LECTURE 24, WEDNESDAY 05.05.04

FRANZ LEMMERMEYER

1. 2-Isogenies

Let us recall what we did last time. Starting from an elliptic curve $E : y^2 = x(x^2+ax+b)$ with discriminant $\Delta = 16b^2(a^2-4b)$ we constructed another elliptic curve $\overline{E} : y^2 = x(x^2+\overline{a}x+\overline{b})$, where $\overline{a} = -2a$ and $\overline{b} = a^2-4b$; this is an elliptic curve with discriminant $\Delta = 16^2 b(a^2-4b)^2$. We also came up with a map

$$\psi : \overline{E}(\mathbb{Q}) \longrightarrow \mathrm{E}(\mathbb{Q}) : (\overline{x},\overline{y}) \longmapsto \Big(\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2-\overline{b})}{8\overline{x}^2}\Big), \tag{1}$$

and our job today is to show that this is a homomorphism.

Before we do that, let us iterate this procedure: since $\overline{E}$ has the same form as E, we can form the elliptic curve $\overline{\overline{E}} : Y^2 = X(X^2+AX+B)$ with $A = -2\overline{a} = 4a$ and $B = \overline{a}^2 - 4\overline{b} = 16b$, and we have a map $\overline{\psi} : \overline{\overline{E}} \longrightarrow \overline{E}$ defined as above. But now the tranformation $Y = 8y$ and $X = 4x$ gives an isomorphism $\iota : \overline{\overline{E}} \longrightarrow E$. The composition of maps

$$E \xrightarrow{\iota^{-1}} \overline{\overline{E}} \xrightarrow{\overline{\psi}} \overline{E}$$

defines a map $\phi = \overline{\psi}\circ\iota^{-1} : E \longrightarrow \overline{E}$ given by

$$\phi(x,y) = \Big(\frac{y^2}{x^2}, \frac{y(x^2-b}{x^2}\Big).$$

Note that $y^2/x^2 = (x^2+ax+b)/x$, hence $\phi(0,0) = \mathcal{O}$.

As we have already seen, we also have homomorphisms $\alpha : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ and $\beta : \overline{E}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. With all these maps in place, we now can claim

Theorem 1. *The maps ϕ and ψ defined above are homomorphism. Moreover, the following sequences are exact:*

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

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

Finally, we have $\psi\circ\phi = [2]_E$ (multiplication by 2 on E) and $\phi\circ\psi = [2]_{\overline{E}}$.

Thus although the situation is more involved than for the 2-descent on curves with three rational points of order 2, we have managed to break up the multiplication-by-2 map into two homomorphisms ϕ and ψ between E and the associated curve $\overline{E}$. Multiplication by 2 has a kernel of order 4 (three points of order 2 and the point at infinity), whereas the isogenies ϕ and ψ have kernels of order 2 (which is why they are called 2-isogenies).

Proof. We have to show that ϕ is a group homomorphism. This is done, you guessed it, by distinguishing several cases:

a) The claim is obviously true if one or more of the points P_1, P_2 or P_1+P_2 is the point $\mathcal{O}$ at infinity.

b) Consider two points $P,Q \in \mathrm{E}(\mathbb{Q})$ and assume that $Q=(0,0)$; the case $P=(0,0)$ is taken care of in a), so assume that $P=(x,y)\ne(0,0)$. Then $P+(0,0)=(b/x,-by/x^2)$, hence

$$\begin{aligned}\phi(P+Q) &= \Big(\frac{y_{P+Q}^2}{x_{P+Q}^2}, \frac{y_{P+Q}(x_{P+Q}^2-b)}{x_{P+Q}^2}\Big)\\ &= \Big(\frac{b^2y^2/x^4}{b^2/x^2}, \frac{-byx^2(b^2/x^2-b)}{b^2x^2}\Big)\\ &= \Big(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\Big) \;=\; \phi(P)\\ &= \phi(P)+\phi(Q).\end{aligned}$$

c) P and Q are points of order 2 different from $T=(0,0)$. If $P+Q=T$, then $P+T=Q$, and this case was covered in b). If $P,Q,P+Q\ne T$, then $P=Q$ and thus $P+Q=\mathcal{O}$, which was covered in a).

d) Since $\phi(-P)=-\phi(P)$ it suffices to show that $\phi(P_1)+\phi(P_2)+\phi(P_3)=\mathcal{O}$ if $P_1+P_2+P_3=\mathcal{O}$. Thus assume that the P_i are collinear and pairwise distinct, and let $y=mx+c$ be the equation of this line. We have to show that the points $\phi(P_i)$ are collinear; more exactly, we will show that they are on the line $y=\overline{m}x+\overline{c}$, where $\overline{m}=\frac{1}{c}(mc-b)$ and $\overline{c}=\frac{1}{c}(c^2-amc+bm^2)$. Note that $c\ne0$ since we may assume that the $P_i\ne(0,0)$.

