The Congruent Number Problem

Pizza Seminar

March 16, 2018

The Pythagorean Theorem

We know the sides of a right triangle must satisfy the equation

$$x^2 + y^2 = z^2.$$

The integer solutions to this equation are of the form

$$(x, y, z) = (q^2 - p^2, 2qp, q^2 + p^2), \qquad q > p$$

This can be found by finding rational points on the unit circle $x^2 + y^2 = 1$.

The Pythagorean Theorem

Question

Given a right triangle with rational sides, what is its area?

The integer solutions to $x^2 + y^2 = z^2$ are of the form

$$(x, y, z) = (q^2 - p^2, 2qp, q^2 + p^2), \qquad q > p,$$

so...

Answer

Up to a rational square factor, it's an integer of the form $qp(q^2 - p^2)$.

We can also ask ourselves the converse.

Hard Problem

Question (Congruent Number Problem)

Up to a rational square factor, which positive integers can be written as

$$qp(q^2 - p^2)$$

with p and q positive integers?

We can rephrased this in plain English.

Question (Congruent Number Problem, Rephrased)

Which positive integers are the area of a right triangle with rational sides?

Observation

Here are the first few congruent numbers.

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

Proposition

Positive integers of the form n^2 and $2n^2$ cannot be congruent numbers.

(Keyphrase: Infinite descent.)

Examples

The integer 5 is a congruent number. The simplest triangle giving area 5 has sides

$$x = \frac{3}{2},$$
$$y = \frac{20}{3},$$
$$z = \frac{41}{6}.$$

Examples

The integer 6 is a congruent number. The simplest triangle giving area 6 has sides

$$x = 3,$$
$$y = 4,$$
$$z = 5.$$

Examples

The integer 7 is a congruent number. The simplest triangle giving area 7 has sides

$$x = \frac{24}{5},$$
$$y = \frac{35}{12},$$
$$z = \frac{337}{60}.$$

Examples

The integer 30 is a congruent number. The simplest triangle giving area 30 has sides

$$x = 5,$$
$$y = 12,$$
$$z = 13.$$

Examples

The integer 157 is a congruent number. The simplest triangle giving area 157 has sides

$$x = \frac{6803298487826435051217540}{411340519227716149383203},$$
$$y = \frac{411340519227716149383203}{21666555693714761309610},$$
$$z = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

What is Known: Test for Noncongruence

Theorem (Tunnell)

Let N be a square-free congruent number.

- *If N is odd, then*

$$\#\{(x,y,z) \in \mathbb{Z}^3 : N = 2x^2 + y^2 + 32z^2\}$$
$$= \frac{1}{2}\#\{(x,y,z) \in \mathbb{Z}^3 : N = 2x^2 + y^2 + 8z^2\}.$$

- *If N is even, then*

$$\#\left\{(x,y,z) \in \mathbb{Z}^3 : \frac{N}{2} = 4x^2 + y^2 + 32z^2\right\}$$
$$= \frac{1}{2}\#\left\{(x,y,z) \in \mathbb{Z}^3 : \frac{N}{2} = 4x^2 + y^2 + 8z^2\right\}.$$

Furthermore, if the Birch and Swinnerton-Dyer Conjecture is true, then the converse of the above statement holds as well.

(Keyphrase: Modular forms.)

Birch and Swinnerton-Dyer Conjecture:

$$\mathrm{ord}_{s=1} L(E, s) = \mathrm{rank}\, E(\mathbb{Q}).$$

(Here E is an elliptic curve.)

What is Known: Test for Noncongruence

Theorem (Iskra, et al.)

Let p_k, q_k denote primes congruent to k modulo 8. The following are not congruent numbers:

- p_3, $2p_5$, $p_3 q_3$, $2p_5 q_5$,
- $2p_1 p_5$ *provided* $\left(\frac{p_1}{p_5}\right) = -1$.
- $p_3^{(1)} p_3^{(2)} \cdots p_3^{(t)}$ *provided* $\left(\frac{p_3^{(m)}}{p_3^{(n)}}\right) = -1$ *for* $m < n$.

(Keyphrase: 2-Descent.)

What is Known: Test for Congruence

Theorem (Monsky, et al.)

