Finishing the Proof of Mordell's Theorem

Fanxin Wu

December 28, 2021

Mordell's Theorem: Strategy

Let $E : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve with rational coefficients. Denote the group of rational points by $E(\mathbb{Q})$. The proof that $E(\mathbb{Q})$ is finitely generated is based on four lemmas:

1. $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ is finite.
2. $h(P + P_0) \leq 2h(P) + \kappa_0$
3. $h(2P) \geq 4h(P) - \kappa$
4. (weak Mordell) The quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

We first prove the weak Mordell Theorem assuming $E(\mathbb{Q})$ has a point of order two, or equivalently $f(x) = x^3 + ax^2 + bx + c$ has a rational root. By translation we may assume $c = 0$. Note that $T = (0, 0)$ is on E. Also $b \neq 0$ since we assume E to be smooth.

We first prove the weak Mordell Theorem assuming $E(\mathbb{Q})$ has a point of order two, or equivalently $f(x) = x^3 + ax^2 + bx + c$ has a rational root. By translation we may assume $c = 0$. Note that $T = (0, 0)$ is on E. Also $b \neq 0$ since we assume E to be smooth.

Then we can define a new curve $\overline{E} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x$, where $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$. There is a homomorphism $\phi : E \to \overline{E}$ defined as follows:

$$\phi(P) = \begin{cases} \overline{\mathcal{O}}, & P = \mathcal{O} \text{ or } P = T \\ (\overline{x}, \overline{y}) = \left(\dfrac{y^2}{x^2}, y\left(\dfrac{x^2 - b}{x^2} \right) \right), & P = (x, y), x \neq 0 \end{cases}$$

ϕ restricts to a homomorphism $E(\mathbb{Q}) \to \overline{E}(\mathbb{Q})$.

The definition of $\overline{E}$ and ϕ can be explained via uniformization by Weierstrass $\wp$ functions[1]. There is also a more direct explanation in *Lectures on Elliptic Curves* by Cassels[2].

The definition of $\overline{E}$ and ϕ can be explained via uniformization by Weierstrass $\wp$ functions[1]. There is also a more direct explanation in *Lectures on Elliptic Curves* by Cassels[2].

$$\mathcal{C}: \quad Y^2 = X(X^2 + aX + b),$$

the point of order 2 being $(0,0)$. The function on the right hand side may not have a double root, so

$$b \neq 0, \qquad a^2 - 4b \neq 0.$$

We take $\mathbf{Q}$ to be the ground field. Let $\mathbf{x} = (x, y)$ be a *generic point* of $\mathcal{C}$; that is, x is transcendental and y is defined by

$$y^2 = x(x^2 + ax + b).$$

The field $\mathbf{Q}(x, y)$ is known as the *function field* of $\mathcal{C}$ over $\mathbf{Q}$.

Let

$$\mathbf{x}_1 = \mathbf{x} + (0,0).$$

The transformation

$$\mathbf{x} \to \mathbf{x}_1$$

is an automorphism of $\mathbf{Q}(x, y)$ of order 2. We will find the fixed field.

We can apply this procedure to $\overline{E}$ again to get $\overline{\overline{E}}$ and $\overline{\phi}$. Direct calculation shows $\overline{\overline{E}}$ is $y^2 = x^3 + 4ax^2 + 16bx$, which can also be written as $(\frac{y}{8})^2 = (\frac{x}{4})^3 + a(\frac{x}{4})^2 + b(\frac{x}{4})$. Therefore it is isomorphic to E and has the same rational points. Denote by ψ the composition of $\overline{\phi}$ and the isomorphism from $\overline{\overline{E}}$ to E.

We can apply this procedure to $\overline{E}$ again to get $\overline{\overline{E}}$ and $\overline{\phi}$. Direct calculation shows $\overline{\overline{E}}$ is $y^2 = x^3 + 4ax^2 + 16bx$, which can also be written as $(\frac{y}{8})^2 = (\frac{x}{4})^3 + a(\frac{x}{4})^2 + b(\frac{x}{4})$. Therefore it is isomorphic to E and has the same rational points. Denote by ψ the composition of $\overline{\phi}$ and the isomorphism from $\overline{\overline{E}}$ to E.