Write $\phi(x_i,y_i)=(\overline{x}_i,\overline{y}_i)$; then

$$\begin{aligned}\overline{m}\,\overline{x}_1+\overline{c} &= \frac{mc-b}{c}\Big(\frac{y_1}{x_1}\Big)^2+\frac{c^2-amc+bm^2}{c}\\ &= \frac{(mc-b)y_1^2+(c^2-amc+bm^2)x_1^2}{cx_1^2}\\ &= \frac{mc(y_1^2-ax_1^2)-b(y_1-mx_1)(y_1+mx_1)+c^2x_1^2}{cx_1^2};\end{aligned}$$

Now we use $y_1^2-ax_1^2=x_1^3+bx_1$, as well as $y_1-mx_1=c$, and get

$$\begin{aligned}\overline{m}\,\overline{x}_1+\overline{c} &= \frac{m(x_1^3+bx_1)-b(y_1+mx_1)+cx_1^2}{x_1^2}\\ &= \frac{x_1^2(mx_1+c)-by_1}{x_1^2} \;=\; \frac{(x_1^2-b)y_1}{x_1^2} \;=\; \overline{y}_1.\end{aligned}$$

The calculations for P_2 and P_3 are analogous.

e) The case $P_1=P_2$ is left as an exercise.

This proves that ϕ (and, by symmetry, ψ) is a group homomorphism.

Now let us see why $\ker\phi=\{\mathcal{O},(0,0)\}$. Clearly $\{\mathcal{O},(0,0)\}\subseteq\ker\phi$. Conversely, assume that $\phi(P)=\mathcal{O}$ for some $P=(x,y)\in E(\mathbb{Q})$; then $x=0$, hence $y=0$ and $P=(0,0)$.

Finally we have to show that $\operatorname{im}\phi=\ker\overline{\alpha}$. Showing that $\operatorname{im}\phi\subseteq\ker\overline{\alpha}$ is easy: the x-coordinate of $\phi(x,y)$ is a square, hence $\overline{\alpha}\circ\phi(x,y)=1\cdot\mathbb{Q}^{\times\,2}$. Conversely, assume that $(x,y)\in\ker\overline{\alpha}$, i.e., that $x=w^2$ for some $w\in\mathbb{Q}$. Define

$$x_j=\frac{1}{2}\Big(x-a+(-1)^j\frac{y}{w}\Big),\quad y_j=(-1)^jwx_j$$

for $j = 1, 2$; then $x_1 x_2 = b$ (use the fact that $y^2 = x(x^2 + ax + b)$), hence $x_j \neq 0$. In order to check that the points (x_j, y_j) are in $E(\mathbb{Q})$, we have to verify that $y_j^2/x_j^2 = x_j + a + b/x_j$, i.e., $x = x_1 + a + b/x_1 = x_1 + a + x_2$ and $x = x_2 + a + b/x_2 = x_2 + a + x_1$; but this is clear. Finally we have $\phi(x_j, y_j) = ((y_j/x_j)^2, y_j(x_j^2 - b)/x_j^2) = (w^2, w(x_2 - x_1)) = (x, y)$.

Finally, let us check that the composition of the 2-isogenies is just multiplication by 2. On the elliptic curve $E : y^2 = x(x^2 + ax + b)$ we have the duplication formula

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

With $\phi(x, y) = (\overline{x}, \overline{y})$ and $\psi(\overline{x}, \overline{y}) = (\overline{\overline{x}}, \overline{\overline{y}})$ we now get

$$\frac{\overline{\overline{x}}}{4} = \frac{\overline{y}^2}{4\overline{x}^2} = \frac{y^2(x^2 - b)^2 x^4}{4y^4 x^4} = \frac{(x^2 - b)^2}{4y^2},$$

if $xy \neq 0$. Similarly,

$$\begin{aligned} \frac{\overline{\overline{y}}}{8} &= \frac{1}{8} \left(y \frac{x^2 - b}{x^2} \Big(1 - (a^2 - 4b) \frac{x^4}{y^4} \Big) \right) \\ &= \frac{(x^2 - b)(y^4 - (a^2 - 4b)x^4)}{8x^2 y^3} = \frac{(x^2 - b)((x^2 + ax + b)^2 - (a^2 - 4b)x^4)}{8y^3} \\ &= \frac{(x^2 - b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2)}{8y^3}. \end{aligned}$$

The special cases $xy = 0$ can easily be taken care of. □

2. The Snake Lemma

Everything we say below about exact sequences of abelian groups also holds in the category of R-modules (note that abelian groups are just $\mathbb{Z}$-modules) or vector spaces (a vector space over K is just a K-module), or, more generally, in abelian categories.

