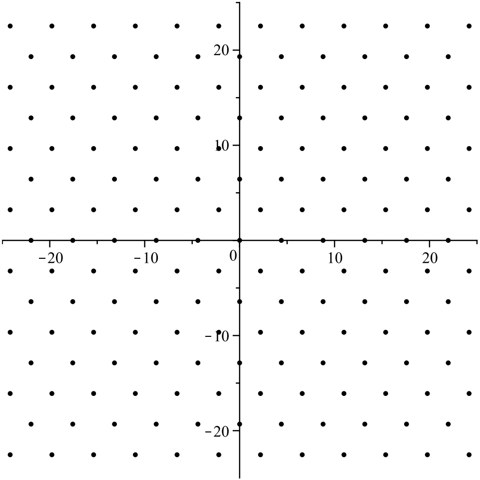
$L_{2,1}$



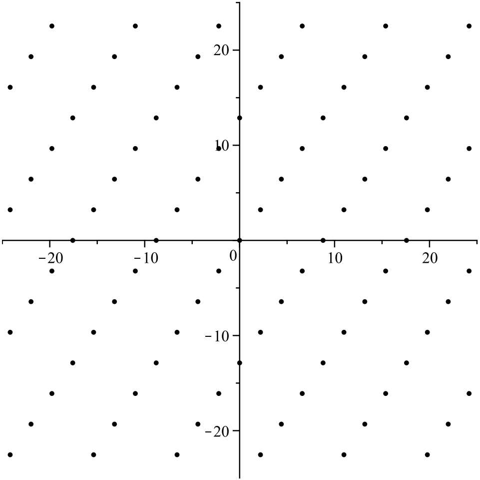
$L_{2,2}$



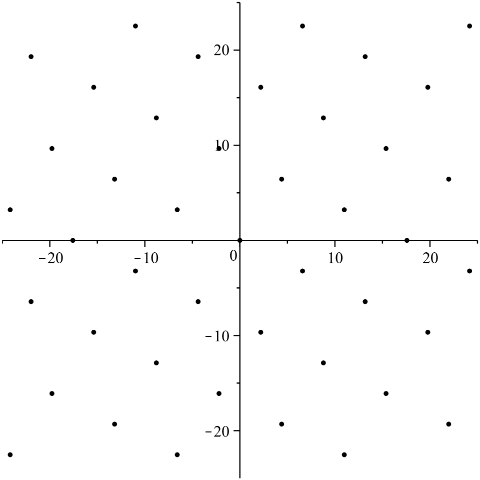
$L_{2,3}$



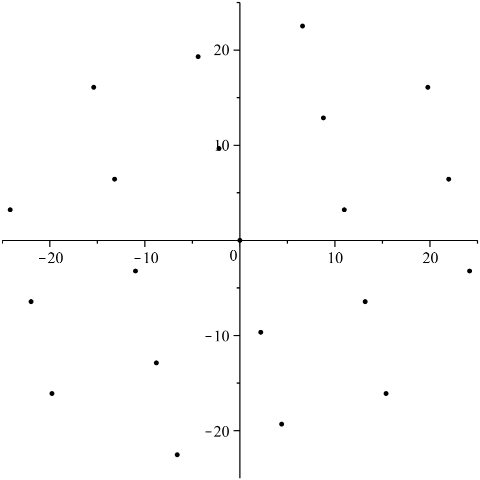
$L_{2,4}$



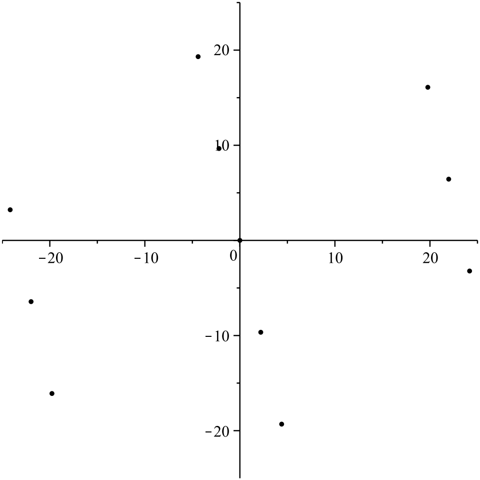
$L_{2,5}$



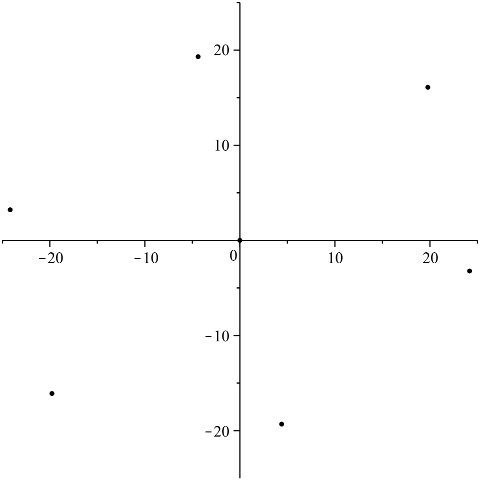
$L_{2,6}$



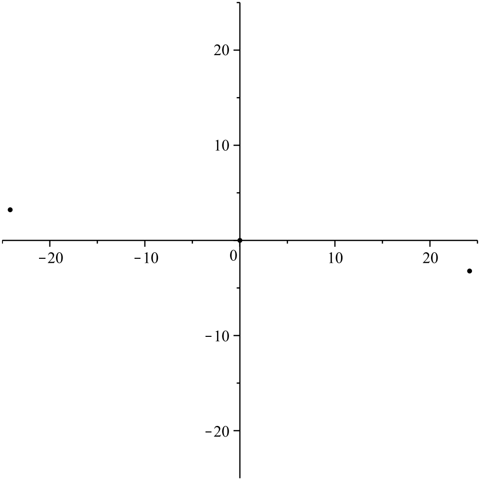
$L_{2,7}$



$L_{2,8}$



$L_{2,9}$



$L_{2,10}$

Short vectors in $L_{n,m}$ give good *abc* 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 some positive integer k. This *abc* triple satisfies

$$c \approx 3.1 \cdot 10^{10}$$
$$\mathrm{rad}(abc) \approx 4.6 \cdot 10^{8}.$$

The index of $L_{n,m}$ in L_n

- 3 and 5 generate $(\mathbb{Z}/2^m\mathbb{Z})^*$, so $\varphi(P) = (\mathbb{Z}/2^m\mathbb{Z})^*$ when $n \geqslant 2$.
- Since $L_n \cong P$ and $L_{n,m} \cong \ker \varphi$, we have

$$L_n / L_{n,m} \cong (\mathbb{Z}/2^m\mathbb{Z})^*$$

  by the first isomorphism theorem.
- Thus the index of $L_{n,m}$ in L_n is $|(\mathbb{Z}/2^m\mathbb{Z})^*| = 2^{m-1}$.

Hermite's constant

- Hermite's constant is the smallest positive γ_n such that a lattice of rank n always contains a nonzero vector x with

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

Bounds on Hermite's constant

- By Minkowski's theorem,

$$\gamma_n \leqslant 4\omega_n^{-2/n} \sim \frac{2n}{\pi e} \approx 0.234n$$

  where ω_n is the volume of the n-dimensional unit sphere.

- Kabatiansky & Levenshtein showed

$$\gamma_n \leqslant \frac{2n}{4^{0.599}\pi e} \approx 0.102n$$

  for sufficiently large n.

Hermite's constant in Manhattan

- The one-norm hermite constant is the smallest positive δ_n such that a lattice of rank n always contains a nonzero vector $\boldsymbol{x}$ with