$\psi \circ \phi : E \to E$ is the duplication map. Recall the explicit formula

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

We can apply this procedure to $\overline{E}$ again to get $\overline{\overline{E}}$ and $\overline{\phi}$. Direct calculation shows $\overline{\overline{E}}$ is $y^2 = x^3 + 4ax^2 + 16bx$, which can also be written as $(\frac{y}{8})^2 = (\frac{x}{4})^3 + a(\frac{x}{4})^2 + b(\frac{x}{4})$. Therefore it is isomorphic to E and has the same rational points. Denote by ψ the composition of $\overline{\phi}$ and the isomorphism from $\overline{\overline{E}}$ to E.

$\psi \circ \phi : E \to E$ is the duplication map. Recall the explicit formula

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

Let $\Gamma = E(\mathbb{Q})$, $\overline{\Gamma} = \overline{E}(\mathbb{Q})$. We want to prove that $\Gamma/2\Gamma = \Gamma/\psi \circ \phi(\Gamma)$ is finite. It suffices to prove that $\overline{\Gamma}/\phi(\Gamma)$ and $\Gamma/\psi(\overline{\Gamma})$ are finite: for a sequence $A \xrightarrow{f} B \xrightarrow{g} C$, if $B/f(A)$ and $C/g(B)$ are finite, then $C/g \circ f(A)$ is also finite. We prove the finiteness of $\Gamma/\psi(\overline{\Gamma})$.

Proposition 1

Any rational point on the curve $y^2 = x^3 + ax^2 + bx + c$ *is of the form* $(\frac{m}{e^2}, \frac{n}{e^3})$*, where* $(m, e) = 1$ *and* $(n, e) = 1$*.*

Proof.

Suppose $(\frac{m}{M}, \frac{n}{N})$ is a rational point in reduced form. WLOG $M, N > 0$. Plugging this into the equation gives us

$$\frac{n^2}{N^2} = \frac{m^3 + am^2M + bmM^2 + cM^3}{M^3}$$

These are both in reduced form, so $N^2 = M^3$, which implies $N = e^3$ and $M = e^2$ for some e. □

We now study $\psi(\overline{\Gamma})$. We can describe it very concretely:

We now study $\psi(\overline{\Gamma})$. We can describe it very concretely:

Lemma 2

(i) $\mathcal{O} \in \psi(\overline{\Gamma})$.
(ii) $T = (0,0) \in \psi(\overline{\Gamma})$ *iff* $b \in \mathbb{Q}^{*2}$.
(iii) If $P = (x,y) \in \Gamma$ *and* $x \neq 0$, *then* $P = (x,y) \in \psi(\overline{\Gamma})$ *iff* $x \in \mathbb{Q}^{*2}$.

We now study $\psi(\overline{\Gamma})$. We can describe it very concretely:

Lemma 2

(i) $\mathcal{O} \in \psi(\overline{\Gamma})$.
(ii) $T = (0,0) \in \psi(\overline{\Gamma})$ *iff* $b \in \mathbb{Q}^{*2}$.
(iii) If $P = (x,y) \in \Gamma$ *and* $x \neq 0$, *then* $P = (x,y) \in \psi(\overline{\Gamma})$ *iff* $x \in \mathbb{Q}^{*2}$.

Proof of (ii):

$$\begin{aligned} T \in \psi(\overline{\Gamma}) &\Leftrightarrow \exists (\overline{x},\overline{y}) \in \overline{\Gamma}, \frac{\overline{y}^2}{\overline{x}^2} = 0 \\ &\Leftrightarrow \exists \overline{x} \neq 0, \overline{x}^3 - 2a\overline{x}^2 + (a^2 - 4b)\overline{x} = 0 \\ &\Leftrightarrow \exists \overline{x}, \overline{x}^2 - 2a\overline{x} + (a^2 - 4b) = 0 \\ &\Leftrightarrow 4a^2 - 4(a^2 - 4b) \in \mathbb{Q}^2 \\ &\Leftrightarrow b \in \mathbb{Q}^{*2} \end{aligned}$$

We now study $\psi(\overline{\Gamma})$. We can describe it very concretely:

Lemma 2

(i) $\mathcal{O} \in \psi(\overline{\Gamma})$.
(ii) $T = (0,0) \in \psi(\overline{\Gamma})$ *iff* $b \in \mathbb{Q}^{*2}$.
(iii) If $P = (x,y) \in \Gamma$ *and* $x \neq 0$, *then* $P = (x,y) \in \psi(\overline{\Gamma})$ *iff* $x \in \mathbb{Q}^{*2}$.

