MORDELL'S THEOREM

SARAH MARSHALL

We will be roughly following the proof for Mordell's Theorem given in [1]. In order to properly understand and prove Mordell's Theorem, the concept of height must be defined and four lemmas must be stated and proven.

Definition: Let x be a rational number such that $x = \frac{m}{n}$ is in lowest terms. The height of x, $H(x)$ is defined as

$$H(x) = H\Big(\frac{m}{n}\Big) = \max\{|m|, |n|\}$$

The height of rational number measures its complexity. The following property of height makes it very useful for the proof of Mordell's Theorem:

Property: (Finiteness Property of the Height) The set of all rational numbers whose height is less than some fixed number is a finite set.

Proof. Suppose the height of a rational number $x = \frac{m}{n} < M$ where M is some fixed number. Then $|m|, |n| < M$ and thus there is only a finite amount of choices for m and n.

□

When considering a ration point $P = (x, y)$ on the elliptic curve $C : y^2 = x^3 + ax^2 + bx + c$, with $a, b, c \in \mathbb{Z}$, the height of the point P is the height of the x-coordinate. The height of the point at infinity, $\mathcal{O}$ is defined to be 1.

Since the height does not behave additively with respect to the addition law for points on the curve, it is more useful to use

$$h(P) = \log H(P).$$

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

Proof. The finiteness property of height applies to the rational points on C with respect to the height, $h(P)$, defined above. Suppose M is positive number. Since the height of a point P is defined as the height of the x-coordinate of P and P is a rational point, there are finitely many x-coordinates with height less than M. Each x-coordinate has only two choices for a y-coordinate. Thus, there are finitely many rational points P on the curve C such that $h(P) \leq M$.

□

Now, using the height of a point, $h(P)$, Lemma 2, relates the height of P_0 and $P + P_0$.

Lemma 2: Let P_0 be a fixed rational point of C. There is a constant κ_0 that depends on P_0 and on a, b, c such that

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

Proof. If $P_0 = \mathcal{O}$, then the lemma is trivial. Thus, assume $P_0 \neq \mathcal{O}$ so $P_0 = (x_0, y_0)$. Take $P = (x, y)$. It suffices to prove the lemma for all P except $P = P_0, -P_0,$ and $\mathcal{O}$. This is good because $x \neq x_0$ so we don't need to use the duplication formula. By excluding these points, κ_0 will depend on these points. This does not pose an issue since κ_0 will already depend P_0, a, b, c and thus excluding these points will not effect the inequality.
Now suppose

$$P + P_0 = (\zeta, \eta)$$

Finding the height of $P + P_0$ amounts to finding the height of ζ. Can write ζ in terms of (x_0, y_0) and (x, y) as such

$$\zeta + x + x_0 = \lambda^2 - a \text{ with } \lambda = \frac{y - y_0}{x - x_0}$$

$$\Leftrightarrow \zeta = \left(\frac{y - y_0}{x - x_0}\right)^2 - a - x - x_0$$

$$= \frac{(y - y_0)^2 - (a + x + x_0)(x - x_0)^2}{(x - x_0)^2}$$

$$= \frac{y^2 - 2yy_0 + y_0^2 - (a + x + x_0)(x^2 - 2xx_0 + x_0^2)}{x^2 - 2xx_0 + x_0^2}$$

$$= \frac{y^2 - 2yy_0 + y_0^2 - (ax^2 + x^3 - 2xx_0a - x_0x^2 - xx_0^2 + ax_0^2 + x_0^3)}{x^2 - 2xx_0 + x_0^2}$$

$$= \frac{ax^2 + bx + c - 2yy_0 + y_0^2 - (ax^2 - 2xx_0a - x_0x^2 - xx_0^2 + ax_0^2 + x_0^3)}{x^2 - 2xx_0 + x_0^2}$$

$$= \frac{bx + c - 2yy_0 + y_0^2 - (-2xx_0a - x_0x^2 - xx_0^2 + ax_0^2 + x_0^3)}{x^2 - 2xx_0 + x_0^2}$$

$$= \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$$

where $A, B, \ldots, G$ depend on a, b, c and x_0, y_0. Multiply by least common denominator so that $A, B, \ldots, G$ are integers.
Since $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$ with x and y in lowest terms and $\gcd(m, e) = \gcd(n, e) = 1$, can rewrite ζ as

$$\zeta = \frac{A\frac{n}{e^3} + B\left(\frac{m}{e^2}\right)^2 + C\frac{m}{e^2} + D}{E\left(\frac{m}{e^2}\right)^2 + F\frac{m}{e^2} + G}$$

Clearing the denominators gives

$$\zeta = \frac{Ane + Bm + Cme^2 + De^4}{Em + Fme^2 + Ge^4}$$

Since it is not known if ζ is in lowest terms,

$$H(\zeta) \leq \max\{|Ane + Bm + Cme^2 + De^4|, |Em + Fme^2 + Ge^4|\}$$

Need to put bounds on m, e^2, and n. When looking at the height of a point $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, $H(P) = \max\{|m|, |e^2|\}$. Thus, $|m| \leq H(P)$ and $|e^2| \leq H(P)$.
Now put bound on n. By substituting in $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$ to $y^2 = x^3 + ax^2 + bx + c$ and clearing the denominator,

$$n^2 = m^3 + am^2e^2 + bme^4 + ce^2$$

Taking absolute values and using triangle inequality gives

$$\begin{aligned}|n^2| &\leq |m^3| + |am^2e^2| + |bme^4| + |ce^2| \\ &\leq H(P)^3 + aH(P)^3 + bH(P)^3 + cH(P)^3\end{aligned}$$

Thus, $|n| \leq KH(P)^{3/2}$ for $K = \sqrt{1 + |a| + |b| + |c|}$.
Therefore,

$$\begin{aligned}|Ane + Bm + Cme^2 + De^4| &\leq |Ane| + |Bm| + |Cme^2| + |De^4| \\ &\leq (|AK| + |B| + |C| + |D|)H(P)^2\end{aligned}$$

and

$$\begin{aligned}|Em + Fme^2 + Ge^4| &\leq |Em| + |Fme^2| + |Ge^4| \\ &\leq (|E| + |F| + |G|)H(P)^2\end{aligned}$$

