Math 4527 (Number Theory 2)

Lecture #19 of 38 $\sim$ March 4, 2021

Integral Points on Elliptic Curves

- Integral Points on Elliptic Curves
- Siegel's Theorem and Thue's Theorem
- Congruent Numbers

This material represents §7.2.3-7.3.1 from the course notes.

Elliptic Curves Over $\mathbb{Q}$, I

We now discuss the problem of computing rational points on elliptic curves. The following quite deep theorem establishes that the group of $\mathbb{Q}$-rational points on any elliptic curve E is always finitely generated:

Theorem (Mordell's Theorem)

Let E be an elliptic curve over $\mathbb{Q}$. Then the group $E(\mathbb{Q})$ of rational points on E is finitely generated.

By applying the structure theorem for finitely-generated abelian groups, we can say a bit more about the group of rational points.

- Explicitly, we have $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_{\mathrm{Tor}}(\mathbb{Q})$ where $E_{\mathrm{Tor}}(\mathbb{Q})$ is the set of $\mathbb{Q}$-torsion points of E (i.e., the set of $\mathbb{Q}$-rational points of E having finite order), which is a finite abelian group and thus is a direct sum of cyclic groups.

Elliptic Curves Over $\mathbb{Q}$, II

Mordell's theorem says that $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_{\text{Tor}}(\mathbb{Q})$.

- For any given elliptic curve E, the torsion subgroup $E_{\text{Tor}}(\mathbb{Q})$ can be computed quite explicitly, as we will describe a bit later.
- The quantity r is called the rank of the elliptic curve, and is equal to the number of linearly-independent points one may construct on E. The rank is much more difficult to compute, and there is no known direct algorithm that is guaranteed to compute it (though in practice the rank of most curves can be computed).
- It is not currently known whether elliptic curves over $\mathbb{Q}$ can have an arbitrarily large rank, and the historical consensus has switched back and forth between thinking ranks can be arbitrarily large and thinking that ranks are uniformly bounded above.

Elliptic Curves Over $\mathbb{Q}$, III

Elkies has given a construction for an elliptic curve that has rank at least 28, and it is expected (although to date, it is not proven) that this curve has rank exactly 28.

- The equation of Elkies' curve is

$$x^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x + 3448161179503055646703298569039072037485594435931918036126600829629$$

- It has been shown by Bhargava and Shankar in 2015 that the average rank (suitably defined) of an elliptic curve is at most $7/6$: the actual average is expected to be $1/2$ (with 50% of elliptic curves having rank 0 and 50% having rank 1, asymptotically).

Elliptic Curves Over $\mathbb{Q}$, IV

The result of the Mordell-Weil theorem is relatively deep, and we will not go through all the calculations in the proof, but rather just outline the main ideas.

- First, one proves the so-called "weak Mordell-Weil theorem": that for any positive integer m, the group $E(\mathbb{Q})/mE(\mathbb{Q})$ is finitely generated.
- Of course, the weak Mordell-Weil theorem does not imply the full Mordell-Weil theorem directly, because there are many non-finitely-generated groups G such that G/mG is finitely generated (e.g., $\mathbb{Q}$ and $\mathbb{R}$ both have $G/mG = 0$ for all m).
- The difficulty is that knowing G/mG is finitely generated does not imply G is finitely generated, because G could contain many elements that are divisible by m.

Elliptic Curves Over $\mathbb{Q}$, V

The second part of the proof requires showing that $E(\mathbb{Q})$ cannot contain a large number of "small" elements that are divisible by m, using the theory of heights.

- First, one defines a "height function", measuring roughly the complexity of a point on the curve, and then shows that the height of large multiples of a point tends to be larger than the height of the original point.
- One such height function on points $(x, y) = (p_x/q_x, p_y/q_y)$ is $\max(\log p_x, \log q_x)$: essentially, the maximum number of digits appearing in the numerator or denominator of the coordinates.
- This is a fundamentally algebraic notion of "size", in contrast to a more analytic notion of size like $|(x, y)| = |x|$: the difference is that analytically, $999/1000$ and 1 are close, but algebraically, the first is far more complicated than the second.

Elliptic Curves Over $\mathbb{Q}$, VI

Using heights, we can show that there are a bounded number of points in $E(\mathbb{Q})$ of height less than any fixed bound: thus, any point that is a multiple of m has to be "large" for large m.

- By fine-tuning the details of this argument, we can deduce that a finite number of generators will suffice to generate the group $E(\mathbb{Q})$.
- The idea is to show that for any point P on E, we may subtract appropriate multiples of the coset representatives of the finite group $E(\mathbb{Q})/mE(\mathbb{Q})$ to obtain a new point whose height is bounded independently of P.
- Since there are then only finitely many such points, adding them to our list will yield a finite generating set for $E(\mathbb{Q})$.

