A GENERALIZATION OF THE CONGRUENT NUMBER PROBLEM

LARRY ROLEN

Abstract. We study a certain generalization of the classical Congruent Number Problem. Specifically, we study integer areas of rational triangles with an arbitrary fixed angle θ. These numbers are called θ-congruent. We give an elliptic curve criterion for determining whether a given integer n is θ-congruent. We then consider the "density" of integers n which are θ-congruent, as well as the related problem giving the "density" of angles θ for which a fixed n is congruent. Assuming the Shafarevich-Tate conjecture, we prove that both proportions are at least 50% in the limit. To obtain our result we use the recently proven p-parity conjecture due to Monsky and the Dokchitsers as well as a theorem of Helfgott on average root numbers in algebraic families.

1. Introduction and Statement of Results

The study of right triangles with integer side lengths dates back to the work of Pythagoras and Euclid, and the ancients completely classified such triangles. Another problem involving triangles with "nice" side lengths was first studied systematically by the Arab mathematicians of the 10^{th} Century. This problem asks for a classification of all possible areas of right triangles with rational side lengths. A positive integer n is *congruent* if it is the area of a right triangle with all rational side lengths. In other words, there exist rational numbers a, b, c satisfying

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

The problem of classifying congruent numbers reduces to the cases where n is square-free. We can scale areas trivially. We can easily generate examples of congruent numbers; for example 6 is congruent and is given by the $3 - 4 - 5$ triangle. Classically, people were able to solve this problem in a few cases using examples and elementary techniques. For example, Fermat proved that 1 is not a congruent number and Euler was the first to find a triangle showing that 7 is. Given an arbitrary integer, however, it traditionally seemed hopeless to find a simple, general algorithm to test for congruency. To demonstrate the potential complexity of finding such triangles in general, consider the following example, due to Zagier. He computed the "simplest" right triangle representing 157 as congruent.

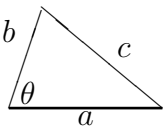
The author is an undergraduate at the University of Wisconsin majoring in mathematics. He is grateful for the support provided by the NSF Research Training Grant in Number Theory (PI: Ono). He would also like to thank Ken Ono for his guidance and support. He also thanks David Brown for providing comments on an earlier draft of this paper.

In this triangle, the hypotenuse is given by $\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$. For more on the history of the congruent number problem see [4].

The natural way to view this problem is in terms of rational points on elliptic curves. Namely, to every n we associate a corresponding elliptic curve E_n whose Mordell-Weil group encodes the data of rational right triangles of area n. For each square-free positive integer n, we define the congruent number curve $E_n : \ y^2 = x^2 - n^2x$. There is a $2-1$ correspondence between rational right triangles of area n and rational points (x, y) on E_n with $y \neq 0$. Now E_n clearly has full 2-torsion as it contains the points $\mathcal{O}, (0, 0), (-n, 0), \text{and } (n, 0)$. It turns out that these are all of the torsion points; i.e $E_n^{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. As a corollary, n is congruent if and only if $\text{rank}_{\mathbb{Q}} E_n > 0$. Using this characterization along with the Hasse-Weil L-function and theory of half-integral weight modular forms, Tunnell was able to derive the a remarkable classification of congruent numbers. Assuming the weak Birch and Swinnerton-Dyer (BSD) conjecture, he gives an equivalent condition for a number n to be congruent in terms of the number of representations of n by two quadratic forms; this condition may be checked as quickly as in time $O(n^{\frac{1}{2}})$ (for example, see [1][15].)