Let p_k, q_k denote primes congruent to k modulo 8. The following are all congruent numbers:

- p_5, p_7, $2p_7$, $2p_3$,
- p_3p_5, p_3p_7, $2p_3p_5$, $2p_5p_7$,
- p_1p_5 *provided* $\left(\frac{p_1}{p_5}\right) = -1$,
- $2p_1p_3$ *provided* $\left(\frac{p_1}{p_3}\right) = -1$,
- p_1p_7, $2p_1p_7$ *provided* $\left(\frac{p_1}{p_7}\right) = -1$.

(Keyphrase: "Mock" Heegner points.)

What is Known: Test for Congruence

Theorem (Tian)

For any given nonnegative integer k, there are infinitely many square-free congruent numbers with exactly $k+1$ odd prime divisors in each residue class of 5, 6, 7 modulo 8.

(Keyphrase: Heegner points.)

Goal of the Talk

Try to explain how (some of) the known results for the Congruent Number Problem are derived.

Translation of Problem

For a squarefree positive integer N, we will consider the elliptic curve E_N defined by $y^2 = x^3 - N^2x$. It has a natural abelian group structure.

Theorem (Mordell-Weil)

$E_N(\mathbb{Q}) \cong \mathbb{Z}^r \oplus (\textit{torsion points})$ *for some finite* $r \geq 0$.

- It can be shown that the torsion part of $E_N(\mathbb{Q})$ is

$$\{(0,0),(N,0),(-N,0),\infty\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

  via Dirichlet's theorem on primes in arithmetic progression. Consequently, all nontorsion points of $E_N(\mathbb{Q})$ have nonzero y-coordinate.
- N is a congruent number if and only if $r > 0$.
- E_N has complex multiplication by $\mathbb{Z}[i]$.

The BSD Conjecture for E_N

One the one hand, the theory of complex multiplication tells us that

$$\begin{aligned} L(E_N, s) &= L(s, \psi_{E_N/\mathbb{Q}[i]}) \\ &= \prod_{\substack{p \nmid 2N \\ p \equiv 3 \pmod 4}} \frac{1}{1-(-p)p^{-2s}} \prod_{\substack{p \nmid 2N \\ p \equiv 1 \pmod 4 \\ p = \pi\overline{\pi}}} \frac{1}{1-\overline{\left(\frac{D}{\pi}\right)_4}\pi p^{-s}} \end{aligned}$$

On the other hand, one shows directly that modularity holds for E_N by showing that the coefficients of $L(E_N, s)$ are the Fourier coefficients of a (twisted) newform f_N of weight 2 and level 32, and satisfies

$$L(E_N, s) = L(f_N, s).$$

It is well-known that the right hand side has an analytic continuation to the entire complex plane. The BSD conjecture predicts that the order of vanishing of $L(E_N, s)$ at $s = 1$ equals the rank r of E_N. In fact, Waldspruger has indirectly computed $L(E_N, 1)$, and Tunnell's theorem is a specialization of Waldspruger's computation to f_N.

A sketch of Tunnell's Theorem

Tunnell used the classical Jacobi theta function

$$g = q \prod_{\mathbb{Z}_{\geq 1}} (1 - q^{8n})(1 - q^{16n}) = \sum_{\mathbb{Z}\times\mathbb{Z}} (-1)^n q^{(4m+1)^2 + 8n^2}$$

and the classial theta functions

$$\theta_2 = \sum_{\mathbb{Z}} q^{2n^2}, \qquad \theta_3 = \sum_{\mathbb{Z}} q^{4n^2}$$

to define $a(n)$ and $b(n)$ by

$$g\theta_2 = \sum a(n) q^n, \qquad g\theta_4 = \sum b(n) q^n.$$

By piecing together many results of Waldspurger, he deduced that

$$L(E_N, 1) = a(N)^2 \beta \frac{N^{-1/2}}{4}, \qquad L(E_{2N}, 1) = b(N)^2 \beta \frac{(2N)^{-1/2}}{2}.$$

where β is the real period of E_1. He then applied the classical theorem of Coates and Wiles to get the characterization of congruent numbers.