Elliptic Curves Over $\mathbb{Q}$, VII

With Mordell's theorem in hand, we know that the group of $\mathbb{Q}$-rational points on any elliptic curve is finitely generated, and breaks up as a direct sum of the (finite) subgroup of torsion points with a free subgroup of non-torsion points.

- So, if we want to compute the group of $\mathbb{Q}$-rational points on E, all we need to do is to compute the torsion subgroup along with a list of generators for the free part.

Elliptic Curves Over $\mathbb{Q}$, VIII

The following theorem of Nagell and Lutz provides a very convenient way to calculate the torsion points on any elliptic curve over $\mathbb{Q}$:

Theorem (Nagell/Lutz Theorem)

Suppose E is an elliptic curve over $\mathbb{Q}$ whose Weierstrass form has integer coefficients, and let $D = -4A^3 - 27B^2$ be the discriminant of E. If $P = (x, y)$ is a rational point of finite order, then x and y are integers. Furthermore, either $y = 0$ or y^2 divides D.

We emphasize here that the Nagell-Lutz theorem is not an if-and-only-if: there can exist points (x, y) with y dividing D that do not have finite order. Nonetheless, for any E, it gives an explicit finite calculation for finding the torsion subgroup of E.

Elliptic Curves Over $\mathbb{Q}$, IX

We will again only outline the ideas in the proof of the Nagell-Lutz theorem, rather than giving the full details.

- First, the idea is to show that if P has finite order, then its coordinates must be integers, which we do by showing that it is not possible for any prime to divide the denominator of either coordinate.
- For this, we can use the same general idea as in the proof of Mordell's theorem: namely, consider what happens to the height of a point P under scaling.

Elliptic Curves Over $\mathbb{Q}$, X

Instead of using the height function in Mordell's theorem, however, we use the so-called p-adic height.

- For any rational a/b, we can pull out the factors of p to write $\frac{a}{b} = p^v \cdot \frac{m}{n}$ for some m, n not divisible by p. We then define the p-adic valuation as $\mathrm{ord}_p(a/b) = v$.
- By analyzing the behavior of the p-adic valuation with respect to the group law on E, we can eventually show that it is not possible to have a point of finite order with negative p-adic valuation for any p, since the valuation of multiples of large multiples of P would have to become arbitrarily large and negative.

Elliptic Curves Over $\mathbb{Q}$, XI

For the second part of the theorem (that $y = 0$ or y^2 divides D), suppose P has finite order.

- If $2P = \infty$ then as we observed earlier, $y = 0$. Otherwise assume $2P \neq 0$: then since $2P$ also has finite order, its coordinates are also integral.
- If $P = (a, b)$ and $2P = (c, d)$, then $c = m^2 - a$ and $d = -m(m^2 - 3a) - b$, with $m = \frac{3a^2+A}{2b}$. Since $m^2 = a + c$ is an integer and m is rational, then m is an integer.
- This means $2b$ hence b divides $3a^2 + A$. But since $b^2 = a^3 + Aa + B$, we see that b^2 divides both $(3a^2 + A)^2$ and $a^3 + Aa + B$. By eliminating a from these relations using (essentially) the Euclidean algorithm, we can eventually conclude that b^2 divides D, which establishes the second part of the theorem.

Elliptic Curves Over $\mathbb{Q}$, XI

The result of the Nagell-Lutz theorem gives us a very effective way to compute all of the torsion points on E.

- First, we compute all of the possible torsion points: these are the integral points (x, y) on E where $y = 0$ or y^2 divides D, per the theorem above.
- We then test whether these points have finite order.
- A priori, a rational point P could potentially have very large order, but since the torsion points form a subgroup and we have just listed all of the possible elements of this group, we have an upper bound on the possible order of the group and hence on the possible order of P.

Elliptic Curves Over $\mathbb{Q}$, XI

More efficiently, to test whether P has finite order, we could simply compute the list $\{P, 2P, 3P, 4P, \dots\}$, or even just $\{P, 2P, 4P, 8P, \dots\}$.

- If any of the multiples of P fail to land on our list, then P cannot have finite order, since our list includes all points that could have finite order.
- Otherwise, the multiples of P must necessarily repeat since our list is finite, in which case P (and all of its multiples) does have finite order.

Elliptic Curves Over $\mathbb{Q}$, XII

Example: Find the rational torsion points on the elliptic curve $E : y^2 = x^3 - 4x + 3$ and identify their group structure.

Elliptic Curves Over $\mathbb{Q}$, XII

Example: Find the rational torsion points on the elliptic curve $E : y^2 = x^3 - 4x + 3$ and identify their group structure.

