Basics.

An abelian group \((G, +)\) is a set \(G\) along with a binary operation \(+\) which satisfies the following:

**Closure:** For all \(a, b \in G\), \(a + b \in G\).

**Associativity:** For all \(a, b, c \in G\), \(a + (b + c) = (a + b) + c\).

**Commutativity:** For all \(a, b \in G\), \(a + b = b + a\).

**Identity:** There exists an element 0 such that for all \(a \in G\), \(a + 0 = a\).

**Inverses:** For all \(a \in G\), there exists an element \(-a\) such that \(a + (-a) = 0\).

An abelian group is finitely generated if there exist finitely many elements \(a_1, a_2, \ldots, a_k\) such that any element of \(G\) can be expressed as a sum \(c_1a_1 + c_2a_2 + \ldots + c_ka_k\), where the \(c_i\) are integers and multiplication denotes repeated addition. Note that this representation need not be unique, so any finite group is also finitely generated.

A subgroup of an abelian group \(G\) is a set \(H \subseteq G\) which is itself a group under the same operation. For any \(a \in G\), \(a + H = \{a + h : h \in H\}\) is a coset of \(H\). \(a\) is called a representative of the coset \(a + H\). Any two cosets of \(H\) are either equal or disjoint. The index of \(H\) in \(G\), denoted \([G : H]\), is the number of disjoint cosets of \(H\). For \(a \in G\), the order of \(a\) is the minimum positive integer \(k\) such that \(ka\) is the identity, or \(\infty\) if there is no such \(k\).

Cubics.

We will only be discussing cubic curves written in Weierstrass normal form:

\[ y^2 = x^3 + ax^2 + bx + c. \]

![Figure 1](image-url)

Figure 1: From left to right, the curves \(y^2 = x^3\), \(y^2 = x^3 - x\), \(y^2 = x^3 + x\), and \(y^2 = x^3 + x^2\).

A rational point on a cubic is a point whose \(x\)- and \(y\)-coordinates are both rational. Let \(C\) denote the curve \(C : y^2 = x^3 + ax^2 + bx + c\), where \(a, b,\) and \(c\) are rational. Let \(C(\mathbb{Q})\) denote the set of rational points on \(C\), together with the point at infinity. Define the operation \(*\) on \(C(\mathbb{Q})\) as follows:

Let \(P\) and \(Q\) be rational points on \(C\). By Bézout’s theorem (see reverse), the line \(L\) through \(P\) and \(Q\) intersects \(C\) in exactly three points (counting multiplicities), which may include complex points and points at infinity. Let \(P * Q\) be the third intersection point of this line with \(C\). (In the case where \(P = Q\), \(L\) is tangent to \(C\) at \(P\).)

Unfortunately, \(*\) is not a group operation. In general, \(P * (Q * R) \neq (P * Q) * R\). However, we can amend this fairly easily. For \(P, Q\) on \(C\), define \(P + Q\) to be the reflection of \(P * Q\) over the horizontal axis.
It turns out that $C(\mathbb{Q})$ is an abelian group under the operation $+$:

**Closure:** Because if $L$ intersects $C$ in two rational points, it intersects $C$ in a third as well.

**Associativity:** The Cayley-Bacharach theorem should be useful.

**Commutativity:** This should be obvious.

**Identity:** Try the vertical point at infinity.

**Inverses:** If $P = (x, y)$, then $-P = (x, -y)$.

**Mordell’s Theorem.**

**Theorem:** Define $C : y^2 = x^3 + ax^2 + bx + c$ with $a$, $b$, and $c \in \mathbb{Q}$. Then the group $(C(\mathbb{Q}), +)$ as defined earlier is finitely generated.

To prove this, we use four lemmas. For a rational number $x = \frac{m}{n}$ in lowest terms, define the **height** of $x$ by

$$H(x) = H\left(\frac{m}{n}\right) = \max\{|m|, |n|\}.$$ 

In turn, this is used to define the height of a point by

$$h(P) = h((x, y)) = \log H(x).$$

The following four lemmas imply Mordell’s theorem.

**Lemma 1.** For every real number $M$, the set \( \{ P \in C(\mathbb{Q}) : h(P) \leq M \} \) is finite.

**Lemma 2.** Let $P_0$ be a fixed rational point on $C$. There is some constant $\kappa_0$, depending on $P_0$ and $C$, so that

$$h(P + P_0) \leq 2h(P) + \kappa_0$$

for all $P \in C(\mathbb{Q})$.

**Lemma 3.** There is a constant $\kappa$, depending on $C$, so that

$$h(2P) \geq 4h(P) - \kappa$$

for all $P \in C(\mathbb{Q})$.

**Lemma 4.** The index $[C(\mathbb{Q}) : 2C(\mathbb{Q})]$ is finite.

**Useful Results.**

**Bézout’s Theorem:** If $f(x,y)$ and $g(x,y)$ are polynomials in $x$ and $y$ of total degrees $m$ and $n$, respectively, then the curves $C : f(x,y) = 0$ and $D : g(x,y) = 0$ intersect in precisely $mn$ points (counting multiplicities), which may include complex points and points at infinity.

**Cayley-Bacharach Theorem:** If we consider the nine intersection points of any two cubics, then any other cubic which passes through eight of them also passes through the ninth.

**Nagell-Lutz Theorem:** Consider a non-singular cubic $C : y^2 = x^3 + ax^2 + bx + c$, with $a$, $b$, and $c$ rational. Let $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ be the discriminant of $C$. If $P = (x, y)$ is a point of finite order in $C(\mathbb{Q})$, then either $y = 0$ (so $P$ has order 2) or $y | D$.

**Mazur’s Theorem:** Let $C$ be a non-singular cubic curve and let $P$ be a point in $C(\mathbb{Q})$ of finite order $m$. Then either $1 \leq m \leq 10$ or $m = 12$. 

2