PAPER ANNOUNCEMENT: A SHIFTED SUM FOR THE CONGRUENT NUMBER PROBLEM

DAVID LOWRY-DUDA

Tom Hulse, Chan Ieong Kuan, Alex Walker, and I have just uploaded a new paper to the arXiv (at `https://arxiv.org/abs/1804.02570`) titled *A Shifted Sum for the Congruent Number Problem*. In this charming, short paper, we investigate a particular sum of terms which are products of square-indicator functions and show that its asymptotics are deeply connected to congruent numbers. This note serves to describe and provide additional context for these results.

1. Congruent Numbers

We consider some triangles. There are many right triangles, such as the triangle with sides $(3, 4, 5)$ or the triangle with sides $(1, 1, \sqrt{2})$. We call a right triangle *rational* when all its side lengths are rational numbers. For illustration, $(3, 4, 5)$ is rational, while $(1, 1, \sqrt{2})$ is not.

There is mythology surrounding rational right triangles. According to legend, the ancient Greeks, led both philosophcally and mathematically by Pythagoras (who was the first person to call himself a philosopher and essentially the first to begin to distill and codify mathematics), believed all numbers and quantities were ratios of integers (rational). When a disciple of Pythagoras named Hippasus found that the side lengths of the right triangle $(1, 1, \sqrt{2})$ were not rational multiples of each other, the other followers of Pythagoras killed him by casting him overboard while at sea for having produced an element which contradicted the gods. (It with some irony that we now attribute this as a simple consequence of the Pythagorean Theorem).

This mythology is uncertain, but what is certain is that even the ancient Greeks were interested in studying rational right triangles, and they began to investigate what we now call the Congruent Number Problem. By the year 972 the CNP appears in Arabic manuscripts in (essentially) its modern formulation. The *Congruent Number Problem* (CNP) may be the oldest unresolved math problem.

We call a positive rational number t *congruent* if there is a rational right triangle with area t. The triangle $(3, 4, 5)$ shows that $6 = 3 \cdot 4/2$ is congruent. The CNP is to describe all congruent numbers. Alternately, the CNP asks whether there is an algorithm to show definitively whether or not t is a congruent number for any t.

We can reduce the problem to a statement about integers. If the rational number $t = p/q$ is the area of a triangle with legs a and b, then the triangle aq and bq has area $tq^2 = pq$. It follows that to every rational number there is an associated squarefree integer for which either both are congruent or neither are congruent. Further, if t is congruent, then ty^2 and t/y^2 are congruent for any integer y.

We may also restrict to integer-sided triangles if we allow ourselves to look for those triangles with squarefree area t. That is, if t is the area of a triangle with

rational sides a/A and b/B, then tA^2B^2 is the area of the triangle with integer sides aB and bA.

It is in this form that we consider the CNP today.

Problem 1. *Given a squarefree integer t, does there exist a triangle with integer side lengths such that the squarefree part of the area of the triangle is t?*

We will write this description a lot, so for a triangle T we introduce the notation

$$\text{sqfree}(T) = \text{The squarefree part of the area of } T.$$

For example, the area of the triangle $T = (6, 8, 10)$ is $24 = 6 \cdot 2^2$, and so $\text{sqfree}(T) = 6$. We should expect this, as T is exactly a doubled-in-size $(3, 4, 5)$ triangle, which also corresponds to the congruent number 6. Note that this allows us to only consider primitive right triangles.

2. Main Result

Let $\tau(n)$ denote the square-indicator function. That is, $\tau(n)$ is 1 if n is a square, and is 0 otherwise. Then the main result of the paper is that the sum

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

is related to congruent numbers through the asymptotic

$$S_t(X) = C_t\sqrt{X} + O_t\Big(\log^{r/2} X\Big),$$

where

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

Each h_i is a hypotenuse of a primitive integer right triangle T with $\text{sqfree}(T) = t$. Each hypotnesue will occur in a pair of similar triangles (a, b, h_i) and (b, a, h_i); $\mathcal{H}(t)$ is the family of these triangles, choosing only one triangle from each similar pair. The exponent r in the error term is the rank of the elliptic curve

$$E_t(\mathbb{Q}) : y^2 = x^3 - t^2x.$$

What this says is that $S_t(X)$ will have a main term if and only if t is a congruent number, so that computing $S_t(X)$ for sufficiently large X will show whether t is congruent. (In fact, it's easy to show that $S_t(X) \neq 0$ if and only if t is congruent, so the added value here is the nature of the asymptotic).

We should be careful to note that this does not solve the CNP, since the error term depends in an inexplicit way on the desired number t. What this really means is that we do not have a good way of recognizing when the first nonzero term should occur in the double sum. We can only guarantee that for any t, understanding $S_t(X)$ for sufficiently large X will allow one to understand whether t is congruent or not.

3. Intuition and Methodology

There are four primary components to this result:

(1) There is a bijection between primitive integer right triangles T with $\text{sqfree}(T) = t$ and arithmetic progressions of squares $m^2 - tn^2, m^2, m^2 + tn^2$ (where each term is itself a square).

