33 and all that

Andrew Booker
University of Bristol

joint with Andrew Sutherland (MIT)

`arxiv.org/abs/2007.01209`

ANTS XIV
July 4th 2020

I think the problem, to be quite honest with you, is that you've never actually known what the question is.
—Deep Thought

A tale of three cubes

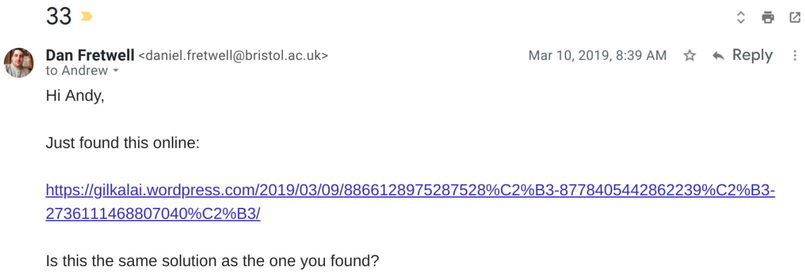
$$\begin{array}{rr}
\multicolumn{2}{r}{(-2\,736\,111\,468\,807\,040)^3 + (-8\,778\,405\,442\,862\,239)^3 + 8\,866\,128\,975\,287\,528^3} \\
= & -20483367622797158223817952754905569383153664000 \\
 & -676467453392982277424361019810585360331722557919 \\
 & \underline{+696950821015779435648178972565490929714876221952} \\
 & 33
\end{array}$$

Keeping secrets is hard. . .

At 9:05am GMT on February 27th 2019, a computer in Bristol found the solution to $x^3 + y^3 + z^3 = 33$ shown on the previous slide.

I told several colleagues about it later that day.

Eleven days later, one of them sent me this:



33

Dan Fretwell <daniel.fretwell@bristol.ac.uk>
to Andrew

Mar 10, 2019, 8:39 AM

Hi Andy,

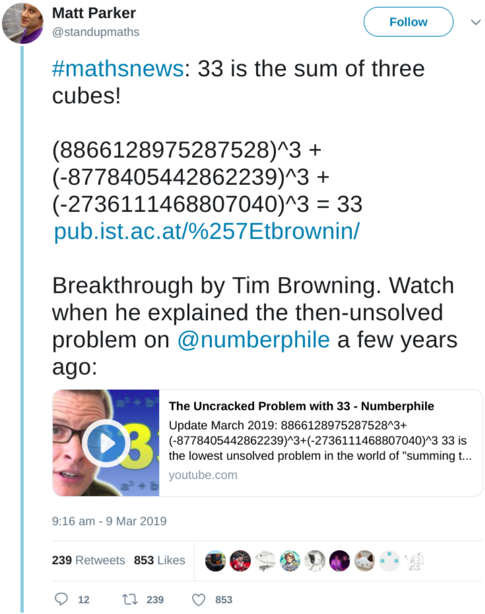
Just found this online:

https://gilkalai.wordpress.com/2019/03/09/8866128975287528%C2%B3-8778405442862239%C2%B3-2736111468807040%C2%B3/

Is this the same solution as the one you found?

Uh oh.

It got worse from there. . .



Matt Parker
@standupmaths

#mathsnews: 33 is the sum of three cubes!

(8866128975287528)^3 +
(-8778405442862239)^3 +
(-2736111468807040)^3 = 33
pub.ist.ac.at/%257Etbrownin/

Breakthrough by Tim Browning. Watch when he explained the then-unsolved problem on @numberphile a few years ago:

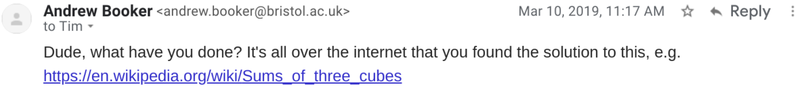
The Uncracked Problem with 33 - Numberphile
Update March 2019: 8866128975287528^3+(-8778405442862239)^3+(-2736111468807040)^3 33 is the lowest unsolved problem in the world of "summing t...
youtube.com