Hence,

$$H(P + P_0) = H(\zeta) \leq \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}H(P)^2$$

Take logarithm

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

where

$$\kappa_0 = \log\max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}$$

□

Lemma 3: For rational points P on the curve $C : y^2 = x^3 + ax^2 + bx$, there is a constant κ depending on a, b, c such that

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

Proof. As with Lemma 2, assume that the inequality holds for all P except for points in a finite fixed set. In this, lemma, points P such that $2P = \mathcal{O}$ will not be considered. As with Lemma 2, excluding these points will cause κ to depend on them but since κ already depends on a, b, c, exclusion of these points will not effect the inequality. Suppose $P = (x, y)$ is a point on C and $2P = (\zeta, \eta)$. Then

$$\zeta + 2x = \lambda^2 - a \text{ with } \lambda = \frac{f'(x)}{2y}$$

Since $y^2 = f(x) = x^3 + ax^2 + bx + c$, can write

$$\zeta = \left(\frac{f'(x)}{2y}\right)^2 - a - 2x$$

$$\zeta = \frac{f'(x)^2 - (4a + 8x)f(x)}{4f(x)}$$

$$\zeta = \frac{(3x^2 + 2ax + b)^2 - 8x^4 - 12ax^3 - 4a^2x^2 - 8bx^2 - 4abx - 8cx - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

$$\zeta = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

Since $f(x)$ and $f'(x)$ have no common complex roots, due to the fact that $f(x)$ is non-singular from assumption, the polynomials with integer coefficients that divide to give ζ have no common complex roots.
Since want to show $h(2P) \geq 4h(P) - \kappa$ and $h(P) = h(x)$, $h(2P) = h(\zeta)$, it suffices to show that $h(\zeta) \geq 4h(x) - \kappa$. Use the following Lemma to do this.

Lemma: Let $\phi(X)$ and $\psi(X)$ be polynomials with integer coefficients and no common complex roots. Let d be the maximum of the degrees of ϕ and ψ.
(a) There is an integer $R \geq 1$, depending on ϕ and ψ, so that for all rational numbers $\frac{m}{n}$,

$$\gcd\left(n^d\phi\Big(\frac{m}{n}\Big), n^d\psi\Big(\frac{m}{n}\Big)\right) \qquad \text{divides } R.$$

(b) There are constants κ_1 and κ_2, depending on ϕ and ψ, so that for all rational numbers $\frac{m}{n}$ that are not roots of ψ,

$$d \cdot h\Big(\frac{m}{n}\Big) - \kappa_1 \leq h\Big(\frac{\phi(m/n)}{\psi(m/n)}\Big) \leq d \cdot h\Big(\frac{m}{n}\Big) + \kappa_2$$

Proof. (a) Since both ϕ and ψ have degree less than or equal to d, $n^d\phi\Big(\frac{m}{n}\Big)$ and $n^d\psi\Big(\frac{m}{n}\Big)$ are integers which means that their gcd can be determined.
Without loss of generality, assume that ϕ has degree d and ψ has degree $e \leq d$. So

$$n^d\phi\Big(\frac{m}{n}\Big) = a_0m^d + a_1m^{d-1}n + \cdots + a_dn^d$$

and

$$n^d\psi\Big(\frac{m}{n}\Big) = b_0m^en^{d-e} + b_1m^{e-1}n^{d-e+1} + \cdots + b_en^d$$

Having no common roots means that $\phi(X)$ and $\psi(X)$ are relatively prime in $\mathbb{Q}[X]$ and generate a unit ideal. So

$$F(X)\phi(X) + G(X)\psi(X) = 1$$

where $F(X)$ and $G(X)$ are polynomials with coefficients in $\mathbb{Q}$. Let the maximum degree of these two polynomials be denoted by D. Multiply $F(X)$ and $G(X)$ by large A so that $AF(X)$ and $AG(X)$ have integer coefficients. Substitute in $X = \frac{m}{n}$ and multiply by An^{D+d} to get

$$n^DAF\Big(\frac{m}{n}\Big) \cdot n^d\phi\Big(\frac{m}{n}\Big) + n^DAG\Big(\frac{m}{n}\Big) \cdot n^d\psi\Big(\frac{m}{n}\Big) = An^{D+d}$$

Suppose $\delta = \gcd\left(n^d\phi\Big(\frac{m}{n}\Big), n^d\psi\Big(\frac{m}{n}\Big)\right)$. Then since $n^DAF\Big(\frac{m}{n}\Big)$ and $n^DAG\Big(\frac{m}{n}\Big)$ are integers, $\delta | An^{D+d}$. The desired result is that $\delta | R$ where R doesn't depend on m, n. Thus, look at

$$An^{D+d-1}n^d\phi\Big(\frac{m}{n}\Big) = Aa_0m^dn^{D+d-1} + Aa_1m^{d-1}n^{D+d} + \cdots + Aa_dn^{D+2d-1}$$

Since δ divides $n^d\phi\Big(\frac{m}{n}\Big)$ and An^{D+d}, then δ divides $Aa_0m^dn^{D+d-1}$. So, δ divides

$\gcd\left(An^{D+d}, Aa_0 m^d n^{D+d-1}\right)$. Since $\gcd(m,n)=1$, δ divides $Aa_0 n^{D+d-1}$. Iterate this argument with $An^{D+d-2} n^d \phi\left(\frac{m}{n}\right)$ to find δ divides $Aa_0^2 n^{D+d-1}$. Continuing this argument results in δ divides Aa_0^{D+d}. Thus, set $R = Aa_0^{D+d}$ and therefore, $\gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right)$ divides R.

