A Natural Generalization of the Congruent Number Problem

Larry Rolen

Emory University

The Classical Congruent Number Problem

Definition

We say that a square-free, positive integer n is <u>*congruent*</u> *if it is the area of some right triangle with rational side lengths.*

The Classical Congruent Number Problem

Definition

We say that a square-free, positive integer n is <u>congruent</u> if it is the area of some right triangle with rational side lengths.

- For example, 6 is a congruent number as it is the area of a $3-4-5$ triangle.

The Classical Congruent Number Problem

Definition

We say that a square-free, positive integer n is congruent if it is the area of some right triangle with rational side lengths.

- For example, 6 is a congruent number as it is the area of a $3-4-5$ triangle.
- Classical techniques solved the problem for $n = 1, 2, 3, 5, 6, 7$.

Is 157 congruent?

- This is not so simple.

Is 157 congruent?

- This is not so simple.
- In fact 157 is congruent, and Zagier computed the hypotenuse of the "simplest" triangle with area 157 as

$$\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

Tunnell's Theorem

Theorem (Tunnell 1983)

For a given integer n, define

$$A_n := \#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 32z^2\},$$

$$B_n := \#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 8z^2\},$$

$$C_n := \#\{x, y, z \in \mathbb{Z} | n = 8x^2 + 2y^2 + y64z^2\},$$

$$D_n := \#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 16z^2\}.$$

Tunnell's Theorem

Theorem (Tunnell 1983)

For a given integer n, define

$$A_n := \#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 32z^2\},$$

$$B_n := \#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 8z^2\},$$

$$C_n := \#\{x, y, z \in \mathbb{Z} | n = 8x^2 + 2y^2 + y64z^2\},$$

$$D_n := \#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 16z^2\}.$$

Suppose n is congruent. If n is even, then $2A_n = B_n$*, and if n is odd then* $2C_n = D_n$*. The converse is also true if we assume BSD.*

A Natural Generalization

Definition

Let $\frac{\pi}{3} \leq \theta \leq \pi$ be an angle. We say that a square-free integer n is <u>*θ-congruent*</u> *if there exists a triangle whose largest angle is θ, whose side lengths are rational, and whose area is n.*

A Natural Generalization

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.

Definition

We say that an angle $\pi/3 \leq \theta \leq \pi$ is admissible if both $\sin\theta$ and $\cos\theta$ lie in $\mathbb{Q}$.

A Natural Generalization

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.

Definition

We say that an angle $\pi/3 \leq \theta \leq \pi$ is admissible if both $\sin\theta$ and $\cos\theta$ lie in $\mathbb{Q}$.

- Admissible angles are parameterized by rational $m > \frac{\sqrt{3}}{3}$ by the formulae

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

Aberrant and Generic Angles

- It is more natural to use the m parameter in the equations; note that $m = 1$ corresponds to the classical congruent number problem.

Aberrant and Generic Angles

- It is more natural to use the m parameter in the equations; note that $m = 1$ corresponds to the classical congruent number problem.

Definition

We say that an admissible $m \in \mathbb{Q}$ is aberrant is $m^2 + 1 \in \mathbb{Q}^2$. Otherwise we say m is generic.

Aberrant and Generic Angles

- It is more natural to use the m parameter in the equations; note that $m = 1$ corresponds to the classical congruent number problem.

Definition

We say that an admissible $m \in \mathbb{Q}$ is aberrant is $m^2 + 1 \in \mathbb{Q}^2$. Otherwise we say m is generic.

- The aberrant m are parameterized by relatively prime u, v as

$$m = \left(\frac{u^2 - v^2}{2uv}\right)^{\pm 1}.$$

Aberrant and Generic Angles

- It is more natural to use the m parameter in the equations; note that $m = 1$ corresponds to the classical congruent number problem.

Definition

We say that an admissible $m \in \mathbb{Q}$ is aberrant is $m^2 + 1 \in \mathbb{Q}^2$. Otherwise we say m is generic.

- The aberrant m are parameterized by relatively prime u, v as

$$m = \left(\frac{u^2 - v^2}{2uv}\right)^{\pm 1}.$$

- For each aberrant m there is a unique square-free n with $nm \in \mathbb{Q}^2$. We call this pair (n, m) aberrant.

Ellitpic Curve Criterion and the Aberrant Case

Definition

To any admissible pair (n, m) we associate the elliptic curve

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

Ellitpic Curve Criterion and the Aberrant Case

Definition

To any admissible pair (n, m) we associate the elliptic curve

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

Theorem (R 2010)

If (n, m) is aberrant, then n is θ_m-congruent and can be represented by an isosceles triangle. Furthermore, all isosceles triangles with rational side lengths correspond to the aberrant case.