9:16 am - 9 Mar 2019

239 Retweets 853 Likes

Browning! 😠

I protested:

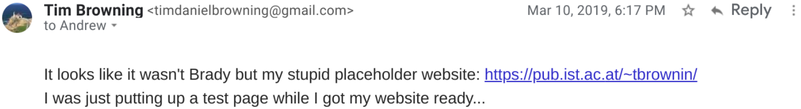

Andrew Booker <andrew.booker@bristol.ac.uk>
to Tim

Mar 10, 2019, 11:17 AM

Dude, what have you done? It's all over the internet that you found the solution to this, e.g. https://en.wikipedia.org/wiki/Sums_of_three_cubes

(Yes, there was already a Wikipedia article.)

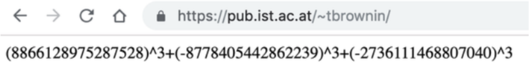
Tim professed his innocence. Eventually we worked it out:


Tim Browning <timdanielbrowning@gmail.com>
to Andrew

Mar 10, 2019, 6:17 PM

It looks like it wasn't Brady but my stupid placeholder website: https://pub.ist.ac.at/~tbrownin/
I was just putting up a test page while I got my website ready...

This was Tim's web page at the time:


https://pub.ist.ac.at/~tbrownin/

(8866128975287528)^3+(-8778405442862239)^3+(-2736111468807040)^3

It turns out that this is a good marketing strategy.

NewScientist

Mathematician cracks centuries-old problem about the number 33

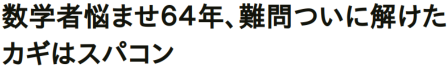
Quantamagazine

Sum-of-Three-Cubes Problem Solved for 'Stubborn' Number 33

Newsweek

MATHEMATICIAN SOLVES 64-YEAR-OLD 'DIOPHANTINE PUZZLE'

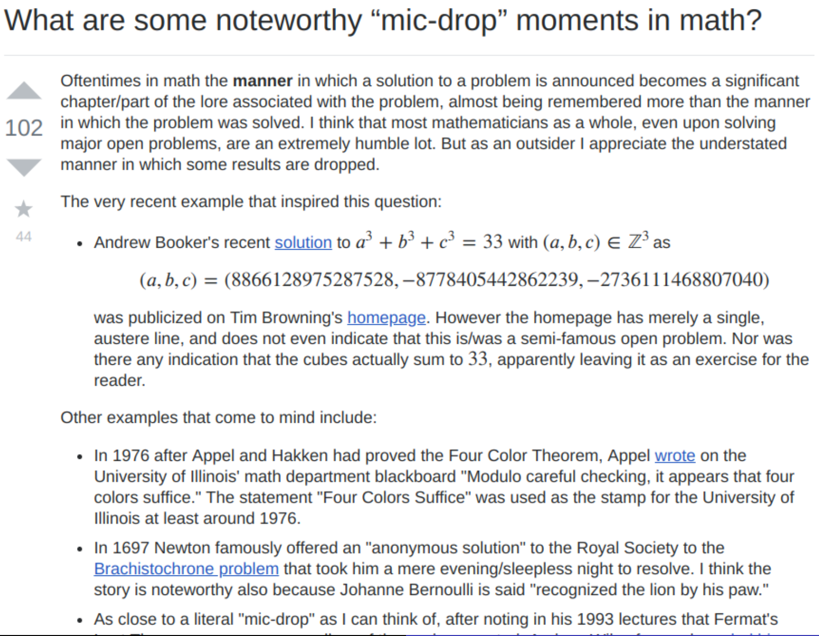
朝日新聞 DIGITAL


数学者悩ませ64年、難問ついに解けた カギはスパコン

University of BRISTOL

Bristol mathematician cracks Diophantine puzzle

Meanwhile, on mathoverflow



What are some noteworthy “mic-drop” moments in math?

