1.18 26/07/13 - The Weak Mordell Theorem

The goal for today is to start making our way through the proof of the weak Mordell Theorem (1.15.9), which says that if $E/\mathbb{Q}$ is an elliptic curve, then the group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. The basic strategy for this is simple: we will try to find an abelian group B and a group homomorphism $\alpha : E(\mathbb{Q}) \to B$ with the property that $\ker \alpha = 2E(\mathbb{Q})$. If we manage to do this, then α would induce an injection $E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow B$. If we further manage to show that $\operatorname{Im} \alpha$ is finite, then we would have succeeded.

Since we're working over $\mathbb{Q}$, we might as well assume we are working with the shorter Weierstrass form $E : y^2 = f(x)$, where $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ is a monic cubic polynomial with distinct (complex) roots. (We could work with the shortest Weierstrass form, but we'll see why the slightly longer form is useful today and next time.) Now here, at least when it comes to 2-torsion, there are essentially three things that can happen (as we have seen already in §1.12.C):

(a) either $f(x)$ splits completely into linear factors over $\mathbb{Q}$,
(b) or $f(x)$ splits into a linear and an irreducible monic quadratic polynomial,
(c) or the cubic polynomial $f(x)$ is irreducible.

It is possible to give a uniform proof that covers all three cases simultaneously (as is done in [1, §15]); but we'll give different proofs (and hopefully have more fun).

The cases (a), (b), and (c) are in some ways very different. It is possible to give "elementary" proofs of (a) and (b), but all the proofs of (c) I know of use at least some algebraic number theory (nothing more than the basics of number field theory). Having said this, I find the proof of (c) conceptually the cleanest, and so let's do this case first.

1.18.A The Case of Irreducible $f(x)$

The following proof has been taken from [1, §15].

Suppose that $f(x)$ is irreducible. The basic idea is to work with the cubic number field $L := \mathbb{Q}[x]/(f(x))$. Let $\beta \in L$ denote the class of x, which is a root of $f(x)$. We will prove

Theorem 1.18.1. Let $E : y^2 = f(x)$ be an elliptic curve over $\mathbb{Q}$ with $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ is a monic irreducible polynomial. Let $L := \mathbb{Q}[x]/(f(x)) = \mathbb{Q}[\beta]$ as above, and consider the map

$$\alpha : E(\mathbb{Q}) \to L^\times/(L^\times)^2 \quad P \mapsto \begin{cases} [1] & \text{if } P = \mathscr{O}, \text{ and} \\ [x - \beta] & \text{if } P = (x, y) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\}. \end{cases}$$

Then

(a) The map $\alpha : E(\mathbb{Q}) \to L^\times/(L^\times)^2$ is a group homomorphism.
(b) We have that $\ker \alpha = 2E(\mathbb{Q})$.
(c) The image $\operatorname{Im} \alpha$ is finite.

Note that the map α is well-defined since for any $x \in \mathbb{Q}$ we have that $x - \beta \neq 0$ in L. Again, as we shall see below, the proofs of (a) and (b) are "elementary", but the proof of (c) needs some theorems from algebraic number theory. Indeed, the proofs of (a) and (b) work in much more generality, and only (c) really uses that we are working with number fields.

Proof.

(a) We invoke 1.15.5. The condition (i) is automatic by definition. The condition (ii) asks us to show that if $P \in E(\mathbb{Q})$, then $\alpha(P) \cdot \alpha(-P) = [1]$ in $L^\times/(L^\times)^2$, but in fact this is clear because $\alpha(P) = \alpha(-P)$ and so $\alpha(P) \cdot \alpha(-P) = \alpha(P)^2 = [1]$, since squares are trivial in $L^\times/(L^\times)^2$. For condition (iii), we have to show using 1.12.17 that if $P_1, P_2, P_3 \in E(\mathbb{Q})$ are collinear (with multiplicities, as usual!), then $\alpha(P_1) \cdot \alpha(P_2) \cdot \alpha(P_3) = [1]$ in $L^\times/(L^\times)^2$. Now one of P_i, say P_1, is $\mathscr{O}$, then the result is clear from what we have done already, since then $P_2 = -P_3$. Therefore, we need only to worry about the case in which none of P_1, P_2, P_3 are $\mathscr{O}$.
When this is the case, the line L through P_1, P_2, P_3 is not vertical, and so has equation $L : y = \lambda x + \nu$ for some $\lambda, \nu \in \mathbb{Q}$. In the case, the x-coordinates x_1, x_2, x_3 of P_1, P_2, P_3 are precisely the roots of

