Finding Congruent Numbers, Arithmetic Progressions of Squares, and Triangles

An invitation to analytic number theory

David Lowry-Duda

February 2019

Warwick Mathematics Institute
University of Warwick

Acknowledgements

Much of this talk comes from past and present work with a few collaborators of mine, including Tom Hulse (Boston College), Chan Ieong Kuan (Sun-Yat Sen University), and Alex Walker (Rutgers).

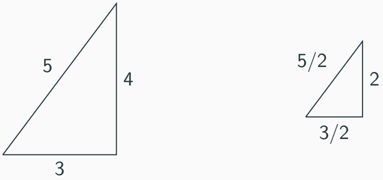
Other parts come from conversations with Joe Silverman (Brown), Keith Conrad (University of Connecticut), and the Warwick Maths Institute number theory and geometry groups.

Having said that, much of the material in this talk is deeply entwined in the history of number theory, algebraic geometry, and (in particular) elliptic curves.

Triangles

What is a Congruent Number?

If a right triangle has rational sidelengths, we call it a rational triangle. For example, the $(3, 4, 5)$ triangle is rational, and scaling a rational triangle by a rational number (such as by $1/2$) gives another rational triangle.



There are infinitely many rational triangles, but "most" triangles are not rational – even if two sides are rational. For example, the $(1, 1, \sqrt{2})$ triangle is not rational.

Every rational triangle has rational area. The two triangles above have areas 6 and $3/2$.

We call a positive rational number n a congruent number if there is a rational right triangle with area n. So we see that 6 and 3/2 are congruent.

Guiding Question

Which rational numbers are congruent? That is, which numbers appear as areas of rational triangles?

This is one of those questions that feel simple, but is challenging, interesting, and closely related to deep mathematics.

Congruent Number Detection

Given a rational number n, can we decide if it is congruent?

For example, is 1 congruent?

Theorem (Fermat 1640)

1 *is not congruent.*

Broad Idea of Fermat's Proof

Suppose there is a rational right triangle of area 1. Call the common denominator of the side lengths d, so that the sides can be written $(a/d, b/d, c/d)$, where a, b, c, and d are integers that satisfy $(a/d)^2 + (b/d)^2 = (c/d)^2$ and $(1/2)(a/d)(b/d) = 1$. Or equivalently,

$$a^2 + b^2 = c^2, \qquad ab = 2d^2.$$

Fermat used the method of infinite descent: given a solution (a, b, c, d), he shows how to construct a new solution (A, B, C, D) with $0 < C < c$. Repeating, he gets a contradiction: there aren't infinite sets of decreasing positive integers.

Historical Interlude I

Infinite descent arguments are very old. Perhaps the oldest use is the classical proof that $\sqrt{2}$ isn't rational: if it was, then you could write

$$2 = \frac{a^2}{b^2} \implies 2b^2 = a^2.$$

But then a is even, so we can write $a = 2A$ and rewrite this as

$$2b^2 = (2A)^2 \implies b^2 = 2A^2.$$

Now b is even! So we can write $b = 2B$, so that

$$4B^2 = 2A^2 \implies 2B^2 = A^2.$$

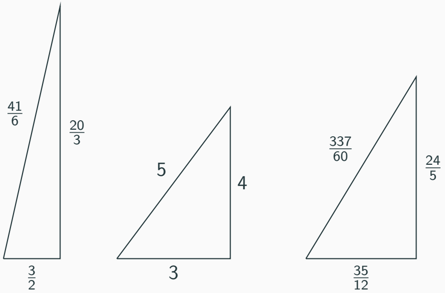
This is the same as the first equation. Repeating gives a sequence $a_1, a_2, a_3, \ldots$ of positive integers satisfying $a_1 > a_2 > a_3 > \ldots$. But that's impossible. And so $\sqrt{2}$ is irrational.

This proof (in geometric form) appeared in Euclid's elements around 300 BCE. Fermat first developed the method of infinite descent for Diophantine problems precisely to decide if 1 was congruent.

Fermat used descent to show that 1, 2, and 3 are not congruent.[1] Proofs using descent for larger integers get much, much more challenging.