Oftentimes in math the **manner** in which a solution to a problem is announced becomes a significant chapter/part of the lore associated with the problem, almost being remembered more than the manner in which the problem was solved. I think that most mathematicians as a whole, even upon solving major open problems, are an extremely humble lot. But as an outsider I appreciate the understated manner in which some results are dropped.

The very recent example that inspired this question:

- Andrew Booker's recent solution to $a^3 + b^3 + c^3 = 33$ with $(a, b, c) \in \mathbb{Z}^3$ as

  $$(a, b, c) = (8866128975287528, -8778405442862239, -2736111468807040)$$

  was publicized on Tim Browning's homepage. However the homepage has merely a single, austere line, and does not even indicate that this is/was a semi-famous open problem. Nor was there any indication that the cubes actually sum to 33, apparently leaving it as an exercise for the reader.

Other examples that come to mind include:

- In 1976 after Appel and Hakken had proved the Four Color Theorem, Appel wrote on the University of Illinois' math department blackboard "Modulo careful checking, it appears that four colors suffice." The statement "Four Colors Suffice" was used as the stamp for the University of Illinois at least around 1976.
- In 1697 Newton famously offered an "anonymous solution" to the Royal Society to the Brachistochrone problem that took him a mere evening/sleepless night to resolve. I think the story is noteworthy also because Johanne Bernoulli is said "recognized the lion by his paw."
- As close to a literal "mic-drop" as I can think of, after noting in his 1993 lectures that Fermat's

A number which will live in infamy

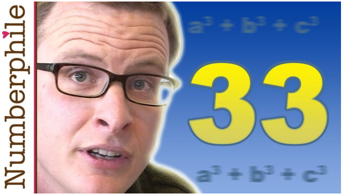
Bjorn Poonen, *Undecidability in Number Theory*,
AMS Notices, March 2008:

"Does the equation $x^3 + y^3 + z^3 = 29$ have a solution in integers?
Yes: $(3, 1, 1)$, for instance.
How about the equation $x^3 + y^3 + z^3 = 30$?
Again yes, although this was not known until 1999: the smallest solution is $(-283059965, -2218888517, 2220422932)$.
And how about $x^3 + y^3 + z^3 = 33$?
This is an unsolved problem."

Popularization

YouTube

Numberphile



History

Ryley (1825): $x = \left(\frac{27x^3-y^9}{3y^2(9x^2+3xy^3+y^6)}\right)^3 + \left(\frac{-27x^3+9xy^6+y^9}{3y^2(9x^2+3xy^3+y^6)}\right)^3 + \left(\frac{3xy(3x+y^3)}{9x^2+3xy^3+y^6}\right)^3$

Verebrusov (1908): $(1+6x^3)^3 + (1-6x^3)^3 + (-6x^2)^3 = 2$
Mahler (1936): $(9x^4)^3 + (9x-9x^4)^3 + (1-9x^3)^3 = 1$

Mordell (1953): $x^3+y^3+z^3 = 3$ other than $(1,1,1)$, $(4,4,-5)$?

Miller and Woollett (1955): Searched for solutions to $x^3+y^3+z^3=k$ for $0 < k \le 100$ using the EDSAC at Cambridge

Gardiner, Lazarus, and Stein (1964): Found one more $k \le 100$

Heath-Brown (1992): Conjectured solutions exist $\forall k \not\equiv \pm 4 \pmod 9$

Heath-Brown, Lionen, and te Riele (1993)
Conn and Vaserstein (1994)
Koyama (1994), (1995)
Jagy (1995)
Bremner (1995)
Lukes (1995)
Koyama, Tsuruoka, and Sekigawa (1997)
Elkies (2000)
Bernstein (2001)
Beck, Pine, Tarrant, and Yarbrough Jensen (2007)
Elsenhans and Jahnel (2009)