(b) First prove the lower bound. Assume $\frac{m}{n}$ is not a root of ϕ. Again, without loss of generality, assume that ϕ has degree d and ψ has degree $e \le d$. Say

$$\zeta = \frac{\phi(m/n)}{\psi(m/n)} = \frac{n^d\phi(m/n)}{n^d\psi(m/n)}$$

Then $H(\zeta) = \max\{|n^d\phi(m/n)|, |n^d\psi(m/n)|\}$. Since there may be common factors, use part (a) to bound $H(\zeta)$ from below. Since $\max\{a,b\} \ge \frac{1}{2}(a+b)$,

$$H(\zeta) \ge \frac{1}{R}\max\{|n^d\phi(m/n)|, |n^d\psi(m/n)|\}$$

$$\ge \frac{1}{2R}\left(|n^d\phi(m/n)| + |n^d\psi(m/n)|\right)$$

Consider

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

Now look at the quotient

$$\frac{H(\zeta)}{H\left(\frac{m}{n}\right)^d} \ge \frac{1}{2R}\frac{|n^d\phi(m/n)| + |n^d\psi(m/n)|}{\max\{|m|^d, |n|^d\}}$$

$$= \frac{1}{2R}\frac{|\phi(m/n)| + |\psi(m/n)|}{\max\{|(m/n)|^d, 1\}}$$

Define a function $p(t)$ such that

$$p(t) = \frac{|\phi(t)| + |\psi(t)|}{\max\{|t|^d, 1\}}$$

Since the $\phi(t)$ has degree d, the numerator will have a polynomial of degree equal to or greater than the degree of the polynomial in the denominator. Thus, as $|t| \to \infty$, $p(t)$ will be a non-zero number. Since $p(t)$ is bounded below, there exists a constant $C_1 > 0$ such that $p(t) \ge C_1$ for all t.Thus,

$$\frac{H(\zeta)}{H\left(\frac{m}{n}\right)^d} \ge \frac{1}{2R}\cdot p\left(\frac{m}{n}\right)$$

$$H(\zeta) \ge \frac{C_1}{2R}\cdot H\left(\frac{m}{n}\right)^d$$

Take logarithm to get

$$h(\zeta) \ge dh\left(\frac{m}{n}\right) - \kappa_1 \text{ with } \kappa_1 = \log\frac{2R}{C_1}$$

Now prove the upper bound. Want to show that

$$h\Big(\frac{\phi(m/n)}{\psi(m/n)}\Big) \leq d \cdot h\Big(\frac{m}{n}\Big) + \kappa_2$$

with κ_2 depending on ϕ and ψ. Again, take

$$\zeta = \frac{\phi(m/n)}{\psi(m/n)} = \frac{n^d\phi(m/n)}{n^d\psi(m/n)}$$

Since it is not known if this is in lowest terms, the height could be less than $\max\{|n^d\phi(m/n)|, |n^d\psi(m/n)|\}$. Thus,

$$\begin{aligned} H(\zeta) &\leq \max\{|n^d\phi(m/n)|, |n^d\psi(m/n)|\} \\ &\leq \max\{|\phi(m/n)|, |\psi(m/n)|\}|n^d| \end{aligned}$$

Consider

$$H\Big(\frac{m}{n}\Big)^d = \max\{|m|^d, |n|^d\}$$

Now look at the quotient

$$\begin{aligned} \frac{H(\zeta)}{H\Big(\frac{m}{n}\Big)^d} &\leq \frac{\max\{|\phi(m/n)|, |\psi(m/n)|\}|n^d|}{\max\{|m|^d, |n|^d\}} \\ &\leq \max\{|\phi(m/n)|, |\psi(m/n)|\} \end{aligned}$$

This is true because if $\max\{|m|^d, |n|^d\} = |n|^d$, then $\frac{|n|^d}{|n|^d} = 1$. If $\max\{|m|^d, |n|^d\} = |m|^d$, then $\frac{|n|^d}{|m|^d} \leq 1$. So,

$$H(\zeta) \leq H\Big(\frac{m}{n}\Big)^d \cdot \max\{|\phi(m/n)|, |\psi(m/n)|\}$$

Take logarithm

$$h(\zeta) \leq dh\Big(\frac{m}{n}\Big) + \kappa_2 \text{ with } \kappa_2 = \log(\max\{|\phi(m/n)|, |\psi(m/n)|\})$$

$\square$

To finish the proof for Lemma 3, see that from the previous Lemma, $h(\zeta) \geq dh\Big(\frac{m}{n}\Big) - \kappa_1$ with κ_1 depending on ϕ and ψ. Since the maximum degree of the polynomials in the numerator and denominator of ζ is 4, can substitute to get

$$h(\zeta) \geq 4h\Big(\frac{m}{n}\Big) - \kappa_1$$

Also use that $h(P) = h(x) = h(m/n)$, $h(2P) = h(\zeta)$, and the fact that the polynomials in the numerator and denominator of ζ depend on a, b, c to get $h(P) = h(x)$, $h(2P) = h(\zeta)$ which is the desired product.

$\square$

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

In order to fully prove Lemma 4, need to consider both the reducible and irreducible cases. Only the proof of the reducible case will be given.
The Reducible Case:

This case considers when $C : y^2 = f(x)$ is reducible, meaning $f(x)$ has at least one rational root or at least one rational point of order two. For simplicity, define $\Gamma = C(\mathbb{Q})$. Suppose x_0 is a rational root of $f(x)$. Then, if $f(x)$ is replaced with $f(x - x_0)$, then it can be assumed that $f(x) = x^3 + ax^2 + bx$ with integer coefficients. Since this change of coordinates takes $(x_0, 0)$ to $(0, 0) = T$, then T is a rational point on C such that $2T = \mathcal{O}$.

Since the index $[\Gamma : 2\Gamma]$, or equivalently the order of the group $\Gamma/2\Gamma$, is of interest, want to look at a map from $C \to C$ such that $P \mapsto 2P$ where P is a rational point on C. Instead of trying to determine one operation that gives this result, look at the composition of two different operations, one from $C \to \bar{C}$ and the other from $\bar{C} \to C$ where $\bar{C}$ is a curve defined as

$$\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$$

with

$$\bar{a} = -2a \text{ and } \bar{b} = a^2 - 4b$$

Consider

$$\bar{\bar{C}} : y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x$$

with

$$\bar{\bar{a}} = -2\bar{a} = 4a \text{ and } \bar{\bar{b}} = \bar{a}^2 - 4\bar{b} = 4a - 4(a^2 - 4b) = 16b$$

So,

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

This means that $\bar{\bar{C}}$ is isomorphic to C with the map $(x, y) \mapsto (\frac{1}{4}x, \frac{1}{8}y)$ and so $\Gamma \cong \bar{\bar{\Gamma}}$.