Method of 2-Descent

Define

$$E_N : y^2 = x^3 - N^2 x, \qquad \widehat{E_N} : y^2 = x^3 + 4N^2 x.$$

Theorem (2-Descent for E_N)

One has the equality

$$2^{r+2} = |\alpha(E_N(\mathbb{Q}))||\widehat{\alpha}(\widehat{E_N}(\mathbb{Q}))|,$$

where $\alpha(E_N(\mathbb{Q}))$ is the set of classes modulo squares of 1, and of b_1 and $(-N^2)/b_1$ for all squarefree divisors b_1 of b such that $|b_1| \leq |-N^2|^{1/2}$, and such that there is an integral solution to

$$Y^2 = b_1 X^4 + \frac{(-N^2)}{b_1} Z^4$$

with $XZ \neq 0$ and $\gcd(X, Z) = 1$. A similar characterization holds for $\widehat{\alpha}(\widehat{E_N}(\mathbb{Q}))$.

A Messier Example After The p_3 case

To show $p_1 q_5$ with $\left(\frac{p_1}{q_5}\right) = -1$ and $p_5 q_5$ aren't congruent numbers, write

$$E_N : y^2 = x^3 - 4p^2q^2x, \qquad \widehat{E_N} : y^2 = x^3 + 16p^2q^2x.$$

Then

$$1 \subset \alpha(E_N(\mathbb{Q})) \subset \{\pm1, \pm2, \pm p, \pm q, \pm pq, \pm 2p, \pm 2q, \pm 2pq\},$$

$$1 \subset \widehat{\alpha}(\widehat{E_N}(\mathbb{Q})) \subset \{1, 2, p, q, pq, 2p, 2q, 2pq\}.$$

Equation	Solution If
$Y^2 = \pm(2X^2 - 2p^2q^2Z^4)$	$p, q \equiv 1, 3, 7 \pmod 8$
$Y^2 = \pm(pX^2 - 4pq^2Z^4)$	$\left(\frac{\pm p}{q}\right) = 1 = \left(\frac{\pm 2q}{p}\right)$
$Y^2 = \pm(pqX^2 - 4pqZ^4)$	$p, q \equiv 1, 3, 7 \pmod 8$
$Y^2 = \pm(2pX^2 - 2pq^2Z^4)$	$\left(\frac{q}{p}\right) = 1 = \left(\frac{2p}{q}\right)$
$Y^2 = \pm(2X^2 + 8p^2q^2Z^4)$	None
$Y^2 = \pm(pX^2 + 16pq^2Z^4)$	$p \equiv 1 \pmod 8$ and $\left(\frac{\pm p}{q}\right) = 1$
$Y^2 = \pm(pqX^2 + 16pqZ^4)$	$p, q \equiv 1 \pmod 8$
$Y^2 = \pm(2pX^2 + 8pq^2Z^4)$	None
$Y^2 = \pm(2pqX^2 + 8pqZ^4)$	None

Demonstrating Method of Heegner Points on p_5

Let $K = \mathbb{Q}(\sqrt{-2p_5})$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2p_5}]$. We let:

- H be the maximal abelian unramified extension (i.e. Hilbert class field) of K.
- $\mathcal{A}$ be an element in the class group $Cl(K)$,
- $\sigma_{\mathcal{A}} \in \text{Gal}(H/K)$ be the element identified with $\mathcal{A} \in Cl(K)$ under class field theory,
- G be the subgroup of $Cl(K)$ with $\sigma_{\mathcal{A}}$ fixing $\sqrt{p_5}$, which is odd by old results of Gauss,
- C be the completion of the curve $y^2 = x^4 + 1$, which is isomorphic to E_1,
- $\Lambda \cong E_N(\mathbb{Q})$ be the subgroup of $C(\mathbb{Q}[\sqrt{p_5}])$ consisting of points which are transformed into their negatives by involution,
- $S = \sum_{\mathcal{A} \in G} P_{\mathcal{A}}$, where $P_{\mathcal{A}}$ are the so-called "Heegner points".

Then the name of the game is to use formal properies of $P_{\mathcal{A}}$ to show that $2S \in \Lambda$, but $2S$ is not a torsion point on C. This shows the existence of a nontorsion point on E_N.

