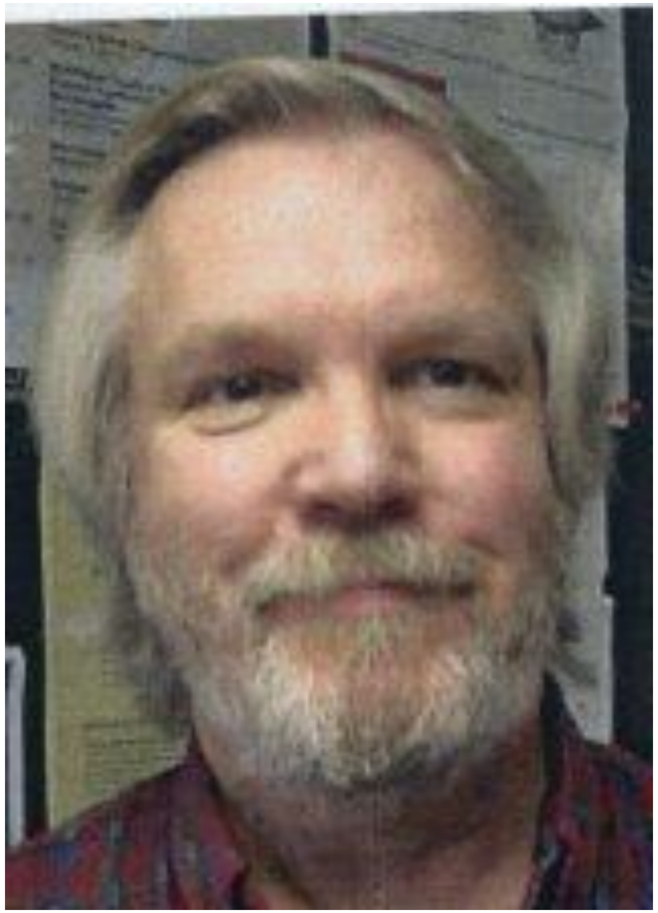
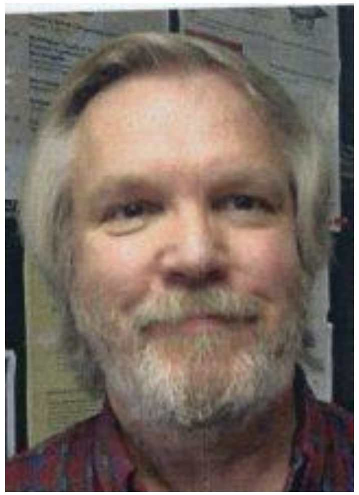
Congruent numbers
(in tribute to Jerrold Tunnell)



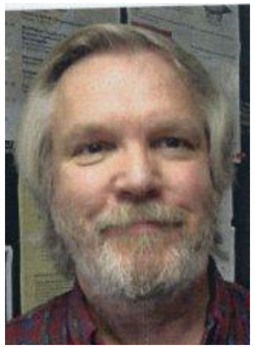
Jerrold Bates Tunnell (1950 – 2022)

Jerrold Bates Tunnell



1950: Tunnell was born September 16, in Dallas, Texas
1972: Graduates from Harvey Mudd College
1977: PhD in Mathematics from Harvard
“*On the Local Langlands Conjecture for GL(2)*”, advised by John Tate (Abel prize, 2010)
1981: The Langlands–Tunnell theorem generalises Langlands' work on the Artin conjecture and is an important ingredient in Wiles’ proof of Fermat’s Last Theorem
1982–83: Member of Institute of Advanced Study at Princeton
1983: Solves congruent number problem up to Birch & Swinnerton-Dyer conjecture
Joins Rutgers
2010: Fellowship of American Mathematical Society
2022: Dies on April 1 in a cycling accident

Tributes



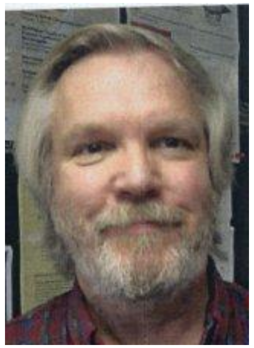
Alex Kontorovich
@AlexKontorovich

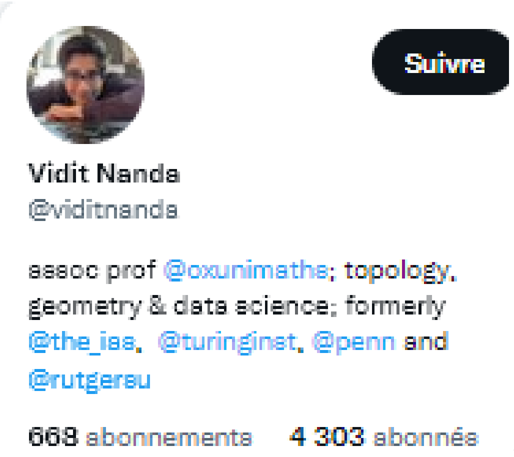
Prof of #Math at @RutgersU + 2020-21 Distinguished Vis Prof at @MoMath1 • Editor-in-Chief of Experimental Mathematics • Advisory Board at @QuantaMagazine

742 abonnements 16,4 k abonnés

I'm devastated to learn of the untimely passing of our longtime Rutgers colleague Jerrold Tunnell (1950-2022), apparently from a tragic bicycling accident. Jerry was a PhD student of Tate's at Harvard, and is perhaps best known for the Langlands-Tunnell theorem, which played a key role in Wiles's attack on Fermat's Last Theorem. He was a great colleague, always learning new things and teaching new courses, popping in to my office to discuss anything from automorphic forms, to dynamical systems and ergodic theory. He will be sorely missed. RIP

Tributes





Vidit Nanda
@viditnanda

assoc prof @oxunimaths; topology, geometry & data science; formerly @the_ias, @turinginst, @penn and @rutgersu

668 abonnements 4 303 abonnés

Here are two stories about my graduate school experience at Rutgers, both about a man who has played a much larger role in my career than he realised.

I wasn't a mathematician in my undergraduate years, mostly because I disliked whatever little abstract algebra I knew. Of course the first class I ever sat through in graduate school was abstract algebra.

I wanted to pay close attention, so I go right up to the front and eagerly await the prof, notebook and pencil at the ready. It's a small classroom with maybe about 15 other students.

Prof walks in, right on time, picks up a piece of chalk and booms at what I can only imagine is > 100 decibels: "WELCOME TO ABSTRACT ALGEBRA!!!" It's the sonic equivalent of being slapped in the face by a tornado. Incredibly, the volume only goes up from here.

This class destroyed me in all the right ways. The lectures were very well organised and I learned a lot. Very happy to have had the experience. But I never sat anywhere near the front of the classroom again!

Next story, a couple of years later. I decide to take algebraic geometry from the same Prof; a veteran by now, I sit at the back and take good notes. It's a nice fast-paced class, and before we know it the semester is over.

Good news, he says, there is no final exam! Just solve five textbook problems from the relevant chapters (I think it was Harris's book --- nice and low-brow, no schemes). Manna from heaven, we thought. Which five problems, prof?

He says "any five that haven't already been turned in by other students before you". We thought he was joking and laughed, ha ha. He was not joking.

The next week was hell. The entire class was engaged in squid/hunger-games, solving the five easiest problems they could find and emailing them to our prof, only to discover that many had been solved & submitted before by others.

