LECTURE 23, MONDAY 03.05.04

FRANZ LEMMERMEYER

1. Descent via 2-Isogenies

Now we will discuss the proof of Mordell-Weil in the case where at least one point of order 2 is rational. By moving this point to the origin we may assume that our elliptic curve is given by the equation

$$y^2 = x(x^2 + ax + b), \quad a, b \in \mathbb{Z}, \quad b(a^2 - 4b) \neq 0. \tag{1}$$

Note that E has discriminant $\Delta = 16b^2(a^2 - 4b)$. If the quadratic factor splits into linear terms over $\mathbb{Q}$, we may use the method of 2-descent we have already discussed; if not, we will have to work a little harder.

First recall that any affine rational point $P = (x, y)$ on E has the form $x = m/e^2$, $y = n/e^3$ for integers m, n, e with $(m, e) = (n, e) = 1$.

Plugging this into equation (1) we get

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

Thus we have two integers whose product is a square; if these integers were coprime we could conclude that each of them is a square since the integers form a UFD. Let us compute a bit: $\gcd(m, m^2 + ame^2 + be^4) = \gcd(m, be^4) = \gcd(m, b)$, since $(m, e) = 1$. If we write $b_1 = \gcd(m, b)$, then $b = b_1 b_2$ and $m = b_1 u$. This gives

$$n^2 = b_1 u(b_1^2 u^2 + ab_1 ue^2 + b_1 b_2 e^4),$$

and with $n = b_1 z$ we get

$$z^2 = u(b_1 u^2 + aue^2 + b_2 e^4).$$

Let us assume for now that $n \neq 0$. The two factors now *are* coprime (we just divided through by the greatest common divisor), and we see that u must be a square up to a unit factor. But by choosing the sign of b_1 appropriately we may assume that $u = M^2$ and $b_1 u^2 + aue^2 + b_2 e^4 = N^2$ for integers $M, N \in \mathbb{N}$ with $MN = z$. Replacing u by M^2 in the second equation we finally get

$$\mathcal{T}^{(\psi)}(b_1) : N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4. \tag{2}$$

Thus every point $(x, y) \in \mathrm{E}(\mathbb{Q})$ gives rise to a point (N, M, e) on the curve $\mathcal{T}^{(\psi)}(b_1)$, where b_1 is given by $b_1 = \gcd(m, b)$ and $x = \frac{m}{e^2}$. Conversely, given (N, M, e) on $\mathcal{T}^{(\psi)}(b_1)$, we can get back our point (x, y) by reversing the construction. We know that $MN = z$ and $n = b_1 z$; moreover $M^2 = u$ and $b_1 u = m$. Thus $(x, y) = (b_1(M/e)^2, b_1 NM/e^3)$. In particular, b_1 and x differ only by a square factor. We have seen this before, of course: the map $\alpha : (x, y) \longmapsto x\mathbb{Q}^{\times 2}$ is the map α_1 defined in the case where the elliptic curve has three rational points of order 2.

In order to define $\alpha(0, 0)$, let us follow the construction of b_1 above: if $(x, y) = (0, 0)$, then $m = 0$, $e = 1$, and $b_1 = \gcd(m, b) = b$; in fact $N^2 = bM^4 + aM^2e^2 + e^4$

has the solution $(N, M, e) = (1, 0, 1)$ giving rise to the point $(0, 0) \in \mathrm{E}(\mathbb{Q})$. Thus we should put $\alpha(0, 0) = b\mathbb{Q}^{\times 2}$.

We have shown that every rational point on (1) corresponds to a non-trivial[1] primitive[2] integral solution of one of the finitely many[3] curves (2); these curves are called torsors of the elliptic curve (1) and will be denoted by $\mathcal{T}^{(\psi)}(b_1)$ in the following (the superscript (ψ) will be explained below). Torsors with a rational point are called trivial. By reversing our construction we already have seen that every integral point on (2) yields a rational point on (1): in fact, if (N, M, e) is a solution of (2), then $P = (x, y)$ is a rational point on (1), where $x = b_1M^2/e^2$ and $y = b_1MN/e^3$; solutions with $e = 0$ correspond to the rational point $\mathcal{O}$ at infinity. Such a solution occurs if and only if $N^2 = b_1M^4$, that is, if and only if b_1 is a square.

