Math 4527 (Number Theory 2)

Lecture #18 of 38 $\sim$ March 3, 2021

Rational Points on Elliptic Curves

- Elliptic Curves over $\mathbb{C}$
- Mordell's Theorem
- The Nagell-Lutz Theorem

This material represents §7.3.1-7.3.2 from the course notes.

Logistical Stuff

Two logistical things:

- If you will be taking classes at Northeastern in Fall 2021 and are interested in taking any of the 3 courses "Elliptic Curves and Modular Forms", "Number Theory in Function Fields", or "Algebraic Number Theory" with me, please let me know! I am still rounding up interest to decide which one to teach.
- Unless I hear objections from any of you, I will be replacing the midterm exam with a regular homework assignment. The final exam will still exist and be comprehensive, but it will be take-home. The exam/homework percentages will still be 60-40, whichever way works out better for you. (The reason is that it works better with the schedule.)

Elliptic Curves over $\mathbb{C}$, I

We can say a bit more about the $\mathbb{C}$-points on the elliptic curve E using a bit of complex analysis and topology.

- The idea is to consider the Riemann surface associated to the nonsingular elliptic curve $y^2 = x^3 + Ax + B$.
- One may prove that this Riemann surface is homeomorphic to a torus $S^1 \times S^1 \cong (\mathbb{R}/\mathbb{Z}) \times (\mathbb{R}/\mathbb{Z})$, which is in turn homeomorphic to $\mathbb{C}$ modulo a discrete lattice $\Lambda \cong \mathbb{Z}^2$.
- The way this works is quite nice, and the result is quite helpful in understanding what the torsion elements look like, so let me explain it a bit more.

Elliptic Curves over $\mathbb{C}$, II

So: how could we try to write down an analytic map from E to $\mathbb{C}$?

- The idea is to integrate something: specifically, we want to integrate the holomorphic differential
$$d\omega = \frac{dx}{y} = \frac{dx}{\sqrt{(x - r_1)(x - r_2)(x - r_3)}}.$$
- We could then try to get a map from E to $\mathbb{C}$ by sending a point P to the integral $\int_0^P d\omega$.
- The problem is that this integral is not well-defined since this function needs branch cuts. So, if we include the point at ∞ (i.e., work with the Riemann sphere instead of $\mathbb{C}$), we can make one branch cut from r_1 to r_2 and another from r_3 to ∞.
- Topologically, this turns the Riemann sphere into a torus.