the polynomial

$$g(x) := f(x) - (\lambda x + \nu)^2,$$

so that $g(x)$ factors as $g(x) = \prod_{i=1}^{3}(x - x_i)$. We wish to evaluate the product of the $x_i - \beta$, but this is precisely

$$\prod_{i=1}^{3}(x_i - \beta) = -\prod_{i=1}^{3}(\beta - x_i) = -g(\beta) = -f(\beta) + (\lambda\beta + \nu)^2 = (\lambda\beta + \nu)^2,$$

since $f(\beta) = 0$. Since $\lambda\beta + \nu \neq 0$ in L, this is enough to conclude the product of the $x_i - \beta$ is a square in L, which says exactly that $\alpha(P_1)\alpha(P_2)\alpha(P_3) = [1]$ in $L^\times/(L^\times)^2$ as needed.

(b) Since α is a group homomorphism, and every element in the codomain squares to one, it follows automatically that $2E(\mathbb{Q}) \subset \ker\alpha$. Indeed, for any $P_1 \in 2E(\mathbb{Q})$, we can find a $P_0 \in E(\mathbb{Q})$ such that $P_1 = 2P_0$; then $\alpha(P_1) = \alpha(2P_0) = \alpha(P_0)^2 = [1]$, since again squares are trivial in $L^\times/(L^\times)^2$. The more interesting direction involves showing that $\ker\alpha \subset 2E(\mathbb{Q})$. To do this, we have to show that if $P_1 \in E(\mathbb{Q})$ is such that $\alpha(P_1) = [1]$, then there is a P_0 such that $P_1 = 2P_0$. If $P_1 = \mathscr{O}$, then we can just take $P_0 = \mathscr{O}$. Hence suppose that $P_1 \neq \mathscr{O}$, and write it as $P_1 = (x_1, y_1) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$. At this point, the proof is just messing around with the algebra. The condition $\alpha(P_1) = [1]$ is saying that there are $u, v, w \in \mathbb{Q}$ such that $x_1 - \beta = (u\beta^2 + v\beta + w)^2$. Now we must have $u \neq 0$, since β does not satisfy a nonzero linear or quadratic equation over $\mathbb{Q}$ (check!). Consider the $t \in \mathbb{Q}$ defined by

$$t := \frac{v}{u} - a.$$

Given this choice of t, if we expand the product $(t-\beta)(u\beta^2+v\beta+w)$ and use that $-\beta^3 = a\beta^2+b\beta+c$, we get that

$$\begin{aligned}(t - \beta)(u\beta^2 + v\beta + w) &= -u\beta^3 + (tu - v)\beta^2 + (tv - w)\beta + tw \\ &= (au + tu - v)\beta^2 + (bu + tv - w)\beta + (cu + tw).\end{aligned}$$

By our choice of t, the coefficient of β^2 in this expression vanishes, and so if we let $(\lambda, \nu) := (bu + tv - w, cu + tw)$, then we get that

$$(t - \beta)(u\beta^2 + v\beta + w) = \lambda\beta + \nu.$$

If we square this and use that $(u\beta^2 + v\beta + w)^2 = x_1 - \beta$, we get that β satisfies

$$(t - \beta)^2(x_1 - \beta) = (\lambda\beta + \nu)^2,$$

or equivalently that β is a root of the monic cubic equation

$$(x - x_1)(x - t)^2 + (\lambda x + \nu)^2.$$

However, $f(x)$ is the minimal polynomial of β, and so it is the *only* monic cubic polynomial that β satisfies (check!)–this means that we must have the equality of polynomials

$$f(x) = (x - x_1)(x - t)^2 + (\lambda x + \nu)^2 \in \mathbb{Q}[x].$$

At this point, we are basically done: if we let L be the line $L : y = \lambda x + \nu$, then the above equality tells us that the line L is tangent to E at the point $P_0 := (t, \lambda t + \nu)$ and passes through the point $P_1' := (x_1, \lambda x_1 + \nu)$, so that, in particular, $P_1' + 2P_0 = \mathscr{O}$ in $E(\mathbb{Q})$. However, there are precisely two points on E with x-coordinate exactly equal to x_1, namely $\pm P_1$, which forces $P_1' \in \{\pm P_1\}$. If $P_1' = -P_1$, then the equation $P_1' + 2P_0 = \mathscr{O}$ is saying precisely what we wanted–that $P_1 = 2P_0$. If, however, $P_1' = P_1$, then we have that $P_1 = 2(-P_0)$, so that P_1 is still the doubling of another rational point on $E(\mathbb{Q})$, finishing the proof.