We would like to consider a natural generalization of the congruent number problem. Namely, we will relax the condition that the triangle have a right angle and consider more general angles. In analogy with the previous definition, let $\frac{\pi}{3} \leq \theta \leq \pi$ be an angle. We say that a square-free integer n is θ-*congruent* if there exists a triangle whose largest angle is θ, whose side lengths are rational, and whose area is n. In other words, there exist rational a, b, c for which

$$a^2 + b^2 - 2ab\cos\theta = c^2 \quad \frac{ab\sin\theta}{2} = n \iff$$



We say that an angle $\pi/3 \leq \theta \leq \pi$ is *admissible* if both $\sin\theta$ and $\cos\theta$ lie in $\mathbb{Q}$. Following the classical parameterization of rational points on the unit circle, define m to be the slope of the line joining $(-1, 0)$ to $(\cos\theta, \sin\theta)$. Call a rational number m *admissible* if it corresponds to an admissible angle. Note that $m = 1$ corresponds to $\theta = \pi/2$. Then the rational points on the circle are in one-to-one correspondence with rational choices of m. It is easy to derive the formulae:

$$\cos\theta = \frac{1 - m^2}{1 + m^2} \quad \sin\theta = \frac{2m}{1 + m^2}.$$

Henceforth the dependence of m on θ will be implicit. Thus, for every such rational $m > \frac{\sqrt{3}}{3}$ we have a separate congruent number problem, with $m = 1$ corresponding to the classical congruent number problem. We are almost in position to give an elliptic curve criterion for the generalized congruent number problem. First we introduce some language which pertains to the special case of certain angles. We say that an admissible $m \in \mathbb{Q}$ is *aberrant* provided that $m^2 + 1 \in \mathbb{Q}^2$. Otherwise, an admissible m is called

generic. We can parameterize all aberrant m as follows. Begin with the parameterization of Pythagorean triples of Euclid which states that any primitive triple is of the form $(u^2 - v^2, 2uv, u^2 + v^2)$ for relatively prime (u, v). It easily follows that all aberrant m can be written in the form $\left(\frac{u^2-v^2}{2uv}\right)^{\pm 1}$ for relatively prime integers u, v.

To each aberrant m, we can associate a (unique) square-free natural number n such that $nm \in \mathbb{Q}^2$ and we call the pair (n, m) aberrant as well. Any other pair is termed generic. To any admissible pair (n, m) we associate the elliptic curve E_{n,θ_m} given by the following Weierstrass equation:

$$E_{n,\theta_m} : \; y^2 = x\left(x - \frac{n}{m}\right)(x + nm)\,. \tag{1}$$

Using this equation it is more "natural" to parameterize angles by the rational m than an angle θ_m. For example, there is a duality between m and $\frac{1}{m}$ in the aberrant case which is much less transparent in the θ-characterization. There are two special properties characterizing aberrant numbers which prompt their name. Note that there are no congruent equilateral triangles. The following two theorems give the first example of the special aberrant behavior as well as our first example of a situation which cannot occur in the classical congruent number case (as $\sqrt{2}$ is irrational):

Theorem 1.1. *If (n, m) is aberrant, then n is a θ_m-congruent number and n can be represented by an isosceles θ_m-triangle.*

In fact, we can give a characterization of all isosceles triangles appearing in the generalized congruent number problem.

Theorem 1.2. *All isosceles triangles with rational side lengths and areas correspond to the aberrant case.*

One property of generalized congruent number case which remains the same as the $\theta = \frac{\pi}{2}$ case is the following correspondence which translates our problem into one of computing Mordell-Weil groups.

Theorem 1.3. *For any positive square-free integer n and any admissible angle θ we have that n is θ-congruent if and only if E_{n,θ_m} has a rational point (x, y) with $y \neq 0$. Moreover, if (n, m) is generic there is a 2-1 correspondence of triangles representing the pair (n, m) and such points on E_{n,θ_m}. In fact, (x, y) and (x', y') correspond to the same triangle if and only if $x = x'$ and $y = \pm y'$.*

In order to use the elliptic curve efficiently in our study we must first compute the torsion subgroup of E_{n,θ_m}. This will allow us to give the desired equivalent condition in terms of Mordell-Weil ranks. We prove the following classification:

Theorem 1.4. *If (n, m) is aberrant, then $E^{\text{tors}}_{n,\theta_m}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. If (n, m) is generic, then $E^{\text{tors}}_{n,\theta_m}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Corollary 1.5. We have that (n, m) is a congruent pair if and only if (n, m) is aberrant or $\operatorname{rank}_{\mathbb{Q}} E_{n,\theta_m}(\mathbb{Q}) > 0$.

