Mordell's Theorem

Alex Tao

7 August 2008

It only remains to prove lemma 4 to put together Mordell's Theorem but this is the hardest lemma out of the four of them and we will need to break the proof down into several steps. Lemma 4 states that if we define $\Gamma = C(\mathbb{Q})$ then 2Γ, as a subgroup of Γ, has finite index in Γ.

To simplify the proof, we will need to assume that our curve has at least one rational point of order 2, $(x_0, 0)$. Moving the origin to the point $(x_0, 0)$ transforms our standard curve to

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

The rational points remain in this curve and we will call this curve C. Introduce another curve $\overline{C}$ given by

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

where $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$. In the similar manner, we can define $\overline{\overline{C}}$ which is isomorphic to C upto a certain translation.

We can think of the map $\Gamma \to 2\Gamma$ as a homomorphism and we will ease the proof by splitting it into 2 separate homomorphisms

$$\phi : C \to \overline{C} \qquad \text{and} \qquad \psi : C \to \overline{\overline{C}} \cong C,$$

so that maps between the group of rational points on each curve are

$$\Gamma \xrightarrow{\phi} \overline{\Gamma} \xrightarrow{\psi} \overline{\overline{\Gamma}}.$$

The explicit formulas for ϕ and ψ for some point $P = (x, y)$ and $\overline{P} = (\overline{x}, \overline{y})$ are:

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

$$\psi(P) = \begin{cases} \left(\dfrac{y^2}{4x^2}, \dfrac{x^2-b}{8x^2}\right), & \text{if } \overline{P} \neq \overline{\mathcal{O}}, \overline{T} \\ \mathcal{O} & \text{if } \overline{P} = \overline{\mathcal{O}}, \overline{T} \end{cases}$$

The composition $\phi \circ \psi$ turns out to be exactly the duplication formula. It will make sense then, to study the the index of the image of these 'smaller' homomorphisms in Γ. We will use a general result of abstract groups which states the following:

Let A and B be abelian groups, ϕ and ψ are homomorphisms with $\phi : A \to B$ and $\psi : B \to A$. Suppose

$$\psi \circ \phi(a) = 2a \quad \text{and} \quad \phi \circ \psi(b) = 2b$$

always holds. Further suppose that $\phi(A)$ and $\psi(B)$ has finite index in B and A repectively, then

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

The two homomorphisms are essentially the same and we only need to study one of them. Now we are only left to show that $\big(\Gamma : \psi(\overline{\Gamma})\big)$ is finite. The interesting part of the proof comes along at this point. A few propositions can been written upon the image of ϕ:

1. $\mathcal{O} \in \phi(\Gamma)$
2. $\overline{T} = (0,0) \in \phi(\Gamma)$ if and only if $\overline{b} = a^2 - 4b$ is a perfect square
3. Let $\overline{P} = (\overline{x}, \overline{y}) \in \overline{\Gamma}$ with $\overline{x} \neq 0$. Then $\overline{P} \in \phi(\Gamma)$ if and only if there is $\overline{x}$ is the square of a rational number.

The key idea of this proof is to introduce some one-to-one homomorphism and 'count' the index $(\Gamma : 2\Gamma)$ on the image of the homomorphism. 1. and 2. involves square numbers and the x-domain of the map ψ, $\overline{\Gamma}$, are essentially square numbers so it is sensible to consider the group of square rational numbers, $\mathbb{Q}^{*2}$. Define a map, $\alpha : \Gamma \to \dfrac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$ by

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

By taking modulo $\mathbb{Q}^{*2}$, we take out all the squares to zero. The kernel of α then, is exactly the image of $\psi(\overline{\Gamma})$. It can be checked that α is a

homomorphism so if we take the kernel-quotient group we have a one-to-one homomorphism

$$\frac{\Gamma}{\psi(\overline{\Gamma})} \longleftrightarrow \frac{\mathbb{Q}}{\mathbb{Q}^{*2}}.$$

We can count the cardinality of the group on the right hand side to effectively know the index on the left. To do this, we can examine what elements it consists of.

The image of α are the values x. From the equation of curve, x is forced to divide b in the form of the square of some rational number and composition of the primes dividing b. The highest power of any element occuring inside $\frac{\mathbb{Q}}{\mathbb{Q}^{*2}}$ is 1 so x has to be in the form $\pm p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ where $p_1, p_2, \ldots, p_n$ are primes dividing b and each e_i's are either 1 or 0. Since b is finite, the number of primes dividing b is finite and hence $\frac{\mathbb{Q}}{\mathbb{Q}^{*2}}$ is a finite group. In fact, we have the inequality for the index $\Gamma : \phi(\overline{\Gamma}) \leq 2^{n+1}$.

We can now conclude that the index $(\Gamma : 2\Gamma)$ is finite proving lemma 4. Together with lemmas 1, 2 and 3, this closes the proof of Mordell's theorem which I'll restate here.

Mordell's Theorem (for curves with a rational point of order 2)
Let C be a non-singular 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.