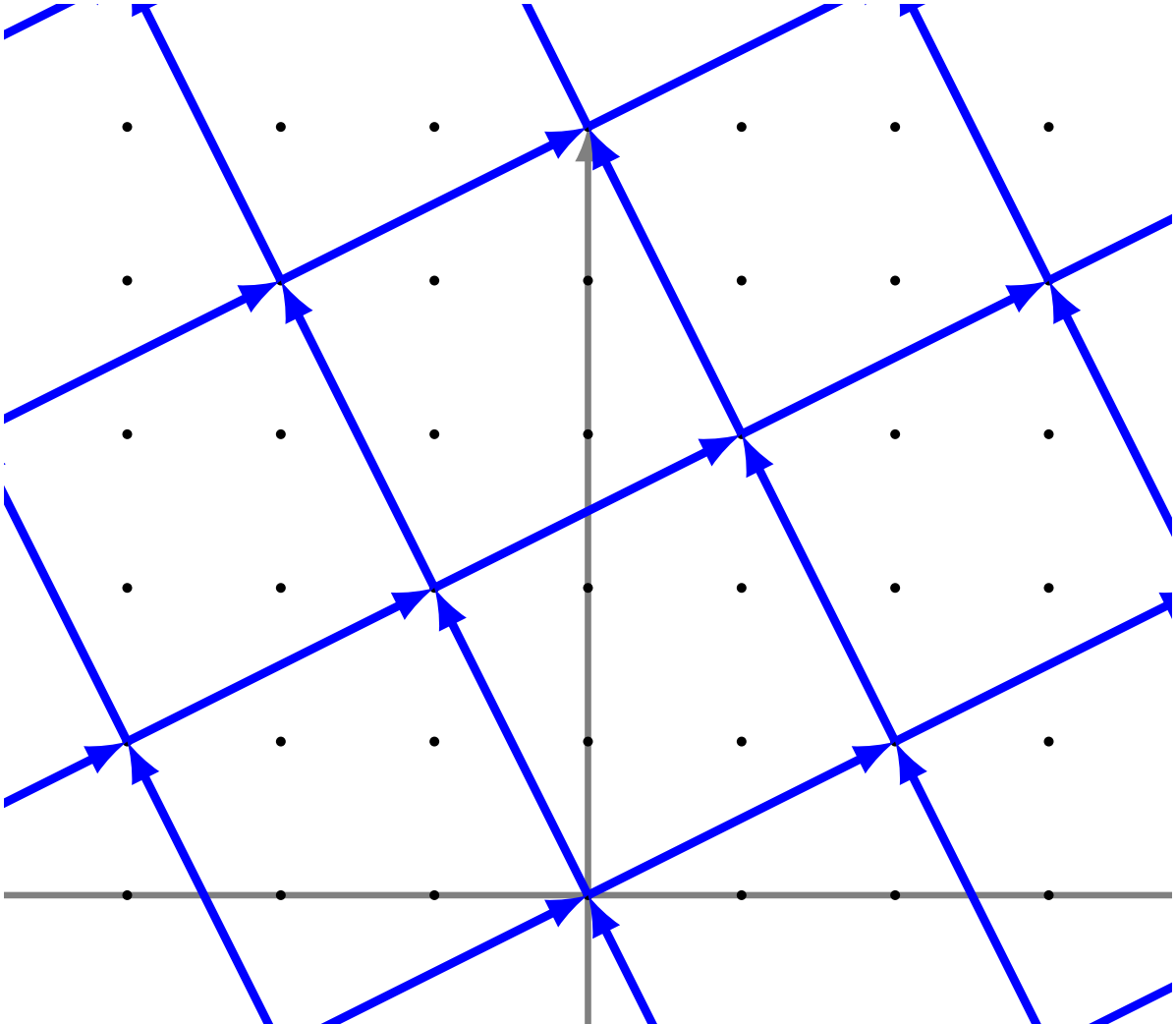
Elliptic Curves over $\mathbb{C}$, III

Let α be a path looping around the r_1-r_2 branch cut once, and let β be a path looping around the r_3-∞ branch cut once.

- Since α and β generate the fundamental group of the torus, the difference between any two paths between 0 and P on our branch-cut Riemann sphere is homotopic to a $\mathbb{Z}$-linear combination of α and β.
- So the integral $\int_0^P d\omega$ is well-defined up to adding a $\mathbb{Z}$-linear combination of $\omega_1 = \int_\alpha d\omega$ and $\omega_2 = \int_\beta d\omega$.
- What this all means is that when we integrate along paths, we get a map from E to $\mathbb{C}$ that is defined only up to adding arbitrary integer multiples of ω_1 and ω_2.
- This is equivalent to saying we get a map from E to the quotient group $\mathbb{C}/\Lambda$ where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{a\omega_1 + b\omega_2 \,:\, a, b \in \mathbb{Z}\}$.