In this paper, we would like to analyze a different aspect of the problem from that considered by Tunnell. Although it remains a difficult problem to determine general conditions to test for congruent numbers (even parts of the classical congruent number problem resolution remain conjectural), we are still able to make general statements about the "distribution" of such points. There are two natural families to consider along with the following questions.

Question 1. If we fix m and let the area n vary, how often is (n, m) congruent?

Question 2. If we fix the area n and let m vary, how often is (n, m) congruent?

For each area n, there is at least one angle making n a θ_m-congruent number. To see this, note that $(\frac{-n+2}{2}, \frac{n^2-4}{4})$ is a rational point on $E_{n,\frac{n-2}{4}}$ with non-zero y-coordinate unless $n = 2$. For $n = 2$, $(9/2, 15)$ is a rational point on $E_{2,4}$ so 2 is 4-congruent. A natural question is if for each n there are infinitely many angles which make n congruent. Even better, we would like to say as much as we can pertaining to approximately how often numbers are congruent or not. To this end, we let $h_m(x)$ be the proportion of positive square-free integers n not exceeding x for which (n, m) is a congruent pair and $v_n(x)$ the proportion of m with height at most x for which (n, m) is a congruent pair. More precisely,

$$h_m(x) := \frac{\#\{1 \leq n \leq x, : \ n \text{ is } \theta_m\text{-congruent and } n \text{ is square-free}\}}{\#\{1 \leq n \leq x \ : \ n \text{ is square-free}\}} \tag{2}$$

$$v_n(x) := \frac{\#\{m \in \mathbb{Q} \ : \ h(m) \leq n \text{ and } n \text{ is } \theta_m\text{-congruent}\}}{\#\{m \in \mathbb{Q} \ : \ h(m) \leq n\}} \tag{3}$$

where for any rational number written in lowest terms $h(\frac{a}{b}) := \max\{|a|, |b|\}$. Then we prove the following:

Theorem 1.6. *Suppose the Shafarevich-Tate conjecture is true for all elliptic curves of rank 0. Then for each $\epsilon > 0$, if $x \gg_\epsilon 0$ then $\frac{1}{2} - \epsilon \leq h_m(x) < 1 - \epsilon$*

That is, when we fix the angle m and let the area n vary, at least $1/2$ of the choices for n are congruent and a positive density are non-congruent. Fixing n and letting m vary, we also obtain the following:

Theorem 1.7. *Suppose the Shafarevich-Tate conjecture is true for all elliptic curves of rank 0. Then for each $\epsilon > 0$, if $x \gg_\epsilon 0$ then $\frac{1}{2} - \epsilon \leq v_n(x) \leq 1 - \epsilon$.*

The paper is organized as follows. In §2 we will prove Theorems 1.1-1.5, establishing the equivalent condition for congruence in terms of ranks of elliptic curves. In §3, we prove the density results Theorem 1.6 and Theorem 1.7. These rely on a theorem of Yu for quadratic twists giving the upper bound in Theorem 1.7 and a remarkable new

result of the Dokchitser brothers which proves the p-parity conjecture in the case when p is odd (the case where $p = 2$ being previously solved by Monsky) in conjunction with a paper of Helfgott providing sufficient conditions for algebraic families of elliptic curves to have average root number zero [16],[5],[8],[11].

2. Proof of the Elliptic Curve Criterion and Computation of Torsion Subgroups for E_{n,θ_m}.

In this section, we prove the theorems necessary to reduce the generalized congruent number problem to one of computing the rank of $E_{n,\theta}$. We begin by establishing the connection between $E_{n,\theta}(\mathbb{Q})$ and congruent numbers.

2.1. **Connecting E_{n,θ_m} to θ_m-Congruent Numbers.** We begin with a proof of Theorem 1.1. Suppose (n, m) is aberrant. Then as nm is a square, so is $\frac{n}{m}$. It is simple to check that the triangle with side lengths $a = b = \sqrt{\frac{n(m^2+1)}{m}},\ c = 2\sqrt{\frac{n}{m}}$ has angle θ_m and area n.