An Ellitptic Curve Criterion

Theorem (R 2010)

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 $y \neq 0$.

An Ellitptic Curve Criterion

Theorem (R 2010)

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 $y \neq 0$.

- The proof is elementary and essentially the same as the proof in the classical congruent number case when $m = 1$.

Structure of Torsion Subgroups

Theorem (R 2010)

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 $E^{\text{tors}}_{n,\theta_m}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Structure of Torsion Subgroups

Theorem (R 2010)

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

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

Proof of the Torsion Subgroup Result

Theorem (Ono)

Let $E(M,N): \ y^2 = x^3 + (M+N)x^2 + MNx$ *for* $M, N \in \mathbb{Z}$.

- $E(M,N)^{\text{tors}}$ *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,* $E(M,N)^{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Examples

- We remark that one can prove Tunnell-style criteria for some specific angles. We would like to address a different problem.

More General Problems

Question

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

More General Problems

Question

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

Question

If we fix the n and let the angle m vary, how often is (n, m) congruent?

More General Problems

Question

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

Question

If we fix the n and let the angle m vary, how often is (n, m) congruent?

- To this end, let

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

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

Density Results

Theorem (R 2010)

Suppose that $\text{Ш}(E/\mathbb{Q})$ *is finite for all elliptic curves of rank 0. Then for each* $\epsilon > 0$, *if* $x \gg_\epsilon 0$ *then* $\frac{1}{2} - \epsilon \leq h_m(x) < 1 - \epsilon$

Density Results

Theorem (R 2010)

Suppose that $\text{Ш}(E/\mathbb{Q})$ *is finite for all elliptic curves of rank 0. Then for each* $\epsilon > 0$*, if* $x \gg_{\epsilon} 0$ *then* $\frac{1}{2} - \epsilon \leq h_m(x) < 1 - \epsilon$

Theorem (R 2010)

Suppose that $\text{Ш}(E/\mathbb{Q})$ *is finite for all elliptic curves of rank 0. Then for each* $\epsilon > 0$*, if* $x \gg_{\epsilon} 0$ *then* $\frac{1}{2} - \epsilon \leq v_n(x) \leq 1 - \epsilon$.

Proof of Density Results

Conjecture (Parity)

Let E be an elliptic curve over $\mathbb{Q}$ and $W(E)$ the root number (i.e. the sign of the functional equation). Then $W(E) = (-1)^{\mathrm{rk}_{\mathbb{Q}}(E)}$.

Proof of Density Results

Conjecture (Parity)

Let E be an elliptic curve over $\mathbb{Q}$ and $W(E)$ the root number (i.e. the sign of the functional equation). Then $W(E) = (-1)^{\mathrm{rk}_{\mathbb{Q}}(E)}$.

Theorem (Dokchitser and Dokchitser 2010)

For every elliptic curve $E/\mathbb{Q}$, either the Parity Conjecture is true for E or $Ш(E/\mathbb{Q})$ contains a copy of $\mathbb{Q}/\mathbb{Z}$. In particular, the Shafarevich-Tate Conjecture implies the Parity Conjecture.

Proof of Density Results

Conjecture (Parity)

Let E be an elliptic curve over $\mathbb{Q}$ and $W(E)$ the root number (i.e. the sign of the functional equation). Then $W(E) = (-1)^{\mathrm{rk}_{\mathbb{Q}}(E)}$.

Theorem (Dokchitser and Dokchitser 2010)

For every elliptic curve $E/\mathbb{Q}$, either the Parity Conjecture is true for E or $Ш(E/\mathbb{Q})$ contains a copy of $\mathbb{Q}/\mathbb{Z}$. In particular, the Shafarevich-Tate Conjecture implies the Parity Conjecture.

Lemma

Assuming the Parity Conjecture, any family of elliptic curves over $\mathbb{Q}$ with average root number 0 consists of at most 50% rank 0 curves.

Proof of Density Results for a Fixed Angle

- If the angle is fixed, the family is a family of quadratic twists.

Proof of Density Results for a Fixed Angle

- If the angle is fixed, the family is a family of quadratic twists.
- It is well-known that a family of quadratic twists has average root number 0.

Proof of Density Results for a Fixed Angle

- If the angle is fixed, the family is a family of quadratic twists.
- It is well-known that a family of quadratic twists has average root number 0.