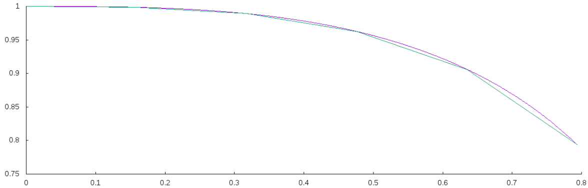
Huisman (2016): Found all solutions for $k < 1000$ with $\max\{|x|,|y|,|z|\} \le 10^{15}$

Elkies' algorithm

Elkies (1996) described an algorithm to find all $(x, y, z) \in \mathbb{Z}^3$ with $\max\{|x|, |y|, |z|\} \leq B$ and $|x^3 + y^3 + z^3| \leq B$ in time $O(B \log^c B)$.

His observation is that we can rewrite $x^3 + y^3 + z^3 = k$ as $\left(-\frac{x}{z}\right)^3 + \left(-\frac{y}{z}\right)^3 = 1 - \frac{k}{z^3}$, so $\left(-\frac{x}{z}, -\frac{y}{z}\right)$ is a rational point "near" the Fermat cubic $X^3 + Y^3 = 1$ (within distance $O(B^{-2})$).

To find these points, he breaks $[0, 1/\sqrt[3]{2}]$ into $\asymp B$ subintervals of size $\asymp \frac{1}{B}$ and computes linear approximations to the curve on each.



If $(X, Y) = \left(\frac{x}{z}, \frac{y}{z}\right)$ is a point of height $O(B)$ within distance $O(B^{-2})$ of one of the line segments, then (x, y, z) lies in a certain parallelopiped of side lengths $O(1)$, $O(B^{-1})$, and $O(B)$.
Finally, apply LLL to find the integer points.

A little algebra

Suppose that $x^3 + y^3 + z^3 = k$, with $|x| \geq |y| \geq |z|$. Then

$$k - z^3 = x^3 + y^3 = (x+y)(x^2 - xy + y^2).$$

Writing $d = |x+y| = |x| + y \operatorname{sgn} x$, we have

$$\frac{|k - z^3|}{d} = x^2 - xy + y^2 = 3x^2 - 3d|x| + d^2,$$

so that

$$\{x, y\} = \left\{ \frac{1}{2} \operatorname{sgn}(k - z^3) \left(d \pm \sqrt{\frac{4|k - z^3| - d^3}{3d}} \right) \right\}.$$

Given a candidate value of z, we can try all $d > 0$ dividing $|k - z^3|$. This finds all solutions to $x^3 + y^3 + z^3 = k$ with $\min\{|x|, |y|, |z|\} \leq B$ in (heuristic) time $O(B^{1+\varepsilon})$.

A better algorithm

Factoring might be subexponential, but it's expensive in practice.

So instead of running through z and solving for $d \mid (k - z^3)$, it's better to run through d and solve for z satisfying $z^3 \equiv k \pmod{d}$. With the Chinese remainder theorem and Hensel's lemma, this can be reduced to finding solutions to $z^3 \equiv k \pmod{p}$ for primes $p \mid d$.

In the particular case $k \equiv 3\epsilon \pmod{9}$ for $\epsilon \in \{\pm 1\}$, we have $x \equiv y \equiv z \equiv \epsilon \pmod{3}$, and it follows that $\operatorname{sgn} z = \epsilon \left(\frac{d}{3}\right)$. That leads to the following system:

$$\frac{d}{\sqrt[3]{2}-1} < |z| \le B, \quad \operatorname{sgn} z = \epsilon\left(\frac{d}{3}\right), \quad z^3 \equiv k \pmod{d},$$
$$3d\left(4\epsilon\left(\frac{d}{3}\right)(z^3-k) - d^3\right) = \square.$$

Also, some congruence constraints come for free, e.g. $z \equiv \frac{4}{3}k(2-d^2) + 9(k+d) \pmod{18}$.

Complexity analysis

Even with the noted optimizations, there are $\gg B\log B$ candidate pairs (d,z) satisfying the first line of the system.