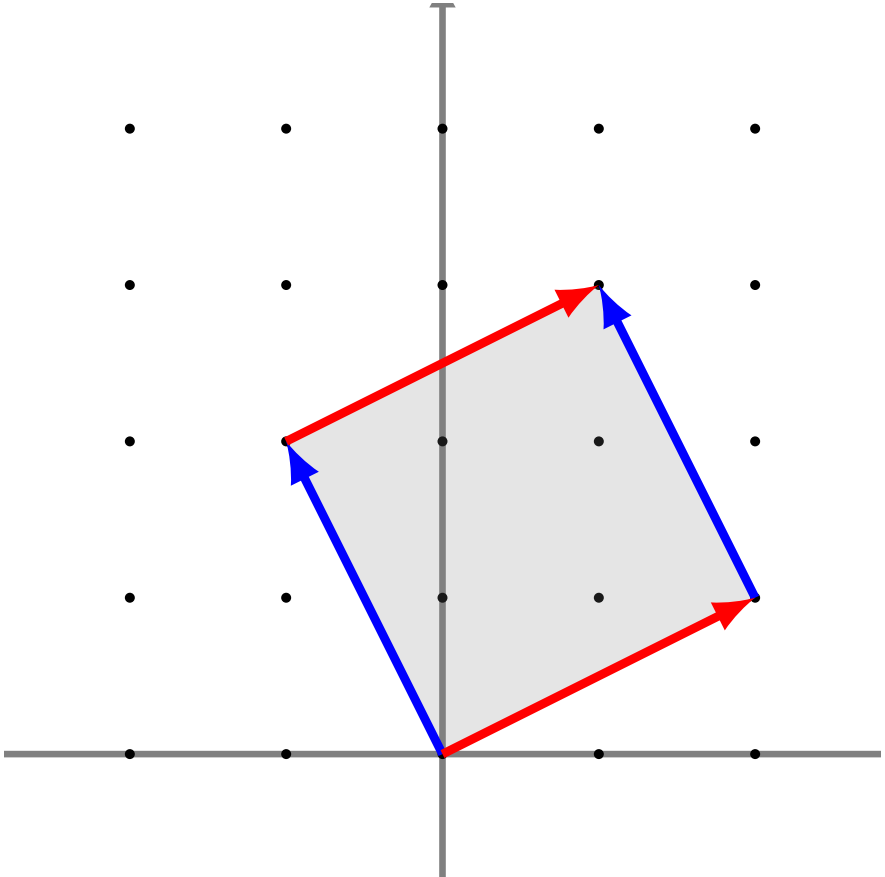
Elliptic Curves over $\mathbb{C}$, IV

For example, suppose that $\omega_1 = 2 + i$ and $\omega_2 = -1 + 2i$, so that our lattice is as below:



Elliptic Curves over $\mathbb{C}$, V

In the quotient group $\mathbb{C}/\Lambda$, we then identify any two points that differ by an element of Λ. Geometrically, we can picture this as being a "fundamental region", with the left and edges identified, and the top and bottom edges also identified (which is a torus):



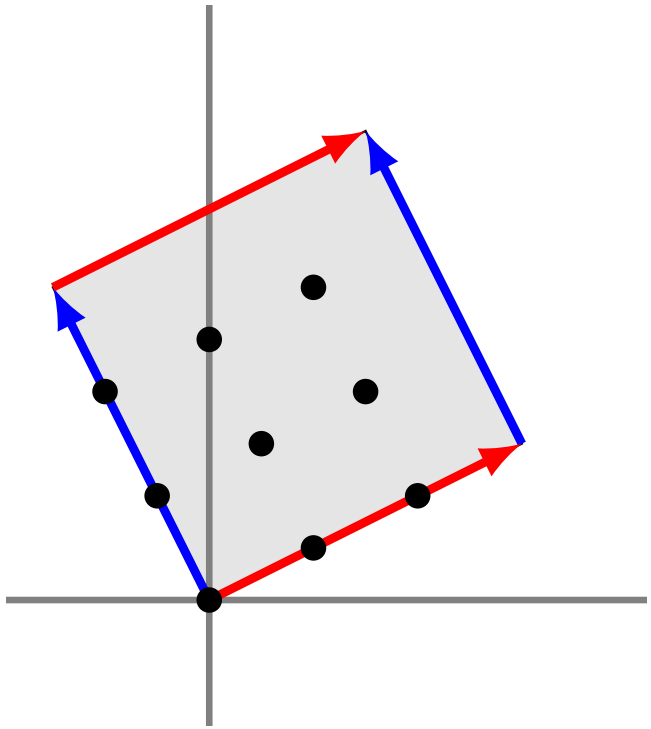
Elliptic Curves over $\mathbb{C}$, VI

The first magical fact is that the map from E to $\mathbb{C}/\Lambda$ is actually a diffeomorphism, and the second magical fact is that the map is an isomorphism of groups.

- The group operation inside $\mathbb{C}/\Lambda$ is just the usual one, namely, addition of complex numbers.
- The identity element of the group is of course 0.
- We can then easily identify the m-torsion elements: they simply form the $m \times m$ grid of "m-division points" in the lattice.
- Equivalently, we are looking for points such that $mP \in \Lambda$, which is simply the lattice $\frac{1}{m}\Lambda$.