A sequence of abelian groups is a diagram

$$\xrightarrow{f} A \xrightarrow{g} B \xrightarrow{h} C \xrightarrow{i} \dots$$

where $A, B, C, \dots$ are abelian groups, and where $f, g, h, i, \dots$ are group homomorphism. Such a sequence is said to be exact at A if $\operatorname{im} f = \ker g$; similarly it is exact at B if $\operatorname{im} g = \ker i$ etc. A sequence

$$A \longrightarrow B \longrightarrow \dots \longrightarrow G \longrightarrow H$$

is said to be exact if it is exact at B, …, G. In exact sequences of finite abelian groups, the alternating products of the group orders equals 1:

Lemma 2. *If the sequence*

$$0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow \dots \longrightarrow A_n \longrightarrow 0$$

of finite abelian groups is exact, then the alternating product of the group orders is trivial, i.e., $\#A_1 \cdot \#A_3 \cdots = \#A_2 \cdot \#A_4 \cdots$.

This is easily proved by induction using the observation that if

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow \dots$$

is an exact sequence of finite abelian groups, then so is

$$0 \longrightarrow B/A \longrightarrow C \longrightarrow \dots$$

Another useful technique is that of breaking up and gluing exact sequences. Assume for example that

$$\longrightarrow A \xrightarrow{f} B \xrightarrow{g}$$

is an exact sequence; then the sequence can be broken up at f into two exact sequences as follows:

$$\longrightarrow A \xrightarrow{\overline{f}} \operatorname{im} f \longrightarrow 0$$

and

$$0 \longrightarrow \operatorname{im} f \xrightarrow{\iota} B \xrightarrow{g} \dots$$

In fact, $\overline{f} : A \longrightarrow \operatorname{im} f$ is surjective, and its kernel coincides with the kernel of the original map $f : A \longrightarrow B$. Thus the first sequence is indeed exact at A and $\operatorname{im} f$, and since we haven't changed anything to the left of A, the whole sequence remains exact. Similarly we can show that the second sequence is exact.

Conversely, assume that

$$\longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

and

$$0 \longrightarrow C \xrightarrow{h} D \xrightarrow{i}$$

are exact sequences; by *gluing* these sequences together we get the exact sequence

$$\begin{array}{ccccccc}
\longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{h\circ g} & D & \xrightarrow{i} \\
 & & & & \searrow^{g}\ \ \nearrow_{h} & & \\
 & & & & C & & \\
 & & & & \nearrow\ \ \searrow & & \\
 & & & 0 & & 0 &
\end{array}$$

which is easily seen to be exact.

Next we are going to discuss a very important tool in homological algebra: the snake lemma. It will help us construct lots of exact sequences. The basic ingredients are pretty innocent:

Lemma 3. *Assume that*

$$\begin{array}{ccc}
A & \xrightarrow{f} & B \\
\downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} \\
A' & \xrightarrow[f']{} & B'
\end{array}$$

is a commutative square of abelian groups. Then the maps f and f' induce homomorphisms $\overline{f} : \ker\alpha \longrightarrow \ker\beta$ and $\overline{f}' : \operatorname{coker}\alpha \longrightarrow \operatorname{coker}\beta$ in such a way that the

diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker\alpha & \longrightarrow & A & \xrightarrow{\alpha} & A' & \longrightarrow & \operatorname{coker}\alpha & \longrightarrow & 0 \\ & & \overline{f}\downarrow & & f\downarrow & & f'\downarrow & & \overline{f}'\downarrow & & \\ 0 & \longrightarrow & \ker\beta & \longrightarrow & B & \xrightarrow{\beta} & B' & \longrightarrow & \operatorname{coker}\beta & \longrightarrow & 0 \end{array}$$

is exact and commutative.

Proof. We define $\overline{f} : \ker\alpha \longrightarrow \ker\beta$ by mapping $a \in \ker\alpha$ to $f(a)$; we have to show that $f(a) \in \ker\beta$. But since $\beta \circ f(a) = f' \circ \alpha(a) = f'(0) = 0$ this is a consequence of the commutativity of the diagram.

