On a particular case of the Weak Mordell-Weil Theorem

Myeong Jae Jeon

Abstract

The weak Mordell-Weil theorem states that for any number field K and integer m, $mE(K)$ has a finite index in $E(K)$. By the descent theorem, combining with the existence of a height function on $E(K)$, the weak Mordell-Weil theorem implies the Mordell-Weil theorem. We prove a particular case of the weak Mordell-Weil theorem: $K = \mathbb{Q}$ and $m = 2$. Nonetheless, we obtain a proof of the Mordell-Weil theorem for an elliptic curve over a rational field which is important enough for its own sake.

1 A Useful Homomorphism

Let $\Gamma = E(\mathbb{Q})$ given by the equation $y^2 = x^3 + ax + b$ with integer coefficients be our elliptic curve. To avoid using some algebraic number theory, for example, some basic facts about the unit group and the ideal class group, we set an assumption that $f(x) = 0$ has at least one rational root x_0. Without losing of generality, we may assume that $x_0 = 0$. So our elliptic curve is of the form

$$C : y^2 = f(x) = x^3 + ax$$

Then a must be nonzero since the discriminant $\Delta = 4a^3 + 27b^2$ should be nonzero. For simplicity, denote $T = (0, 0)$. Note that $2T = \infty$ where ∞ is the infinity point on C.

Since we are interested in the factor group $\Gamma/2\Gamma$, we look into the addition map $P \mapsto 2P$. One can think of this map as a map of degree four in some sense since the x-coordinate of $2P$ is given by the rational function of degree four in the x-coordinate of P. We will express this map as a composition of two degree two maps. It is not clear what the degree of a map means but you may agree with this term soon. What is interesting here is that we factor the multiplication by two map on C through another curve $\overline{C}$.

The other curve $\overline{C}$ is given by the equation

$$\overline{C} : y^2 = x^3 + \bar{a}x, \quad \bar{a} = -4a$$

We may also consider another curve given by

$$\overline{\overline{C}} : y^2 = x^3 + \bar{\bar{a}}x, \quad \bar{\bar{a}} = -4\bar{a} = 16a$$

An interesting fact is that the curve $\overline{\overline{C}}$ is isomorphic the curve C via the map $(x, y) \to (\frac{1}{4}x, \frac{1}{8}y)$. Applying group laws on both curves, one can see that this map is indeed a group isomorphism. Now we define two homomorphisms between two curves C and $\overline{C}$.

Theorem 1.1. *Define* $\phi : C \to \overline{C}$ *by*

$$\phi(P) = \begin{cases} \left(\dfrac{y^2}{x^2}, \dfrac{y(x^2-a)}{x^2}\right), & \text{if } P = (x,y) \neq T, \infty, \\ \overline{\infty} & \text{if } P = \infty \text{ or } P = T \end{cases}$$

(a) ϕ *is a homomorphism with kernel* $\{\infty, T\}$
(b) Applying the same process to $\overline{C}$ *gives a map* $\overline{\phi} : C \to \overline{\overline{C}}$. *Compositing this map with the isomorphism* $\overline{\overline{C}} \to C$ *gives a homomorphism* $\psi : \overline{C} \to C$ *with kernel* $\{\overline{\infty}, T\}$.
(c) $\psi \circ \phi : C \to C$ *and* $\phi \circ \psi : \overline{C} \to \overline{C}$ *are the multiplication by two map.*

The proof is tedious applications of group laws on elliptic curves into several cases. Now we are ready to prove the weak Mordell-Weil theorem.

2 The Weak Mordell-Weil Theorem

Our proof is based on the following lemma on abelian groups.

Lemma 2.1. *Let* A *and* B *be abelian groups, and suppose that* $\phi : A \to B$ *and* $\psi : B \to A$ *are homomorphisms satisfying*

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

Then the following inequality on indices holds.

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

Proof. Let $\{a_i\}$ and $\{b_j\}$ be complete representatives for the cosets of $\psi(B)$ in A and the cosets of $\phi(A)$ in B. We claim that $\{a_i + \psi(b_j)\}$ is the set of complete representatives for the cosets of $2A$ in A. Let $a \in A$. Then we can let $a = a_i + \psi(b)$ for some i and $b \in B$. On the other hand, $b = b_j + \phi(a`)$ for some j and $a' \in A$. Then

$$\begin{aligned} a &= a_i + \psi(b) \\ &= a_i + \psi(b_j + \phi(a')) \\ &= a_i + \psi(b_j) + (\psi \circ \phi)(a') \\ &= a_i + \psi(b_j) + 2a' \end{aligned}$$

which gives the desired result. □

Since we are interested in proving finiteness of $[\Gamma, 2\Gamma]$, lemma 2.1. allows us to reduce the problem to proving finiteness of $[\Gamma : \psi(\overline{\Gamma})]$ and $[\overline{\Gamma}, \phi(\Gamma)]$. Since there is a symmetry between constructions of ϕ and ψ, it is enough to prove finiteness of $[\overline{\Gamma} : \phi(\Gamma)]$. The idea of the proof is embedding $\overline{\Gamma}/\phi(\Gamma)$ into a finite group. So we should look into the set $\phi(\Gamma)$. Note that ϕ sends a rational point on C to a rational point on $\overline{C}$. So $\phi(\Gamma)$ forms a subgroup of $\overline{\Gamma}$. Then several facts are obtained as follows.