We can see that 4 isn't congruent because 1 isn't congruent: if 4 were congruent, then we could scale the triangle by a factor of 1/2 and get a rational triangle with area 1. Similarly 8 and 9 aren't congruent.

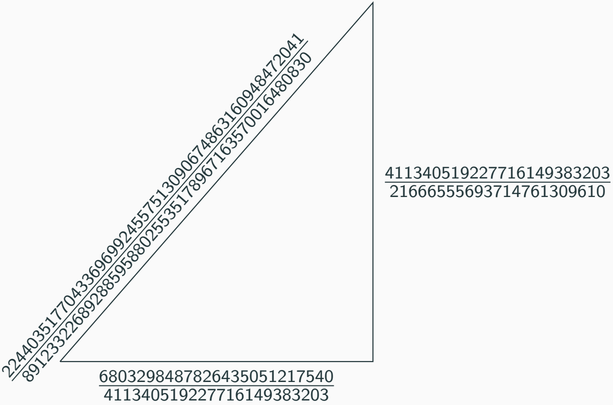
Each of $5, 6, 7$ are congruent, but finding triangles can be very hard.



[1] If you would like to see Fermat's proof that 1 isn't congruent, I would be happy to chat after my talk.

Finding triangles can be very, very hard

Sometimes, finding triangles for a number can be very, very hard. The “simplest” rational triangle with area 157 is


$\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$
$\frac{411340519227716149383203}{21666555693714761309610}$
$\frac{6803298487826435051217540}{411340519227716149383203}$

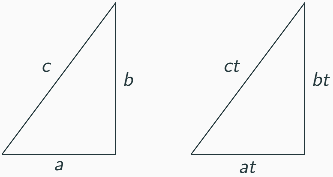
We’re going to need to develop a better approach to determine if a number is congruent.

Arithmetic Progressions of Squares

Restricting to Integers

We can simplify our search with a few observations.

If n is congruent, then nt^2 is congruent for any rational t. Why? Because we can scale the triangle by t.



For example, 6 is congruent (from the $(3, 4, 5)$ triangle), and so $24 = 6 \cdot 2^2$ is congruent (from the $(6, 8, 10)$ triangle).

Similarly, $3/2 = 6 \cdot (1/2)^2$ is congruent (from the $(3/2, 2, 5/2)$ triangle).

We can use this to restrict our attention to only the integers without losing any generality. Instead of looking for a rational triangle with area $\frac{1}{12}$, we can look for a rational triangle with area $\frac{1}{12} \cdot 4 \cdot 9 = 3$ (which Fermat showed doesn't exist).

Every rational number can be multiplied by an appropriate rational square to become an integer. Further, we can choose the integer to be squarefree (meaning that it's not divisible by any square other than 1).

This gives another definition for congruent numbers. We say an integer n is congruent if there is an integer right triangle whose area has squarefree part n.

(The squarefree part of an integer is the part that remains after dividing out by the squares. The squarefree part of $24 = 2^2 \cdot 6$ is 6).

Now we only need to look at integer-sided right triangles.

Recall that an arithmetic progression (AP) is a sequence of the form

$$a, a + d, a + 2d, a + 3d, \dots$$

where each term differs from the next term by the same amount.

There is a relationship between three term arithmetic progressions (3AP) of squares and the difference being a congruent number.

The three squares $1, 25, 49$ form a 3AP of squares with common difference 24, which corresponds to the fact that 24 (and in particular its squarefree part, 6) is congruent.

3APs and Congruent Numbers

Theorem

There is a one-to-one correspondence between right triangles with area n and 3APs of squares with common difference n.

This correspondence can is given explicitly between the sets

$$\mathrm{RightTriangles}(n) : \{(a, b, c) : a^2 + b^2 = c^2, (1/2)ab = n\}$$
$$\mathrm{3APSquares}(n) : \{[r, s, t] : s^2 - r^2 = t^2 - s^2 = n\}$$

through

$$(a, b, c) \mapsto \left[\frac{b-a}{2}, \frac{c}{2}, \frac{b+a}{2}\right], \qquad [r, s, t] \mapsto (t - r, t + r, 2s).$$

For example, the triangle $(6, 8, 10)$ corresponds to the 3AP represented by $\left[\frac{8-6}{2}, \frac{10}{2}, \frac{8+6}{2}\right] = [1, 5, 7]$, which is $1, 25, 49$.