Proof of (iii): Suppose $(x,y) \in \Gamma$ and $x \neq 0$. If $x = \frac{\overline{y}^2}{\overline{x}^2}$ for some $(\overline{x},\overline{y}) \in \overline{\Gamma}$ then of course it is a rational square. Conversely if $x = w^2$ then one can explicitly write down a point that maps to P, see [1].

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

$\alpha(\mathcal{O}) = 1 \mod \mathbb{Q}^{*2}$

$\alpha(T) = b \mod \mathbb{Q}^{*2}$

$\alpha(x, y) = x \mod \mathbb{Q}^{*2}$ for $x \neq 0$.

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

$\alpha(\mathcal{O}) = 1 \mod \mathbb{Q}^{*2}$

$\alpha(T) = b \mod \mathbb{Q}^{*2}$

$\alpha(x, y) = x \mod \mathbb{Q}^{*2}$ for $x \neq 0$.

Note that the kernel of α is exactly $\psi(\overline{\Gamma})$, so α induces an embedding of $\Gamma/\psi(\overline{\Gamma})$ into $\mathbb{Q}^*/\mathbb{Q}^{*2}$ (once we show that α is a homomorphism). We don't need to worry about $\psi(\overline{\Gamma})$ henceforth.

α is a homomorphism

$\alpha(P) = \alpha(x, y) = \alpha(x, -y) = \alpha(-P)$. The group $\mathbb{Q}^*/\mathbb{Q}^{*2}$ has exponent 2, so any element is its own inverse. This shows α preserves inverse.

α is a homomorphism

$\alpha(P) = \alpha(x, y) = \alpha(x, -y) = \alpha(-P)$. The group $\mathbb{Q}^*/\mathbb{Q}^{*2}$ has exponent 2, so any element is its own inverse. This shows α preserves inverse.

Now we show that $\alpha(P_1 + P_2) = \alpha(P_1) \cdot \alpha(P_2)$. Let $P_1 + P_2 = -P_3$. For simplicity assume all three points are different from $\mathcal{O}, T$. Since α preserves inverse, $\alpha(-P_3) = \alpha(P_1) \cdot \alpha(P_2)$ is the same as saying $\alpha(P_1) \cdot \alpha(P_2) \cdot \alpha(P_3) = 1 \mod \mathbb{Q}^{*2}$. If P_1, P_2, P_3 lie on a line $y = px + q$, then substituting this into $y^2 = x^3 + ax^2 + bx$ we get $x^3 + ax^2 + bx - (px + q)^2 = 0$, so $x_1 x_2 x_3 = q^2 = 1 \mod \mathbb{Q}^{*2}$.

Lemma 3

The image of α is finite.

Lemma 3

The image of α is finite.

Proof.

Suppose $(\frac{m}{e^2}, \frac{n}{e^3})$ is a rational point in reduced form. Substituting this into $y^2 = x^3 + ax^2 + bx$ and clearing denominators gives $n^2 = m(m^2 + ame^2 + be^4)$. Any integer can be uniquely written as dq^2, where d is a square-free integer. Suppose $m = dq^2$. If $p \mid d$, then for the product to be a square we must have $p \mid m^2 + ame^2 + be^4$; since $p \mid m$ we get $p \mid be^4$, and since $(m, e) = 1$ we get $p \mid b$. Since $m = d \mod \mathbb{Q}^{*2}$, $\alpha(\Gamma)$ is contained in the finite subgroup generated by -1 and all primes dividing b. □

Theorem

If E is an elliptic curve defined over $\mathbb{Q}$ that has a point of order 2, then $E(\mathbb{Q})$ is finitely generated.