To finish the characterization of isosceles congruent number triangles in Theorem 1.2, suppose that $a = b$. By the law of cosines

$$c^2 = 2a^2 - 2a^2\frac{m^2-1}{m^2+1} = 4a^2\left(\frac{1}{m^2+1}\right).$$

We can write $m^2 + 1 = (\frac{2a}{c})^2$. Now by the area formula we can rewrite $\frac{n}{m} = \frac{a^2}{1+m^2}$, establishing the aberrance of (n, m).

We proceed to establish the elliptic curve condition in the generic case as per Theorem 1.3. Thus, suppose n is θ_m-congruent. Then define $(x, y) := (\frac{c^2}{4}, \frac{b^2c-a^2c}{8})$. In the generic case, the triangle cannot be isosceles by Theorem 1.2 and hence $a \neq b$ giving $y \neq 0$. It is trivial to verify that this point indeed lies on E_{n,θ_m}.

Conversely, given a rational point (x, y) with non-zero y coordinate, define a triangle with side lengths

$$a = \left|\frac{n(\frac{x}{m} + xm)}{y}\right|,\ b = \left|\frac{(x+nm)(x-nm)}{y}\right|,\ c = \left|\frac{x^2+n^2}{y}\right|.$$

Note that if (n, m) is an aberrant pair, then by Theorem 1.4 the torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. This is aberrant by Theorem 1.1 and evidently contains a torsion point with $y \neq 0$, proving Theorem 1.3.

2.2. **Computing the Torsion Subgroups.** In this section we compute the torsion subgroup of

$$E_{n,\theta_m} : y^2 = x(x - \frac{n}{m})(x + nm) = x^3 + \frac{n(m^2-1)}{m}x^2 - n^2x.$$

First choose $0 \neq \alpha \in \mathbb{Z}$ such that α^2nm, α^2nm^3 are both integral. Then by the change of variables $(x, y) \mapsto ((\alpha m)^{-2}x, (\alpha m)^{-3}y)$ this curve is isomorphic (over $\mathbb{Q}$) to $y^2 =$

$x^3 + \alpha^2 nm(m^2-1)x^2 - \alpha^4 m^4 n^2 x$. If we define $M := nm^3\alpha^2$ and $N := -nm\alpha^2$, we can write the curve in the form $y^2 = x^3 + (M+N)x^2 + MNx$ with M and N integral. Now there is a complete characterization of torsion subgroups of curves of this form in [12]. Note that they all have full 2-torsion, so by Mazur's Theorem the torsion subgroup is of the form $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $n \in \{1,2,3,4\}$.

Theorem 2.1. *(Ono [12]). The following criteria uniquely determine the torsion subgroups of $E(M,N): \ y^2 = x^3 + (M+N)x^2 + MNx$.*

- *$E(M,N)^{\text{tors}}$ contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ if M and N are both squares, or $-M$ and $N-M$ are both squares or $-N$ and $M-N$ are both squares.*
- *$E(M,N)^{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ if there exists a non-zero integer d such that $M = d^2u^4$ and $N = d^2v^4$, or $M = -d^2v^4$ and $N = d^2(u^4 - v^4)$, or $M = d^2(u^4 - v^4)$ and $N = -d^2v^4$ where (u,v,w) forms a Pythagorean triple (i.e. $u^2 + v^2 = w^2$).*
- *$E(M,N)^{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ if there exist integers a, b such that $\frac{a}{b} \notin \{-2, -1, -\frac{1}{2}, 0, 1\}$ and $M = a^4 + 2a^3b$ and $N = 2ab^3 + b^4$.*
- *Otherwise, $E(M,N)^{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

We continue by checking the conditions outlined there. To check if the torsion subgroup contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, note first that neither N nor $-M$ can be a square as both n, m are positive. Thus, the torsion subgroup will have a 4-torsion point if and only if $-N = nm\alpha^2$ and $M - N = \alpha^2 nm(m^2+1)$ are both squares. This is clearly equivalent to the aberrant condition. Thus, in the generic case, there can be no 4-torsion.