- Here, we have $A = -4$ and $B = 3$, so the discriminant is $D = -4A^3 - 27B^2 = 13$.
- Since D is squarefree, the only possible y-coordinates are 0 and ± 1.
- Testing $y = 0$ (so that $x^3 - 4x + 3 = 0$) yields a single rational solution $x = 1$, giving a 2-torsion point $(1, 0)$.
- Testing $y = \pm 1$ (so that $x^3 - 4x + 3 = \pm 1$) yields no rational solutions in either case, as the resulting cubic is irreducible.
- Therefore, we see that there are two rational torsion points on E: $\boxed{(1, 0) \text{ and } \infty}$. The torsion group has order 2 and is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Elliptic Curves Over $\mathbb{Q}$, XIII

Example: Find the rational torsion points on the elliptic curve $E : y^2 = x^3 + 16$ and identify their group structure.

Elliptic Curves Over $\mathbb{Q}$, XIII

Example: Find the rational torsion points on the elliptic curve $E : y^2 = x^3 + 16$ and identify their group structure.

- Here, we have $A = 0$ and $B = 16$, so the discriminant is $D = -4A^3 - 27B^2 = -2^8 3^3$.
- Then the possible y-coordinates are 0, ± 1, ± 2, ± 4, ± 8, ± 16, ± 3, ± 6, ± 12, ± 24, and ± 48.
- Testing each of these in turn yields two potential torsion points, namely, $(0, \pm 4)$.
- If we take $P = (0, 4)$ then we can compute $2P = (0, -4)$ and $3P = \infty$, so these points are indeed torsion points.
- Thus, there are three rational torsion points on E: $\boxed{(0, \pm 4) \text{ and } \infty}$. The torsion group has order 3 and is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

Elliptic Curves Over $\mathbb{Q}$, XIV

Example: Find the rational torsion points on the elliptic curve $E : y^2 = x^3 - 2x + 1$ and identify their group structure.

Elliptic Curves Over $\mathbb{Q}$, XIV

Example: Find the rational torsion points on the elliptic curve $E : y^2 = x^3 - 2x + 1$ and identify their group structure.

- Here, we have $A = -2$ and $B = 1$, so the discriminant is $D = -4A^3 - 27B^2 = 5$.
- Then the possible y-coordinates are 0 and ± 1. Testing yields the potential torsion points $(1, 0)$, $(0, \pm 1)$.
- If we take $P = (0, 1)$ then we can compute $2P = (1, 0)$, $3P = (0, -1)$, and then $4P = \infty$, so all of these points are indeed torsion points.
- Thus, there are four rational torsion points on E: $\boxed{(0, \pm 1),\ (1, 0),\ \text{and}\ \infty}$. The torsion group has order 4 and is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

Elliptic Curves Over $\mathbb{Q}$, XV

Example: Find the rational torsion points on the elliptic curve $E : y^2 = x^3 - 351x + 1890$ and identify their group structure.

Elliptic Curves Over $\mathbb{Q}$, XV

Example: Find the rational torsion points on the elliptic curve $E : y^2 = x^3 - 351x + 1890$ and identify their group structure.

- Here, we have $A = -351$ and $B = 1890$, so the discriminant is $D = -4A^3 - 27B^2 = 2^4 3^{14}$.
- Then the possible y-coordinates are 0 and $\pm 2^a 3^b$ for $a \in \{0, 1, 2\}$ and $b \in \{0, 1, 2, 3, 4, 5, 6, 7\}$.
- If $y = 0$ then we obtain three 2-torsion points, namely $(-21, 0)$, $(6, 0)$, $(15, 0)$.
- For the other 24 possible values of y, some computation yields four additional candidate points: $(-3, \pm 54)$ and $(33, \pm 162)$.
- With $P = (33, 162)$ we can compute $2P = (15, 0)$, $3P = (33, -162)$, and $4P = \infty$, so this point has order 4.
- Likewise, with $Q = (-3, 54)$ we can compute $2Q = (15, 0)$, $3Q = (-3, -54)$, and $4Q = \infty$, so this point also has order 4.

Elliptic Curves Over $\mathbb{Q}$, XVI

Example: Find the rational torsion points on the elliptic curve $E : y^2 = x^3 - 351x + 1890$ and identify their group structure.

Elliptic Curves Over $\mathbb{Q}$, XVI

Example: Find the rational torsion points on the elliptic curve $E : y^2 = x^3 - 351x + 1890$ and identify their group structure.

- Thus, there are eight rational torsion points on E:
  $\boxed{(-3, \pm 54),\ (33, \pm 162),\ (-21, 0),\ (6, 0),\ (15, 0),\ \text{and } \infty}$.
- The torsion group has order 8 and is isomorphic to $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, where we can take (a, b) mapping to $aP + b(Q - P)$.