We also see that the solvability of (2) only depends on b_1 modulo squares: in fact, if (N, M, e) solves the torsor $\mathcal{T}^{(\psi)}(b_1)$, then (fN, M, fe) solves the torsor $\mathcal{T}^{(\psi)}(b_1f^2)$. Thus we only need to look at squarefree values of b_1:

Theorem 1. *The rational points on the elliptic curve (1) are in bijection with non-trivial primitive integral solutions on the torsors* (2)*, where b_1 runs through the squarefree divisors of $b = b_1b_2$.*

Given (N, M, e) on $\mathcal{T}^{(\psi)}(b_1)$, the point $(x, y) = (b_1M^2/e^2, b_1MN/e^3)$ is a rational point on $\mathrm{E}(\mathbb{Q})$*. Conversely, $P = (x, y) \in \mathrm{E}(\mathbb{Q})$ gives a primitive integral solution (N, M, e) on the torsor $\mathcal{T}^{(\psi)}(b_1)$; here b_1 is the squarefree number determined by $\alpha(P) = b_1\mathbb{Q}^{\times 2}$, and $\alpha : \mathrm{E}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is the map given by*

$$\alpha(P) = \begin{cases} 1\mathbb{Q}^{\times 2} & \text{if } P = \mathcal{O}; \\ b\mathbb{Q}^{\times 2} & \text{if } P = (0,0); \\ x\mathbb{Q}^{\times 2} & \text{if } P = (x, y) \in E(\mathbb{Q}) \setminus \{\mathcal{O}, (0, 0)\}. \end{cases} \tag{3}$$

We have already proved that $\alpha = \alpha_1$ is a homomorphism.

Observe that if (N, M, e) is a rational point on some torsor, and if d is the product of the denominators of N, M and e, then (d^2N, dM, de) is a point on the torsor with integral coordinates, and this point gives rise to the same point on E as (N, M, e).

Remark. Note that in our proof we have shown that $\gcd(N, M) = 1$; we did, however, not assume that b_1 is squarefree. Thus we may assume that $\gcd(N, M) = 1$ as long as b_1 runs through *all* divisors of b. If we restrict the values of b_1 to the squarefree divisors of b, then we have to allow common divisors of N and M. In any case we may assume that $(N, e) = (M, e) = 1$: a common prime divisor of N and e divides M since b_1 is squarefree, and we may cancel the fourth power of the common divisor; similarly we can ensure that $(M, e) = 1$.

We shall call $\alpha : \mathrm{E}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ the Weil map (it was introduced by André Weil in his proof of Mordell's theorem). We found the Weil map from the group of rational points on E to the group $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ by studying the rational points on elliptic curves (1).

[1] That is, we do not count the solution $N = M = e = 0$.

[2] This is our abbreviation for $(N, e) = (M, e) = 1$.

[3] There are only finitely many divisors b_1 of b.

2. 2-Isogenies

Now let me explain how to go from the elliptic curve $E : y^2 = x(x^2 + ax + b)$ to some other curve $\overline{E} : y^2 = x(x^2 + \overline{a}x + \overline{b})$, where $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$.

To this end let us look at the torsor

$$\mathcal{T}^{(\psi)}(1) : n^2 = m^4 + am^2 + b. \tag{4}$$

Multiplying through by 4 and rearranging terms, we find

$$a^2 - 4b = (2m^2 + a)^2 - 4n^2 = (2m^2 + a + 2n)(2m^2 + a - 2n).$$

Let us put $t = 2m^2+a+2n$; then $(t-a)^2 = t(t-2a)+a^2$, and since $a^2 = t(t-4n)+4b$, this gives

$$(t - a)^2 - 4b = t(t - 2a + t - 4n) = 4m^2 t.$$

But now $(t - a)^2 - 4b = t^2 + \overline{a}\,t + \overline{b}$, where $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$. Thus $t(t^2 + \overline{a}\,t + \overline{b}) = 4m^2t^2$, in other words: the point $(\overline{x}, \overline{y}) = (t, 2mt)$ is a rational point on the curve

$$\overline{E} : \overline{y}^2 = \overline{x}(\overline{x}^2 + \overline{a}\,\overline{x} + \overline{b}). \tag{5}$$

Note that $\Delta(\overline{E}) = 16\overline{b}^2(\overline{a}^2 - \overline{b}) = 256b(a^2 - 4b)^2$ is nonzero if $\Delta \neq 0$. Thus if E is an elliptic curve, then so is $\overline{E}$.