Let us rule out the possibility of 8-torsion. Suppose the torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Then again by sign considerations neither N nor $-M$ are squares and so this happens if and only if we can write $M = d^2(u^4 - v^4)$ and $N = -d^2v^4$ for a non-zero integer d and a Pythagorean triple (u,v,w). In this case, we have $\frac{M}{N} = -m^2 = \frac{v^4 - u^4}{v^4} = 1 - (\frac{u}{v})^4$ and so $1 + m^2$ is a rational fourth power. I claim that this is not possible. For suppose $1 + (\frac{c}{d})^2 = (\frac{e}{f})^4$ with c, d, e, f integral. Then $(f^2c)^2 + (f^2d)^2 = (e^2d)^2$ and so $f^4c^2 = d^2(e^4 - f^4)$. But this forces $e^4 - f^4$ to be a perfect square g^2 and hence gives a Pythagorean triple (g, f^2, e^2), which is impossible as it is well-known that a Pythagorean triple can contain at most one square (as was shown by Fermat).

To finish the characterization of the torsion subgroups, we have only to exlude the possibility $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Suppose we have a, b as in the Theorem. In this case, if we have $\frac{M}{N} = -\frac{a^2}{b^2}\frac{a^2+2ab}{b^2+2ab} = -m^2$ and so we can write $\frac{a^2+2ab}{b^2+2ab} = \frac{c^2}{d^2}$ for $c, d \in \mathbb{Z}$. By rearranging and considering this as a quadratic equation in the variable a, by the quadratic formula the discriminant must be integral and this gives that $c^4 + d^4 - c^2d^2$ must be a perfect square. This is a special case of a well-studied class of equations. In particular, Diophantine equations of the form $x^4 + nx^2y^2 + y^4 = z^2$ have been studied intensely for over 300 years. Fermat's proof that there are no nontrivial integral solutions when $n = 0$ is a classic example of infinite descent, and when $n = -1$ this equation is central to the well-known proof that four perfect squares cannot lie in arithmetic progression. The only integral solutions occur when $cd = 0$ or $c^2 = d^2$. An elementary proof of this

fact may be found in [13]. Then if $cd = 0$, $d \neq 0$ and so $c = 0$ giving $m = 0$, which is a contradiction. In the latter case, we also have that $a^2 = b^2$ and so $m^2 = 1$ giving $m = 1$. But the case $m = 1$ was already proven to have no 3-torsion in Lemma 1, being the classical congruent number case.

3. Proof of Density Results

In this section we prove Theorems 1.7 and 1.8 describing the average behavior of congruent numbers in one-parameter families. This will be done by computing averages of root numbers and using the parity conjecture.

3.1. **A Sufficient Condition for Lower Bounds.** In order to describe the proof, we first need to discuss a famous conjecture on the parity of ranks of elliptic curves. Let us recall that every elliptic curve has an associated Hasse-Weil L-function which provides the connection to modular forms in the Modularity Theorem of Wiles, Taylor, et. al and whose value at $s = 1$ conjecturally (BSD) gives the rank of E. For each prime p, let $N(p)$ be the number of points (including the point at infinity) of the reduced curve E_p. Then set $a(p) := p + 1 - N(p)$. Finally, define the L-series by the Euler product:

$$L(E, s) := \sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{p|\Delta} \frac{1}{1 - a(p)p^{-s}} \prod_{p\nmid\Delta} \frac{1}{1 - a(p)p^{-s} + p^{1-2s}},$$

where Δ denotes the minimal discriminant of E. This L-function can be analytically continued to an entire function, as proven by Wiles et al. It also has a special symmetry which is expressed in the *functional equation*:

$$N_E^{\frac{2-s}{2}} (2\pi)^{s-2} \Gamma(2 - s) L(E, 2 - s) = W(E) N_E^{\frac{s}{2}} (2\pi)^{-s} \Gamma(s) L(E, s).$$