How might we discover this?

This correspondence is perhaps easier to see starting with 3APs. If $s^2 - r^2 = n$ and $t^2 - s^2 = n$, then adding these together gives

$$t^2 - r^2 = 2n \implies (t - r)(t + r) = 2n.$$

This (loosely) suggests setting $a = (t - r)$ and $b = (t + r)$, so that $(1/2)ab = n$ and

$$a^2 + b^2 = 2(t^2 + r^2) = 2(2s^2) = (2s)^2,$$

so set $c = 2s$.

It seems this was actually discovered several times in antiquity, thousands of years ago — likely through several people playing around with number patterns.

Historical Interlude II

Both studying congruent numbers and 3APs of squares were fasionable in and around the year 1000 CE. There are Arabic manuscripts from the 10th century collecting congruent numbers.

Fibonacci was proud to discover that 7 is congruent and he stated (without proof) that 1 is not congruent.

The term "congruent number" comes from Fibonacci. In his 1225 book *Liber Quadratorum* (Book of Squares), Fibonacci called an integer n congruum if there was an integer x such that $x^2 - n, x^2, x^2 + n$ are all squares.

Congruum and congruent both come from the Latin *congruere*, which means "to meet", similar to the modern *to congregate*. Congruum slowly morphed to congruent, though this is not the same as congruent triangles or modular arithmetic congruences.

Looking for 3APs

This correspondence relates 3APs of squares to congruent numbers.

As a corollary to this correspondence (and our ability to scale triangles), the fact that 1, 2, and 3 are not congruent implies that there are no 3APs of squares whose common difference is a square, twice a square, or three times a square.

This correspondence also suggests that we might try to find 3APs of squares as a way of finding congruent numbers.

Let $\tau(n)$ denote the square indicator function,

$$\tau(n) = \begin{cases} 1 & \text{if } n = a^2 \text{ for some integer } a \\ 0 & \text{else.} \end{cases}$$

Note that $m - n, m, m + n$ is a 3AP of squares if and only if

$$\tau(m-n)\tau(m)\tau(m+n) = 1.$$

Further, $m - n, m, m + n$ is a 3AP of squares whose common difference has squarefree part t if and only if

$$\tau(m-n)\tau(m)\tau(m+n)\tau(tn) = 1.$$

For example, the $1, 25, 49$ 3AP of squares has common difference 24 (with squarefree part 6), and

$$\begin{aligned} \tau(25-24)\tau(25)\tau(25+24)\tau(6 \cdot 24) = \\ \tau(1)\tau(5^2)\tau(7^2)\tau(2^4 3^2) = 1. \end{aligned}$$

A Naive Idea to Determine if t is Congruent

We can use this observation to build a naive idea to determine if t is congruent. The sum

$$\sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \tau(m-n)\tau(m)\tau(m+n)\tau(tn)$$

will either consist entirely of 0s (if t is not congruent) or will contain infinitely many 1s and diverge (if t is congruent).

On the one hand, this is essentially the same as iterating through all triangles and hoping to find a triangle with squarefree area t.

But on the other hand, this is just the beginning of a new idea. We can't add up infinitely many numbers, but if we knew how many terms we might need to check before finding a nonzero term, we would have a finite algorithm for determining if a given number was congruent.

Our goal will be to study the size of the (finite) sums

$$S_t(X) := \sum_{m=1}^{X} \sum_{n=1}^{X} \tau(m-n)\tau(m)\tau(m+n)\tau(tn).$$

The underlying idea for this goal is similar to the major ideas from analytic number theory to count the number of primes up to a certain size.