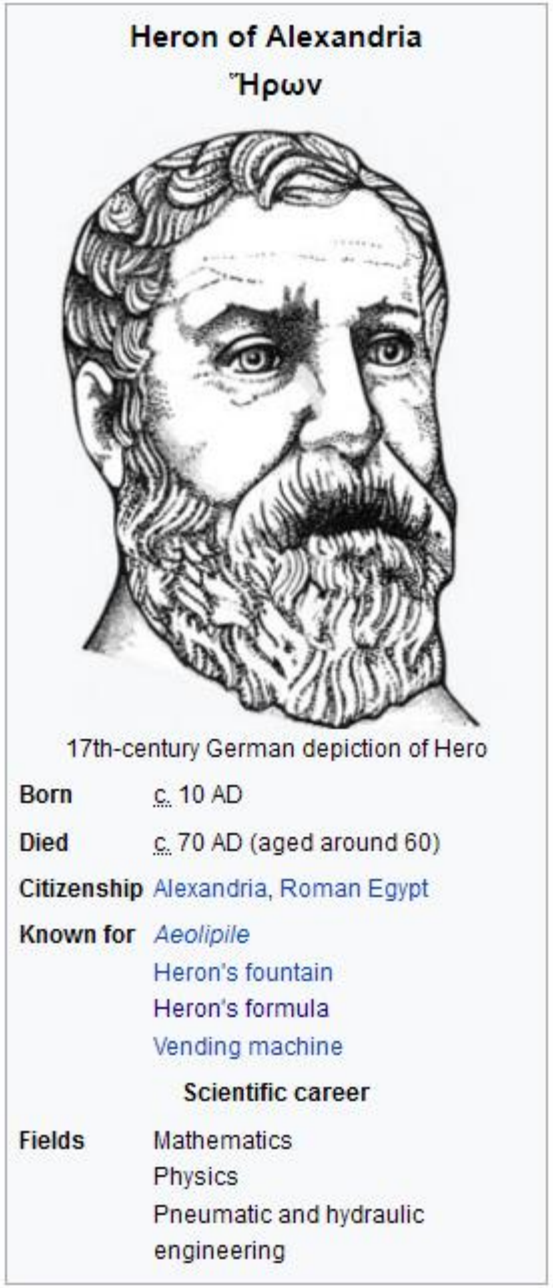
I ended up submitting 12 solutions in all because I had been scooped on 7 occasions. Remember, the easy problems got done first, so if your early efforts got scooped then the remaining problems were much harder!

I was quite frustrated at the time, even after managing to submit my 5 solutions. But with every passing year, I realise that there were important lessons in all this, far more valuable than the algebraic geometry that I'd learned in the course.

Why mention any of this now? This prof was Jerrold Tunnell, made famous by the Langlands-Tunnell theorem, which formed a key ingredient in Wiles's proof of Fermat's last theorem.

I've just learned from @AlexKontorovich that Prof Tunnell passed away a few days ago. I haven't even exchanged email with him in well over a decade, but somehow the loss seems personal

Heron Triangles



Heron of Alexandria

Ἥρων

17th-century German depiction of Hero

Born	c. 10 AD
Died	c. 70 AD (aged around 60)
Citizenship	Alexandria, Roman Egypt
Known for	*Aeolipile* Heron's fountain Heron's formula Vending machine

Scientific career

Fields	Mathematics Physics Pneumatic and hydraulic engineering

A triangle with rational sides and rational area is called a Heron (or Heronian) triangle, presumably in connection with Heron's formula for triangle area, which appeared in his *Metrica* of AD 60:

$$A = \frac{1}{4}\sqrt{4a^2b^2 - (a^2 + b^2 - c^2)^2}$$

where *a*, *b* and *c* are the triangle sides.

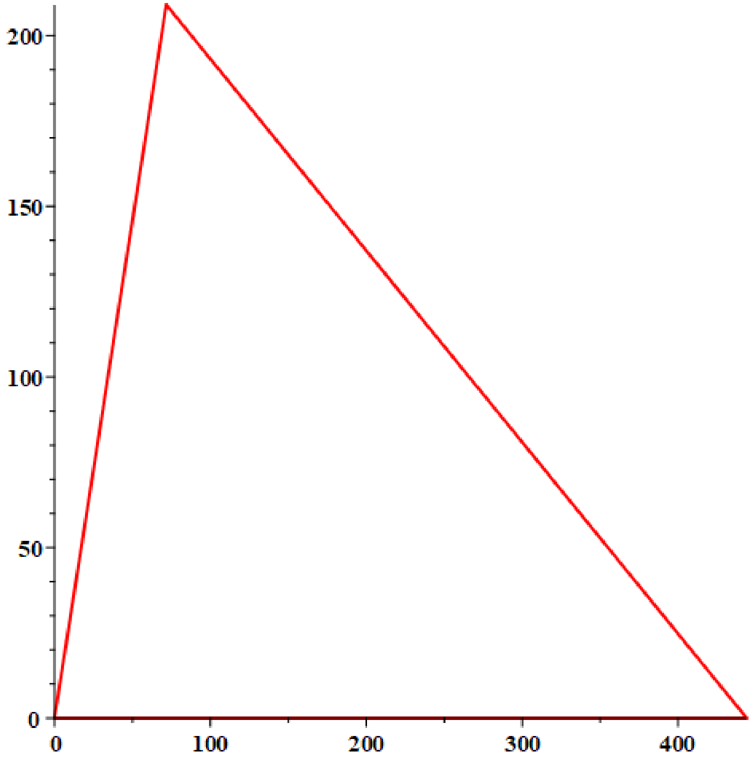
Brahmagupta (C7th) constructed all such triangles as those with sides proportional to

$$a = n(m^2 + k^2)$$
$$b = m(n^2 + k^2)$$
$$c = (m + n)(mn - k^2)$$

where *m, n* and *k* are positive integers satisfying

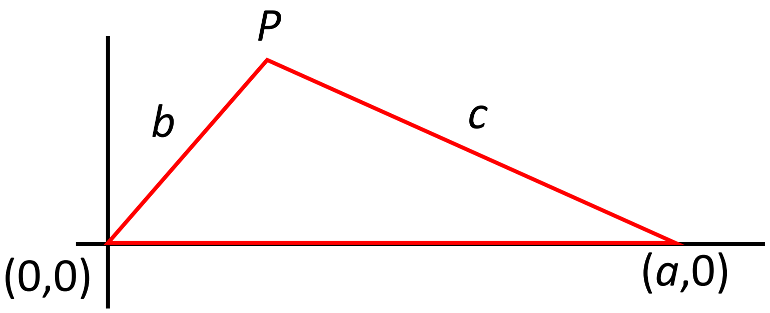
$$m \geq n \geq 1, \qquad mn > k^2 \geq 1,$$
$$\text{and} \quad \gcd(m, n, k) = 1$$

E.g. (*m*,*n*,*k*) = (7,6,5) gives (*a*,*b*,*c*) = (444, 427, 221) with area 46410.



Digression: plotting Heron triangles

Given (*a*,*b*,*c*) we want to plot the triangle with the minimum of fuss and bother. So, like this:



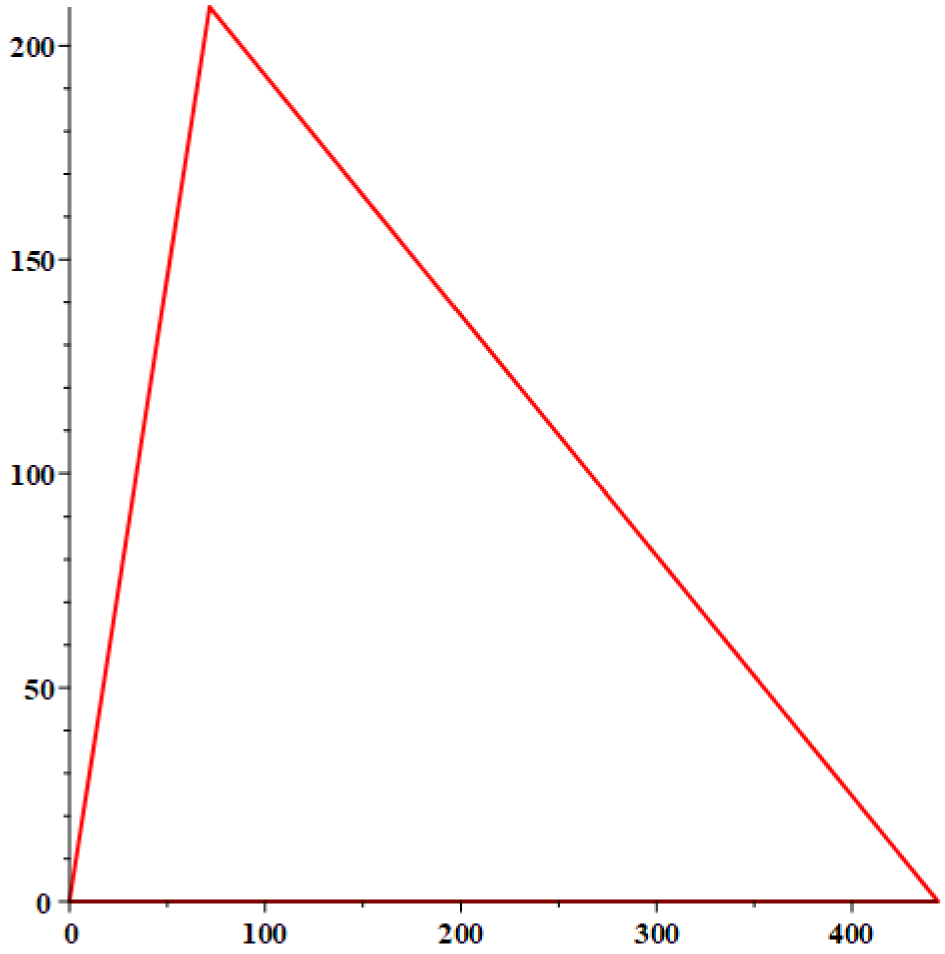
Now $P = (b\cos t\,, b\sin t) = \left(\frac{a^2+b^2-c^2}{2a}\,, b\sin t\right)$ by cosine rule.