To get better than $O(B\log B)$ running time, we use a time-space tradeoff: If $\Delta = 3d\left(4\epsilon\left(\frac{d}{3}\right)(z^3-k)-d^3\right)$ is a square then $\left(\frac{\Delta}{p}\right)\in\{0,1\}$ for any odd prime p. Setting $M=\prod_{5\le p\le P}p$ for some auxiliary parameter P, we can restrict to the residue classes of $z \pmod{M}$ satisfying this criterion for all $p \mid M$. This comes with $O(M)$ setup cost, but typically reduces the number of z by a factor of $2^{\omega(M)}$.

Optimally choosing $P \asymp \log\log B\log\log\log B$, we get a total (heuristic) running time of $O\big(B\log\log B\log\log\log B\big)$.

There are many practical issues: 64-bit arithmetic, fast cube roots mod p, fast sieving for primes, Montgomery multiplication, . . .

42 is the new 33

Finding a solution to the three cubes problem for 33 left only one value of $k \leq 100$ with no local obstructions and no known solutions: $k = 42$. I searched for solutions with $\min\{|x|, |y|, |z|\} \leq 10^{16}$ without success.

Likewise, I found no solutions to Mordell's question.

Enter Drew Sutherland.

42 is the new 33

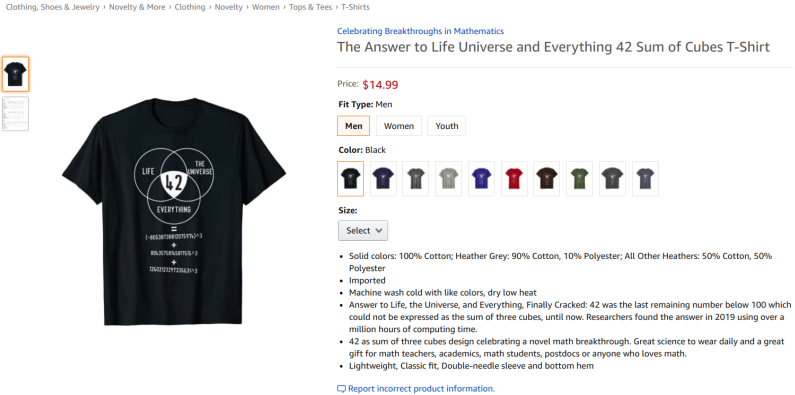
Finding a solution to the three cubes problem for 33 left only one value of $k \leq 100$ with no local obstructions and no known solutions: $k = 42$. I searched for solutions with $\min\{|x|, |y|, |z|\} \leq 10^{16}$ without success.

Likewise, I found no solutions to Mordell's question.

Enter Drew Sutherland. With help from our friends at charityengine and half a million volunteers, we found

$$\begin{aligned}
42 &= (-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3 \\
3 &= 569936821221962380720^3 + (-569936821113563493509)^3 + (-472715493453327032)^3 \\
165 &= (-385495523231271884)^3 + 383344975542639445^3 + 98422560467622814^3 \\
906 &= (-74924259395610397)^3 + 72054089679353378^3 + 35961979615356503^3
\end{aligned}$$

Merchandising!



Clothing, Shoes & Jewelry › Novelty & More › Clothing › Novelty › Women › Tops & Tees › T-Shirts