For primes, the idea was to study the prime indicator function

$$\mathrm{IsPrime}(n) = \begin{cases} 1 & \text{if } n \text{ is prime} \\ 0 & \text{else.} \end{cases}$$

The birth of the field of analytic number theory came with the proof of the Prime Number Theorem, stating that

$$\pi(X) := \sum_{n=1}^{X} \mathrm{IsPrime}(n) \approx \frac{X}{\log X}.$$

To study these sums, we will first rearrange them into a slightly different form. First we note that we can rewrite

$$S_t(X) = \sum_{m=1}^{X} \sum_{n=1}^{X} \tau(m-n)\tau(m)\tau(m+n)\tau(tn)$$

as

$$\sum_{m=1}^{X} \sum_{n=1}^{X/t} \tau(m-tn)\tau(m)\tau(m+tn)\tau(nt^2)$$

by changing variables $n \mapsto nt$. (Changing variables in sums can be very confusing, but it's very similar to changing variables in integration). With $m \leq X$, we see that $\tau(m-tn) = 0$ for $n \geq X/t$ — so we can write the upper bound for the n sum as X. And $\tau(nt^2) = \tau(n)$, since multiplying n by a square doesn't change whether n is a square. Together we can rewrite this as

$$S_t(X) = \sum_{m=1}^{X} \sum_{n=1}^{X} \tau(m-tn)\tau(m)\tau(m+tn)\tau(n).$$

Note the $\tau(m)$ and $\tau(n)$ in

$$S_t(X) = \sum_{m=1}^{X} \sum_{n=1}^{X} \tau(m - tn)\tau(m)\tau(m + tn)\tau(n).$$

This means that only terms where m and n are squares are nonzero in the sum, so we can rewrite this as

$$S_t(X) = \sum_{m=1}^{\sqrt{X}} \sum_{n=1}^{\sqrt{X}} \tau(m^2 - tn^2)\tau(m^2 + tn^2).$$

(This is the end of the technical combinatorial portion of the talk).

This last equality is interesting, as it suggests a different relationship.

Another Correspondence

The original summands had the form $\tau(m-n)\tau(m)\tau(m+n)\tau(tn)$, which came from the correspondence between rational right triangles and 3APs of squares.

The main terms in the last sum have the form $\tau(m^2-tn^2)\tau(m^2+tn^2)$. And these reveal another, slightly different correspondence.

Theorem ([HKLDW19])

There is a one-to-one correspondence between

$\{$*Right triangles* (a,b,c)
with $a<b<c$, *squarefree area* t, *and* $\gcd(a,b,c)=1\}$
and
$\{$*coprime pairs of integers* $[m,n]$
such that both m^2-tn^2 *and* m^2+tn^2 *are squares*$\}$.

In one direction, the correspondence can be written

$$(a,b,c)\mapsto[c,\sqrt{2ab/t}].$$

This correspondence associates the right triangle (a, b, c) to the 3AP of squares $m^2 - tn^2, m^2, m^2 + tn^2$ where $[m, n] = [c, \sqrt{2ab/t}]$.

To see an example, we look to the $(3, 4, 5)$ triangle, which has squarefree area $t = 6$. This correspondence says that $[m, n] = [5, \sqrt{2 \cdot 3 \cdot 4/6}] = [5, 2]$ should give a 3AP of squares. We check that $m^2 - tn^2 = 25 - 6 \cdot 4 = 1$ and $m^2 + tn^2 = 25 + 6 \cdot 4 = 49$ are squares, and they are!

This correspondence reveals an interesting relationship: the hypotenuse of the triangle is the root of the middle square in the 3AP. The $(3, 4, 5)$ triangle has hypotenuse 5, and the middle square of the associated 3AP is 25.

We can use this to better understand $S_t(X)$.

In particular, the main advantage of this correspondence over the previous correspondence is the direct relation on the middle square (m^2) in the 3AP and the common difference (tn^2) in the 3AP.

The summand for any individual pair (m,n) will either be 0 or 1 in

$$S_t(X) = \sum_{m=1}^{\sqrt{X}} \sum_{n=1}^{\sqrt{X}} \tau(m^2 - tn^2)\tau(m^2 + tn^2).$$

The previous correspondence shows that a coprime pair (m,n) will contribute a 1 if and only if m is the hypotenuse of a primitive right triangle with squarefree part of the area equal to t. If (m,n) contributes, then (rm, rn) will also contribute for every integer multiple r.