And $\sin t = \sqrt{1-\left(\frac{a^2+b^2-c^2}{2ab}\right)^2} = \frac{1}{2ab}\sqrt{4a^2b^2-(a^2+b^2-c^2)^2}$

$= \frac{1}{2ab} \times 4 \times$ area *A* of triangle

So $P = \frac{1}{2a}(a^2+b^2-c^2, 4A)$

Note that *b* and *c* could be square roots and still be plotted with rational points



(*a*,*b*,*c*) = (444, 427, 221)

Pythagorean triples

A right triangle with rational sides *a* <*b* < *c* is Heron since area is $\frac{1}{2}ab$.

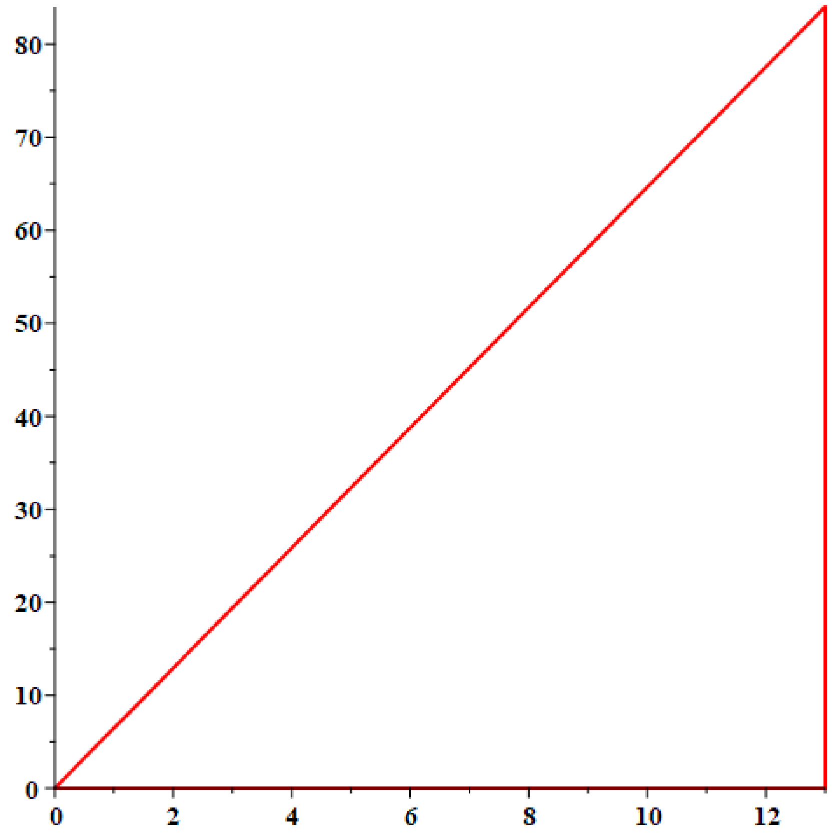
All such triangles have also been constructed (by Euclid) as those with sides proportional to

$$a = m^2 - n^2$$
$$b = 2mn$$
$$c = m^2 + n^2$$

where *m, n* are positive integers satisfying

$$m > n \text{ and } \gcd(m,n) = 1$$

E.g. (*m,n*) = (7,6) gives (*a,b,c*) = (13, 84, 85), with area 546.



Brahmagupta's construction, for comparison:

$$a = n(m^2 + k^2)$$
$$b = m(n^2 + \ k^2)$$
$$c = (m+n)(mn - k^2)$$

where *m, n* and *k* are positive integers satisfying

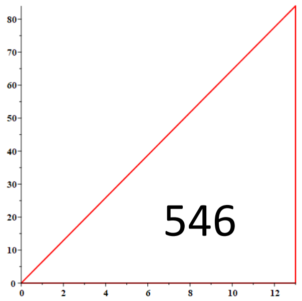
$$m \geq n \geq 1, \qquad mn > k^2 \geq 1,$$

and $\gcd(m,n,k) = 1$.

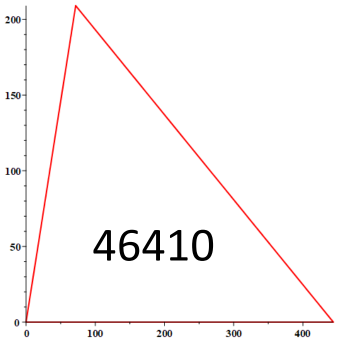
Exercise: find *m,n,k* giving right triangle (13, 84, 85).

The oldest unsolved problem in mathematics?

A positive integer is **congruent** if it is the area of some right rational triangle

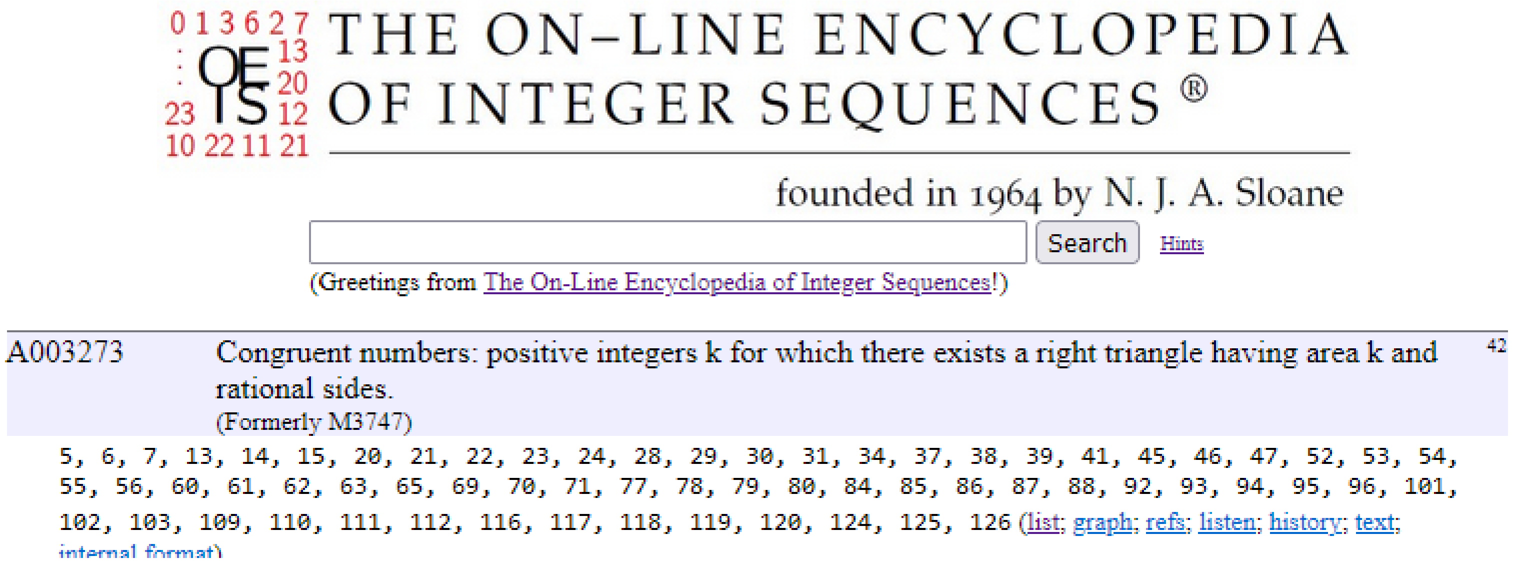


Congruent: area of (13, 84, 85)



Not congruent: no right rational triangle has this area

How do we know 46410 is not congruent? (We will see later). We are looking for a practical test to determine if a given positive integer is **congruent** or not.



THE ON-LINE ENCYCLOPEDIA OF INTEGER SEQUENCES ®

founded in 1964 by N. J. A. Sloane

Search Hints

(Greetings from The On-Line Encyclopedia of Integer Sequences!)