Similarly, we put $\overline{f}'(a' + \operatorname{im}\alpha) = f'(a') + \operatorname{im}\beta$. We have to show that $f' \circ \alpha(A) \subseteq \beta(B)$: but since $f' \circ \alpha(A) = \beta \circ f(A) \subseteq \beta(B)$ this is again clear. Moreover, it is immediately checked that the induced maps $\overline{f}$ and $\overline{f}'$ are homomorphisms, since they essentially are restrictions of homomorphisms. □

The next lemma is the one we will actually be using for deriving Tate's formula for the rank of an elliptic curve:

Lemma 4. *Assume that $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are homomorphisms between abelian groups. Then there exists an exact sequence*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \ker f & \longrightarrow & \ker(g \circ f) & \longrightarrow & \ker g \\ & & & & & & \downarrow \\ 0 & \longleftarrow & \operatorname{coker} g & \longleftarrow & \operatorname{coker}(g \circ f) & \longleftarrow & \operatorname{coker} f \end{array}$$

Proof. Consider the homomorphism $\overline{f} : \ker(g \circ f) \longrightarrow \ker g : a \longmapsto f(a)$. This is well defined since if $a \in \ker g \circ f$, then $f(a) \in \ker g$. Clearly $\ker\overline{f} = \ker f$, hence we get an exact sequence

$$0 \longrightarrow \ker f \longrightarrow \ker g \circ f \longrightarrow \ker g.$$

Similarly, consider the homomorphism $\overline{g} : \operatorname{coker} f \longrightarrow \operatorname{coker} g \circ f : b + \operatorname{im} f \longmapsto g(b) + \operatorname{im} g \circ f$. This is again well defined and provides us with an exact sequence

$$\operatorname{coker} f \longrightarrow \operatorname{coker} g \circ f \longrightarrow \operatorname{coker}\overline{g} \longrightarrow 0.$$

We can glue these sequences together in the following way. Define a homomorphism $\phi : \ker g \longrightarrow \operatorname{coker} f$ by $\phi(b) = b + \operatorname{im} f$. Then $\ker\phi = \ker g \cap \operatorname{im} f = f(\ker g \circ f) = \operatorname{im}\overline{f}$. Moreover, $\operatorname{im}\phi = \ker\overline{g}$: in fact, $\operatorname{im}\phi$ is the subgroup of $B/\operatorname{im} f$ whose cosets are represented by elements in the kernel of g, hence $\operatorname{im}\phi \subseteq \ker\overline{g}$. On the other hand, $b + \operatorname{im} f \in \ker\overline{g}$ is equivalent to $g(b) \in \operatorname{im} g \circ f$, which holds if and only if b can be written in the form $b = b' + f(a)$ for some $b' \in \ker g$. But this implies $b + \operatorname{im} f \in \operatorname{im}\phi$.

The claim now follows from the simple observation that $\operatorname{coker}\overline{g} = \operatorname{coker} g$. In fact, the map $\operatorname{coker} g \circ f \longrightarrow \operatorname{coker} g : c + \operatorname{im} g \circ f \longmapsto c + \operatorname{im} g$ is clearly surjective, and the kernel consists of all elements of the form $f(b) + \operatorname{im} g \circ f$, that is, the kernel of this map is $\operatorname{im}\overline{g}$. □

Theorem 5 (Snake Lemma)**.** *Assume that*

$$\begin{array}{ccccccc} & & A & \xrightarrow[f]{} & B & \xrightarrow[g]{} & C \longrightarrow 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} \\ 0 & \longrightarrow & A' & \xrightarrow[f']{} & B' & \xrightarrow[g']{} & C' \end{array}$$

is a commutative diagram of abelian groups with exact rows. Then there exists a homomorphism $\delta : \ker\gamma \longrightarrow \operatorname{coker}\alpha$ such that the following sequence is exact:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker f & \longrightarrow & \ker\alpha & \longrightarrow & \ker\beta & \longrightarrow & \ker\gamma \\ & & & & & & & & \downarrow{\scriptstyle\delta} \\ 0 & \longleftarrow & \operatorname{coker} g' & \longleftarrow & \operatorname{coker}\gamma & \longleftarrow & \operatorname{coker}\beta & \longleftarrow & \operatorname{coker}\alpha \end{array}$$

Proof. Applying Lemma 4 to the homomorphisms f and β and observing that

- $\beta\circ f = f'\circ\alpha$
- $\ker f'\circ\alpha = \ker\alpha$ since f' is injective

gives the exact sequence

$$0 \longrightarrow \ker f \longrightarrow \ker\alpha \longrightarrow \ker\beta.$$

Lemma 3 provides us with a homomorphism $\overline{g} : \ker\beta \longrightarrow \ker\gamma$, the sequence

$$0 \longrightarrow \ker f \longrightarrow \ker\alpha \xrightarrow{\overline{f}} \ker\beta \xrightarrow{\overline{g}} \ker\gamma$$

is exact if we can show it is exact at $\ker\beta$.

