3 $E(\mathbb{Q})$

Let $E$ be the elliptic curve $y^2 = ax^3 + bx^2 + cx + d$, and define $E(\mathbb{Q})$ as the set of all points $(x, y)$ with $x$ and $y$ in $\mathbb{Q}$ and that satisfy the equation $E$. If we set $O$ to be a rational point, then the group structure on $E(\mathbb{R})$ restricts naturally to the group structure on $E(\mathbb{Q})$. In particular, if $O$ is set to be $[0, 1, 0]$, then we have a group. The structure of this group has been fascinating to mathematicians for decades. Some extremely important and difficult theorems have been proved about the group, but there are still unanswered questions that many people have been trying to solve.

3.1 Finitely Generated Groups

We begin by making sure we have the proper background in group theory.

**Definition 3.1.** Let $G$ be an abelian group. If $g \in G$, define $mg, m \in \mathbb{Z}$, to be $g$ added to itself $m$ times. If $m$ is negative, then we think of this as adding $-g$. If $m$ is 1, then this is just $g$. If $m$ is zero, then $0g = O$.

**Example 3.2.** Let $\mathbb{Z}^2$ be the set of pairs of integers. Then $5(1, 3) = (5, 15)$, $-3(1, 0) = (-3, 0)$, etc.

**Example 3.3.** Let $\mathbb{Z}/m\mathbb{Z}$ be the set $\{0, 1, 2, \ldots, m-1\}$ with addition defined mod $m$. Then, say in $\mathbb{Z}/10\mathbb{Z}$, we have $3 \cdot 2 = 6, 5 \cdot 2 = 0, -3 \cdot 2 = 4$, etc.

**Example 3.4.** Let $E(\mathbb{Q})$ be the group of rational points for the elliptic curve $y^2 = x^3 + 1$ with $O = [0, 1, 0]$. Then

$$3(2, 3) = (2, 3) + (2, 3) + (2, 3) = (0, 1) + (2, 3) = (-1, 0)$$

If we have an element or a set of elements of $G$, we can take these integer multiples of our element/elements, and this will give us a subgroup of $G$. We are especially interested when this subgroup is actually $G$ itself.

**Definition 3.5.** Let $G$ be an abelian group, and let $X \subseteq G$ be a subset. We say that $X$ generates $G$ if every element of $G$ can be written as an integer combination of elements of $X$.

**Example 3.6.** The group $G$ will always generate $G$.

**Example 3.7.** The set $\{0\}$ will never generate $G$, unless $G = \{0\}$.

**Example 3.8.** The set $\{1\}$ generates $\mathbb{Z}$. It also generates $\mathbb{Z}/m\mathbb{Z}$ for any $m$.

**Example 3.9.** The set $\{(1, 0), (0, 1)\}$ generates $\mathbb{Z}^2$. The set $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ generates $\mathbb{Z}^3$. And so on. Think of this as a basis from linear algebra, only we are only using integers as opposed to real numbers.

**Example 3.10.** The set $\{1/2, 1/3, 1/4, 1/5, \ldots\}$ generates $\mathbb{Q}$. Slightly less obvious, the set $\{1/2, 1/3, 1/5, 1/7, 1/11, 1/13, 1/17, \ldots\}$ generates $\mathbb{Q}$. 

1
All groups can be generated, but sometimes the generating set has to be infinite. We have a lot more control over the group if we can find a generating set that is finite. Thus finitely generated sets deserve to be looked at explicitly.

**Definition 3.11.** Let $G$ be an abelian group. The group is **finitely generated** if there is a finite set $X \in G$ such that $X$ generates $G$.

**Example 3.12.** From our examples above, the sets $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}^n$ are finitely generated for any choice of $m$ or $n$.

**Example 3.13.** Given two abelian groups $G_1$ and $G_2$, let $G_1 \oplus G_2$ be the group of ordered pairs from $G_1$ and $G_2$. If $G_1$ and $G_2$ are finitely generated, then so is $G_1 \oplus G_2$.