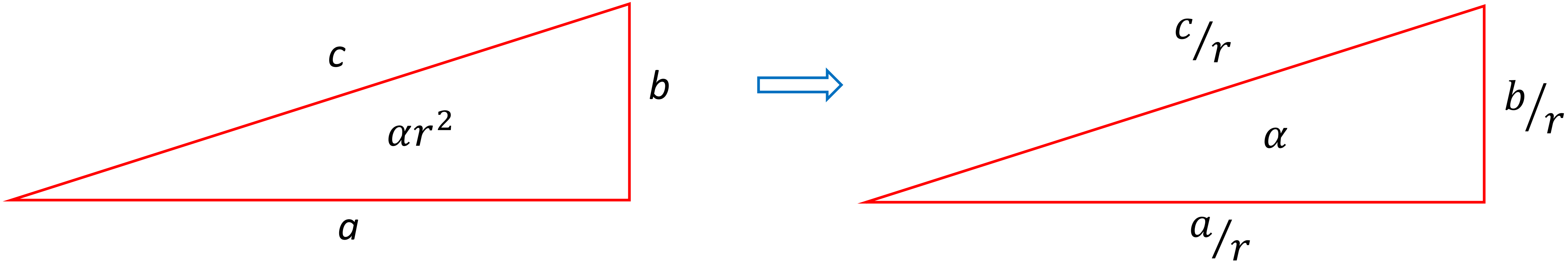
A003273 Congruent numbers: positive integers k for which there exists a right triangle having area k and rational sides. 42

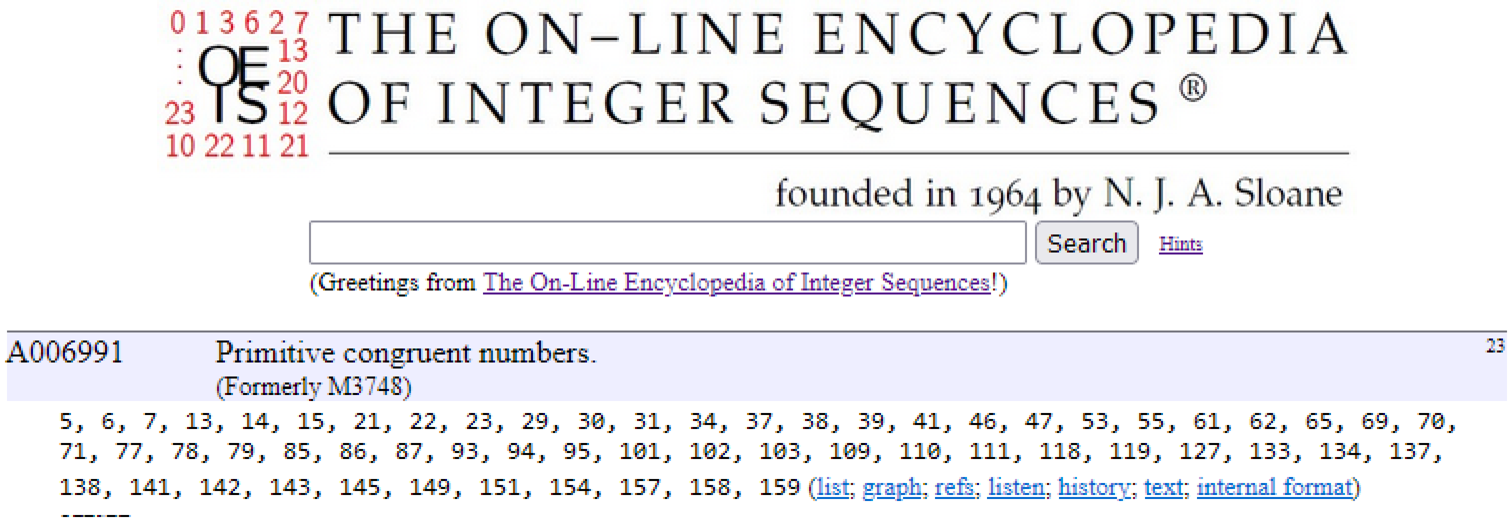
(Formerly M3747)

5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47, 52, 53, 54, 55, 56, 60, 61, 62, 63, 65, 69, 70, 71, 77, 78, 79, 80, 84, 85, 86, 87, 88, 92, 93, 94, 95, 96, 101, 102, 103, 109, 110, 111, 112, 116, 117, 118, 119, 120, 124, 125, 126 (list; graph; refs; listen; history; text; internal format)

> "The congruent number problem, the written history of which can be traced back at least a millennium, is the oldest unsolved major problem in number theory, and perhaps in the whole of mathematics."
>
> John H. Coates

Non-square-free congruent numbers are not very interesting





THE ON-LINE ENCYCLOPEDIA OF INTEGER SEQUENCES ®

founded in 1964 by N. J. A. Sloane

(Greetings from The On-Line Encyclopedia of Integer Sequences!)

A006991 Primitive congruent numbers. 23
(Formerly M3748)

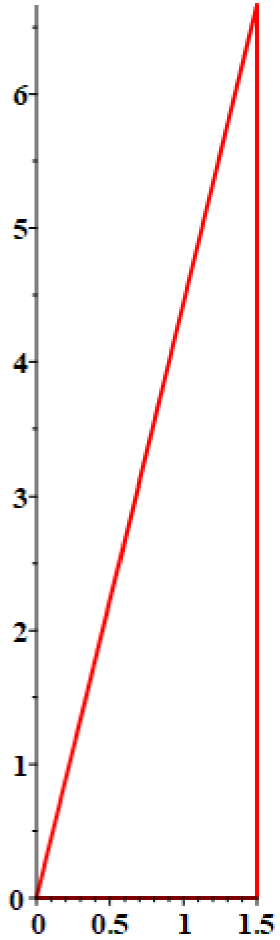
5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, 34, 37, 38, 39, 41, 46, 47, 53, 55, 61, 62, 65, 69, 70, 71, 77, 78, 79, 85, 86, 87, 93, 94, 95, 101, 102, 103, 109, 110, 111, 118, 119, 127, 133, 134, 137, 138, 141, 142, 143, 145, 149, 151, 154, 157, 158, 159 (list; graph; refs; listen; history; text; internal format)

Why congruent?

The word ‘congruent’ comes from Fibonacci’s use of the term ‘congruum’ to mean the common different in a sequence of three rational squares in arithmetic progression.

Any such sequence, u^2, v^2, w^2, with common difference ns^2 corresponds to a right rational triangle $\frac{w-u}{s}, \frac{w+u}{s}, \frac{2v}{s}$ with area n.

For example, the sequence $(31/6)^2, (41/6)^2, (49/6)^2$ is in arithmetic progression with common difference 5×2^2 and corresponds to the triangle $\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$ with area 5.



Fibonacci (C13th) discovered that 7 is congruent (5 and 6 were known to 10th century Muslim scholars). He asserted without proof that 1 is not congruent.

Fermat, 1640, proved that 1 is not congruent, and therefore that no rational square is congruent. He observed that this implies that the equation $x^4 + y^4 = 1$ has no non-trivial rational solutions, perhaps inspiring his Last Theorem.

By the way, Fermat also proved that there is no 4-term arithmetic progression consisting of rational squares.

Which numbers are congruent?