References

- Henri Cohen, *Number Theory Volume I: Tools and Diophantine Equations*, Springer, 2007.
- Henryk Iwaniec, *Topics in Classical Automorphic Forms*, American Mathematical Society, 1997.
- Farzali Izadi and Hamid Reza Azdolmaleki, *On the rank of congruent elliptic curves*, arXiv:1701.02686.
- Paul Monsky, *Mock Heegner points and congruent numbers*, Mathematische Zeitschrift **204** (1990), 45–67.
- Goro Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1968.
- Goro Shimura, *On modular forms of half-integral weight*, Annals of Mathematics **97** (1973), 440–481.
- Joseph Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.
- Joseph Silverman and John Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Math, 1992.
- Ye Tian, *Congruent numbers and Heegner points*, Cambridge Journal of Mathematics **2** (2014), 117–161.
- Jerrold Tunnell, *A classical Diophantine problem and modular forms of weight 3/2*, Inventiones Mathematicae **72** (1983), 323–334.

Appendix to Page 17 of the Slides

1 The group law on elliptic curves

We will always let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{Q}$. (We ignore the problem of singularity for a moment.) The homogenized version of E in projective space is $y^2z = x^3 + axz^2 + bz^3$, with $[0 : 1 : 0]$ acting as the point at infinity. We will use the nonhomogeneous and homogeneous definitions of E interchangeably throughout the appendix. Here are two important definitions.

Definition 1. $E(\mathbb{Q})$ is the set of *rational points* of E, i.e. the set of solutions (x, y) of E with $x, y \in \mathbb{Q}$.

Definition 2. Let $F = y^2z - x^3 - axz^2 - bz^3$ be the equation defining an elliptic curve E. It is said to be *singular at* $p = (x_0, y_0, z_0)$ if $F(p) = 0$ and all the partial derivatives of F vanish at p. If there are no singular points on E, then E is said to be *nonsingular*.

We do not concern ourselves with the types of singularities, but we do need the notion of good reduction.

Definition 3. Let E be a nonsingular elliptic curve $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. It is said to have *good reduction at prime* p if, writing E_p to be E viewed over $\mathbb{Z}/p\mathbb{Z}$, the curve E_p is still nonsingular. For such an E_p, we write $E_p(\mathbb{F}_p)$ with the analogous meaning as in definition 1.

The most important thing about elliptic curves is that there is a group law on it (which works, in particular, over $\mathbb{Q}$ and finite fields). The picture of this group law is the usual one, and I will write down the algebraic equations one can deduce.

Definition 4. Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be two points on $E = \{(x, y) \in \overline{\mathbb{Q}}^2 : y^2 = x^3 + ax + b\}$. Define λ and ν by

$$\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} & \text{if } x_P \neq x_Q, \\ \dfrac{3x_P^2 + a}{2y_P} & \text{if } x_P = x_Q, \end{cases} \qquad \nu = \begin{cases} \dfrac{y_P x_Q - y_Q x_P}{x_Q - x_P} & \text{if } x_P \neq x_Q, \\ \dfrac{-x_P^3 + ax_1 + 2b}{2y_P} & \text{if } x_P = x_Q. \end{cases}$$

Then $P + Q$ has coordinates (x, y) with

$$x := \lambda^2 - x_P - x_Q, \qquad y := -\lambda x - \nu.$$

One can easily check that the algebraic definition for group law makes E into an abelian group, and in fact descends to a group operation on $E(\mathbb{Q})$. Hence we can now ask what $E(\mathbb{Q})$ looks like as a $\mathbb{Z}$-module.

Theorem 5 (Mordell-Weil). *$E(\mathbb{Q})$ is a finitely generated abelian group.*

Thus, by the fundamental theorem of finitely generated $\mathbb{Z}$-modules, the Mordell-Weil theorem implies that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tor},$$

where r is called the *algebraic rank* of E, and $E(\mathbb{Q})_{tor}$ is called the *torsion group* of E. In fact, there are only finitely many possibilities for the torsion group due to a famous theorem of Barry Mazur.

Theorem 6 (Mazur). *$E(\mathbb{Q})_{tor}$ is isomorphic to one of the following groups:*

- $\mathbb{Z}/m\mathbb{Z}$ *with* $m \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$,
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$ *with* $m \in \{1, 2, 3, 4\}$.