Let $\mathcal{H}(t)$ denote the set of hypotenuses of primitive right triangles with squarefree part of the area t. Then

$$S_t(X) = \sum_{\substack{h_i \le \sqrt{X} \\ h_i \in \mathcal{H}(t)}} \sum_{r=1}^{\sqrt{X}/h_i} 1 = \sum_{\substack{h_i \le \sqrt{X} \\ h_i \in \mathcal{H}(t)}} \left\lfloor \frac{\sqrt{X}}{h_i} \right\rfloor.$$

So we should expect to need to search through about as many terms as the size of the smallest hypotenuse before we find the first triangle. . . but how large is the smallest hypotenuse?

Elliptic Curves

A Geometric Approach

Fix an area n and consider the two equations

$$a^2 + b^2 = c^2, \qquad \frac{1}{2}ab = n.$$

Each equation describes a surface in $\mathbb{R}^3$ (thinking of a, b, c as the coordinates in $\mathbb{R}^3$). Simultaneous solutions will lie on the intersection of the two surfaces, which we should heuristically expect to be a curve.

We can show that the curve will have the equation $Y^2 = X^3 - n^2X$ (with the right choice of coordinates).

Finding the Curve

To find this curve, it's better to write $c = t + a$. Then the equation $a^2 + b^2 = c^2$ can be written as

$$2at = b^2 - t^2.$$

From $\frac{1}{2}ab = n$, we see that neither a nor b is 0, and we can write $a = 2n/b$. Substituting above gives

$$\frac{4nt}{b} = b^2 - t^2.$$

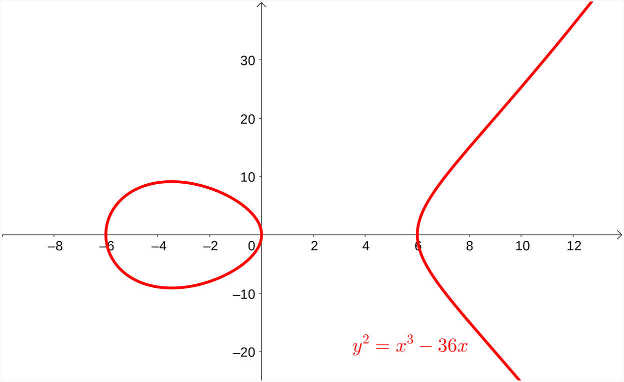
Multipliying through by bn^3/t^3 transforms this into

$$\left(\frac{2n^2}{t}\right)^2 = \left(\frac{nb}{t}\right)^3 - n^2\left(\frac{nb}{t}\right).$$

With $Y = 2n^2/t$ and $X = nb/t$, this is the curve $Y^2 = X^3 - n^2X$.

An Elliptic Curve

The curve $Y^2 = X^3 - n^2X$ is an example of something called an elliptic curve. The curve corresponding to $n = 6$ looks like



Elliptic curves are special plane curves that have many special properties that make them very well behaved.

Another Correspondence

Further, the coordinates $Y = 2n^2/t$ and $X = nb/t$ (with $c = t + a$) we identified above are yet another one-to-one correspondence in disguise, this time between right triangles and points on these curves.