Conversely, assume that $(\overline{x}, \overline{y}) \in \overline{E}(\mathbb{Q})$. If $\overline{x} \neq 0$, then $m = \overline{y}/2\overline{x}$ gives us back m, and then $n = \frac{1}{2}(\overline{x} - a) - m^2 = \frac{1}{4}(2\overline{x} - \overline{a}) - m^2$; this way we get a map $\overline{E}(\mathbb{Q}) \setminus \{\mathcal{O}, (0, 0)\} \longrightarrow \mathcal{T}^{(\psi)}(\mathbb{Q})$ defined by $(\overline{x}, \overline{y}) \longmapsto (n, m)$.

As long as we only look at the affine parts of these curves, we don't get a bijection between rational points: in fact, if the point $(0, 0)$ on $\overline{E}$ is in the image of the map $\mathcal{T}^{(\psi)} \longrightarrow \overline{E}$, then it must come from a point with $t = 0$. But this implies $-n = m^2 + \frac{1}{2}a$, hence $n^2 = m^4 + am^2 + \frac{1}{4}a^2$, and so this point is on $\mathcal{T}^{(\psi)}$ if and only if $a^2 - 4b = 0$, that is, if and only if $\overline{E}$ is singular.

We have proved:

Proposition 2. *Assume that $a^2 - 4b \neq 0$. Then the map $(n, m) \longmapsto (x, y)$ with $x = 2m^2 + 2n + a$ and $y = 2mx$ defines a bijection between the set of rational points on the affine curve (4) and $\overline{E}(\mathbb{Q}) \setminus \{\mathcal{O}, (0, 0)\}$.*

Now we compose the map $\overline{E}(\mathbb{Q})\setminus\{\mathcal{O}, (0, 0)\} \longrightarrow \mathcal{T}^{(\psi)}(1)$ with the map $\mathcal{T}^{(\psi)}(1) \longrightarrow E(\mathbb{Q})$ constructed above; this defines a map $\psi : \overline{E}(\mathbb{Q}) \setminus \{\mathcal{O}, (0, 0)\} \longrightarrow E(\mathbb{Q})$. Let us compute where ψ sends a point $(\overline{x}, \overline{y}) \in \overline{E}(\mathbb{Q}) \setminus \{\mathcal{O}, (0, 0)\}$; first it gets mapped to

$$(n, m) = \Big(\frac{2\overline{x} + \overline{a}}{4} - \frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}}{2\overline{x}}\Big) \in \mathcal{T}^{(\psi)}(1).$$

Now $(n, m) \longmapsto (m^2, nm)$ under the map $\mathcal{T}^{(\psi)}(1) \longrightarrow \mathrm{E}(\mathbb{Q})$, and since

$$\frac{2\overline{x} + \overline{a}}{4} - \frac{\overline{y}^2}{4\overline{x}^2} = \frac{2\overline{x}^3 + \overline{a}\overline{x}^2 - \overline{y}^2}{4\overline{x}^2} = \frac{\overline{x}^3 - b\overline{x}}{4\overline{x}^2}$$

we find that $(\overline{x}, \overline{y}) \in \overline{E}(\mathbb{Q}) \setminus \{\mathcal{O}, (0, 0)\}$ gets mapped to

$$\psi(\overline{x}, \overline{y}) = \Big(\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2 - \overline{b})}{8\overline{x}^2}\Big). \tag{6}$$

Proposition 3. *Formula* (6)*, together with* $\psi(0,0) = \psi(\mathcal{O}) = \mathcal{O}$*, defines a homomorphism* $\psi : \overline{E}(\mathbb{Q}) \longrightarrow \mathrm{E}(\mathbb{Q})$ *with kernel* $\ker\psi = \{\mathcal{O}, (0,0)\}$*. Moreover, if* $\alpha : \mathrm{E}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$ *is the map defined by (3), then* α *is a group homomorphism with* $\ker\alpha = \mathrm{im}\ \psi$*. In other words: there is an exact sequence*

$$0 \longrightarrow \{\overline{\mathcal{O}}, (0,0)\} \longrightarrow \overline{E}(\mathbb{Q}) \stackrel{\psi}{\longrightarrow} \mathrm{E}(\mathbb{Q}) \stackrel{\alpha}{\longrightarrow} \mathbb{Q}^\times/\mathbb{Q}^{\times\,2}.$$

The fact that ψ is a homomorphism should not surprise you: every rational map between elliptic curves that preserves the point at infinity is a homomorphism.