Theorem

If E is an elliptic curve defined over $\mathbb{Q}$ that has a point of order 2, then $E(\mathbb{Q})$ is finitely generated.

Theorem

If E is an elliptic curve defined over a number field K, then $E(K)$ is finitely generated.

Theorem

If E is an elliptic curve defined over $\mathbb{Q}$ that has a point of order 2, then $E(\mathbb{Q})$ is finitely generated.

Theorem

If E is an elliptic curve defined over a number field K, then $E(K)$ is finitely generated.

The proof of number field case requires more machinery. For general rational case there is a quite elementary proof in Cassels' book; it's concise and has a typo; [3] may be helpful.

Let $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ be such that $f(x)$ has no rational root, i.e., irreducible (the proof actually also works for reducible case with minor modification, but for simplicity let's focus on irreducible case). Also we may assume $a, b, c \in \mathbb{Z}$.

Let $\theta, \theta', \theta'' \in \mathbb{A}$ be the roots of $f(x)$ and $K = \mathbb{Q}(\theta)$, $L = \mathbb{Q}(\theta, \theta', \theta'')$. Define a map $\alpha : E(\mathbb{Q}) \to K^*/{K^*}^2$ as follows

Let $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ be such that $f(x)$ has no rational root, i.e., irreducible (the proof actually also works for reducible case with minor modification, but for simplicity let's focus on irreducible case). Also we may assume $a, b, c \in \mathbb{Z}$.

Let $\theta, \theta', \theta'' \in \mathbb{A}$ be the roots of $f(x)$ and $K = \mathbb{Q}(\theta)$, $L = \mathbb{Q}(\theta, \theta', \theta'')$. Define a map $\alpha : E(\mathbb{Q}) \to K^*/{K^*}^2$ as follows

$$\alpha(\mathcal{O}) = 1 \mod {K^*}^2$$

$$\alpha(x, y) = x - \theta \mod {K^*}^2$$

α is a homomorphism

By the same argument as before, it suffices to show that if $P_1, P_2, P_3 \in E(\mathbb{Q})$ lie on a line $y = px + q$, then $\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1 \mod K^{*2}$. x_1, x_2, x_3 are the solutions to $f(x) - (px + q)^2 = 0$, so $x_1 - \theta, x_2 - \theta, x_3 - \theta$ are the solutions to $f(x + \theta) - (px + p\theta + q)^2 = 0$. The constant term of $f(x + \theta)$ is zero since θ is a root, so $(x_1 - \theta)(x_2 - \theta)(x_3 - \theta) = (p\theta + q)^2 = 1 \mod K^{*2}$.

The kernel of α is $2E(\mathbb{Q})$

Suppose $P = (x_0, y_0)$ is in the kernel, so $x_0 - \theta = 1 \mod K^{*2}$, or

$$x_0 - \theta = (p\theta^2 + q\theta + r)^2$$

for some $p, q, r \in \mathbb{Q}$, $p \neq 0$. Let $g(x) = px^2 + qx + r$, so

$$x_0 - \theta = g(\theta)^2$$

By Euclidean algorithm there exists $s, t, u \in \mathbb{Q}$ so that $(s - x)g(x) = tx + u \mod f(x)$, so

$$(s - \theta)g(\theta) = t\theta + u$$

Therefore

$$(s - \theta)^2(x_0 - \theta) = (s - \theta)^2 g(\theta)^2 = (t\theta + u)^2$$

This means $h(x) = (tx + u)^2 - (s - x)^2(x_0 - x)$ has a root θ. Since $h(x)$ has degree 3 and leading term coefficient 1, it must be equal to $f(x)$!

The kernel of α is $2E(\mathbb{Q})$

Consequently

$$(tx+u)^2-(s-x)^2(x_0-x)=f(x)$$

We can also rearrange it as

$$(tx+u)^2-f(x)=(s-x)^2(x_0-x)$$

Solving $(tx+u)^2-f(x)=0$ means finding the intersection points of $y=tx+u$ and $E: y^2=f(x)$, so by the above the line $y=tx+u$ intersects E twice at $(s,ts+u)$ and once at $(x_0,tx_0+u)=\pm P$. In either case $P\in 2E(\mathbb{Q})$.