Elliptic Curves Over $\mathbb{Q}$, XVI

We can also use the Nagell-Lutz theorem to establish that a given point has infinite order on E.

- Most obviously, if the point does not have integral coordinates, then it is not a torsion point. Even if its coordinates are integral, if its y-coordinate is nonzero and its square does not divide D, then the point cannot be a torsion point.
- Furthermore, even if all of these conditions are satisfied, if we compute $2P, 3P, 4P, \ldots$ and any of these points have non-integral coordinates or have a nonzero y-coordinate with y^2 not dividing D, then P must have infinite order.

Elliptic Curves Over $\mathbb{Q}$, XVI

Example: Show that the elliptic curve $E : y^2 = x^3 + 2$ has infinitely many rational points.

Elliptic Curves Over $\mathbb{Q}$, XVI

Example: Show that the elliptic curve $E : y^2 = x^3 + 2$ has infinitely many rational points.

- Testing small values of x reveals two integral points: $(x, y) = (-1, \pm 1)$.
- If we take $P = (-1, -1)$, then P could be a torsion point, since its y-coordinate -1 has its square dividing the discriminant $D = -108$.
- However, we can calculate $2P = (17/4, 71/8)$, and so since $2P$ does not have integral coordinates, it is not a torsion point, and thus neither is P.
- This means that P has infinite order, which is to say, all of the points $P, 2P, 3P, 4P, \ldots$ are distinct. Since these all have rational coordinates, E has infinitely many rational points.
- Remark: It is much harder to prove, but in fact E has rank 1 and its group of rational points is generated by P.

Elliptic Curves Over $\mathbb{Q}$, XVII

It follows from the Nagell-Lutz theorem that the group of rational torsion points on an elliptic curve is always finite.

- You will see examples (either from the ones we just did now, or the ones on the homework) showing that the group of rational points can have order 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, or 16.
- Although it may seem that the group could potentially be arbitrarily large, in fact, no other orders are possible. Furthermore, since (as we showed) the group of m-torsion points for any m is generated by at most 2 elements, this list quite substantially narrows down the possible group structures.

Elliptic Curves Over $\mathbb{Q}$, XVIII

The following quite deep theorem of Mazur establishes that there is a fairly small list of possible torsion groups:

Theorem (Mazur's Theorem)

If E is an elliptic curve, then the number of rational torsion points (including ∞) can be any integer from 1 to 12 inclusive, excluding 11, or 16. More explicitly, there are 15 possible group structures for the rational torsion points: the trivial group (order 1), $\mathbb{Z}/2\mathbb{Z}$ (order 2), $\mathbb{Z}/3\mathbb{Z}$ (order 3), $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ or $\mathbb{Z}/4\mathbb{Z}$ (order 2), $\mathbb{Z}/5\mathbb{Z}$ (order 5), $\mathbb{Z}/6\mathbb{Z}$ (order 6), $\mathbb{Z}/7\mathbb{Z}$ (order 7), $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ or $\mathbb{Z}/8\mathbb{Z}$ (order 8), $\mathbb{Z}/9\mathbb{Z}$ (order 9), $\mathbb{Z}/10\mathbb{Z}$ (order 10), $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$ or $\mathbb{Z}/12\mathbb{Z}$ (order 12), or $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})$ (order 16).

It was shown 60 years before Mazur's proof that there exist infinite families having each of the groups listed as its torsion group.

Elliptic Curves Over $\mathbb{Q}$, XIX

The proof of Mazur's theorem involves quite advanced methods.

- The idea is to study the points on various modular curves and use a (tremendous!) amount of case analysis to eliminate all of the other possible torsion orders and other possible group structures.
- Just to give you an idea of how much goes into the proof, I once saw a semester-long graduate-level topics in number theory course, where the entire semester was devoted to the proof of Mazur's theorem. In that class, they covered all of the material we have covered on elliptic curves (in full depth)... in the first half-hour of the first lecture of the course.

Elliptic Curves Over $\mathbb{Q}$, XX

In some situations (e.g., if we are solving a Diophantine equation) we are often interested particularly in the integral points on an elliptic curve.

- As we have remarked, an elliptic curve of positive rank necessarily has infinitely many rational points.
- However, the following result of Siegel establishes that only finitely many of these rational points can be integral:

Theorem (Siegel's Theorem)

If E is a (nonsingular) elliptic curve over $\mathbb{Q}$, then E has only finitely many integral points.

We emphasize here that E must be nonsingular, since (for example) the singular curve $y^2 = x^3$ has infinitely many integral points, namely $(x, y) = (n^2, n^3)$ for any integer n.