(c) This is the part that does need a little algebraic number theory. The idea is very simple: even though the group $L^\times/(L^\times)^2$ is not finite, we can only really have "finitely many primes" showing up in the image of α. To say this more precisely, consider for each finite set S of primes of $\mathscr{O}_L$ the subgroup

$$L(S, 2) := \{[a] \in L^\times/(L^\times)^2 : \text{ for all primes } \mathfrak{q} \notin S \text{ we have } v_{\mathfrak{q}}(a) \equiv 0 \pmod 2\}.$$

Standard finiteness results in algebraic number theory show that for each finite set S of primes, the subgroup $L(S,2)$ is finite (2.5.15). Therefore, if we can find a finite set S such that $\operatorname{Im}\alpha \subset L(S,2)$, then we would be done.
To find such an S, we need to study the primes dividing $x-\beta$ more carefully. For this, we first note that since $\beta \in L$ is a root of $f(x)$, it can be factored as

$$f(x) = (x-\beta)\cdot q(x) = (x-\beta)(x^2+rx+s) \in L[x]$$

for some monic quadratic polynomial $q(x) = x^2+rx+s \in L[x]$. Since E is smooth, the polynomial f does not have a repeated root at β, i.e., $q(\beta) \neq 0$. Therefore, there are only finitely many primes dividing $q(\beta)$. If we let $S := \{\mathfrak{p} : \mathfrak{p} \mid q(\beta)\}$ be this finite set, then we will show that $\operatorname{Im}\alpha \subset L(S,2)$, finishing the proof.
It remains to show that if $P = (x,y) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$, then $\alpha(P) \in L(S,2)$; in other words, that if $\mathfrak{p}$ is prime of $\mathscr{O}_L$ and $v_{\mathfrak{p}}(x-\beta) \equiv 1 \pmod 2$, then $\mathfrak{p} \mid q(\beta)$. To see this, write $P = (m/e^2, n/e^3)$ as in 1.14.8, so that $m,n,e \in \mathbb{Z}$ with $\gcd(m,e) = \gcd(n,e) = 1$. Then the fact that $P \in E(\mathbb{Q})$ can be expressed by the equation

$$n^2 = (m-e^2\beta)(m^2+rme^2+se^4) \tag{1.18.2}$$

obtained by clearing denominators. Now if $\mathfrak{p}$ is a prime of S such that $v_{\mathfrak{p}}(x-\beta) \equiv 1 \pmod 2$, then certainly also $v_{\mathfrak{p}}(m-e^2\beta) = v_p(x-\beta) + 2v_{\mathfrak{p}}(e) \equiv 1 \pmod 2$. The advantage of clearing denominators is that since $\beta \in \mathscr{O}_L$, we must have $v_{\mathfrak{p}}(m-e^2\beta) \geq 0$, so that if it is odd, we must have that $\mathfrak{p} \mid m-e^2\beta$, or equivalently

$$m \equiv e^2\beta \pmod{\mathfrak{p}}.$$

Now from the equation 1.18.2 it follows immediately that $v_{\mathfrak{p}}(m^2+rme^2+se^4) \equiv 1 \pmod 2$ as well, and hence as above that $\mathfrak{p} \mid m^2+rme^2+se^4$. Using that $m \equiv e^2\beta \pmod{\mathfrak{p}}$, this can be written as

$$\mathfrak{p} \mid e^4(\beta^2+r\beta+s) = e^4 q(\beta).$$

Now since $\mathfrak{p} \mid m-e^2\beta$, we cannot have that $\mathfrak{p} \mid e$; indeed, if $\mathfrak{p} \mid e$, then $\mathfrak{p} \mid m$ also, but $\gcd(m,e) = 1$. Therefore, $\mathfrak{p} \nmid e$, and so from $\mathfrak{p} \mid e^4 q(\beta)$, we conclude that $\mathfrak{p} \mid q(\beta)$, finishing the proof.

■

Example 1.18.3. Let's work through the example $E : y^2 = x^3 - 432$ of §1.2.B carefully. The polynomial $f(x) = x^3 - 432 \in \mathbb{Q}[x]$ is irreducible, and so we are indeed in case (c). The number field $L = \mathbb{Q}[\beta] := \mathbb{Q}[x]/(x^3-432)$ is isomorphic to $\mathbb{Q}[\sqrt[3]{2}]$ via the map $\beta \mapsto 6\sqrt[3]{2}$. For convenience, let us fix this isomorphism and let $\gamma := \sqrt[3]{2}$, so that $\beta := 6\gamma$.

(a) As above, we have a group homomorphism $\alpha : E(\mathbb{Q}) \to L^\times/(L^\times)^2$ given on points $P = (x,y) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$ by $P \mapsto [x-\beta]$.