The following proposition will prove that specific maps from $C \to \bar{C}$ and $\bar{C} \to C$ are homomorphisms that will be useful in proving Lemma 4.

Proposition: Let C and $\bar{C}$ be elliptic curves given by the equations

$$C : y^2 = x^3 + ax^2 + bx \text{ and } \bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x,$$

where

$$\bar{a} = -2a \text{ and } \bar{b} = a^2 - 4b.$$

Let $T = (0, 0) \in C$.

(a) There is a homomorphism $\phi : C \to \bar{C}$ defined by:

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right), & \text{if } P = (x, y) \neq \mathcal{O}, T, \\ \bar{\mathcal{O}}, & \text{if } P = \mathcal{O} \text{ or } P = T. \end{cases}$$

The kernel of ϕ is $\{\mathcal{O}, T\}$.

(b) There is a homomorphism $\psi : \bar{C} \to C$ defined by:

$$\psi(\bar{P}) = \begin{cases} \left(\frac{\bar{y}^2}{\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b})}{\bar{x}^2}\right), & \text{if } \bar{P} = (x, y) \neq \bar{\mathcal{O}}, \bar{T}, \\ \mathcal{O}, & \text{if } \bar{P} = \bar{\mathcal{O}} \text{ or } \bar{P} = \bar{T}. \end{cases}$$

(c) Define $h : \bar{\bar{C}} \to C$ with the map $(x, y) \mapsto (\frac{1}{4}x, \frac{1}{8}y)$. Now say $\bar{\phi} = h \circ \psi$. The composition $\psi \circ \phi : C \to C$ is the multiplication by two map,

$$\bar{\phi} \circ \phi(P) = 2P$$

Proof. (a) First, need to check that this map is well defined. Thus, need to ensure that $\bar{P} = (\bar{x}, \bar{y})$ satisfies $\bar{C}$.

$$\begin{aligned}\bar{x}^3 + \bar{a}\bar{x}^2 + \bar{b}\bar{x} &= \bar{x}(\bar{x}^2 - 2a\bar{x} + (a^2 - 4b)) \\ &= \frac{y^2}{x^2}\Big(\frac{y^4}{x^4} - 2a\frac{y^2}{x^2} + (a^2 - 4b)\Big) \\ &= \frac{y^2}{x^2}\Big(\frac{y^4 - 2ay^2x^2 + (a^2 - 4b)(x^4)}{x^4}\Big) \\ &= \frac{y^2}{x^2}\Big(\frac{(y^2 - ax^2)^2 - 4bx^4}{x^4}\Big) \\ &= \frac{y^2}{x^6}\Big((x^3 + bx)^2 - 4bx^4\Big) \\ &= \Big(\frac{y(x^2 - b)}{x^2}\Big)^2 \\ &= \bar{y}\end{aligned}$$

Now, need to show that ϕ is a homomorphism which amounts to proving that

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2) \text{ for all } P_1, P_2 onC$$

If P_1 or P_2 is $\mathcal{O}$, then assuming $P_1 = \mathcal{O}$ without loss of generality,

$$\phi(P_1 + P_2) = \phi(\mathcal{O} + P_2) = \phi(P_2) = \bar{\mathcal{O}} + \phi(P_2) = \phi(\mathcal{O}) + \phi(P_2)$$

If P_1 or P_2 is T, then assuming $P_1 = T$ without loss of generality, need to show that $\phi(T+P) = \phi(P)$. Since P is a point (x, y),

$$P + T = (x, y) + (0, 0) = \Big(\frac{b}{x}, -\frac{by}{x^2}\Big)$$

Now, write $P + T$ as

$$P + T = (x(P + T), y(P + T)) \text{ and } \phi(P + T) = (\bar{x}(P + T), \bar{y}(P + T))$$

Thus,

$$\bar{x}(P + T) = \Big(\frac{y(P + T)}{x(P + T)}\Big)^2 = \Big(\frac{-by/x^2}{(b/x)}\Big)^2 = \frac{y^2}{x^2} = \bar{x}(P)$$

$$\bar{y}(P + T) = \Big(\frac{y(P + T)(x(P + T)^2 - b)}{(x(P + T))^2}\Big) = \Big(\frac{(-by/x^2)((b/x)^2 - b)}{(b/x)^2}\Big) = \bar{y}(P)$$

Hence, by this argument, $\phi(T + P) = \phi(P)$ unless $P = T$. Then,

$$\phi(T + T) = \phi(\mathcal{O}) = \bar{\mathcal{O}} = \bar{\mathcal{O}} + \bar{\mathcal{O}} = \phi(T) + \phi(T)$$

Now need to show that ϕ takes negatives to negatives. Since $-P = -(x, y) = (x, -y)$,

$$\phi(-P) = \phi(x, -y) = \Big(\Big(\frac{-y}{x}\Big)^2, \frac{-y(x^2 - b)}{x^2}\Big) = -\phi(x, y) = -\phi(P)$$

Thus, all that is left to show is that $P_1 + P_2 + P_3 = \mathcal{O}$ implies that $\phi(P_1) + \phi(P_2) + \phi(P_3) = \bar{\mathcal{O}}$ where P_1, P_2, P_3 are not $\mathcal{O}$ or T. The equation $P_1 + P_2 + P_3 = \mathcal{O}$ is equvalent to saying that P_1, P_2, P_3 lie on a line that intersects C. Suppose the equation for that line is given by

$y = \lambda x + \nu$. Want to show that there is line intersecting $\bar{C}$ at the points $\phi(P_1), \phi(P_2), \phi(P_3)$. Suppose that a line that intersects $\bar{C}$ is given by

$$y = \bar{\lambda} x + \bar{\nu}$$

where

$$\bar{\lambda} = \frac{\nu\lambda - b}{\nu} \text{ and } \bar{\nu} = \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu}$$

Thus, need to check that the points $\phi(P_1), \phi(P_2), \phi(P_3)$ lie on this line.