Celebrating Breakthroughs in Mathematics

The Answer to Life Universe and Everything 42 Sum of Cubes T-Shirt

Price: $14.99

Fit Type: Men

Men | Women | Youth

Color: Black

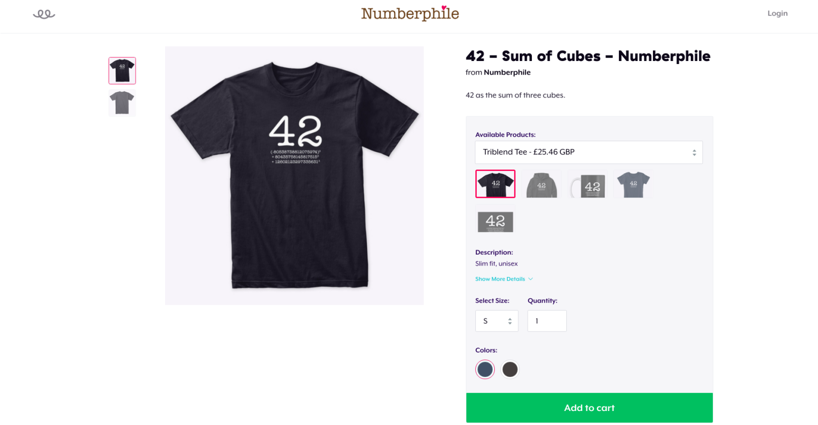
Size:

Select

- Solid colors: 100% Cotton; Heather Grey: 90% Cotton, 10% Polyester; All Other Heathers: 50% Cotton, 50% Polyester
- Imported
- Machine wash cold with like colors, dry low heat
- Answer to Life, the Universe, and Everything, Finally Cracked: 42 was the last remaining number below 100 which could not be expressed as the sum of three cubes, until now. Researchers found the answer in 2019 using over a million hours of computing time.
- 42 as sum of three cubes design celebrating a novel math breakthrough. Great science to wear daily and a great gift for math teachers, academics, math students, postdocs or anyone who loves math.
- Lightweight, Classic fit, Double-needle sleeve and bottom hem

Report incorrect product information.

Merchandising!



42 – Sum of Cubes – Numberphile

from **Numberphile**

42 as the sum of three cubes.

Available Products:

Triblend Tee - £25.46 GBP

Description:

Slim fit, unisex

Show More Details

Select Size: S

Quantity: 1

Colors:

Some features of the new algorithm

- CRT enumeration

Drew suggested ditching the big table of arithmetic progressions mod M and internally representing z as the solution to a bunch of congruences, working out the CRT on the fly.

This eliminates the time-space tradeoff, improving the memory footprint, and ends up being faster. It also allows us to consider z larger than 64 bits, and to optimize the choice of sieving primes.

Some features of the new algorithm

- CRT enumeration
- Cubic reciprocity constraints

Cassels proved via cubic reciprocity that any solution to $x^3 + y^3 + z^3 = 3$ satisfies $x \equiv y \equiv z \pmod 9$.
(This is a **global** constraint, and is not imposed 3-adically.)

It follows that for a fixed value of d, z is uniquely determined mod 81 (out of four locally admissible residues).

We extended Cassels' analysis to all $k \equiv \pm 3 \pmod 9$. For fixed d this imposes constraints on $z \pmod q$ for a certain $q \mid 27k$.

Some features of the new algorithm

- CRT enumeration
- Cubic reciprocity constraints
- Looking for solutions where they're most likely to be

An exhaustive search over all $d \leq (\sqrt[3]{2} - 1)B$ is expensive, because one ends up testing very few z for most large d. So it's usually more efficient to decouple the ranges of d and z.

An extreme example is our solution for $k = 3$, which has $d/|(\sqrt[3]{2} - 1)z| < 10^{-6}$.

This raises the question of how to choose $d_{\max}$ and $z_{\max}$ to maximize the likelihood of finding a solution within a given computing budget. We answered that with a heuristic analysis of the expected distribution of $d/|z|$, based on the the real density of points on the Fermat cubic $x^3 + y^3 + z^3 = 0$.

Some features of the new algorithm

- CRT enumeration
- Cubic reciprocity constraints
- Looking for solutions where they're most likely to be

Together, these optimizations make the search about 25 times faster than my original search for 33. With reasonable parameter choices (and no cherry picking!), the new code can find the solutions for all $k \in \{3, 33, 42, 165, 795, 906\}$ in under 50 core-years.