(2) There is a bijection between primitive integer right triangles T with $\text{sqfree}(T) = t$ and points on the elliptic curve $E_t(\mathbb{Q}) : y^2 = x^3 - tx$ with $y \neq 0$.
(3) If the triangle T corresponds to a point P on the curve E_t, then the size of the hypotenuse of T can be bounded below by $H(P)$, the (naive) height of the point on the elliptic curve.
(4) Néron (and perhaps Mordell, but I'm not quite fluent in the initial history of the theory of elliptic curves) proved strong (upper) bounds on the number of points on an elliptic curve up to a given height. (In fact, they proved asymptotics which are much stronger than we use).

In this paper, we use (1) to relate triangles T to the sum $S_t(X)$ and we use (2) to relate these triangles to points on the elliptic curve. Tracking the exact nature of the hypotenuses through these bijections allows us to relate the sum to certain points on elliptic curves. In order to facilitate the tracking of these hypotenuses, we phrase these bijections in slightly different ways than have appeared in the literature. By (3) and (4), we can bound the number and size of the hypotenuses which appear in terms of numbers of points on the elliptic curve up to a certain height. Intuitively this is why the higher the rank of the elliptic curve (corresponding roughly to the existence of many more points on the curve), the worse the error term in our asymptotic.

I would further conjecture that the error term in our asymptotic is essentially best-possible, even though we have thrown away some information in our proof.

4. Additional Context

We are not the first to note either the bijection between triangles T and arithmetic progressions of squares or between triangles T and points on a particular elliptic curve. The first is surely an ancient observation, but I don't know who first considered the relation to elliptic curves. But it's certain that this was a fundamental aspect in Tunnell's famous work *A Classical Diophantine Problem and Modular Forms of Weight 3/2* from 1983, where he used the properties of the elliptic curve E_t to relate the CNP to the Birch and Swinnerton-Dyer Conjecture.

One statement following from the Birch and Swinnerton-Dyer conjecture (BSD) is that if an elliptic curve E has rank r, then the L-function $L(s, E)$ has a zero of order r at 1. The relation between lots of points on the curve and the existence of a zero is intuitive from the approximate relation that

$$L(1, E) \approx \lim_X \prod_{p \leq X} \frac{p}{\#E(\mathbb{F}_p)},$$

so if E has lots and lots of points then we should expect the multiplicands to be very small.

On the other hand, the elliptic curve $E_t : y^2 = x^3 - t^2x$ has the interesting property that any point with $y \neq 0$ generates a free group of points on the curve. From the bijections alluded to above, a primitive right integer triangle T with $\text{sqfree}(T) = t$ corresponds to a point on E_t with $y \neq 0$, and thus guarantees that there are lots of points on the curve. Tunnell showed that what I described as "lots of points" is actually enough points that $L(1, E)$ must be zero (assuming the relation between the rank of the curve and the value of $L(1, E)$ from BSD).

Tunnell proved that if BSD is true, then $L(1, E) = 0$ if and only if n is a congruent number.

Yet for any elliptic curve we know how to compute $L(1, E)$ to guaranteed accuracy (for instance by using Dokchitser's algorithm). Thus a corollary of Tunnell's theorem is that BSD implies that there is an algorithm which can be used to determine definitively whether or not any particular integer t is congruent.

This is the state of the art on the congruent number problem. Unfortunately, BSD (or even the somewhat weaker between BSD and mere nonzero rank of elliptic curves as is necessary for Tunnell's result for the CNP) is quite far from being proven.

In this context, the main result of this paper is not as effective at actually determining whether a number is congruent or not. But it does have the benefit of not relying on any unknown conjecture.

And there is some potential follow-up questions. The sum $S_t(X)$ appears as an integral transform of the multiple Dirichlet series

$$\sum_{m,n} \frac{\tau(m-n)\tau(m)\tau(nt)\tau(m+n)}{m^s n^w} \approx \sum_{m,n} \frac{r_1(m-n)r_1(m)r_1(nt)r_1(m+n)}{m^s n^w},$$

where $r_1(n)$ is 1 if $n = 0$ or 2 if n is a positive square, and 0 otherwise. Then $r_1(n)$ appears as the Fourier coefficients of the half-integral weight standard theta function

$$\theta(z) = \sum_{n \in \mathbb{Z}} e^{2\pi i n^2 z} = \sum_{n \geq 0} r_1(n) e^{2\pi i n z},$$

and $S_t(X)$ is a shifted convolution sum coming from some products of modular forms related to $\theta(z)$.

It may be possible to gain further understanding of the behavior of $S_t(X)$ (and therefore the congruent number problem) by studying the shifted convolution as coming from theta functions.

I would guess that there is a deep relation to Tunnell's analysis in his 1983 paper, as in some sense he constructs appropriate products of three theta functions and uses them centrally in his proof. But I do not understand this relationship well enough yet to know whether it is possible to deepen our understanding of the CNP, BSD, or Tunnell's proof. That is something to explore in the future.