First check that $\phi(P_1) = \phi(x_1, y_1) = (\bar{x_1}, \bar{y_1})$ is on the line.

$$\begin{aligned}
\bar{\lambda}\bar{x_1} + \bar{\nu} &= \frac{\nu\lambda - b}{\nu}\Big(\frac{y_1^2}{x_1^2}\Big) + \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu} \\
&= \frac{y_1^2(\nu\lambda - b) + x_1^2(\nu^2 - a\nu\lambda + b\lambda^2)}{\nu x_1^2} \\
&= \frac{(y_1^2 - x_1^2 a)\nu\lambda + (x_1^2\lambda^2 - y_1^2)b + x_1^2\nu^2}{\nu x_1^2} \\
&= \frac{(x_1^3 + bx_1)\nu\lambda + (x_1\lambda - y_1)(x_1\lambda + y_1)b + x_1^2\nu^2}{\nu x_1^2} \\
&= \frac{(x_1^3 + bx_1)\nu\lambda + (-\nu)(x_1\lambda + y_1)b + x_1^2\nu^2}{\nu x_1^2} \\
&= \frac{(x_1^3 + bx_1)\lambda - (x_1\lambda + y_1)b + x_1^2\nu}{x_1^2} \\
&= \frac{x_1^2(x_1\lambda + \nu) - y_1 b}{x_1^2} \\
&= \frac{y_1(x_1^2 - b)}{x_1^2} \\
&= \bar{y_1}
\end{aligned}$$

The same is true for $\phi(P_2)$ and $\phi(P_3)$.

To give the complete proof that this is a homomorphism, would need to show that $\bar{x}(P_1), \bar{x}(P_2), \bar{x}(P_3)$ are the roots of the equation $(\bar{\lambda}x + \bar{\nu})^2 - \bar{f}(x) = 0$.

The kernel of ϕ is very clearly $\{\mathcal{O}, T\}$ since these are the only two elements that map to $\bar{\mathcal{O}}$.

(b) Using part (a), a homomorphism $\bar{\phi} : \bar{C} \to \bar{\bar{C}}$ can be defined by the same equations for ϕ, just adding bars over a and b. Since $\bar{\bar{C}} \to C$ is an isomorphism, $\psi : \bar{C} \to C$ can be written as composition of $\bar{\phi}$ with this isomorphism to give a well defined homomorphism.

(c) Need to show that the composition map $\bar{\phi} \circ \phi$ gives a multiplication by two map. The duplication formula for a point P is given by

$$2P = 2(x, y) = \Big(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2)}{8y^3}\Big)$$

So,

$$\begin{aligned}
\bar{\phi} \circ \phi(P) = \bar{\phi} \circ \phi(x, y) &= \bar{\phi}\Big(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\Big) \\
&= \left(\frac{\left(\frac{y(x^2-b)}{x^2}\right)^2}{\left(\frac{y^2}{x^2}\right)^2}, \frac{\frac{y(x^2-b)}{x^2}\left(\left(\frac{y^2}{x^2}\right)^2 - (a^2-4b)\right)}{\left(\frac{y^2}{x^2}\right)^2} \right) \\
&= \left(\frac{(x^2-b)^2}{y^2}, \frac{(x^2-b)(y^4-(a^2-4b)x^4)}{y^3x^2} \right)
\end{aligned}$$

Since $y^2 = x^3 + ax^2 + bx = x(x^2 + ax + b)$, $y^4 = x^2(x^2 + ax + b)^2$ and so

$$\begin{aligned}
&= \left(\frac{(x^2-b)^2}{y^2}, \frac{(x^2-b)(x^2(x^2+ax+b)^2-(a^2-4b)x^4)}{y^3x^2} \right) \\
&= \left(\frac{(x^2-b)^2}{y^2}, \frac{(x^2-b)((x^2+ax+b)^2-(a^2-4b)x^2)}{y^3} \right) \\
&= \left(\frac{(x^2-b)^2}{y^2}, \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{y^3} \right) \\
&= 2(\frac{x}{4}, \frac{y}{8}) = 2P
\end{aligned}$$

To show that $\phi \circ \bar{\phi}(\bar{P}) = 2(\bar{P})$, use that since ϕ is a homomorphism,

$$\phi(2P) = \phi(P+P) = \phi(P) + \phi(P) = 2\phi(P)$$

Thus,

$$\phi \circ \bar{\phi}(\bar{P}) = \phi \circ \bar{\phi}(\phi(P)) = \phi(2P) = 2\phi(P)$$

The above argument only works when x and y are not zero. Thus, need to check points of order 2.

$$\bar{\phi} \circ \phi(T) = \bar{\phi}(\bar{\mathcal{O}}) = \mathcal{O}$$
$$\bar{\phi} \circ \phi(\mathcal{O}) = \bar{\phi}(\bar{\mathcal{O}}) = \mathcal{O}$$

Therefore, $\bar{\phi} \circ \phi$ is a multiplication by two map.

□

The description of the homomorphism ϕ shows that ϕ maps $\Gamma \to \bar{\Gamma}$. It is not obvious that a given rational point in $\bar{\Gamma}$ comes from a rational point in Γ. Thus, need to look at the image of ϕ. Denote the subgroup of rational points in $\bar{\Gamma}$ obatined by applying ϕ to Γ as $\phi(\Gamma)$.

Claim:
(i) $\bar{\mathcal{O}} \in \phi(\Gamma)$
(ii) $\bar{T} = (0, 0) \in \phi(\Gamma)$ if and only if $\bar{b} = a^2 - 4b$ is a perfect square.
(iii) Let $\bar{P} = (\bar{x}, \bar{y}) \in \bar{\Gamma}$ with $\bar{x} \neq 0$. Then $\bar{P} \in \phi(\Gamma)$ if and only if $\bar{x}$ is the square of a rational number.