There is no such classification for the algebraic rank, and in fact it is very hard to compute it for elliptic curves. The *Birch and Swinnerton-Dyer conjecture* predicts that the algebraic rank can be computed by evaluating the order of vanishing of the Hasse-Weil L-function associated to E at $s = 1$.

Before ending this section, let us note the following computational result.

Theorem 7. *Let E be a nonsingular elliptic curve $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$. If $(x, y) \in E(\mathbb{Q})$ is a torsion point, then it must satisfy the following two conditions.*

- *$x, y \in \mathbb{Z}$.*
- *Either $P + P = 0$, or y^2 divides $4A^3 + 27B^2$ (the discriminant of E).*

The above result is sometimes useful to compute torsion points of an explicitly defined elliptic curve, but certainly will not work with the general family $y^2 = x^3 - N^2x$ that we deal with in section 3.

Example 8. The elliptic curve E defined by $y^2 = x^3 - 43x + 166$ has discriminant $2^{15} \cdot 13$. Thus any nonzero torsion points in $E(\mathbb{Q})$ has y-coordinate in the set

$$\{\pm1, \pm2, \pm4, \pm8, \pm16, \pm32, \pm64, \pm128\},$$

and a computation tells us that the nonzero torsion points in $E(\mathbb{Q})$ are

$$\{(3, \pm8), (-5, \pm16), (11, \pm32)\}.$$

One can check that $E(\mathbb{Q})_{tor} \cong \mathbb{Z}/7\mathbb{Z}$.

2 Somehow these two results come into play later

In this section we record two well-known results that will be used in the next section. The first can be proven easily, while the second is proven using a classic argument of Dirichlet by showing that certain Dirichlet L-functions $L(\chi, s)$ are nonzero at $s = 1$.

Euler's Criterion. *Let p be an odd prime and let a be an integer coprime to p. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Dirichlet's Theorem on Arithmetic Progressions. *Let $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$. The arithmetic progression $\{a + kb : k \in \mathbb{Z}_{\geq 1}\}$ contains infinitely many primes.*

3 The torsion points of $y^2 = x^3 - N^2x$

In this section, E_N will denote the nonsingular elliptic curve $y^2 = x^3 - N^2x$ for a fixed positive squarefree integer N. Our aim is to prove the following result.

Theorem 9. *$E_N(\mathbb{Q})_{tor} = \{[0 : 1 : 0], [0 : 0 : 1], [N : 0 : 1], [-N : 0 : 1]\}$ for a positive squarefree integer N.*

Hence $E_N(\mathbb{Q})_{tor} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, as one can easily check. In what follows, given any prime p, we let $E_{N,p}$ to be the elliptic curve E_N viewed over $\mathbb{Z}/p\mathbb{Z}$.

Lemma 10. *Let p be a prime number.*

(a) $[x_1 : y_1 : z_1]$ and $[x_2 : y_2 : z_2]$ defines the same point in $\mathbb{P}^2_{\mathbb{F}_p}$ if and only if p divides all of $x_1y_2 - x_2y_1$, $x_1z_2 - x_2z_1$ and $y_1z_2 - y_2z_1$.

(b) $E_{N,p}$ has good reduction at prime p if and only if p does not divide $2N$.

(c) The only 2-torsion points in $E_{N,p}(\mathbb{F}_p)$ are $[0 : 1 : 0]$, $[0 : 0 : 1]$, $[N : 0 : 1]$ and $[-N : 0 : 1]$.

Proof. Three easy computations, and left to the reader. □

Lemma 11. *Let p be an odd prime with p not dividing $2N$ and $p \equiv 3 \pmod{4}$. Then $\#E_{N,p}(\mathbb{F}_p) = p + 1$.*

Proof. Let $(x,y) \in E_{N,p}(\mathbb{F}_p)$, and assume $(x,y) \notin \{[0:1:0],[0:0:1],[N:0:1],[-N:0:1]\}$ so that $x \neq 0, \pm N$. We need to show that there are $p-3$ such (x,y). Pair off the $p-3$ numbers in $\mathbb{Z}/p\mathbb{Z}\setminus\{0,\pm N\}$ as pairs $\{\alpha,-\alpha\}$ of cardinality two, and let $f(\alpha)=\alpha^3-N^2\alpha$. Notice that $f(\alpha)$ is an odd function, and by Euler's Criterion,

$$\left(\frac{-f(x)}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{f(x)}{p}\right)=-\left(\frac{f(x)}{p}\right).$$