Elliptic Curves over $\mathbb{C}$, VII

Here, for example, are the 3-division points of the lattice $\Lambda = (1+2i)\mathbb{Z} + (-2+i)\mathbb{Z}$ from earlier:



Algebraically, these points are $a \cdot \dfrac{1+2i}{3} + b \cdot \dfrac{-2+i}{3}$ for $a, b \in \{0, 1, 2\}$.

Elliptic Curves over $\mathbb{C}$, VIII

Conversely, one can construct a map from lattices $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ inside $\mathbb{C}$ back to elliptic curves by considering "elliptic functions": functions defined on $\mathbb{C}/\Lambda$.

- Equivalently, we are looking for meromorphic functions on $\mathbb{C}$ such that are "periodic relative to Λ": namely, with $f(z+\omega) = f(z)$ for all $\omega \in \Lambda$ and $z \in \mathbb{C}$.
- These are, equivalently, "doubly-periodic" functions, with $f(z+\omega_1) = f(z+\omega_w) = f(z)$ for all z.
- Functions like $\sin x$ only have one period in $\mathbb{C}$: we want functions with two different periods.

Elliptic Curves over $\mathbb{C}$, IX

Here is the standard example of an elliptic function, called the Weierstrass $\wp$-function: it is defined as

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda,\omega\neq 0}\left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right].$$

- One can check that the series converges uniformly on compact subsets of $\mathbb{C}$, and that it has double poles at each point of Λ but nowhere else in the plane.
- Another example of an elliptic function is the derivative $\wp'_\Lambda(z) = -2\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3}$.
- The sum used to define $\wp'$ converges absolutely, and is much easier to see that it is invariant under translation by elements of Λ.

Elliptic Curves over $\mathbb{C}$, X

So now here is the magic: by comparing Laurent expansions, we can use the $\wp$-function to map from lattices back to elliptic curves.

- To see this, first one computes the Laurent series for $\wp$ around $z = 0$, which is $\wp(z) = z^{-2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}$, where $G_{2k}(\Lambda) = \sum_{\omega \in \Lambda *} \omega^{-2k}$ is the Eisenstein series of weight $2k$.
- By comparing Laurent expansions, for $g_2 = 60G_4$ and $g_3 = 140G_6$ one has $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$.
- The point is that the Laurent series for the difference between the two sides has no negative-degree terms. This means the difference is actually holomorphic on all of $\mathbb{C}$, and it is bounded because it is doubly-periodic. Thus, by Liouville's theorem, it is constant (and the constant is in fact zero).
- Thus, the map $\mathbb{C}/\Lambda \to E$ sending $z \to (\wp(z), \wp'(z))$, where E is the elliptic curve $y^2 = 4x^3 - g_2x - g_3$, is a complex-analytic isomorphism of complex Lie groups.

Elliptic Curves over $\mathbb{C}$, XI

As a final comment, I will remark that the terminology of "complex multiplication" for elliptic curves also arises from this correspondence between elliptic curves over $\mathbb{C}$ and quotients $\mathbb{C}/\Lambda$.

- Specifically, if we happen to have a complex number ζ such that $\zeta\Lambda \subseteq \Lambda$, then we obtain a corresponding "multiplication-by-ζ" endomorphism of the elliptic curve.
- The obvious "multiplication by m" maps are of this form with $\zeta = m$, and for most Λ these are the only such ζ. But for certain lattices, there are nonreal ζ such that $\zeta\Lambda \subseteq \Lambda$.
- For example, if $\Lambda = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$, then $\zeta = i$ has $\zeta\Lambda \subseteq \Lambda$, and so the corresponding elliptic curve has a "multiplication by i" map. One can then compute the values of g_2 and g_3 for this lattice to see that the curve is exactly $y^2 = x^3 + x$, which you analyzed on Homework 6.

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 $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_{\mathrm{Tor}}(\mathbb{Q})$.

- For any given elliptic curve E, the torsion subgroup $E_{\mathrm{Tor}}(\mathbb{Q})$ can be computed quite explicitly, as I will describe 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 (in practice, the ranks of most curves can be computed).
- It is not currently known whether elliptic curves over $\mathbb{Q}$ can have an arbitrarily large rank. The historical consensus has switched back and forth between "ranks can be arbitrarily large" and "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.

Summary

We discussed Mordell's theorem that the group of rational points on an elliptic curve is finitely generated.

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

Next lecture: Integral points on elliptic curves, congruent numbers.