Heath-Brown's conjecture

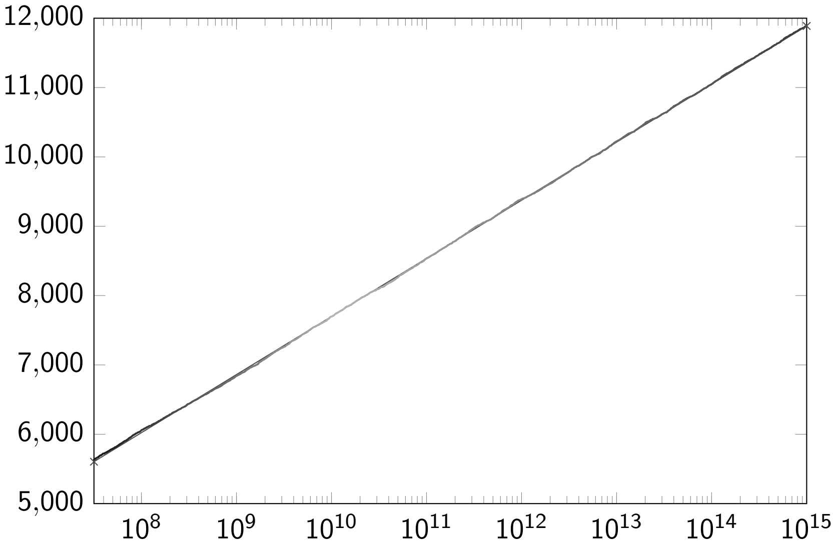
Heath-Brown (1992) conjectured that for a fixed cubefree $k \geq 3$ with no local obstructions, the number of solutions to

$$x^3 + y^3 + z^3 = k \quad \text{with } \max\{|x|, |y|, |z|\} \leq B$$

is asymptotic to $\rho \log B$ as $B \to \infty$, for a certain explicit number ρ (depending on k).

As part of our analysis, we computed the expected densities ρ to high precision, and compared Heath-Brown's prediction to the actual solution counts for $k < 1000$, $B \leq 10^{15}$ compiled by Huisman (2016).

Heath-Brown's conjecture



Future challenges

There are still eight candidate values of $k < 1000$ with no known three cube representations:

$$114,\ 390,\ 579,\ 627,\ 633,\ 732,\ 921,\ 975$$

For comparison, Miller and Woollett found representations for all but nine $k < 100$ in 1954. It took another 65 years (and Moore's Law) to complete their search.

The most direct analogue of Gauss' Eureka theorem is

$$k = \binom{x}{3} + \binom{y}{3} + \binom{z}{3}.$$

A similar algorithm should apply to this equation, except that instead of $z^3 \equiv k \pmod{d}$, one would have to solve $z^3 - z \equiv 6k \pmod{d}$.

Future challenges (continued)

When I shared the news of the 33 discovery with Heath-Brown (over a pint at the Nettle and Rye in Bristol), he asked "What about $x^3 + y^3 + 2z^3$?"

Drew and I found

$$\begin{aligned}
3676 &= (-1040743660046111)^3 + 1040742887519425^3 + 2(10786916701381)^3 \\
&= 36330027574363^3 + 16201371125359^3 + 2(-29663565976595)^3 \\
4108 &= 1037892936142982 5^3 + (-1000723420829657 3)^3 + 2(-386941905028601 0)^3 \\
5540 &= (-9766714092174289)^3 + 9706646342356061^3 + 2(2044177502818754)^3 \\
&= (-1274248491925945)^3 + 1094658539478551^3 + 2(723458325298043)^3
\end{aligned}$$

but there are still four numbers below 10,000 with no known representations:

$$148, \ 671, \ 5468, \ 7799$$

Life, the Universe, and Everything

- On February 27th 2019, Tim Browning, Brady Haran and I were all aged 42.
- “On a question of Mordell”, joint with Andrew Sutherland, is my 42nd paper.
- Mordell posed his question on $x^3 + y^3 + z^3 = 3$ in Cambridge in 1952.
- Douglas Adams was born in Cambridge in 1952.
- Very recently, and for the first time in 42 years, The Daily Mail overtook The Sun to become the highest selling newspaper in the UK.