Hence $f(x)$ is a quadratic residue modulo p if and only if $-f(x)$ is not a quadratic residue modulo p. Thus, every such pair $\{\alpha,-\alpha\}\neq\{0\},\{-N,N\}$ in $\mathbb{Z}/p\mathbb{Z}$ admits exactly two points of $E_{N,p}$ among the four possibilities $\left\{\left(x,\pm\sqrt{f(x)}\right),\left(-x,\pm\sqrt{f(x)}\right)\right\}$. One concludes that there are $p-3$ more points on $E_{N,p}(\mathbb{F}_p)$ other than $[0:1:0]$, $[0:0:1]$, $[N:0:1]$ or $[-N:0:1]$. □

These two Lemmas allows us to prove Theorem 9.

Proof of Theorem 9. Suppose for a contradiction that $E_N(\mathbb{Q})_{tor}$ contains a point $\mathfrak{P}$ other than $[0:1:0]$, $[0:0:1]$, $[N:0:1]$ or $[-N:0:1]$. Then $\mathfrak{P}$ must have order greater than two by an easy application of Lemma 10(c) to suitable primes p, and easy elementary group theory tells us that $E_N(\mathbb{Q})_{tor}$ either has a subgroup S of odd order, or of order 8.

Enumerate the points of S as $S=\{\mathfrak{P}_1,\ldots,\mathfrak{P}_{\#S}\}$. We now want to show that S injects into $E_{N,p}(\mathbb{F}_p)$ for all but finitely many primes p. Consider two distinct points $\mathfrak{P}_i=[x_i,y_i,z_i]$ and $\mathfrak{P}_j=[x_j,y_j,z_j]$ of $E_N(\mathbb{Q})_{tor}$. Let

$$d_{ij}=\gcd(x_iy_j-x_jy_i,x_iz_j-x_jz_i,y_iz_j-y_jz_i),\qquad D_{ij}=\operatorname{lcm}(x_iy_j-x_jy_i,x_iz_j-x_jz_i,y_iz_j-y_jz_i).$$

Then any prime $p>|D_{ij}|$ has the property that p does not divide d_{ij}, so by Lemma 10(a) we have $\mathfrak{P}_i\neq\mathfrak{P}_j$ in $E_{N,p}(\mathbb{F}_p)$. Thus S injects into $E_{N,p}(\mathbb{F}_p)$, and so $\#S$ divides $\#E_{N,p}(\mathbb{F}_p)$, for all primes $p>\max_{i,j}\{|D|_{ij}\}$.

Now let p be a prime satisfying the following properties: p does not divide $2N$, and $p\equiv 3 \pmod 4$, and $p>\max_{i,j}\{|D|_{ij}\}$. The previous paragraph, together with Lemma 11, implies that $\#S$ divides $\#E_{N,p}(\mathbb{F}_p)=p+1$ for all such p. This implies that, among the primes p with $p\equiv 3 \pmod 4$, all but finitely many of them satisfies $p\equiv -1 \pmod{\#S}$. We now break down into three cases, all of which gives a contradicts.

Case 1: $\#S=8$. Then there are only finitely many primes in the arithmetic progression $8k+3$, a contradiction to Dirichlet's Theorem.

Case 2: $\#S$ is odd and 3 does not divide $\#S$. Then there are only finitely many primes in the arithmetic progression $4(\#S)k+3$, a contradiction to Dirichlet's Theorem. (Notice this argument does not work if 3 divides $\#S$, else $\gcd(4\#S,3)=3\neq 1$.)

Case 3: $\#S$ is odd and 3 divides $\#S$. Then there are only finitely many primes in the arithmetic progression $12k+7$, a contradiction to Dirichlet's Theorem. □

4 Congruent Numbers and $y^2=x^3-N^2x$

Proposition 12. *N is a congruent number if and only if the algebraic rank of E_N is positive.*

Proof. Given a congruent number N, with an associated rational right triangle of sides (X,Y,Z) with $X^2+Y^2=Z^2$ and area N, one produces a rational point on E_N defined by

$$\left(\frac{Z^2}{4},\frac{Z(X^2-Y^2)}{8}\right).$$

Notice that the y-coordinate of this point is nonzero, so by Theorem 9 it is not a torsion point.