Here N_E is the conductor of E and $W(E) = \pm 1$ is the root number of E. It is expected that the root number controls the parity of the rank of E. Specifically, the following is also an immediate consequence of BSD:

Conjecture. (Parity) For any elliptic curve $E/\mathbb{Q}$, $W(E) = (-1)^{rk_{\mathbb{Q}}(E)}$

In certain cases, the parity conjecture may be shown to be true unconditionally. In particular, a powerful new result of Doskchitser proving the p-parity conjecture has the following corollary:

Theorem 3.1. *(Corollary 4.20 of Dokchitser* [5]*) If $E/\mathbb{Q}$ is an elliptic curve, either the parity conjecture is true for E or $Ш(E/\mathbb{Q})$ contains a copy of $\mathbb{Q}/\mathbb{Z}$.*

Here $Ш(E/\mathbb{Q})$ is the group of homogenous spaces for $E/\mathbb{Q}$ which have a solution in every completion of $\mathbb{Q}$ modulo equivalence. Together with the *Selmer group* it measures how badly the Hasse principle fails for E (i.e. the inability to lift solutions over every completion to a solution over the global field). As a corollary to Theorem 3.1, we now state our sufficient condition for the density lower bounds in Theorems 1.6 and 1.7.

Theorem 3.2. *If a family of elliptic curves over $\mathbb{Q}$ has average root number 0 and the Shafarevich-Tate Conjecture is true for elliptic curves of rank 0, then the proportion of rank 0 curves in this family is at most $\frac{1}{2}$.*

Proof. If $Ш(E)/\mathbb{Q}$ is finite and $\text{rank}(E(\mathbb{Q}))$ is zero, then E will have positive root number by the previous theorem. Given that the average root number is zero, the total proportion of positive root number curves is $\frac{1}{2}$ and so the proportion of rank 0 curves cannot exceed this amount. □

3.2. **Proof of Theorem 1.6.** We are now in position to prove the bounds on the proportion of quadratic twists with positive rank stated in Theorem 1.6. For the lower bound, we recall the well-known fact that the average root number in families of quadratic twists is 0. For the upper bound, we apply a theorem of Yu. This is proven by computing the average 2-Selmer group size. The result follows from the Dokchitsers' result and the proof of the p-parity conjecture for the case $p = 2$ [11].

Theorem 3.3. *(Yu* [16]*) Let $E/\mathbb{Q}$ be an elliptic curve with torsion subgroup containing $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then a positive proportion of quadratic twists have rank 0.*

By Theorem 1.4, our curves always satisfy this condition as $(m, 1)$ is never aberrant by the parameterization of all aberrant pairs stated in the introduction.

3.3. **Proof of Theorem 1.7.** To prove the lower bound on the proportion of positive-rank curves in the family of curves obtained by fixing the area n, we need a more general theorem describing average root numbers in elliptic fibrations. Although in our case the following conjectures will hold unconditionally, let us state the following hypotheses which relate to classical arithmetic conjectures.

Hypothesis. ($\mathcal{A}$) Let $P(x, y)$ be a homogenous polynomial. Then only for a zero proportion of all pairs of coprime integers (x, y) do we have a prime $p > \max\{x, y\}$ such that $p^2 | P(x, y)$.

It is believed that this is true for all such square-free P. In particular, this is implied by the *abc*-conjecture [7]. Fortunately in our case, it has been proven unconditionally true whenever P has no irreducible factor of degree exceeding 6 [10]. Another hypothesis we will need is:

Hypothesis. ($\mathcal{B}$) Let $\lambda(n) := \prod_{p|n} (-1)^{\nu_p(n)}$ be the Liouville function. Then $\lambda(P(x, y))$ has strong zero average over $\mathbb{Z}^2$.

Chowla has conjectured that this holds for all non-constant, square-free homogenous polynomials P [2]. The prime number theorem is essentially equivalent to the case where $\deg(P) = 1$, and it has been proven unconditionally whenever $\deg(P) = 1, 2, 3$ [9].