**Example 3.14.** The sets $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Q}$ are NOT finitely generated. The set of complex and real numbers are both uncountable, and any finitely generated group must be countable (it’s a Foundations of Mathematics style proof). For the rationals, we need a better proof:

**Theorem 3.15.** The group $\mathbb{Q}$ is not finitely generated.

**Proof** Assume that $\mathbb{Q}$ is finitely generated. Then there is a finite set $X$ which generates $\mathbb{Q}$. Write $X$ as \{\(m_1/n_1, m_2/n_2, \ldots, m_k/n_k\}\}. Let \(p/q\) be a rational number where \(q\) is relatively prime to \(n_1n_2n_3\cdots n_k\) (such a \(q\) always exists: we could set \(q = n_1n_2n_3\cdots n_k + 1\)). Since any integer combinations of the \(m_i/n_i\’s\) will have a denominator that divides \(n_1n_2\cdots n_k\), the fraction \(p/q\) cannot be generated by \(X\). This is a contradiction, so $\mathbb{Q}$ is not finitely generated. \(\Box\)

**Example 3.16.** The circle group $C(\mathbb{Q})$ is not finitely generated. The proof is similar to the proof for rationals, and it is left as an exercise.

If we have a finitely generated group, then the structure of the group is very limited:

**Theorem 3.17.** If $G$ is a finitely generated abelian group, then

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

for some nonnegative integer $r$ and positive integers $n_1, \ldots, n_k$. Furthermore, we may enforce that $n_1|n_2$, $n_2|n_3$, $\ldots$, $n_{k-1}|n_k$. With this enforcement, the values of $r$, $n_1$, $n_2$, $\ldots$, $n_k$ are unique.

The congruence means an isomorphism. This means we can put the elements of $G$ and the elements of the other set in a one-to-one correspondence with each other, and the addition is preserved by this structure.

**Example 3.18.** Consider $E(\mathbb{Q})$ for the elliptic curve $y^2 = x^3 + 1$ with $O = [0, 1, 0]$. This set is finite, and hence obviously finitely generated. Specifically, it is isomorphic to the set $\mathbb{Z}/6\mathbb{Z}$ by the map:
Definition 3.19. Let \( g \in G \). The order of \( g \) is the smallest positive integer \( m \) such that \( mg = O \). If no such \( m \) exists, then the order is infinity.

Example 3.20. For \( y^2 = x^3 + 1 \), the order for each element of \( E(\mathbb{Q}) \) is the same as the order of the corresponding element in \( \mathbb{Z}/6\mathbb{Z} \), namely \( O \) has order 1, \((2,3)\) and \((2,-3)\) have order 6, \((0,1)\) and \((0,-1)\) have order 3, and \((-1,0)\) has order 2.

Example 3.21. Now consider \( E(\mathbb{Q}) \) for the elliptic curve \( y^2 = 2x^3 - x \). The point \((0,0)\) has order 2, while the point \((1,1)\) has order infinity. In particular, we have \( E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \), where the group is generated by the two elements \((0,0)\) and \((1,1)\). You should think of \( E(\mathbb{Q}) \) as two copies of \( \mathbb{Z} \): one copy is \( m(1,1) \), while the other copy is \( m(1,1) + (0,0) \).

So, why do we need to know about finitely generated groups? In the two examples we have seen, it looks like both of them are finitely generated. It turns out that this is true for any elliptic curve over the rationals:

Theorem 3.22. (Mordell, 1923) Let \( E(\mathbb{Q}) \) be the set of rational points on an elliptic curve with rational coefficients. Then \( E(\mathbb{Q}) \) is finitely generated.

This theorem is huge, and it was very unexpected. If you look at the rational points on a line or a quadratic, then the resultant group is not finitely generated. It would be more believable to expect that this trend would continue: that any time we look at a group of rational points on a curve, the group should not be finitely generated. The fact that the \( E(\mathbb{Q}) \) is finitely generated opens up a whole bunch of new questions.

3.2 Torsion of \( E(\mathbb{Q}) \)

Since our group \( E(\mathbb{Q}) \) is finitely generated, we know that the group has the form

\[
E(\mathbb{Q}) \cong \mathbb{Z}/r \times \mathbb{Z}/n_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_k\mathbb{Z}
\]

Our goal is to see if there are any restrictions on what structures are possible for \( E(\mathbb{Q}) \).

Definition 3.23. Let \( G \) be an abelian group. Define Tor(\( G \)) to be the set of all elements of \( g \) with finite order. This set is a group, and we call it the torsion subgroup.