Conversely, suppose the algebraic rank of E_N is positive. Then there exists a point $(x,y)\in E(\mathbb{Q})$ with $y\neq 0$, and one produces a rational right triangle of area N with lengths

$$\left(\frac{N^2-x^2}{y},\frac{-2xN}{y},\frac{N^2+x^2}{y}\right),$$

showing N is a congruent number. □

Remark. Perhaps I shall also type out the notes to the other pages of the slides in the future.

Appendix to Page 20 of the Slides

1 The method of 2-descent

Refer to Henri Cohen's book for more details on 2-descent. We state the definitions and theorems we need in this section. Say $E' : y^2 = x^3 + a'x + b'$ has a nontrivial 2-torsion point $T = (x_T, 0)$. Then, by the change of variables $x \mapsto x + x_T$, we transform E' into the isomorphic curve

$$E : y^2 = x^3 + ax^2 + bx.$$

Let

$$\widehat{E} : y^2 = x^3 + \widehat{a}x^2 + \widehat{b}x, \qquad \widehat{a} = -2a, \qquad \widehat{b} = a^2 - 4b.$$

Note that

$$\widehat{\widehat{E}} : y^2 = x^3 + 4ax^2 + 16bx$$

is isomorphic to our original elliptic curve E by the change of variables $(x, y) \mapsto 4x, 8y$.

Proposition 1. *There are group homomorphisms*

$$E \xrightarrow{\phi} \widehat{E} \qquad\qquad \widehat{E} \xrightarrow{\widehat{\phi}} E$$

$$(x, y) \longrightarrow (\widehat{x}, \widehat{y}) = \left(\frac{y^2}{x^2}, \frac{y^2(x^2 - b)}{x^2}\right) \qquad\qquad (x, y) \longrightarrow \left(\frac{\widehat{y}^2}{4\widehat{x}^2}, \frac{\widehat{y}(\widehat{x}^2 - b)}{8\widehat{x}^2}\right)$$

with $\ker \phi = \{0, T\}$ *and* $\ker \widehat{\phi} = \{0, \widehat{T}\}$*. Furthermore*

$$(\widehat{\phi} \circ \phi)(P) = 2P \qquad \textit{and} \qquad (\phi \circ \widehat{\phi})(\widehat{P}) = 2\widehat{P}.$$

Remark. One should note that the maps in this proposition are not isogenies over $\mathbb{Q}$.

Let us now define $\alpha : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$ by

$$\alpha(P) = \begin{cases} 1 & \text{if } P = \mathcal{O}, \\ b & \text{if } P = (0, 0), \\ x & \text{if } P = (x, y) \text{ and } x \neq 0. \end{cases}$$

We also define $\widehat{\alpha}$ analogously by putting hats on top of everything. Letting r be the rank of E, and specializing to the curve $E_N : y^2 = x^3 - N^2$, the fundamental theorem of 2-descent is as follows.

Theorem 2 (2-Descent for E_N)**.** *One has the equality*

$$2^{r+2} = |\alpha(E_N(\mathbb{Q}))||\widehat{\alpha}(\widehat{E_N}(\mathbb{Q}))|,$$

where $\alpha(E_N(\mathbb{Q}))$ *is the set of classes modulo squares of* 1*, and of* b_1 *and* $(-N^2)/b_1$ *for all squarefree divisors* b_1 *of* b *such that* $|b_1| \leq |-N^2|^{1/2}$*, and such that there is an integral solution to*

$$Y^2 = b_1 X^4 + \frac{(-N^2)}{b_1} Z^4$$

with $XZ \neq 0$ *and* $\gcd(X, Z) = 1$*. A similar characterization holds for* $\widehat{\alpha}(\widehat{E_N}(\mathbb{Q}))$*.*

It is now a matter of sitting down and verifying the results stated in slide 13. Refer to Farzali Izadi and Hamid Reza Azdolmaleki's paper to see how such computations are done.

Remark. Perhaps I shall also type out the notes to the other pages of the slides in the future.