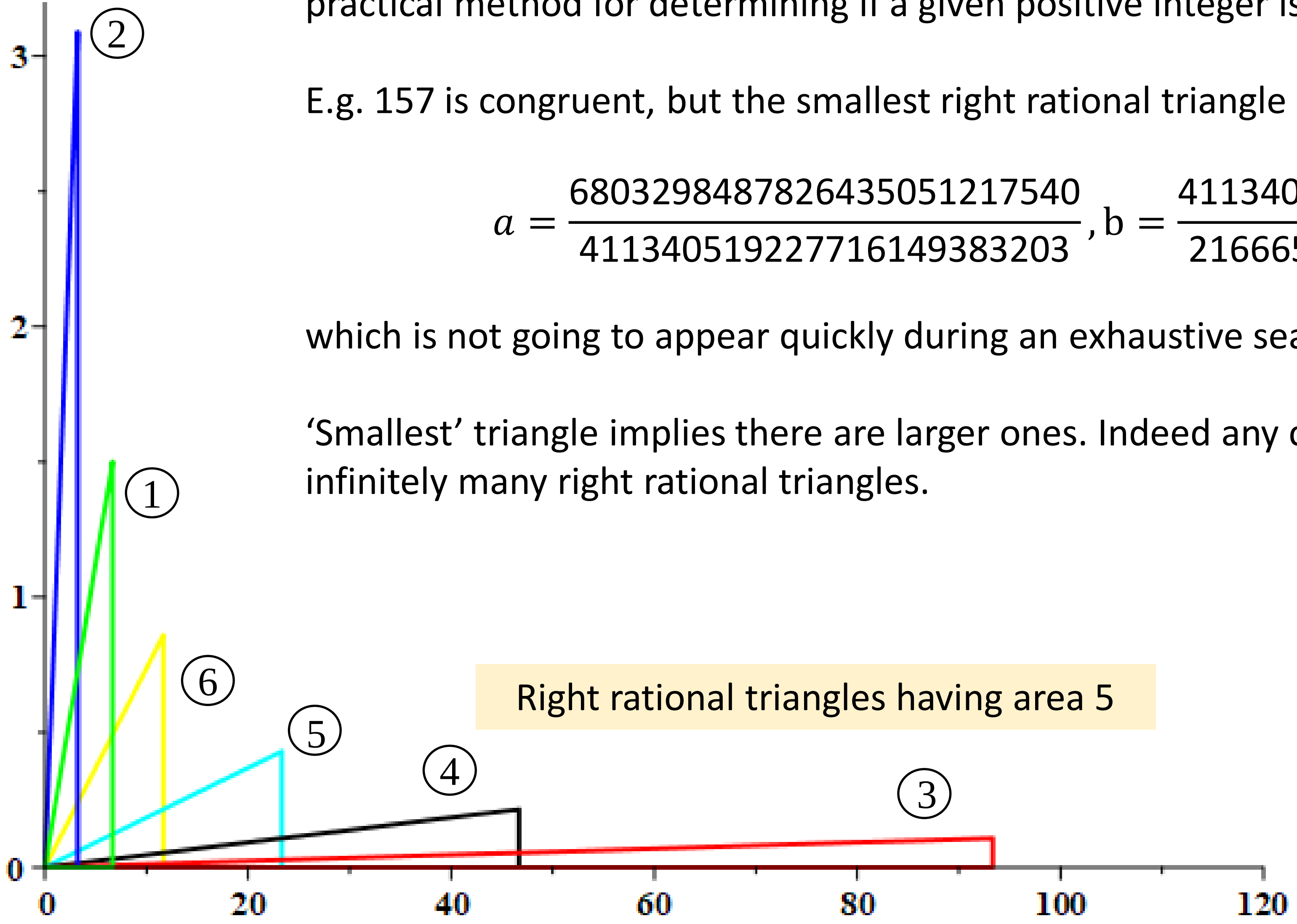
We can construct all Heron triangles and all Pythagorean triples. But this does not give a practical method for determining if a given positive integer is congruent!

E.g. 157 is congruent, but the smallest right rational triangle having area 157 has legs

$$a = \frac{6803298487826435051217540}{411340519227716149383203}, \mathrm{b} = \frac{411340519227716149383203}{21666555693714761309610}$$

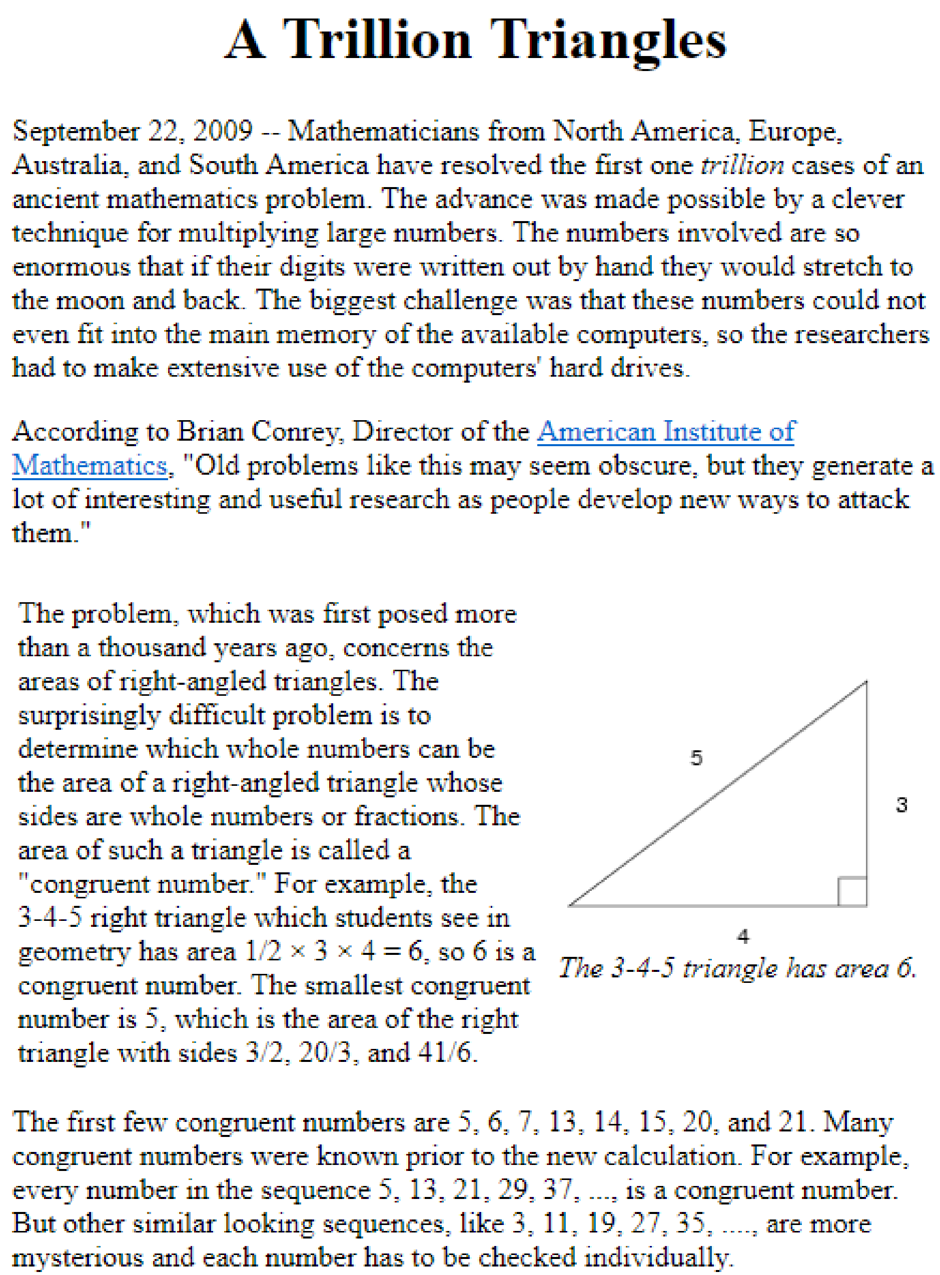
which is not going to appear quickly during an exhaustive search!

‘Smallest’ triangle implies there are larger ones. Indeed any congruent number is the area of infinitely many right rational triangles.



Right rational triangles having area 5

Nevertheless…



A Trillion Triangles

September 22, 2009 -- Mathematicians from North America, Europe, Australia, and South America have resolved the first one *trillion* cases of an ancient mathematics problem. The advance was made possible by a clever technique for multiplying large numbers. The numbers involved are so enormous that if their digits were written out by hand they would stretch to the moon and back. The biggest challenge was that these numbers could not even fit into the main memory of the available computers, so the researchers had to make extensive use of the computers' hard drives.

According to Brian Conrey, Director of the American Institute of Mathematics, "Old problems like this may seem obscure, but they generate a lot of interesting and useful research as people develop new ways to attack them."

The problem, which was first posed more than a thousand years ago, concerns the areas of right-angled triangles. The surprisingly difficult problem is to determine which whole numbers can be the area of a right-angled triangle whose sides are whole numbers or fractions. The area of such a triangle is called a "congruent number." For example, the 3-4-5 right triangle which students see in geometry has area 1/2 × 3 × 4 = 6, so 6 is a congruent number. The smallest congruent number is 5, which is the area of the right triangle with sides 3/2, 20/3, and 41/6.