Proof. (i) Since $\phi(\mathcal{O}) = \bar{\mathcal{O}}$ and $\mathcal{O} \in \Gamma$, $\bar{\mathcal{O}} \in \phi(\Gamma)$.

(ii) In order for $\bar{T} = (0,0) \in \phi(\Gamma)$, need to find a point P in Γ such that $\bar{x}(P) = \frac{y^2}{x^2} = 0$. If $x = 0$, then $P = T = (0,0)$. This can not be the case because $\phi(T) = \bar{\mathcal{O}}$ and not $\bar{T}$. Thus, need to find a point in Γ such that $y = 0$

$$0 = x^3 + ax^2 + bx = x(x^2 + ax + b)$$

The case where $x = 0$ has already been ruled out. Thus, look at the case where $0 = x^2 + ax + b$. By the quadratic formula, this equation has a non-zero rational root if and only if $a^2 - 4b$ is a perfect square.

(iii) Suppose $\bar{P} = (\bar{x}, \bar{y}) \in \bar{\Gamma}$ with $\bar{x} \neq 0$ and $\bar{P} \in \phi(\Gamma)$. Then $\bar{x} = \frac{y^2}{x^2}$ so $\bar{x}$ is the square of a rational number.

Now suppose $\bar{P} = (\bar{x}, \bar{y}) \in \bar{\Gamma}$ with $\bar{x} \neq 0$ and $\bar{x} = w^2$ where w is a rational number. Need to find a point in Γ that is mapped to $\bar{P} = (\bar{x}, \bar{y})$. Since $\mathcal{O}$ and T are in the kernel of ϕ, if $(\bar{x}, \bar{y})$ is in $\phi(\Gamma)$ then the points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ map to $(\bar{x}, \bar{y})$ where

$$x_1 = \frac{1}{2}\Big(w^2 - a + \frac{\bar{y}}{w}\Big), \qquad y_1 = x_1 w$$
$$x_2 = \frac{1}{2}\Big(w^2 - a - \frac{\bar{y}}{w}\Big), \qquad y_2 = -x_2 w$$

Since $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are rational points, just need to show that $P_i = (x_i, y_i) \in C$ for $i = 1, 2$ and $\phi(P_i) = (\bar{x}, \bar{y})$. To show that P_i is on C, need to show that

$$\bar{x_i} = x_i + a + \frac{b}{x_i} = \frac{y_i^2}{x_i^2}$$

Want to get b in terms of x_i. It turns out that

$$\begin{aligned} x_1 x_2 &= \frac{1}{4}\Big((w^2 - a) - \frac{\bar{y^2}}{w^2}\Big) \\ &= \frac{1}{4}\Big((\bar{x} - a) - \frac{\bar{y^2}}{\bar{x}}\Big) \\ &= \frac{1}{4}\Big(\frac{\bar{x}^3 - 2a\bar{x}^2 + a^2 - \bar{y^2}}{\bar{x}}\Big) \\ &= \frac{1}{4}\Big(\frac{\bar{y}^2 + 4b\bar{x} - \bar{y^2}}{\bar{x}}\Big) \\ &= b \end{aligned}$$

This combined with the fact that $\frac{y_i}{x_i} = \pm w$ from the definitions of y_1 and y_2 gives

$$\frac{y_i^2}{x_i^2} = x_i + a + \frac{b}{x_i} \Leftrightarrow w^2 = x_1 + a + x_2$$

Thus, it suffices to show that $w^2 = x_1 + a + x_2$ is true. Using the definitions of x_1 and x_2,

$$\begin{aligned} x_1 + a + x_2 &= \frac{1}{2}\Big(w^2 - a + \frac{\bar{y}}{w}\Big) + a + \frac{1}{2}\Big(w^2 - a - \frac{\bar{y}}{w}\Big) \\ &= \frac{1}{2}\Big(w^2 - a + \frac{\bar{y}}{w} + w^2 - a - \frac{\bar{y}}{w}\Big) + a \end{aligned}$$

$$= w^2$$

Now all that is left to show is for $i = 1, 2$ and $\phi(P_i) = (\bar{x}, \bar{y})$. Thus, need to show

$$\frac{y_i^2}{x_i^2} = \bar{x} \text{ and } \frac{y_i(x_i^2 - b)}{x_i^2} = \bar{y}$$

Since $\frac{y_i}{x_i} = \pm w$ and $\bar{x} = w^2$,

$$\frac{y_i^2}{x_i^2} = w^2 = \bar{x}$$

Now, use $b = x_1 x_2$ and definitions of y_1, x_1, y_2, and x_2 to show $\frac{y_i(x_i^2 - b)}{x_i^2} = \bar{y}$.

$$\frac{y_1(x_1^2 - b)}{x_1^2} = \frac{x_1 w(x_1^2 - x_1 x_2)}{x_1^2} = w(x_1 - x_2) = w\Big(\frac{1}{2}\Big(w^2 - a + \frac{\bar{y}}{w}\Big) - \frac{1}{2}\Big(w^2 - a - \frac{\bar{y}}{w}\Big)\Big) = \bar{y}$$

$$\frac{y_2(x_2^2 - b)}{x_2^2} = \frac{-x_2 w(x_2^2 - x_1 x_2)}{x_2^2} = w(x_1 - x_2) = w\Big(\frac{1}{2}\Big(w^2 - a + \frac{\bar{y}}{w}\Big) - \frac{1}{2}\Big(w^2 - a - \frac{\bar{y}}{w}\Big)\Big) = \bar{y}$$

□

If it can be shown that the indices $(\bar{\Gamma} : \phi(\Gamma))$ and $(\Gamma : \psi(\bar{\Gamma}))$ are finite, the fact that $(\Gamma : 2\Gamma)$ is finite will follow. It will be enough to prove that one of these indicies is finite.