(1) $\overline{\infty} \in \phi(\Gamma)$.
(2) $\overline{T} = (0,0) \in \phi(\Gamma)$ if and only if $\bar{a} = -4a$ is a square.
(3) If $\overline{P} = (\bar{x}, \bar{y}) \in \overline{\Gamma}$ with $\bar{x} \neq 0$, then $\overline{P} \in \phi(\Gamma)$ if and only if $\bar{x}$ is a rational square.

(1) is obvious from the definition of ϕ. Let's see (2). Note that $\overline{T} \in \phi(\Gamma)$ if and only if Γ has a point with the y-coordinate 0. It is equivalent to the existence of a nonzero rational root of the equation $0 = x^3 + ax$. It can happen if and only if $-4a$ is a square. For statement (3), only if part is immediate from the definition of ϕ. For the if part, let $\bar{x} = w^2$ with $\in \mathbb{Q}$. Note that ϕ has two elements in its kernel so that if the statement is true, we would find two points in the fibre of $\overline{P}$. Let

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

Then we can check that the fibre of $\overline{P}$ consists of (x_1, y_1) and (x_2, y_2). In summary, $\phi(\Gamma)$ is the set consisting of $(\bar{x}, \bar{y}) \in \overline{\Gamma}$ such that $\bar{x}$ is a non-zero rational square, together with $\overline{\infty}$, and $\overline{T}$ if $\bar{a}$ is a square. Now we will construct a homomorphism from $\overline{\Gamma}$ to a finite group whose kernel fits into the description above.. Let $\mathbb{Q}^{*2}$ be the set of rational squares. Define $\alpha : \overline{\Gamma} \to \mathbb{Q}/\mathbb{Q}^{*2}$ by

$$\alpha(\overline{\infty}) = 1 \pmod{\mathbb{Q}^{*2}}$$
$$\alpha(\overline{T}) = \bar{a} \pmod{\mathbb{Q}^{*2}}$$
$$\alpha(\bar{x}, \bar{y}) = \bar{x} \pmod{\mathbb{Q}^{*2}} \text{ if } x \neq 0$$

Theorem 2.2. *The map α is a homomorphism with the kernel $\phi(\Gamma)$. Moreover, let $p_1, \dots p_n$ be prime factors of $\bar{a}$. Then the image of α is contained in the subgroup*

$$H = \{\pm p_1^{\epsilon_1} \dots p_n^{\epsilon_n} : \textit{each } \epsilon_i \textit{ is } 0 \textit{ or } 1\}$$

of $\mathbb{Q}/\mathbb{Q}^{*2}$. Hence, $\overline{\Gamma}/\phi(\Gamma)$ can be embedded to H and $[\overline{\Gamma} : \phi(\Gamma)]$ is finite.

Proof. First, observe that α sends inverses to inverses. Hence, to show α is a homomorphism, it is enough to show that whenever $\overline{P_1} + \overline{P_2} + \overline{P_3} = \overline{\infty}$, then $\alpha(\overline{P_1})\alpha(\overline{P_2})\alpha(\overline{P_3}) \equiv 1 \bmod \mathbb{Q}^{*2}$. It is easy to see that it is true if one of $\overline{P_1}$, $\overline{P_2}$, $\overline{P_3}$ is $\overline{\infty}$ or $\overline{T}$. If not, the sum of three points is equivalent to the point of infinity if and only if they are colinear. Letting this line $y = \lambda x + \nu$, we obtain the desired result by solving defining equation of an elliptic curve. Considering the definition of α, our description of $\phi(\Gamma)$ exactly coincides with the kernel of α. Now let $(\bar{x}, \bar{y}) \in \overline{\Gamma}$. We have seen that $\bar{x} = m/e^2$ and $\bar{y} = n/e^3$ in reduced forms. Using the equation of $\overline{\Gamma}$, we see that

$$n^2 = m(m^2 + ame^2 + be^4)$$

Note that image of α consists of those $\bar{x} \equiv m \bmod \mathbb{Q}^{*2}$, 1, and $\bar{a}$. 1 and $\bar{a}$ are obviously in H. For m, we see its prime factors. From the above equality, if prime factors of m appears even times in a factorization of m unless it divides b. Therefore, factorization of m is of the form

$$m = \pm(\text{integer})^2 p_1^{\epsilon_1} \dots p_n^{\epsilon_n}$$

with ϵ_i is either 0 or 1. So $m \in H$ in $\mathbb{Q}/\mathbb{Q}^{*2}$. Finally, since H consists of at most 2^{n+1} elements, the last statement follows. □

References

[1] Silverman, J. H., *The Arithmetic of Elliptic Curves*. 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 2009

[2] Silverman, J. H., Tate, J. T., *Rational Points on Elliptic Curves*. 2nd ed., Undergraduate Texts in Mathematics, Springer International Publishing, 2015