Example 3.24. If \( G \) is a finite group, then Tor(\( G \)) = \( G \). If \( G \) is a finitely generated group from Theorem 3.17, then Tor(\( G \)) = \( \mathbb{Z}/r \times \mathbb{Z}/n_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_k\mathbb{Z} \).

Example 3.25. The torsion subgroup of \( \mathbb{Z}, \mathbb{Q}, \mathbb{R} \) or \( \mathbb{C} \) is just the identity.
So what kind of torsion subgroups can \( E(\mathbb{Q}) \) take? It turns out that we are very restricted on what we can get:

**Theorem 3.26. (Mazur, 1977)** The torsion subgroup \( \text{Tor}(E(\mathbb{Q})) \) is isomorphic to one of the following groups: \( \mathbb{Z}/n\mathbb{Z} \) for \( n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12 \) or \( \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \) for \( n = 2, 4, 6, 8 \).

The case when \( n = 1 \) means that our subgroup is \( \mathbb{Z}/\mathbb{Z} = \{0\} \), i.e., just the identity. So there are only fifteen different torsion subgroups possible. And we can get \( \mathbb{Z}/n\mathbb{Z} \) for all \( n \leq 12 \) EXCEPT for 11. The restriction on possible torsion subgroups is simply remarkable.

Of course, we have examples of elliptic curves with each possible subgroup:

**Example 3.27.** The following chart gives examples of elliptic curves with each of the possible torsion subgroups:

<table>
<thead>
<tr>
<th>Elliptic Curve</th>
<th>Tor(( E(\mathbb{Q}) ))</th>
</tr>
</thead>
<tbody>
<tr>
<td>( y^2 = x^3 - 2 )</td>
<td>( {0} )</td>
</tr>
<tr>
<td>( y^2 = x^3 + 8 )</td>
<td>( \mathbb{Z}/2\mathbb{Z} )</td>
</tr>
<tr>
<td>( y^2 = x^3 + 4 )</td>
<td>( \mathbb{Z}/3\mathbb{Z} )</td>
</tr>
<tr>
<td>( y^2 = x^3 + 4x )</td>
<td>( \mathbb{Z}/4\mathbb{Z} )</td>
</tr>
<tr>
<td>( y^2 - y = x^3 - x^2 )</td>
<td>( \mathbb{Z}/5\mathbb{Z} )</td>
</tr>
<tr>
<td>( y^2 = x^3 + 1 )</td>
<td>( \mathbb{Z}/6\mathbb{Z} )</td>
</tr>
<tr>
<td>( y^2 = x^3 + 43x + 166 )</td>
<td>( \mathbb{Z}/7\mathbb{Z} )</td>
</tr>
<tr>
<td>( y^2 + 7xy = x^3 + 16x )</td>
<td>( \mathbb{Z}/8\mathbb{Z} )</td>
</tr>
<tr>
<td>( y^2 + xy + y = x^3 - x^2 - 14x + 29 )</td>
<td>( \mathbb{Z}/9\mathbb{Z} )</td>
</tr>
<tr>
<td>( y^2 + xy = x^3 - x^2 - 14x + 29 )</td>
<td>( \mathbb{Z}/10\mathbb{Z} )</td>
</tr>
<tr>
<td>( y^2 + 43xy - 210y = x^3 - 210x^2 )</td>
<td>( \mathbb{Z}/12\mathbb{Z} )</td>
</tr>
<tr>
<td>( y^2 = x^3 - 4x )</td>
<td>( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} )</td>
</tr>
<tr>
<td>( y^2 = x^3 + 2x^2 - 3x )</td>
<td>( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} )</td>
</tr>
<tr>
<td>( y^2 + 5xy - 6y = x^3 - 3x^2 )</td>
<td>( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} )</td>
</tr>
<tr>
<td>( y^2 + 17xy - 120y = x^3 - 60x^2 )</td>
<td>( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} )</td>
</tr>
</tbody>
</table>

Note that many of these are not in standard form. It’s not that they could not be put in standard form (ALL elliptic curves can be put in standard form), but if we put them in standard form, we would have some messy fractions, and we are avoiding those.