Proposition: Let $\mathbb{Q}^*$ be the multiplicative group of non-zero rational numbers and let $\mathbb{Q}^{*2}$ denote the group of squares of elements of $\mathbb{Q}^*$ such that

$$\mathbb{Q}^{*2} = \{u^2 : u \in \mathbb{Q}^*\}$$

Define a map $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ as follows:

$$\alpha(P) = \begin{cases} 1 \mod \mathbb{Q}^{*2} & \text{if } P = \mathcal{O} \\ b \mod \mathbb{Q}^{*2} & \text{if } P = T \\ x \mod \mathbb{Q}^{*2} & \text{if } P = (x, y), x \neq 0 \end{cases}$$

(a) The map $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ described above is a homomorphism.
(b) The kernel of α is the image $\psi(\bar{\Gamma})$. Hence α induces a one-to-one homomorphism

$$\Gamma/\psi(\bar{\Gamma}) \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$$

(c) Let $p_1, p_2, \ldots, p_t$ be the distinct primes dividing b. Then the image of α is contained in the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ consisting of the elements

$$\{\pm p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} : \text{ each } e_i \text{ equals 0 or 1}\}$$

(d) The index $(\Gamma : \psi(\bar{\Gamma}))$ is at most 2^{t+1}.

Proof. (a) Need to show that α is a homomorphism which amounts to proving that

$$\alpha(P_1 + P_2) = \alpha(P_1)\alpha(P_2) \text{ for all } P_1, P_2 \in \Gamma$$

If P_1 or P_2 is $\mathcal{O}$, then assuming $P_1 = \mathcal{O}$ without loss of generality,

$$\alpha(P_1 + P_2) = \alpha(\mathcal{O} + P_2) = \alpha(P_2) = 1 \cdot \alpha(P_2) = \alpha(\mathcal{O})\alpha(P_2)$$

If P_1 or P_2 is T, then assuming $P_1 = T$ without loss of generality, need to show that $\alpha(T+P) = b \cdot \alpha(P) = b \cdot x$. Since P is a point (x, y),

$$P + T = (x, y) + (0, 0) = \left(\frac{b}{x}, -\frac{by}{x^2}\right)$$

Then,

$$\alpha(P + T) = \frac{b}{x}$$

Since $\alpha(P) = x = \frac{1}{x} \cdot x^2 \equiv \frac{1}{x} \mod \mathbb{Q}^{*2}$,

$$\alpha(P + T) = \frac{b}{x} = b \cdot \frac{1}{x} = \alpha(T) \cdot \alpha(P)$$

Hence, by this argument, $\alpha(T + P) = \alpha(T) \cdot \alpha(P)$ unless $P = T$. Since $\alpha(T) = b = \frac{1}{b} \cdot b^2 \equiv \frac{1}{b} \mod \mathbb{Q}^{*2}$, then

$$\alpha(T + T) = \alpha(\mathcal{O}) = 1 = \frac{b}{b} = b \cdot \frac{1}{b} = \alpha(T) \cdot \alpha(T)$$

Now need to show that α takes negatives to negatives. Since $-P = -(x, y) = (x, -y)$,

$$\alpha(-P) = \alpha(x, -y) = x = x^2 \cdot \frac{1}{x} \equiv \frac{1}{x} \mod \mathbb{Q}^{*2} = \frac{1}{\alpha(x, y)} = \alpha(P)^{-1} \mod \mathbb{Q}^{*2}$$

Thus, all that is left to show is that $P_1 + P_2 + P_3 = \mathcal{O}$ implies that $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1 \mod \mathbb{Q}^{*2}$ where P_1, P_2, P_3 are not $\mathcal{O}$ or T. The equation $P_1 + P_2 + P_3 = \mathcal{O}$ is equvalent to saying that P_1, P_2, P_3 lie on a line that intersects C. Suppose the equation for that line is given by $y = \lambda x + \nu$, and the intersection points have x-coordinates x_1, x_2, x_3. These x-coordinates are roots of the equation

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0$$

Therefore,

$$x_1 + x_2 + x_3 = \lambda^2 - a$$
$$x_1x_2 + x_2x_3 + x_2x_3 = b - 2\lambda\nu$$
$$x_1x_2x_3 = \nu^2 - c$$

Since $c = 0$, $x_1x_2x_3 = \nu^2 \equiv 1 \mod \mathbb{Q}^{*2}$. Hence $\alpha(P_1)\alpha(P_2)\alpha(P_3)x_1x_2x_3 = \nu^2 \equiv 1 \mod \mathbb{Q}^{*2}$.

(b) From the Claim, $\psi(\bar{\Gamma}) = \{(x, y) \in \Gamma : x \in \mathbb{Q}^{2*}\} \cup \{\mathcal{O}\} \cup \{T\}$ (if b is a square). Thus, for every point P in $\{(x, y) \in \Gamma : x \in \mathbb{Q}^{2*}\}$, $\alpha(P) = 1 \mod \mathbb{Q}^{*2}$ since x is a square. By definition, $\alpha(\mathcal{O}) = 1 \mod \mathbb{Q}^{*2}$. Since $\alpha(T) = b \mod \mathbb{Q}^{*2}$, if b is a square, $\alpha(T) = 1 \mod \mathbb{Q}^{*2}$. Thus, the kernel of α is $\psi(\bar{\Gamma})$.

(c) Need to determine what rational numbers can be the x-coordinate of a point in Γ. It is known that $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$. Then,

$$y^2 = x^3 + ax^2 + bx \Leftrightarrow \frac{n}{e^3}^2 = \frac{m}{e^2}^3 + a\frac{m}{e^2}^2 + b\frac{m}{e^2} \Leftrightarrow n^2 = m^3 + am^2e^2 + bme^4 = m(m^2 + ame^2 + be^4)$$

This equation expresses a square as the product of two integers. Let $d = \gcd(m, m^2 + ame^2 + be^4)$. Since d divides m and $m^2 + ame^2 + be^4$, d must divide be^4. Since the assumption is that m and e are relatively prime, then d divides b. Thus, every prime that divides m is of even power except for perhaps primes that divide b. Thus, $\alpha(P) = x = \frac{m}{e^2} \equiv \pm p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ mod $\mathbb{Q}^{*2}$ where each e_i equals 0 or 1.