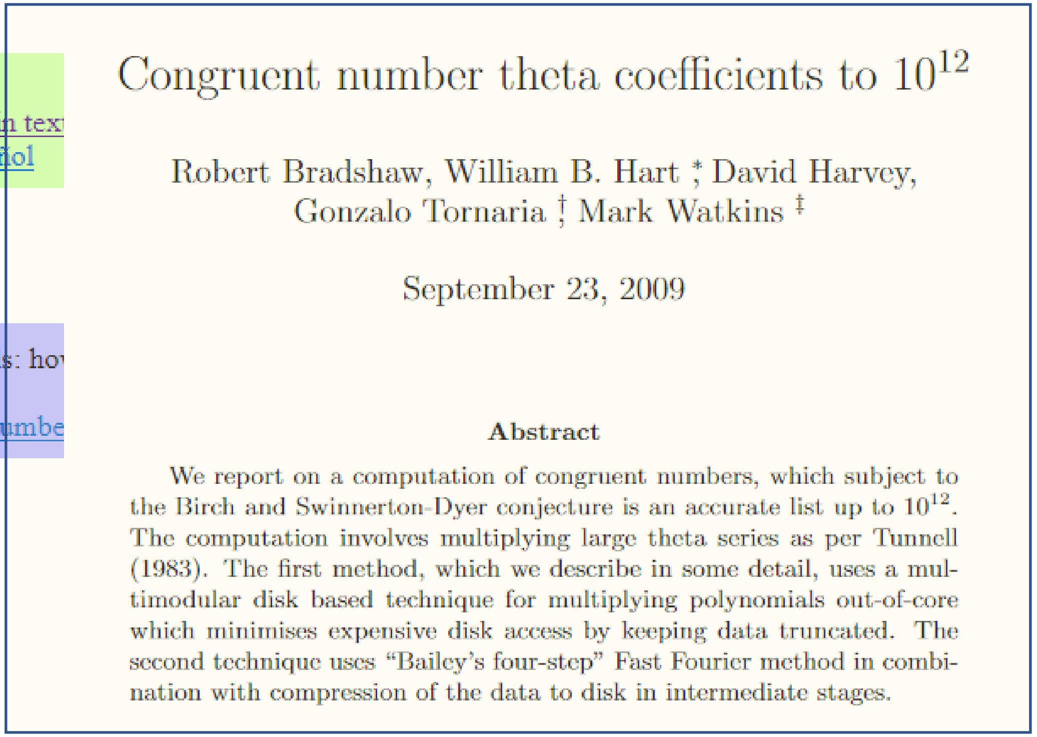
The 3-4-5 triangle has area 6.

The first few congruent numbers are 5, 6, 7, 13, 14, 15, 20, and 21. Many congruent numbers were known prior to the new calculation. For example, every number in the sequence 5, 13, 21, 29, 37, ..., is a congruent number. But other similar looking sequences, like 3, 11, 19, 27, 35, ..., are more mysterious and each number has to be checked individually.

Press release in
MSWord or plain tex
Versión en español

Computer details: hov
to
multiply large numbe

Math details:
triangles and elliptic
curves



Congruent number theta coefficients to 10^{12}

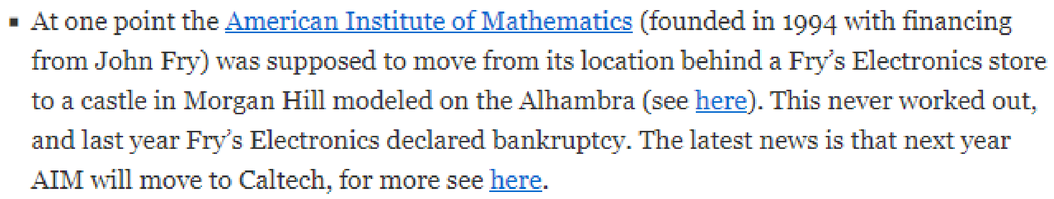
Robert Bradshaw, William B. Hart[*], David Harvey,
Gonzalo Tornaria[†], Mark Watkins[‡]

September 23, 2009

Abstract

We report on a computation of congruent numbers, which subject to the Birch and Swinnerton-Dyer conjecture is an accurate list up to 10^{12}. The computation involves multiplying large theta series as per Tunnell (1983). The first method, which we describe in some detail, uses a multimodular disk based technique for multiplying polynomials out-of-core which minimises expensive disk access by keeping data truncated. The second technique uses "Bailey's four-step" Fast Fourier method in combination with compression of the data to disk in intermediate stages.

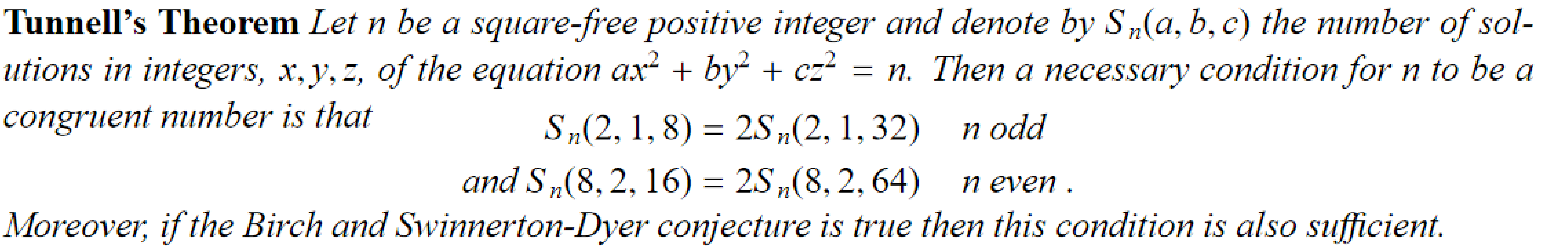
Incidentally…



- At one point the American Institute of Mathematics (founded in 1994 with financing from John Fry) was supposed to move from its location behind a Fry's Electronics store to a castle in Morgan Hill modeled on the Alhambra (see here). This never worked out, and last year Fry's Electronics declared bankruptcy. The latest news is that next year AIM will move to Caltech, for more see here.

Not Even Wrong blog, April 18, 2022

So how did Bradshaw et al do it (up to BSD)?



Tunnell's Theorem *Let n be a square-free positive integer and denote by $S_n(a,b,c)$ the number of solutions in integers, x, y, z, of the equation $ax^2 + by^2 + cz^2 = n$. Then a necessary condition for n to be a congruent number is that*

$$S_n(2,1,8) = 2S_n(2,1,32) \quad n \text{ odd}$$

$$\text{and } S_n(8,2,16) = 2S_n(8,2,64) \quad n \text{ even}.$$

Moreover, if the Birch and Swinnerton-Dyer conjecture is true then this condition is also sufficient.

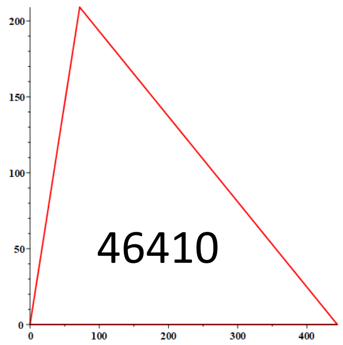
1 is not a congruent number because $2x^2 + y^2 + 8z^2 = 1$ and $2x^2 + y^2 + 32z^2 = 1$ both have one solution in integers, namely $(0, \pm 1, 0)$.

157 is (up to BSD) congruent because $2x^2 + y^2 + 8z^2 = 157$ has twice as many integer solutions as $2x^2 + y^2 + 32z^2 = 157$. Namely zero.

26 is not congruent because $8x^2 + 2y^2 + 16z^2 = 26$ has 12 solutions $(\pm 1, \pm 1, \pm 1), (\pm 1, \pm 3, 0)$ while $8x^2 + 2y^2 + 64z^2 = 26$ has 4: $(\pm 1, \pm 3, 0)$.

34 is congruent (up to BSD) because $8x^2 + 2y^2 + 16z^2 = 34$ has 8 solutions $(0, \pm 3, \pm 1), (\pm 2, \pm 1, 0)$ while $8x^2 + 2y^2 + 64z^2 = 34$ has 4: $(\pm 2, \pm 1, 0)$.

Our example from earlier:



Not congruent:

$S_{46410}(8,2,16) = 256$

$S_{46410}(8,2,64) = 160$

Whereof Birch and Swinnerton-Dyer?