Theorem

There is a one-to-one correspondence between the sets

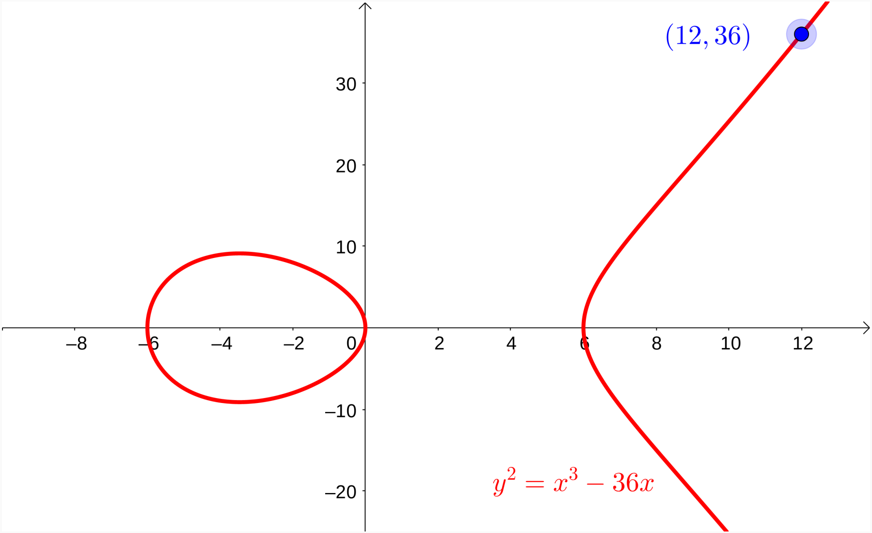
$$\mathrm{RightTriangles}(n) : \{(a, b, c) : a^2 + b^2 = c^2, (1/2)ab = n\}$$
$$\mathrm{PtsOnCurve}(n) : \{[X, Y] : Y^2 = X^3 - n^2X, Y \neq 0\}$$

The correspondence is given in one direction by

$$(a, b, c) \mapsto \left[\frac{nb}{c - a}, \frac{2n^2}{c - a}\right].$$

In this correspondence, integer right triangles correspond to rational points on the elliptic curve with nonzero Y coordinate.

Under this correspondence, the $(3, 4, 5)$ right triangle corresponds to the point $(12, 36)$ on the curve $Y^2 = X^3 - 36X$.



We have shown that the following properties of a positive integer n are equivalent.

- There is a rational right triangle with area n.
- There is an integer right triangle with squarefree part of the area equal to n.
- There is a 3AP of rational squares with common difference n.
- There is a rational solution to $Y^2 = X^3 - n^2X$ with $Y \neq 0$.

We've used the first 3 equivalences to develop a partial understanding of the sum $S_t(X)$ for understanding whether t is a congruent number. What can we expect to gain from elliptic curves? (Answer: potentially quite a bit!)

Using the Curve

One of the remarkable properties of elliptic curves is that we can define a form of "addition" on their rational points.

That is, we can define an operation $\oplus$ such that if P and Q are two rational points on an elliptic curve, then $P \oplus Q$ is another rational point on the curve. In fact, with this operation, the rational points on an elliptic curve form an Abelian group.

In particular, we can define $P \oplus Q$ as follows: the line through P and Q will intersect the curve in one additional place with coordinates (x, y). Define $P \oplus Q = (x, -y)$ — But really it's simpler if we draw a picture.

It is possible to study how the geometry of the curve interacts with the additive structure of the curve.

One of the most fundamental questions we can ask about an elliptic curve is *How many rational points are on the curve?* Or equivalently, we can ask *What does the additive structure of the curve look like?*

It turns out that the elliptic curves $Y^2 = X^3 - n^2X$ always have exactly 4 "trivial" points — i.e. points where $y = 0$ (or infinity). Sometimes (exactly when n is congruent) these curves have more points, in which case there are infinitely many points.

In particular, the additive structure of the curve will look like

$$\mathbb{Z}^r \times (\text{finite}).$$

We should think of this as saying that there are r points that sort of span the space, except for some small finite deviations coming from the trivial points. We call r the rank of the curve, and we should heuristic that high rank $\implies$ lots of points.

(For those familiar with some group theory, the structure is exactly given by $\mathbb{Z}^r \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.)

Using the Curve to Find More Triangles

Since rational points on these curves correspond to right triangles, and since we can add these points together, it is possible to find more rational points (and therefore more triangles). For example, if we compute $(12, 36) \oplus (12, 36)$ on the curve $Y^2 = X^3 - 36X$, we get the point $(25/4, -35/8)$, which corresponds to the triangle $(49, 1200, 1201)$. And we can check that the squarefree part of the area of this triangle is 6.