(b) Consider the point $P_1 = (12,36) \in E(\mathbb{Q})$. Note that $\alpha(P_1) = [12-\beta]$. Since

$$12-\beta = (\gamma^2+2\gamma-2)^2,$$

we have that $\alpha(P_1) = [1]$. Let us use the theory above to construct a point P_0 such that $2P_0 = P_1$. We can take $(u,v,w) := (1/36, 1/3, -2)$, and hence $t = 12$, which gives $(\lambda,\nu) = (6,-36)$ (check!). Indeed, we have that

$$x^3 - 432 = (x-12)^3 + (6x-36)^2.$$

The line $y = 6x-36$ meets the curve E *thrice* at P_1, so that $P_0 = P_1' = P_1$ above and $P_1 = 2(-P_1)$, which is indeed correct and shows that $P_1 \in 2E(\mathbb{Q})$.3

(c) We can factor $f(x)$ as $f(x) = (x-\beta)(x^2+\beta x+\beta^2)$, so that $q(x) = x^2+\beta x+\beta^2 \in L[x]$. In particular, $q(\beta) = 3\beta^2 = 108\gamma^2$, which factors as an ideal (check!) as

$$(q(\beta)) = (\gamma)^8(\gamma+1)^9.$$

Therefore, we can take $S := \{(\gamma),(\gamma+1)\}$. At this point, some algebraic number theory of L shows that $L(S,2)$ has size 16 (2.5.17), and hence that $E(\mathbb{Q})/2E(\mathbb{Q})$ injects into a group of size 16, as in in particular finite.

The above example shows that if we can get a better handle on $\operatorname{Im}\alpha$, then this can allow us to prove statements about rational points on the curve E. In particular, doing this for the curve $E : y^2 = x^3 - 432$ can allow us to prove Fermat's Last Theorem for $n = 3$. This is indeed the case. Since this is fun to figure out on your own, I won't spoil it; this argument can be found in the form of an extended exercise (2.5.17) on Exercise Sheet 5. This is all I am going to say about Fermat's Last Theorem for $n = 3$, although we will visit the case of $n = 4$ later.

We have now finished the proof of the Mordell Theorem 1.15.8 in the special case that $E[2](\mathbb{Q}) = \{\mathscr{O}\}$. Let's now discuss the other cases, the proofs of which will not use any serious algebraic number theory.

1.18.B The Case of Completely Split $f(x)$

Let's start this argument today; we'll finish it next time. Suppose now that $f(x) \in \mathbb{Z}[x]$ splits completely over $\mathbb{Q}$ into linear factors, and so can be written as

$$f(x) = (x - e_1)(x - e_2)(x - e_3)$$

for pairwise distinct integers $e_1, e_2, e_3 \in \mathbb{Z}$. In this case, if we let $T_i := (e_i, 0)$ for $i = 1, 2, 3$, then

$$E[2](\mathbb{Q}) = \{\mathscr{O}, T_1, T_2, T_3\} \cong_{\mathsf{Ab}} \mathbb{Z}/2 \oplus \mathbb{Z}/2$$

and the elliptic discriminant is

$$\Delta = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2.$$

We want to do something similar to what we did above. The key idea here is that, in fact, most of the proof above goes through.

Let $L := \mathbb{Q}[\beta] := \mathbb{Q}[x]/(f(x))$ as above, which this time is *not* a field, and in fact (thanks to the Chinese Remainder Theorem) splits as

$$L \xrightarrow{\sim} \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q},$$

with the map given by sending the polynomial $g(\beta) \in L$ to the triple $(g(e_1), g(e_2), g(e_3))$. Now we can still ask for $L^\times$ (the group of *units* of L, and not the nonzero elements of L), and the group $L^\times/(L^\times)^2$, which again splits as

$$L^\times/(L^\times)^2 \xrightarrow{\sim} \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

Finally, the map

$$\alpha : E(\mathbb{Q}) \to L^\times/(L^\times)^2 \xrightarrow{\sim} \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

still *mostly* makes sense. Indeed, we still send $\mathscr{O}$ to $[1] \leftrightarrow ([1], [1], [1])$ of course, and a point $P = (x, y) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$ to $[x - \beta] \leftrightarrow ([x - e_1], [x - e_2], [x - e_3])$. This does make sense when $x \neq e_1, e_2, e_3$, but in fact something goes wrong when $x \in \{e_1, e_2, e_3\}$. Indeed, if say $P = T_1$, then the "second and third components" $e_1 - e_2$ and $e_1 - e_3$ still make sense, but the "first component" is broken, since 0 is not allowed as an element of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Therefore, we need to come up with some sort of patch. I encourage you to think about how to patch this until next time, when we will finish the proof of this case.