Elliptic Curves Over $\mathbb{Q}$, XXI

Siegel's original proof, like the proof of Mordell's theorem, is ineffective, in the sense that it does not give an explicit bound on the possible size of the integral points in terms of the coefficients of E.

- For certain curves, the results can be made explicit using results of Baker on linear forms in logarithms, but the results typically are still computationally infeasible in practice.
- For example, one such result says that if (x, y) is an integral point on $y^2 = x^3 + ax^2 + bx + c$, then $\max(|x|, |y|) \leq \exp\left[(1,000,000 \max(|a|, |b|, |c|))^{1,000,000}\right]$.
- But even for quite small a, b, c, this bound is completely infeasible to work with.

Elliptic Curves Over $\mathbb{Q}$, XXII

For certain special curves, such as $x^3 - by^3 = c$, one can establish better results, using Diophantine approximation ideas similar to those we used in studying Pell's equation $x^2 - Dy^2 = r$.

- Explicitly, as shown by Thue, if b is a positive integer that is not a cube and C is any fixed positive constant, then there are only finitely many rational numbers p/q such that $\left|p/q - \sqrt[3]{b}\right| < C/q^3$.
- In fact, Thue showed that there are only finitely many p/q satisfying $\left|p/q - \sqrt[3]{b}\right| < C/q^{5/2+\epsilon}$ for any $\epsilon > 0$, and this result has been improved by Roth to show that there are only finitely many p/q satisfying $\left|p/q - \sqrt[3]{b}\right| < C/q^{2+\epsilon}$ for any $\epsilon > 0$. Since (as we showed via continued fractions) there are infinitely many p/q with $|p/q - \alpha| < C/q^2$ for any irrational α, Roth's result is essentially the best possible.

Elliptic Curves Over $\mathbb{Q}$, XXII

We can obtain a finiteness result using Thue's result that if b is a positive integer that is not a cube and C is any fixed positive constant, then there are only finitely many rational numbers p/q such that $\left|p/q - \sqrt[3]{b}\right| < C/q^3$.

- Specifically, if $x^3 - by^3 = c$ then $\left|x/y - \sqrt[3]{b}\right| \leq \dfrac{4\,|c|}{3b^{2/3}} \cdot \dfrac{1}{|y|^3}$.
- This inequality is of the form above with $C = 4\,|c|\,/(3b^{2/3})$.
- Thus, Thue's result implies immediately that there are only finitely many integral pairs (x, y) with $x^3 - by^3 = c$.

Elliptic Curves Over $\mathbb{Q}$, XXIII

For arbitrary elliptic curves over $\mathbb{Q}$, as we have seen, it is not so difficult to write down a sensible finite calculation to compute the torsion subgroup.

- It is much harder to compute the rank of an elliptic curve, and it is also hard to list all integral points on the curve.
- Nonetheless, various computational improvements have been made that allow efficient calculation of integral points on most elliptic curves.
- Such algorithms are implemented in some algebra packages such as Sage and Magma, and a large number of elliptic curves have been tabulated in various databases such as the *L*-Functions and Modular Forms Database (LMFDB).
- Using these, one may generate examples of elliptic curves having relatively small coefficients that have quite a few integral points.

Elliptic Curves Over $\mathbb{Q}$, XXIV

For example, the curve $E : y^2 = x^3 - 1267x + 17230$ has 82 integral points.

- They are $(-41, \pm 16)$, $(-37, \pm 116)$, $(-33, \pm 152)$, $(-29, \pm 172)$, $(-17, \pm 184)$, $(-10, \pm 170)$, $(-1, \pm 136)$, $(3, \pm 116)$, $(11, \pm 68)$, $(15, \pm 40)$, $(18, \pm 16)$, $(19, \pm 4)$, $(22, \pm 2)$, $(23, \pm 16)$, $(27, \pm 52)$, $(31, \pm 88)$, $(34, \pm 116)$, $(47, \pm 248)$, $(51, \pm 292)$, $(54, \pm 326)$, $(87, \pm 752)$, $(107, \pm 1052)$, $(115, \pm 1180)$, $(151, \pm 1808)$, $(239, \pm 3656)$, $(279, \pm 4624)$, $(363, \pm 6884)$, $(418, \pm 8516)$, $(491, \pm 10852)$, $(515, \pm 11660)$, $(703, \pm 18616)$, $(1167, \pm - 39848)$, $(1362, \pm 50248)$, $(3967, \pm 249848)$, $(4559, \pm 307816)$, $(6623, \pm 538984)$, $(14006, \pm 1657562)$, $(18127, \pm 2440552)$, $(42331, \pm 8709388)$, $(77169, \pm 21624796)$, $(878838, \pm 823878634)$.