Theorem (Gang Yu)

If $E/\mathbb{Q}$ has full 2-torsion, then a positive proportion of quadratic twists of E have rank 0.

A Theorem of Helfgott

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 $p^2 | P(x, y)$.

A Theorem of Helfgott

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 $p^2 | P(x, y)$.

- The *abc*-Conjecture implies this is true for all square-free P.

A Theorem of Helfgott

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 $p^2 | P(x, y)$.

- The *abc*-Conjecture implies this is true for all square-free P.
- It has been proven when $\deg(f) \leq 6$ for all irreducible factors.

A Theorem of Helfgott

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 $p^2 | P(x, y)$.

- The *abc*-Conjecture implies this is true for all square-free P.
- It has been proven when $\deg(f) \leq 6$ for all irreducible factors.

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 $\mathbb{Z}^2$.

A Theorem of Helfgott

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 $p^2 | P(x, y)$.

- The *abc*-Conjecture implies this is true for all square-free P.
- It has been proven when $\deg(f) \leq 6$ for all irreducible factors.

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 $\mathbb{Z}^2$.

- This has been proven unconditionally for $\deg(P) = 1, 2, 3$.

Helfgott's Result

- Let

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

Helfgott's Result

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

Helfgott's Result

- Let
$$M_{\mathcal{E}} := \prod_{\mathcal{E} \text{ has mult. red. at } \nu} P_\nu \quad , \quad B_{\mathcal{E}} := \prod_{\mathcal{E} \text{ has q. bad red. at } \nu} P_\nu .$$
- 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 say a curve has quite bad (q. bad) reduction at a place if every quadratic twist also has bad reduction at the same place.

Helfgott's Result

- Let

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

- 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 say a curve has quite bad (q. bad) reduction at a place if every quadratic twist also has bad reduction at the same place.

Theorem (Helfgott)

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.

Proof of Density Results for Fixed Area

- In our case, the relevant constants are

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

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

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

Proof of Density Results for Fixed Area

- In our case, the relevant constants are

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

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

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

- We find that $M_{\mathcal{E}} = x^2 + y^2$ and $B_{\mathcal{E}} = xy(x^2 + y^2)$.

Proof of Density Results for Fixed Area

- In our case, the relevant constants are

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

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

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

- We find that $M_{\mathcal{E}} = x^2 + y^2$ and $B_{\mathcal{E}} = xy(x^2 + y^2)$.
- Both hypotheses are unconditional for these polynomials, so the average root number is unconditionally zero.

Conjectures on Rank 0 Twists

Conjecture (Goldfeld)

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%.

Conjectures on Rank 0 Twists

Conjecture (Goldfeld)

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%.

Theorem (Ono-Skinner)

If $E/\mathbb{Q}$ is an elliptic curve, then

$$\#\{|D| \leq X \ : \ \mathrm{rk}(E(D)) = 0\} \gg_E \frac{X}{\log X}.$$

Conjectures on Rank 0 Twists

Conjecture (Goldfeld)

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%.

Theorem (Ono-Skinner)

If $E/\mathbb{Q}$ is an elliptic curve, then

$$\#\{|D| \leq X \ : \ \mathrm{rk}(E(D)) = 0\} \gg_E \frac{X}{\log X}.$$

Conjecture (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 $n+2$.

Conjectural Density of Non-congruent pairs

Conjecture (R)

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

Conjectural Density of Non-congruent pairs

Conjecture (R)

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

Table: Ranks for $m = 1, 2, \ldots, 100$

	rank=0	1	2	≥ 3
n=1	48	46	6	0
n=2	50	45	5	0
n=3	43	50	7	0
n=4	46	48	6	0
n=5	38	49	13	0

Conclusion

- For each positive rational $m > \frac{\sqrt{3}}{3}$ we have a generalization of the congruent number problem.

Conclusion

- For each positive rational $m > \frac{\sqrt{3}}{3}$ we have a generalization of the congruent number problem.
- A similar elliptic curve criterion holds in general as in the classical case.

Conclusion

- For each positive rational $m > \frac{\sqrt{3}}{3}$ we have a generalization of the congruent number problem.
- A similar elliptic curve criterion holds in general as in the classical case.
- We computed the torsion subgroups for each curve.

Conclusion

- For each positive rational $m > \frac{\sqrt{3}}{3}$ we have a generalization of the congruent number problem.
- A similar elliptic curve criterion holds in general as in the classical case.
- We computed the torsion subgroups for each curve.
- Assuming the finiteness of $\text{Ш}(E/\mathbb{Q})$, we proved a density result on the number of congruent numbers when the angle or the area is fixed.