(d) The subgroup $\{\pm p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} :$ each e_i equals 0 or 1$\}$ has exactly 2^{t+1} elements where t is the number of distinct primes dividing b. Since $\Gamma/\psi(\bar{\Gamma})$ maps one-to-one with the subgroup, the index $(\Gamma : \psi(\bar{\Gamma}))$ is at most 2^{t+1}.
The proof for the finiteness of the index $(\Gamma : \psi(\bar{\Gamma}))$ is the same except putting bars on everything.

$\square$

Lemma: Let A and B be abelian groups, and supppose that $\phi : A \to B$ and $\psi : B \to A$ are homomorphisms satisfying

$$\psi \circ \phi(a) = 2a \quad \text{for all } a \in A \quad \text{and} \quad \phi \circ \psi(b) = 2b \quad \text{for all } b \in B$$

Suppose further that $\phi(A)$ has finite index in B and $\psi(B)$ has finite index in A. Then $2A$ has finite index in A. More precisely, the indicies satisfy

$$(A : 2A) \leq (A : \psi(B))(B : \phi(A))$$

Proof. Since $\phi(A)$ has finite index in B and $\psi(B)$ has finite index in A, there are elements $b_1, \ldots, b_n \in B$ that represent the cosets $\phi(A)$ in B and elements $a_1, \ldots, a_n \in A$ that represent the cosets $\psi(B)$ in A. Thus, can find $b \in b_i + \phi(A)$ for some $1 \leq i \leq n$ and $a \in a_j + \psi(B)$ for some $1 \leq j \leq m$. Suppose $b = b_i + \phi(a')$ for some $1 \leq i \leq n$ and $a' \in A$ and $a = a_j + \psi(b)$ for some $1 \leq j \leq m$ and $b \in B$. Then,

$$\begin{aligned} a &= a_j + \psi(b) \\ &= a_j + \psi(b_i + \phi(a')) \\ &= a_j + \psi(b_i) + \psi(\phi(a')) \\ &= a_j + \psi(b_i) + 2a' \end{aligned}$$

Therefore, a can be written as the sum of an element in the set $\{a_j + \psi(b_i) | 1 \leq j \leq m, 1 \leq i \leq n\}$ and an element in $2A$ which implies that the set $\{a_j + \psi(b_i) | 1 \leq j \leq m, 1 \leq i \leq n\}$ contains all of the representatives of cosets of $2A$ in A. Thus, $2A$ has a finite index in A.

$\square$

Notice that if $A = \Gamma$ and $B = \bar{\Gamma}$, the index $[\Gamma : 2\Gamma]$ is finite. Thus, $[C(\mathbb{Q}) : 2C(\mathbb{Q})]$ is finite.
Mordell's Theorem: Let C be a non-singular cubic curve given by an equation

$$C : y^2 = x^3 + ax^2 + bx$$

where a and b are integers. Then the group of rational points $C(\mathbb{Q})$ is a finitely generated abelian group.

Proof. Let $Q_1, Q_2, \ldots, Q_n$ be representatives for the cosets in $\Gamma/2\Gamma$. For all points P in Γ, there exsists i_1 depending on P such that $P - Q_{i_1} \in 2\Gamma$. Since P is in one of the cosets, say $P - Q_{i_1} = 2P_1$ for $P_1 \in \Gamma$. Iterating this process shows that for $Q_{i_1}, \ldots, Q_{i_m} \in \{Q_1, Q_2, \ldots, Q_n\}$ and $P_1, \ldots, P_m \in \Gamma$,

$$P_1 - Q_{i_2} = 2P_2$$

$$P_2 - Q_{i_3} = 2P_3$$
$$\dots$$
$$P_{m-1} - Q_{i_m} = 2P_m$$

Now, rearranging and substituting the equations gives

$$P = Q_{i_1} + 2P_1 = Q_{i_1} + 2Q_{i_2} + 4P_2 = \dots Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \dots + 2^{m-1}Q_{i_m} + 2^m P_m$$

Applying Lemma 2 and replacing P_0 with $-Q_i$ gives

$$h(P - Q_i) \leq 2h(P) + \kappa_i$$

for all $P \in \Gamma$. Do this for each $Q_1, Q_2, \dots, Q_n$. Take $\kappa' := \max\{\kappa_1, \dots, \kappa_n\}$. This can be done due to Lemma 4 which says that there are finitely many $Q_i's$. Then,

$$h(P - Q_i) \leq 2h(P) + \kappa'$$

for all $P \in \Gamma$ with $1 \leq i \leq n$. Now use Lemma 3.

$$\begin{aligned} h(2P_j) &\geq 4h(P_j) - \kappa \\ \Leftrightarrow 4h(P_j) &\leq h(2P_j) + \kappa \\ &= h(P_{j-1} - Q_{i_j}) + \kappa \\ &\leq 2h(P_{j-1}) + \kappa' + \kappa \\ \Leftrightarrow h(P_j) &\leq \frac{h(P_{j-1})}{2} + \frac{\kappa' + \kappa}{4} \\ &= \frac{3h(P_{j-1})}{4} - \frac{h(P_{j-1}) - (\kappa' + \kappa)}{4} \end{aligned}$$

If $h(P_{j-1}) \geq \kappa' + \kappa$,

$$h(P_j) \leq \frac{3h(P_{j-1})}{4}$$

This means that as long as $h(P_{j-1}) \geq \kappa' + \kappa$ for a point P_j, the next point has a much smaller height. This condition can be satisfied for any point because any number multiplied by $\frac{3}{4}$ repeatedly will get close to zero.

It has been shown that every element $P \in \Gamma$ can be written as

$$P = a_1 Q_1 + a_2 Q_2 + \dots + a_n Q_n + 2^m R$$

for integers $a_1, \dots, a_n$ and R such that $h(R) \geq \kappa' + \kappa$. Therefore,

$$\{Q_1, Q_2, \dots, Q_n\} \cup \{R \in \Gamma : h(R) \geq \kappa' + \kappa\}$$

generates Γ. By Lemma 1 and Lemma 4, this set if finite and thus finished the proof that Γ is finitely generated.

□

References

[1] Silverman, J. H.; Tate, J. T. Rational Points on Elliptic Curves. *Undergraduate Texts in Mathematics* **2015**.