If we compute $(12, 36) \oplus (12, 36) \oplus (12, 36)$, we get the triangle $(2896804, 7216803, 7776485)$, which is significantly more complicated.

Aside: If this is something that interests you, I can show you how one can use a computer to compute this addition for you. On my website there is a description of how to compute this exact example in Sage.

Hypotenuses up to a Given Size

At first, we might be surprised that $(12, 36) \oplus (12, 36) \oplus (12, 26)$ seems so complex. But this is no accident. There is a general philosophy that repeatedly adding together points on elliptic curves very rapidly increases complexity. This is a major idea of the 1965 Annals paper of Néron [Nér65] (but we don't describe this fully here).

For us, the important idea is that we can use this to bound the number of hypotenuses of primitive right triangles.

Theorem ([HKLDW19])

The number of hypotenuses of primitive right triangles with squarefree part of the area equal to t and up to length X is bounded by

$$\#\{h_i \in \mathcal{H}(t) : h_i \leq X\} < c_t(\log X)^{r/2},$$

where r is the rank of the elliptic curve $y^2 = x^3 - t^2 x$.

Using this bound, one can better understand our estimate $S_t(X)$. Recall that we showed that

$$S_t(X) = \sum_{m=1}^{X} \sum_{n=1}^{X} \tau(m-n)\tau(m)\tau(m+n)\tau(tn) = \sum_{h_i \leq \sqrt{X}} \left\lfloor \frac{\sqrt{X}}{h_i} \right\rfloor.$$

Using that $|x - \lfloor x \rfloor| \leq 1$, we see that

$$\Big| S_t(X) - \sum_{h_i \leq \sqrt{X}} \frac{\sqrt{X}}{h_i} \Big| \leq \sum_{h_i \leq \sqrt{X}} 1,$$

and the sum on the right is at most a constant times $(\log X)^{r/2}$ since there are only that many hypotenuses up to size $\sqrt{X}$. Further, the sum

$$\sum_{h_i \in \mathcal{H}(t)} \frac{1}{h_i}$$

converges very rapidly to a constant C_t for the same reason — the size of the hypotenuses grows very quickly.

Main Result

Putting these together, we see the primary theorem of [HKLDW19]:

Theorem

Let $S_t(X)$ *denote*

$$S_t(X) = \sum_{m \leq X} \sum_{n \leq X} \tau(m-n)\tau(m)\tau(m+m)\tau(tn).$$

Then

$$S_t(X) = C_t\sqrt{X} + \mathrm{Error}(X),$$

where

$$\mathrm{Error}(X) \ll (\log X)^{r/2},$$

$C_t = \sum_{h_i}(h_i)^{-1}$ *is the sum of the reciprocals of the hypotenuses of primitive right triangles with squarefree part of area equal to* t*, and* r *is the rank of the elliptic curve* $y^2 = x^3 - t^2x$*.*

Million Dollar Question

This doesn't resolve the congruent number problem or the search for congruent numbers, but it does show that there are many interesting and (surprisingly) interrelated ideas in arithmetic, algebra, geometry, number theory, and analysis.

The observant among the audience might have noted that instead of searching for triangles, we could search for rational points on the elliptic curve $Y^2 = X^3 - n^2X$. But it turns out this is very hard!

Simply deciding if an elliptic curve has many rational points seems hard. There is a conjecture that gives a (somewhat complicated but still feasible) method to decide the rank of an elliptic curve. This is called the Birch–Swinnerton-Dyer Conjecture, and any who solve it will be offered a million dollars from the Clay Math Institute.

(But in fact working through elliptic curves does seem to be the best way to determine if a number is congruent or not).

Thank you very much.

Please note that these slides (and references for the cited works) are available on my website (davidlowryduda.com).

References i

Thomas A Hulse, Chan Ieong Kuan, David Lowry-Duda, and Alexander Walker.
A shifted sum for the congruent number problem.
arXiv preprint arXiv:1804.02570, 2019.

André Néron.
Quasi-fonctions et hauteurs sur les variétés abéliennes.
Annals of Mathematics, pages 249–331, 1965.