The next question is: how do we find the elements of \( \text{Tor}(E(\mathbb{Q})) \)? As usual, this should be a horrendously difficult problem. We are fortunate that we do have one theorem that will help us out in special cases:

**Theorem 3.28. (Nagell-Lutz)** Let \( E \) be the elliptic curve \( y^2 = x^3 + ax + b \), where \( a \) and \( b \) are integers. Let \( \Delta = 4a^3 + 27b^2 \) be the discriminant of \( x^3 + ax + b \). If \( (x, y) \in \text{Tor}(E(\mathbb{Q})) \), then \( x \) and \( y \) are both integers, and either \( y = 0 \) or \( y^2 | \Delta \).

The discriminant formula is a bit different than what we had when we were studying \( E(\mathbb{R}) \). There are legitimate reasons for including or excluding the \(-16\) from the definition. For this theorem, it is better to include it.
Note that this is not an “if and only if” theorem. You can have a point \((x, y) \in E(\mathbb{Q})\) with both numbers integers and with \(y\) dividing \(\Delta\), but without \((x, y) \in \text{Tor}(E(\mathbb{Q}))\). It can happen.

**Example 3.29.** Let’s see how difficult it is to use Nagell-Lutz. We begin with the elliptic curve \(y^2 = x^3 - 43x + 166\). In our char above, we claimed that this curve has a torsion subgroup isomorphic to \(\mathbb{Z}/7\mathbb{Z}\). The discriminant for this curve is:

\[
\Delta = 4(-43)^3 + 27(166)^2 = 425,984 = (-1)(2^{15})(13)
\]

Nagell-Lutz says that \(y = 0\) or \(y^2\) divides \(\Delta\), so our options for \(y\) are:

\[
y = 0, \pm 1, \pm 2, \pm 2^2, \pm 2^3, \pm 2^4, \pm 2^5, \pm 2^6, \pm 2^7
\]

For each \(y\), plug it into \(y^2 = x^3 - 43x + 166\) and solve for \(x\). If the equation has an integer solution, then it is an option. We find that the points \((3, \pm 8), (-5, \pm 16)\) and \((11, \pm 32)\) are all in \(E(\mathbb{Q})\). Then you can check that all of these points have order seven, and so they, along with \([0, 1, 0]\), make up \(E(\mathbb{Q}) \cong \mathbb{Z}/7\mathbb{Z}\).

### 3.3 Rank of \(E(\mathbb{Q})\)

**BIG CONJECTURE:** Let \(r\) be a positive integer. Then there exists an elliptic curve with rank \(r\).

**Note:** While this conjecture is generally believed among researchers, the fact is that we only have examples of curves with rank \(\leq 28\). And we don’t have examples of ranks for all the numbers less than 28.

**Definitions:** Let \(E\) be an elliptic curve \(y^2 = x^3 + ax + b\) with \(a\) and \(b\) integers, and let \(E(\mathbb{Z}_n)\) be the set of all points \((x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n\) such that \(y^2 \equiv x^3 + ax + b \mod n\). Note that \(\mathbb{Z}_n\) is not a field unless \(n\) is prime, and so \(E(\mathbb{Z}_n)\) is not a group unless \(n\) is prime. But we still have the set.

Let \(X(n) = n + 1 - \#E(\mathbb{Z}_n)\).

The **Hecke \(L\)-series** for an elliptic curve \(E\) is defined to be

\[
L_E(s) = \sum_{n=1}^{\infty} \frac{X(n)}{n^s}
\]

(in reality, we need to exclude the values of \(n\) with \(n^2 \mid \Delta\)). The series \(L_E(s)\) is a series depending on \(s\), and it converges if \(Re(s) > 3/2\) (this follows from Hasse’s theorem and \(p\)-series, since \(|X(n)| < 2\sqrt{n}\)). As a function, \(L_E(s)\) is an analytic function for \(Re(s) > 3/2\). Through analytic continuation, we can extend \(L_E(s)\) to all complex numbers. Thus we have a function \(L_E(s)\).

**BIG CONJECTURE (Birch and Swinnerton-Dyer):** The rank of \(E\) is equal to the order of the zero of \(L_E(s)\) at \(s = 1\). In particular, the rank of \(E\) is zero iff \(L_E(1) \neq 0\).