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

- Since $\|\boldsymbol{x}\|_1 \leqslant \sqrt{n}\|\boldsymbol{x}\|_2$, one has that $\delta_n \leqslant \sqrt{n\gamma_n} = O(n)$.
- Let δ be a constant such that $\delta_n \leqslant n/\delta$ for all sufficiently large n.
    - By Minkowski's theorem, one can take $\delta \coloneqq e$.

Lemma 3

- For all $m \geqslant 1$ and sufficiently large n, there exists an abc triple satisfying:

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

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

Proof of Lemma 3

- By definition of δ, for all sufficiently large n there exists a nonzero $\boldsymbol{x} \in L_{n,m}$ with

$$\|\boldsymbol{x}\|_1 \leqslant \frac{n}{\delta}(\det(L_{n,m}))^{1/n}.$$

- Let $\boldsymbol{x} = \sum_{i=1}^{n} e_i \boldsymbol{b}_i$ and let $\prod_{i=1}^{n} p_i^{e_i} = p/q$ be expressed in lowest terms. By construction of the kernel sublattice,

$$p/q \equiv 1 \pmod{2^m}.$$

Proof of Lemma 3

- Let $c \coloneqq \max\{p, q\}$, $b \coloneqq \min\{p, q\}$, and $a \coloneqq c - b$. Then

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

for some positive integer $k = a/2^m \leqslant c/2^m$.

- Examining the prime factorizations of a, b, c:

$$\mathrm{rad}(a) \leqslant 2k \leqslant c/2^{m-1}$$
$$\mathrm{rad}(bc) \leqslant \prod_{i=1}^{n} p_i$$

  - The first inequality follows.

Proof of Lemma 3

- The second inequality follows using Lemmas 1 and 2:

$$\begin{aligned}\log c &= \log \max\{p, q\} \\ &= \log h(p/q) \\ &\leqslant \|\boldsymbol{x}\|_1 \\ &\leqslant \frac{n}{\delta}\left(\det(L_{n,m})\right)^{1/n} \\ &= \frac{n}{\delta}\left(2^{m-1}\prod_{i=1}^{n}\log p_i\right)^{1/n}\end{aligned}$$

How to choose m optimally?