Elliptic Curves Over $\mathbb{Q}$, XXV

For example, the curve $E : y^2 = x^3 - 1267x + 17230$ has 82 integral points.

- It can be shown that the group of rational points on this curve is isomorphic to $\mathbb{Z}^4$, and is generated by the four points $(15, 40)$, $(19, 4)$, $(23, 16)$, and $(31, 88)$.
- The difficulty is in proving that these four points are linearly independent. (Try thinking about why this is very difficult.)
- In order to do this, the standard approach is to use the fact that there is a "canonical height" function obtained by taking the limit of large multiples of the point, appropriately scaled.
- A linear dependence between the points yields a linear dependence between their canonical heights, which can then be detected by evaluating a "canonical height matrix" and computing its kernel numerically.

Elliptic Curves Over $\mathbb{Q}$, XXV

Changing the coefficients slightly can drastically affect the number of integral points.

- As we just showed, the curve $E : y^2 = x^3 - 1267x + 17230$ has 82 integral points.
- In contrast, the curve $E : y^2 = x^3 - 1267x + 17231$, which differs only by 1 in the constant term, has no integral points at all.
- Furthermore, the curve $E : y^2 = x^3 - 1266x + 17230$, differing by 1 in the linear term, has two integral points $(5, \pm 105)$.

Elliptic Curves Over $\mathbb{Q}$, XXVI

As another example, the curve $E : y^2 = x^3 - 1386747x + 368636886$ is the curve with the smallest discriminant in this Weierstrass form whose $\mathbb{Q}$-torsion group is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})$.

- This curve can also be shown to have rank 0, so in fact its full group of $\mathbb{Q}$-rational points is $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})$.
- The integral points on this curve are therefore just its torsion points, which (along with ∞) are $(-1293, 0)$, $(-933, \pm 29160)$, $(-285, \pm 27216)$, $(147, \pm 12960)$, $(282, 0)$, $(1011, 0)$, $(1227, \pm 22680)$, $(2307, \pm 97200)$, and $(8787, \pm 816480)$.
- Explicitly, one can verify that $P = (-933, 29160)$ has order 8, and that $4P = (1011, 0)$. Thus, P and $Q = (282, 0)$ generate the group of rational points on E.

The Congruent Number Problem, I

We will finish our discussion of elliptic curves with a brief examination of a famous classical number theory problem that turns out to reduce to the question of whether an elliptic curve has a nontrivial rational point.

Definition

We say a positive integer n is a congruent number if there exists a right triangle with rational side lengths whose area is n.

Examples:

- 6 is a congruent number as it is the area of a 3-4-5 triangle.
- 5 is a congruent number: although 5 cannot be the area of a right triangle with integer side lengths, it is the area of a triangle with side lengths 3/2, 20/3, and 41/6 (which is similar to the integer-sided 9-40-41 triangle).

The Congruent Number Problem, II

Example: No square is a congruent number (thus in particular, 1 and 4 are not congruent numbers).

- If it were true that $\frac{1}{2}ab = k^2$ and $a^2 + b^2 = c^2$, then $c^2 + 4k^2 = (a+b)^2$ and $c^2 - 4k^2 = (a-b)^2$.
- Multiplying these equations would then yield $c^4 - (2k)^4 = (a^2 - b^2)^2$, which is equivalent to the equation $c^4 = d^4 + e^2$.
- By clearing denominators and then using essentially the same infinite descent argument as for the Diophantine equation $c^4 + d^4 = e^2$, we can show that there is no solution to this congruence in positive integers, and thus no square can be a congruent number.

This result was first proven by Fermat using infinite descent.

The Congruent Number Problem, III

A few more observations:

- From similarity, n is a congruent number if and only if $k^2 n$ is a congruent number for any positive integer k.
- Also, from our characterization of Pythagorean triples, we can see that the area of any right triangle with integer side lengths is of the form $k^2 st(s^2 - t^2)$.
- Thus, if we take out the square factors, we are equivalently searching for integers that are the squarefree part of $st(s^2 - t^2)$ for some s and t.
- Although it might seem that congruent numbers would be easy to enumerate from this procedure, the squarefree part of $st(s^2 - t^2)$ varies greatly even for s, t of similar sizes.
- For example, $(s, t) = (5, 4)$ gives $st(s^2 - t^2) = 5 \cdot 4 \cdot 9$ with a squarefree part of 5, while $(s, t) = (5, 2)$ gives $st(s^2 - t^2) = 5 \cdot 2 \cdot 3 \cdot 7 = 210$ with a squarefree part of 210.

The Congruent Number Problem, IV

There are many other ways to characterize congruent numbers.