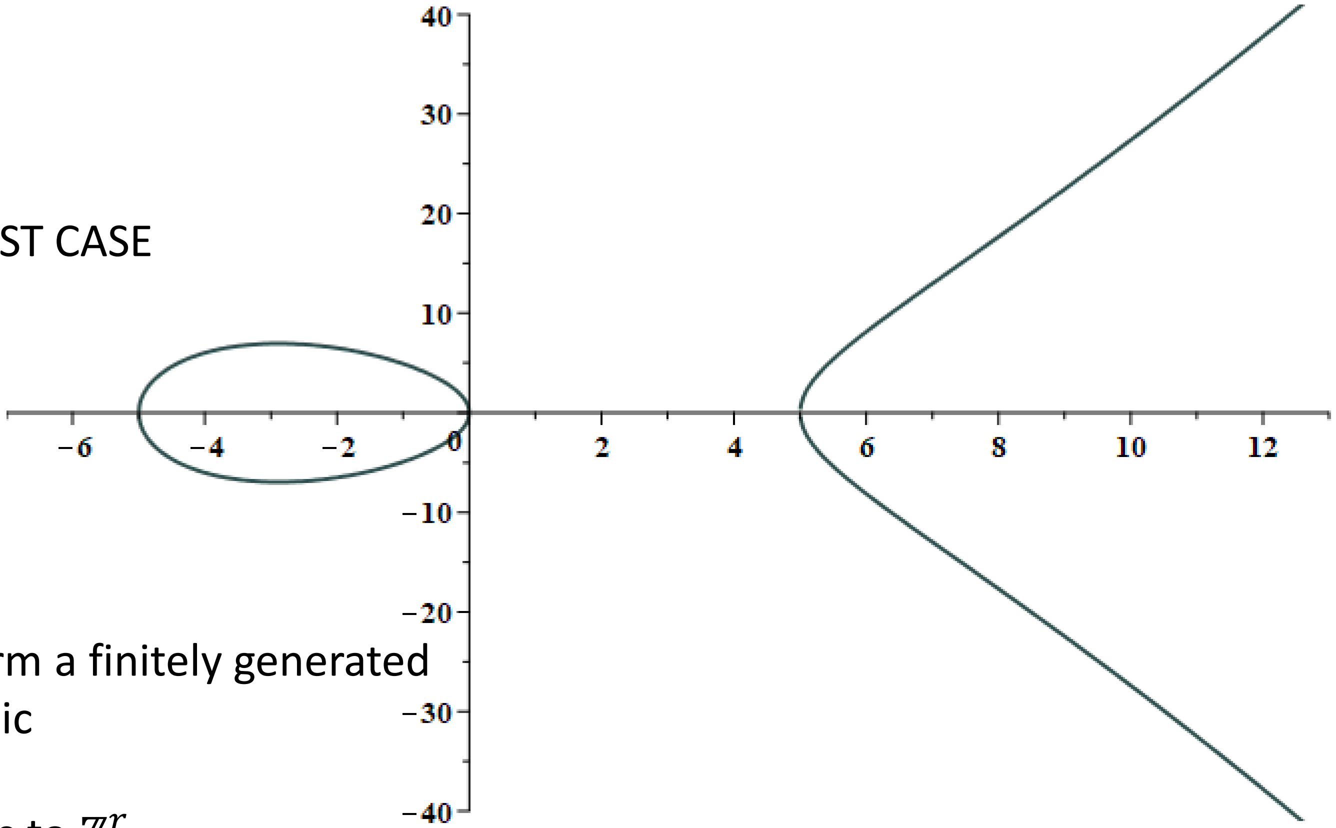
Equations in degree 1 – SOLVED (linear equations)

Equations in degree 2 – SOLVED (conics)

Equations in degree 3 – WIDE OPEN EVEN IN THE SIMPLEST CASE

$$y^2 = x^3 + ax + b$$

i.e. elliptic curves

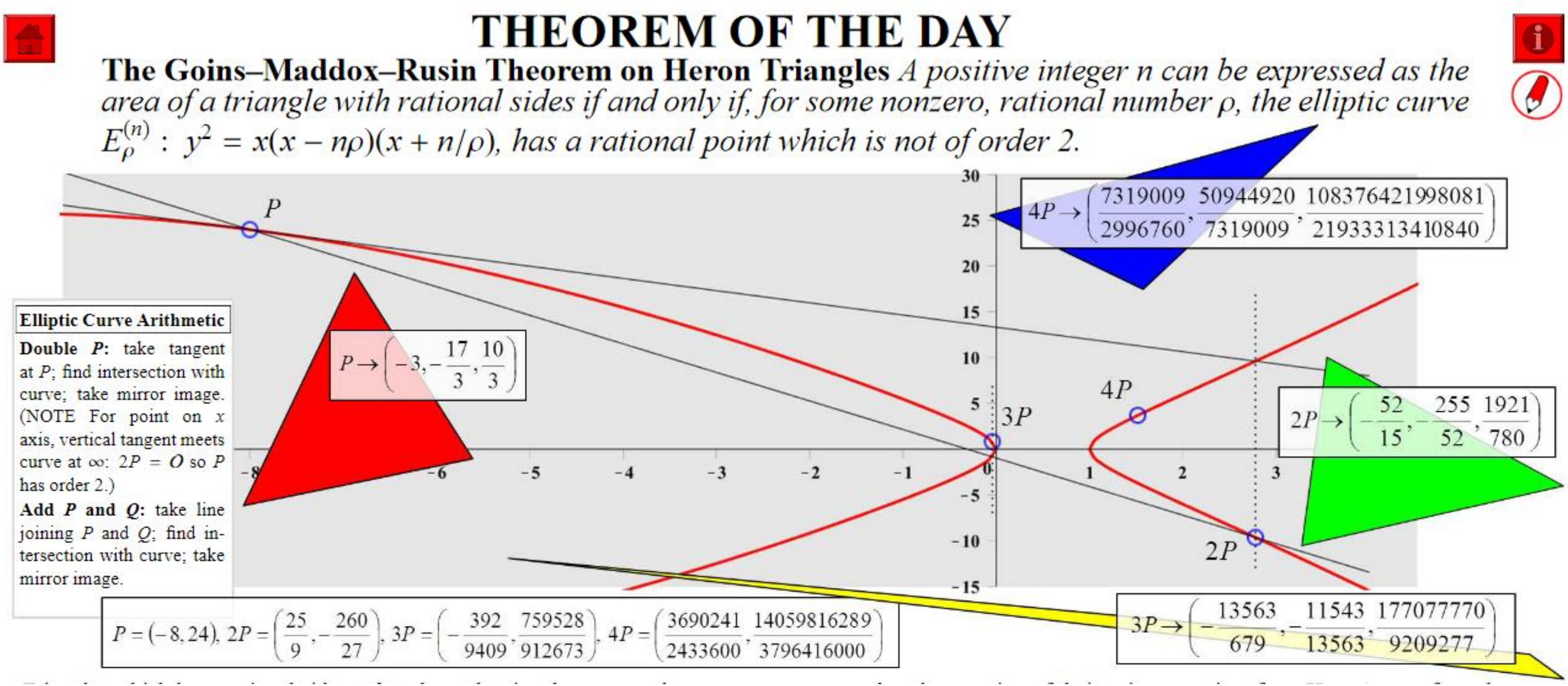


However, we know

- The rational points, together with a point at infinity, form a finitely generated abelian group under an appropriately defined arithmetic
- The points of finite order form a finite subgroup
- The points of infinite order form a subgroup isomorphic to $\mathbb{Z}^r$
- How to calculate *r,* the **rank** of the elliptic, provided that Birch and Swinnerton-Dyer's conjectural calculation is valid.

Heron triangles and elliptic curves

There is a deep connection between elliptic curves and rational triangles with integer area



THEOREM OF THE DAY

The Goins–Maddox–Rusin Theorem on Heron Triangles *A positive integer n can be expressed as the area of a triangle with rational sides if and only if, for some nonzero, rational number ρ, the elliptic curve* $E_\rho^{(n)}: y^2 = x(x - n\rho)(x + n/\rho)$, *has a rational point which is not of order 2.*

Elliptic Curve Arithmetic

Double P**:** take tangent at P; find intersection with curve; take mirror image. (NOTE For point on x axis, vertical tangent meets curve at ∞: $2P = O$ so P has order 2.)

Add P **and** Q**:** take line joining P and Q; find intersection with curve; take mirror image.