Now if we have an elliptic curve $\mathcal{E}$ over $\mathbb{Q}(t)$, we can form two polynomials formed by a product over the places of bad reduction based on type:

$$M_{\mathcal{E}} := \prod_{\mathcal{E} \text{ has mult. red. at } \nu} P_\nu \quad , \quad B_{\mathcal{E}} := \prod_{\mathcal{E} \text{ has q. bad red. at } \nu} P_\nu.$$

Here $P_\nu := y$ if ν is the infinite place and otherwise $P_\nu := y^{\deg(Q)} Q(\frac{x}{y})$ for the irreducible polynomial Q inducing ν. We also say a curve has *quite bad* (q. bad) reduction at a place if every quadratic twist also has bad reduction at the same place. We are ready to state the sufficient conditions for computing our average of root numbers:

Theorem 3.4. *(Helfgott [8]) Let $\mathcal{E}$ be an elliptic curve over $\mathbb{Q}(t)$. Suppose $M_{\mathcal{E}} \neq 1$ (i.e. $\mathcal{E}$ has a point of multiplicative reduction). Suppose further that Hypothesis $\mathcal{A}$ holds for $B_{\mathcal{E}}$ and Hypothesis $\mathcal{B}$ holds for $M_{\mathcal{E}}$. Then the strong average over $\mathbb{Q}$ of $W(E_t)$ of the fibres exists and is* 0.

Let us observe how this applies to our case. Our family of elliptic curves with m varying is an elliptic curve over $\mathbb{Q}(t)$ with $t = m$. First we calculate the usual constants associated to this curve:

$$c_4 = \frac{16n^2(m^2 - m + 1)(m^2 + m + 1))}{m^2}, \quad c_6 = \frac{-32n^3(m-1)(m+1)(m^2+2)(2m^2+1)}{m^3}$$

$$\Delta = \frac{16n^6(m^2+1)^2}{m^2}$$

Thus, the curve has bad reduction at three places: $\{\infty, m, m^2 + 1\}$. By checking the valuation criteria for reduction type, we find that $M_{\mathcal{E}} = x^2 + y^2$ and $B_{\mathcal{E}} = xy(x^2 + y^2)$. From the above remarks, the required hypothesis on $M_{\mathcal{E}}$, $B_{\mathcal{E}}$ hold unconditionally and so Helfgott's theorem applies to show the strong average of root numbers is zero. The exact statement of what strong average means is complicated, but it is a certain notion of average which does not depend on which intervals in $\mathbb{Q}$ we sample or how we add terms (a precise definition may be found in Helfgott). In particular it is clearly a strict enough notion to give us the conditions we need to apply our Lemma and conclude the truth of Theorem 1.7.

3.4. **Discussion of Conjectural Densities.** Although we are only able to bound the densities as in Theorems 1.6 and 1.7, in fact much more is believed to be true. For example, we have the following well-known hypothesis

Conjecture. (Goldfeld [6]) For any family of quadratic twists, the proportion of curves with rank 0 is 50% and the proportion of curves with rank 1 is 50%. All higher ranks occur only with density 0.

In particular, for any family of quadratic twists and any other "reasonable" family of curves such as the second family with the area n fixed and the angle m varying, it is believed that a similar heuristic should hold. In particular, we make the following:

Conjecture 1. *For each positive, square-free integer n, (n, m) is not a congruent pair for a positive proportion of angles m.*

For the family of curves we are considering, the generic rank is 0. The following is a plausible conjecture:

Conjecture 2. *(Density). Let $\mathcal{E}$ be an elliptic curve over $\mathbb{Q}(t)$ and generic rank n. Then only a zero proportion of fibers have rank at least $n + 2$.*

We also say that a curve has *elevated rank* if only finitely many fibers have generic rank. Thus, our conjecture implies that the family of curves does not have elevated rank. For suitably manipulated families, the rank has been shown to be elevated (see [3] for a discussion of known methods for constructing examples). All such proofs rely heavily on the fact that these families are isotrivial, meaning that the j-invariant $j(\mathcal{E}) \in \mathbb{Q}$ does not depend on t. It is believed no non-isotrivial families can have elevated rank. In particular an arithmetic conjecture known as the *square-free*-conjecture implies that the average root number of a non-isotrivial family is not ± 1 [3]. Thus, our conjecture would follow from the square-free and density conjectures (assuming the parity conjecture for rank 0 curves). If the full parity conjecture is further assumed, there would be no non-isotrivial families of elevated rank over $\mathbb{Q}$.