- If the legs of the right triangle are a, b and the hypotenuse is c, we want $ab = 2n$ and $a^2 + b^2 = c^2$.
- These equations imply $c^2 + 4n = (a + b)^2$ and $c^2 - 4n = (a - b)^2$, so if we set $s = a + b$ and $d = a - b$ we equivalently have $(c/2)^2 + n = (s/2)^2$, $(c/2)^2 - n = (d/2)^2$.
- Since $(c/2)^2$ is also a square, the above calculations show that n is a congruent number if and only if there exists an arithmetic progression $x - n = (a - b)^2/4$, $x = c^2/4$, $x + n = (a + b)^2/4$ of nonzero rational squares having common difference n.

The Congruent Number Problem, V

We see n is a congruent number iff there is an arithmetic progression $x - n = (a-b)^2/4$, $x = c^2/4$, $x + n = (a+b)^2/4$ of nonzero rational squares having common difference n.

- If we multiply these conditions, this means (equivalently) that the product $x(x-n)(x+n) = x^3 - n^2x$ must also be the square of some nonzero rational number y.
- Thus, if n is a congruent number, we must have a rational point on the elliptic curve $E_n : y^2 = x^3 - n^2x$ with $y \neq 0$ (equivalently, not a 2-torsion point).

The Congruent Number Problem, VI

In fact, the converse of this statement is true as well:

Proposition (Congruent Numbers)

The positive integer n is a congruent number if and only if the elliptic curve $E : y^2 = x^3 - n^2x$ has a rational point with $y \neq 0$.

Here is the motivation for the argument:

- If we follow through the algebra, we can see that we can take $x = n\dfrac{(a+c)}{b}$ and $y = 2n^2\dfrac{(a+c)}{b^2}$.
- If we run these calculations backwards, we can rederive the values of a, b, c from n, x, y as $a = \dfrac{y}{x}$, $b = \dfrac{2nx}{y}$, and $c = \dfrac{2x^2}{y} - \dfrac{y}{x} = \dfrac{x^2+n^2}{y}$, and then we just have to show that these will work.

The Congruent Number Problem, VII

Proof:

- Clearly, if (x, y) is a rational point on $E : y^2 = x^3 - n^2x$ with $y \neq 0$, then $x \neq 0, \pm n$.
- First, if (a, b, c) has $a^2 + b^2 = c^2$ and $ab = 2n$, then for $x = n\dfrac{(a+c)}{b}$ and $y = 2n^2\dfrac{(a+c)}{b^2}$ we can see $x = \dfrac{1}{2}a(a+c)$ and $y = \dfrac{1}{2}a^2(a+c)$.
- Then $y^2/x = \dfrac{1}{2}a^3(a+c)$, and also $x^2 - n^2 = \dfrac{1}{4}a^2(a+c)^2 - \dfrac{1}{4}a^2b^2 = \dfrac{1}{4}a^2(2a^2+2ac) = \dfrac{1}{2}a^3(a+c)$.
- Thus $y^2/x = x^2 - n^2$, so $y^2 = x^3 - n^2x$, as claimed. We therefore obtain a rational point on E with $y \neq 0$ as claimed.

The Congruent Number Problem, VIII

Proof (continued):

- Conversely, suppose that $y^2 = x^3 - n^2x$ has $y \neq 0$ so that $x \neq 0$ also, and then set $a = \frac{y}{x}$, $b = \frac{2nx}{y}$, and $c = \frac{2x^2}{y} - \frac{y}{x} = \frac{2x^3 - y^2}{xy} = \frac{x^2 + n^2}{y}$. Note that a, b, c are well-defined, nonzero rational numbers since $x, y \neq 0$.
- Then clearly we have $\frac{1}{2}ab = n$, and we also have $(c - b)(c + b) = \frac{(x - n)^2}{y} \cdot \frac{(x + n)^2}{y} = \frac{(x^2 - n^2)^2}{x(x^2 - n^2)}$ $= \frac{x(x^2 - n^2)}{x^2} = \frac{y^2}{x^2} = a^2$, so $a^2 + b^2 = c^2$ as required.
- We can then replace any of a, b, c with their absolute values without affecting these conditions. Thus n is a congruent number, as claimed.

The Congruent Number Problem, IX

It can be shown that the only torsion points on the congruent-number elliptic curve $E_n : y^2 = x^3 - n^2x$ are the 2-torsion points ∞, $(0, 0)$, and $(\pm n, 0)$.

- One way to do this is to observe that the reduction-mod-p map from the torsion points of E_n (which have integer coordinates) to the $\mathbb{F}_p$-points of E_n modulo p is a group homomorphism, and that it is injective whenever p does not divide the discriminant of E_n.
- The first part follows essentially from the observation that the definition of the group law is the same over $\mathbb{Q}$ and over $\mathbb{F}_p$.
- The second part follows from noting that no nontrivial torsion point can reduce to ∞ modulo p when p does not divide the discriminant of E, since its denominator cannot be zero.