$P \rightarrow \left(-3, -\frac{17}{3}, \frac{10}{3}\right)$

$4P \rightarrow \left(\frac{7319009}{2996760}, \frac{50944920}{7319009}, \frac{108376421998081}{21933313410840}\right)$

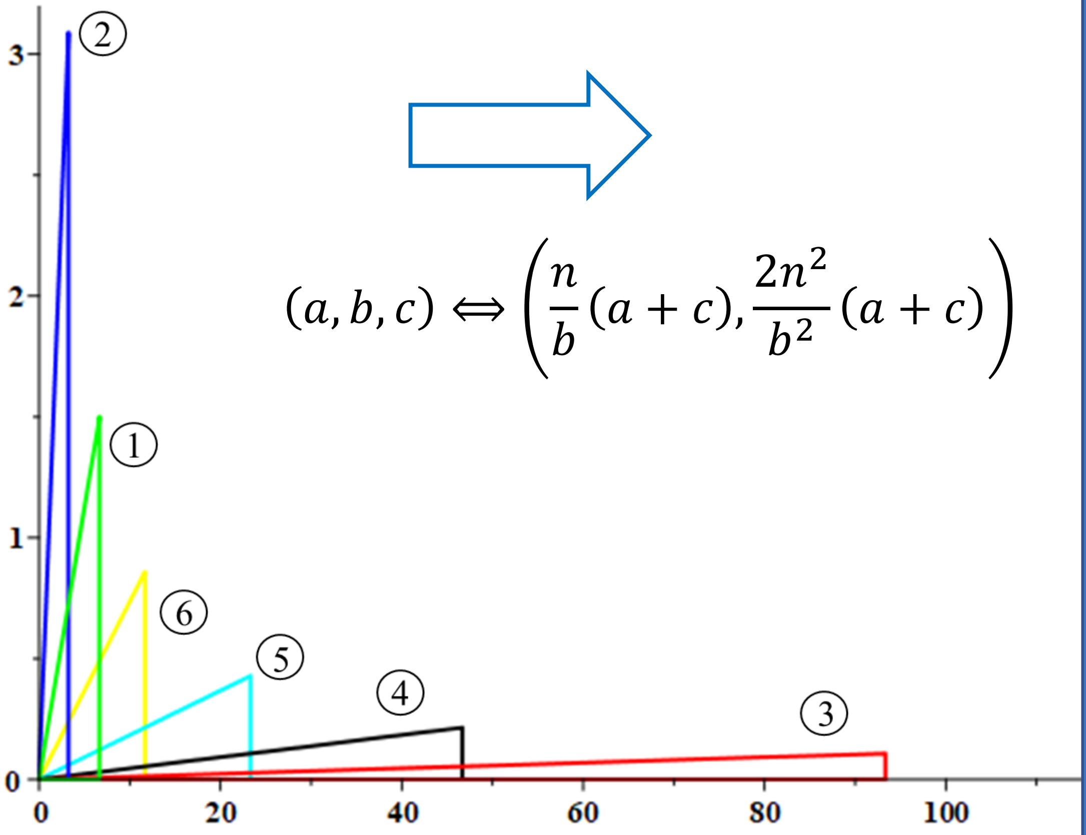
$2P \rightarrow \left(-\frac{52}{15}, -\frac{255}{52}, \frac{1921}{780}\right)$

$3P \rightarrow \left(-\frac{13563}{679}, -\frac{11543}{13563}, \frac{177077770}{9209277}\right)$

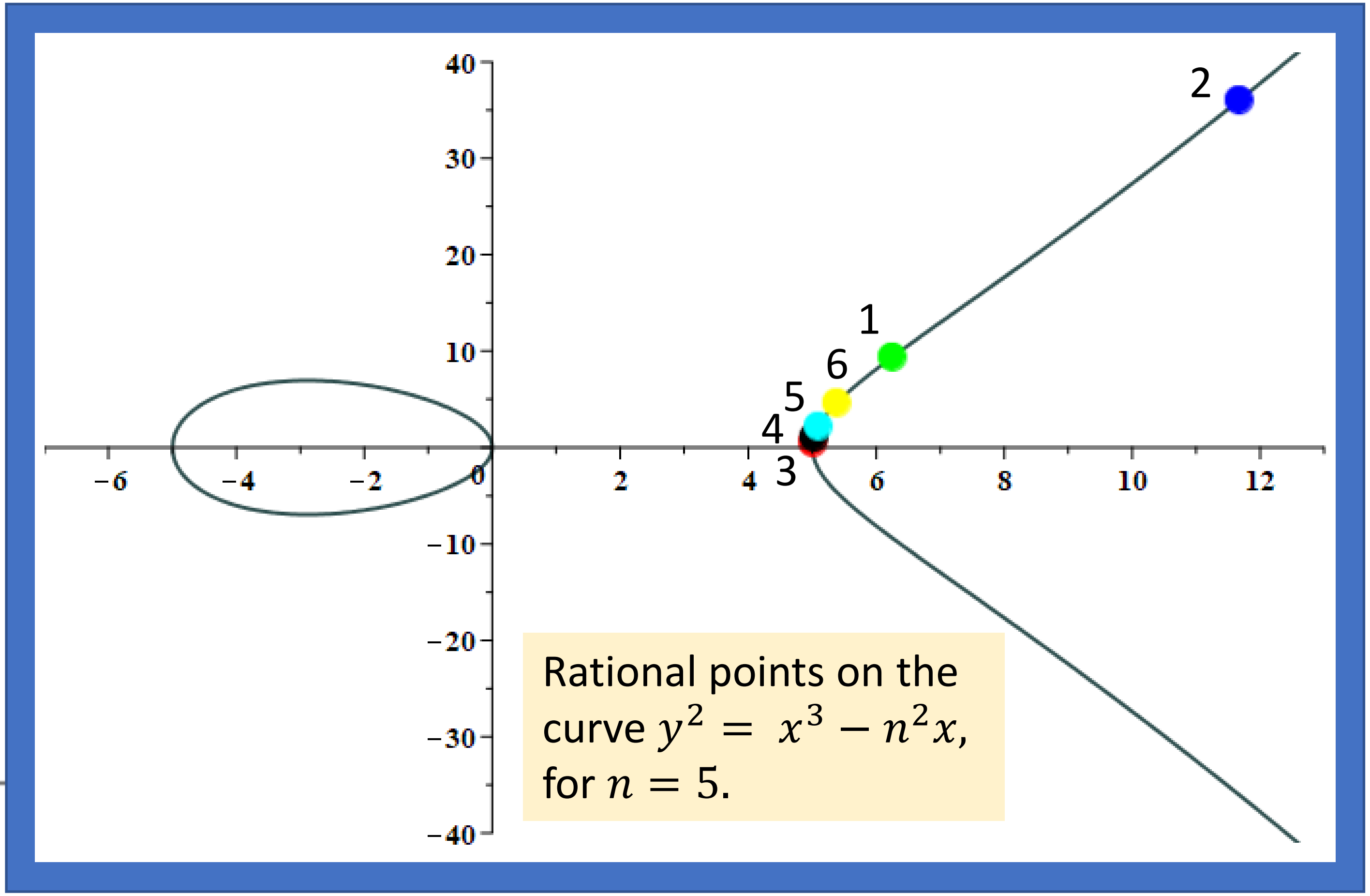
$P = (-8, 24)$, $2P = \left(\frac{25}{9}, -\frac{260}{27}\right)$, $3P = \left(-\frac{392}{9409}, \frac{759528}{912673}\right)$, $4P = \left(\frac{3690241}{2433600}, \frac{14059816289}{3796416000}\right)$

Congruent numbers and elliptic curves

For right-angled Heron triangles, corresponding to congruent numbers, we have a very simple mapping between triangles and elliptic curves, shown here for the six rational right triangles of area 5 shown earlier:



$$(a,b,c) \Leftrightarrow \left(\frac{n}{b}(a+c), \frac{2n^2}{b^2}(a+c)\right)$$



Rational points on the curve $y^2 = x^3 - n^2x$, for $n = 5$.

Birch and Swinnerton-Dyer and Jerrold Bates Tunnell

Tunnell was able to extract, for the special case of the elliptic curves $y^2 = x^3 - n^2x$, an explicit version of the rank calculation of BSD for the case $r = 0$, i.e. the subgroup of rational points on the curve of infinite order is trivial, meaning there can be no congruent numbers for the given value of n. This took the form of the degree 2 equations specified in his theorem. Enough is known about BSD for these equations to give a necessary condition for rank zero.
Forty years later, going the other way is one of the Clay Mathematics Institute's $1 million prizes!