We also note that, assuming the parity conjecture is true for rank 1 curves, the conjecture would follow if we could bound the average rank strictly by $\frac{3}{2}$. If this could be shown it would constitute the first example of a non-quadratic twist elliptic fibration which is known to have average rank not exceeding $\frac{3}{2}$. We can say, assuming a few conjectures such as BSD and the Generalized Riemann Hypothesis, that a Theorem of Silverman tells us that the average rank is no larger than $\frac{5}{2}$ [14]. Thus, although the conjecture is almost certainly true, a powerful new theorem would be required to say this with certainty. We conclude with a small table of data illustrating the plausibility of the conjecture as computed in Sage.

TABLE 1. Ranks for $m = 1, 2, \ldots, 100$

	rank=0	1	2	3
n=1	51	42	6	1
n=2	53	40	7	0
n=3	40	53	7	0
n=5	37	55	8	0
n=6	38	56	6	0

REFERENCES

[1] E. Bach and N. Ryan. *Efficient Verification of Tunnell's Criterion.* Japan J. Indust. Appl. Math., Volume 24, Number 3 (2007), 229-239.

[2] S. Chowla. *The Riemann Hypothesis and Hilbert's Tenth Problem.* Mathematics and its Applications, Vol. 4 Gordon and Breach Science Publishers, New York-London-Paris, 1965.

[3] B. Conrad, K. Conrad, and H. Helfgott. *Root Numbers and Ranks in Positive Characteristic*. Adv. Math., **198** (2005), pp. 684-731.
[4] L.E. Dickson. *History of the Theory of Numbers*. Volume II, Chapter XVI, Dover Publications.
[5] T. Dokchitser and V. Dokchitser. *On the Birch-Swinnerton-Dyer quotients modulo squares*. Annals of Math. 172 no. 1 (2010), 567-596.
[6] D. Goldfeld. *Conjectures on elliptic curves over quadratic fields*. Number Theory, Carbondale, 1979.
[7] A. Granville. *ABC allows us to count squarefrees.*. Inernat. Math. Res. Notices, **1998**, 991-1009.
[8] H. Helfgott. *On the Behaviour of Root Numbers in Families of Elliptic Curves*. preprint, arxiv.org:math.NT/040814.
[9] H. Helfgott. *The Parity Problem for Irreducible Cubic Forms*. preprint, arxiv.org:math/0501177v1.
[10] H. Helfgott. *On the square-free sieve*. Acta Arithmetica, **115** (2004) pp. 349-402.
[11] P. Monsky, Generalizing the Birch-Stephens theorem. I: Modular curves, Math. Z., 221 (1996),.415-420.
[12] K. Ono. *Euler's Concordant Forms*. Acta Arithmetica **65**, 1996, pp. 101-123.
[13] H. C. Pocklington. *Some Diophantine Impossibilities*. Proc. Camb. Phil. Soc., **17** (1914), 110-118.
[14] J. Silverman. *The average rank of an algebraic family of elliptic curves*. J. Reine Agnew. Math. **504** (1988), 227-236.
[15] J. Tunnell. *A classical Diophantine problem and modular forms of weight 3/2*. Inventiones Mathematicae, 1983. **72** (2): 323Ð334
[16] G. Yu. *Rank 0 Quadratic Twists of a Family of Elliptic Curves*. Compositio Mathematica, Volume 135, Number 3, 331-356 (2003).

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: lrolen@wisc.edu