The image of α is finite

Suppose $(\frac{m}{e^2}, \frac{n}{e^3})$ is a rational point in reduced form. We want to show there are only finitely many possibilities for $\frac{m}{e^2} - \theta$ modulo K^{*2}. Since $f(x) = (x - \theta)(x - \theta')(x - \theta'')$, we have

$$(\frac{n}{e^3})^2 = (\frac{m}{e^2} - \theta)(\frac{m}{e^2} - \theta')(\frac{m}{e^2} - \theta''), \text{ or}$$

$$n^2 = (m - \theta e^2)(m - \theta' e^2)(m - \theta'' e^2)$$

Passing to ideals in O_L, we have

$$(n)^2 = (m - \theta e^2)(m - \theta' e^2)(m - \theta'' e^2)$$

$$(n)^2 = (m - \theta e^2)(m - \theta' e^2)(m - \theta'' e^2)$$

Write $(m - \theta e^2)$ as IJ^2 where I is square-free. If P is a prime factor of I, then it must also divide either $(m - \theta' e^2)$ or $(m - \theta'' e^2)$. Say $P \mid (m - \theta' e^2)$. Note that

$$(m - \theta' e^2) - (m - \theta e^2) = (\theta - \theta')e^2$$
$$\theta(m - \theta' e^2) - \theta'(m - \theta e^2) = (\theta - \theta')m$$

Thus $P \mid (\theta - \theta')(e^2)$ and $P \mid (\theta - \theta')(m)$, and thus (because (e^2) and (m) are coprime) $P \mid (\theta - \theta')$.

$$(n)^2 = (m - \theta e^2)(m - \theta' e^2)(m - \theta'' e^2)$$

Write $(m - \theta e^2)$ as IJ^2 where I is square-free. If P is a prime factor of I, then it must also divide either $(m - \theta' e^2)$ or $(m - \theta'' e^2)$. Say $P \mid (m - \theta' e^2)$. Note that

$$(m - \theta' e^2) - (m - \theta e^2) = (\theta - \theta')e^2$$
$$\theta(m - \theta' e^2) - \theta'(m - \theta e^2) = (\theta - \theta')m$$

Thus $P \mid (\theta - \theta')(e^2)$ and $P \mid (\theta - \theta')(m)$, and thus (because (e^2) and (m) are coprime) $P \mid (\theta - \theta')$.

Let $\mathcal{F}(L)$ be the group of nonzero fractional ideals in L. To summarize, there are only finitely many possibilities for the ideal generated by $m - \theta e^2$ (equivalently $\frac{m}{e^2} - \theta$) modulo $\mathcal{F}(L)^2$.

Consider the sequence of maps

$$E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{\alpha} K^*/(K^*)^2 \xrightarrow{\psi} \mathcal{F}(K)/\mathcal{F}(K)^2 \xrightarrow{\eta} \mathcal{F}(L)/\mathcal{F}(L)^2$$

We have shown that the composition has finite image.

Consider the sequence of maps

$$E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{\alpha} K^*/(K^*)^2 \xrightarrow{\psi} \mathcal{F}(K)/\mathcal{F}(K)^2 \xrightarrow{\eta} \mathcal{F}(L)/\mathcal{F}(L)^2$$

We have shown that the composition has finite image.

$\ker \eta$ is finite because only finitely many prime ideals of K ramify in L. Also $\ker \psi$ can be shown to be finite using finiteness of class group and Dirichlet's unit theorem. So α has finite image.

Reference

J. Silverman, J. Tate, and J. Tate, *Rational Points on Elliptic Curves*.
Structure and Bonding, Springer-Verlag, 1992.

J. W. S. Cassels, *LMSST: 24 Lectures on Elliptic Curves*.
London Mathematical Society Student Texts, Cambridge University Press, 1991.

T. (https://math.stackexchange.com/users/763302/tobi), "Difficulties in understanding cassels proof of the weak mordell-weil theorem." Mathematics Stack Exchange.
URL:https://math.stackexchange.com/q/3594791 (version: 2020-03-25).