The Congruent Number Problem, X

Next, one observes that E_n always has exactly $p+1$ points over $\mathbb{F}_p$ when p is a prime congruent to 3 modulo 4.

- This follows by a similar argument to the one you worked out on homework 5 for the curve $y^2 = x^3 + 1$ modulo primes congruent to 2 modulo 3.
- Finally, since the reduction-mod-p map must be injective for sufficiently large p, one then uses the fact[1] that there are arbitrarily large primes lying in any residue class a modulo m with a relatively prime to m to select various primes p for which the greatest common divisor of the values $p_i + 1$ is 4.
- Putting all of this together establishes that the size of the torsion subgroup of E over $\mathbb{Q}$ must have order dividing 4, and since there are in fact four 2-torsion points, there cannot be any other torsion points.

[1] This is Dirichlet's theorem on primes in arithmetic progressions.

The Congruent Number Problem, XI

Thus, since the only torsion points on E_n have $y = 0$, we see that there is a rational point on E_n with $y \neq 0$ if and only if E_n has rank at least 1.

- Since we just showed that this condition is equivalent to saying that n is a congruent number, we deduce that n is a congruent number precisely when E_n has rank at least 1.
- If we could compute the rank of E_n for a given n, we would then be able to determine conclusively whether or not n is a congruent number.

The Congruent Number Problem, XII

One may use software to compute the rank of E_n for various n.

- For example, for $n = 1, 2, 3, 4$, the rank is 0, so these are not congruent numbers.
- For $n = 5$, we have a rational point $(x, y) = (-4, 6)$, which yields $(a, b, c) = (-3/2, -20/3, 41/6)$, which (up to sign) is the triangle of area 5 we identified earlier.
- For $n = 7$ we can find a rational point $(x, y) = (25, 120)$, which yields $(a, b, c) = (24/5, 35/12, 337/60)$, which indeed yields a right triangle having area 7.
- Much work has been done in classifying congruent numbers, but as of 2021, a full characterization is still not known. It has been shown that if p is a prime congruent to 3 modulo 8, then p is not a congruent number, while if p is a prime congruent to 5 or 7 modulo 8, then p is a congruent number.

The Congruent Number Problem, XIII

A 1983 theorem of Tunnell, which relies quite heavily on modular forms, gives an efficient way to determine if n is a congruent number.

Theorem (Tunnell's Theorem)

If n is an odd congruent number then the number of solutions in integers to $n = 2x^2 + y^2 + 32z^2$ is equal to half the number of solutions of $n = 2x^2 + y^2 + 8z^2$, while if n is an even congruent number then the number of solutions to $n/2 = 4x^2 + y^2 + 32z^2$ is equal to half the number of solutions of $n/2 = 4x^2 + y^2 + 8z^2$.

Tunnell also showed that if the weak Birch/Swinnerton-Dyer conjecture (which states that the algebraic rank r of an elliptic curve is equal to the "analytic rank", which is the order of vanishing of the L-function associated to the elliptic curve at $s = 1$) holds for E_n, then the converse holds also.

The Congruent Number Problem, XIV

Examples:

1. If $n = 2$ then there are two solutions to $n/2 = 4x^2 + y^2 + 32z^2$ (namely, $(0, \pm 1, 0)$) and also two solutions to $n/2 = 4x^2 + y^2 + 8z^2$ (namely, $(0, \pm 1, 0)$). Thus, 2 is not a congruent number.
2. If $n = 3$ then there are four solutions to $n = 2x^2 + y^2 + 32z^2$ (namely, $(\pm 1, \pm 1, 0)$ and also four solutions to $n = 2x^2 + y^2 + 8z^2$ (also $(\pm 1, \pm 1, 0)$). Thus, 3 is not a congruent number.

The Congruent Number Problem, XV

Examples (continued):

3. If $n = 13$ then there are no solutions to $n = 2x^2 + y^2 + 32z^2$ or to $n = 2x^2 + y^2 + 8z^2$.

- This suggests n is in fact a congruent number, and indeed, searching for rational points on $y^2 = x^3 - 13^2x$ will eventually identify the point $(x, y) = (-36/25, 1938/125)$, which yields the triangle sides $(a, b, c) = (323/30, 780/323, 106921/9690)$.
- Thus, 13 is a congruent number.

Summary

We discussed the Nagell-Lutz theorem and used it to calculate the group of rational torsion points on an elliptic curve.

We discussed integral points on elliptic curves.

We discussed the congruent number problem, the congruent-number elliptic curves, and Tunnell's theorem.

Next lecture: Quadratic integer rings.