- For convenience, let R denote the upper bound on the second inequality. Rewriting the inequalities in terms of R:

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

$$\log c \leqslant R$$

Taking the log...

$$n \log\left(\frac{\delta R}{n}\right) - \sum_{i=1}^{n} \log p_i - \sum_{i=1}^{n} \log\log p_i + \log \operatorname{rad}(abc) \leqslant \log c$$

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

  this becomes

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

- Being more careful, one can show the inequality is strict.

Optimal choice of R

- Need to maximize
$$n \log\left(\frac{e\delta R}{p_n^2}\right).$$
- Need $R > p_n^2/(e\delta)$ for the log to be positive.
- With $R \coloneqq kp_n^2$ for some constant k this becomes
$$n \log(ke\delta) = \Theta\left(\frac{\sqrt{R}}{\log R}\right).$$

Optimal choice of k

- Need to maximize

$$\begin{aligned} n\log(ke\delta) &\sim \frac{p_n}{\log p_n}\log(ke\delta) \\ &= \frac{\sqrt{R/k}}{\log\sqrt{R/k}}\log(ke\delta) \\ &\sim \frac{2\sqrt{R/k}}{\log R}\log(ke\delta) \\ &= \frac{4\sqrt{(\delta/e)R}}{\log R} \qquad (\text{take } k \coloneqq e/\delta) \end{aligned}$$

Putting it together

- Using $\log c \leqslant R$,

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

- With $\delta := e$,

$$\exp\left(\frac{4\sqrt{\log c}}{\log\log c}\right)\operatorname{rad}(abc) < c.$$

Improvement

- Modify the odd prime number lattice L_n to have basis

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

Modified Lemma 1

- Let $\boldsymbol{x} = \sum_{i=1}^{n} e_i \boldsymbol{b}_i$ and let $\prod_{i=1}^{n} p_i^{e_i} = p/q$ be expressed in lowest terms. Then:

$$\begin{aligned}
\|\boldsymbol{x}\|_1 &= \left|\sum_{i=1}^{n} e_i \log p_i\right| + \sum_{i=1}^{n} \left|e_i \log p_i\right| \\
&= \left|\log p - \log q\right| + \sum_{e_i > 0} e_i \log p_i - \sum_{e_i < 0} e_i \log p_i \\
&= \left|\log p - \log q\right| + \log p + \log q \\
&= 2 \max\{\log p, \log q\} \\
&= 2 \log h(p/q)
\end{aligned}$$

Modified Lemma 2

- The determinant of L_n has a simple form:

$$
\begin{aligned}
\det(L_n) &= \sqrt{BB^T} \\
&= \sqrt{\det\left(\begin{bmatrix} 1 & & & 1 \\ & \ddots & & \vdots \\ & & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ 1 & \cdots & 1 \end{bmatrix}\right)} \cdot \prod_{i=1}^{n} \log p_i \\
&= \sqrt{\det\left(\begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix} + \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}\begin{bmatrix} 1 & \cdots & 1 \end{bmatrix}\right)} \cdot \prod_{i=1}^{n} \log p_i \\
&= \sqrt{\det\left(\begin{bmatrix} 1 \end{bmatrix} + \begin{bmatrix} 1 & \cdots & 1 \end{bmatrix}\begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}\right)} \cdot \prod_{i=1}^{n} \log p_i \\
&= \sqrt{n+1} \cdot \prod_{i=1}^{n} \log p_i
\end{aligned}
$$

Modified Lemma 3

- For all $m \geqslant 1$ and sufficiently large n, there exists an abc triple satisfying:

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

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

Errata: δ should be replaced with an upper bound on γ_n.

Putting it together

- Using $2 \log c \leqslant R$,

$$\exp\left(\frac{4\sqrt{2(\delta/e)\log c}}{\log\log c}\right)\operatorname{rad}(abc) < c.$$

- van Frankenhuysen (1999) performs this construction not in terms of δ, but essentially uses $\delta \approx 3.13$ and obtains

$$\exp\left(\frac{6.07\sqrt{\log c}}{\log\log c}\right)\operatorname{rad}(abc) < c.$$

Bound on δ_n

- Blichfeldt (1914) showed that

$$\delta_n \leqslant \sqrt{\frac{4(n+1)(n+2)}{3\pi(n+3)}} \left(\frac{2(n+1)}{n+3} \left(\frac{n}{2} + 1 \right)! \right)^{1/n}$$

$$\sim \sqrt{\frac{2}{3\pi e} n}$$

- Thus, we can take $\delta \approx 3.579$.

Bound on δ_n

- Rankin (1948) showed that

$$\delta_n \leqslant \left(\frac{2-x}{1-x}\right)^{x-1} \left(\frac{1+xn}{x \cdot x!^n}(xn)!\right)^{1/n} n^{1-x}$$
$$\sim \left(\frac{2-x}{1-x}\right)^{x-1} \frac{(x/e)^x}{x!} n$$

  for any $x \in [1/2, 1]$. This has a minimum at $x \approx 0.645$.

- Thus, we can take $\delta \approx 3.659$.