Observe that if $a \in \ker\alpha = \ker\beta\circ f$, then $f(a) \in \ker\beta$, hence $\beta(f(a)) = 0$; this shows that $\operatorname{im}\overline{f} \subseteq \ker\overline{g}$. Conversely, assume that $b \in \ker\beta$ is in the kernel of $\overline{g}$. Then $\beta(b) = 0$, hence $b = f(a)$ for some $a \in A$. Moreover, $0 = \beta(b) = \beta\circ f(a) = f'\circ\alpha(a)$, hence $a \in \ker f'\circ\alpha(a)$ and $f(a) \in \operatorname{im}\overline{f}$.

The last three terms of the second sequence

$$0 \longleftarrow \operatorname{coker} g' \longleftarrow \operatorname{coker}\gamma \longleftarrow \operatorname{coker}\beta \longleftarrow \operatorname{coker}\alpha$$

again come from Lemma 4, the map $\operatorname{coker}\alpha \longrightarrow \operatorname{coker}\beta$ from Lemma 3, and exactness at $\operatorname{coker}\beta$ has to be proved by hand.

Let us now construct a homomorphism $\delta : \ker\gamma \longrightarrow \operatorname{coker}\alpha$. This construction is the heart of the proof of the snake lemma, and the homomorphism δ is called the connecting homomorphism.

We start with $c \in \ker\gamma$; the idea is to pull c back to B, map it down to B', pull it back to A', and finally map it to $\operatorname{coker}\alpha$. Here are the details: since g is surjective, there is some $b \in B$ with $c = g(b)$; then $\beta(b) \in \ker g' = \operatorname{im} f'$, hence $\beta(b) = f'(a')$, for some $a' \in A'$. Now we put $\delta(c) = a' + \operatorname{im}\alpha$; in other words: $\delta = \pi\circ {f'}^{-1}\beta\circ g^{-1}$, where $\pi : A' \longrightarrow \operatorname{coker}\alpha$ is the canonical projection.

This map is well defined: if $c = g(b_1)$ with $b_1 \in B$ and $\beta(b_1) = f'(a_1')$, then $b_1 - b \in \ker g = \operatorname{im} f$, hence $\beta(b_1 - b) \in \operatorname{im}\beta\circ f = \operatorname{im} f'\circ\alpha$. This shows that a' and a_1' are in the same coset modulo $\operatorname{im}\alpha$.

We next show that the sequence is exact at $\ker\gamma$. If $c \in \ker\gamma$ satisfies $c = g(b)$ for some $b \in \ker\beta$, then $\beta(b) = 0$ and $\delta(c) = 0 + \operatorname{im}\alpha$; this proves that $\operatorname{im}\overline{g} \subseteq \ker\delta$. Conversely, let $c \in \ker\delta$. Then $c = \beta(b)$, $\beta(b) = f'(a')$, and $\delta(c) = 0$ means that $a' = \alpha(a)$ for some $a \in A$. But then $\beta(b) = f'(a') = f'\circ\alpha(a) = \beta\circ f(a)$. Thus

$b = f(a) + b_1$ for some $b_1 \in \ker g$. Applying g then shows $c = g(b) = g(b_1)$, hence $c \in \operatorname{im} \overline{g}$.

Finally, we have to show that the snake sequence is exact at $\operatorname{coker} \alpha$. Since $\delta(c) = {f'}^{-1}\beta \circ g^{-1}(c) + \operatorname{im} \alpha$ and the map $\overline{f}' : \operatorname{coker} \alpha \longrightarrow \operatorname{coker} \beta$ is induced by f', we have $f'({f'}^{-1}\beta \circ g^{-1}(c) + \operatorname{im} \beta) = \beta \circ g^{-1}(c) + \operatorname{im} \beta = 0 + \operatorname{im} \beta$, hence $\operatorname{im} \delta \subseteq \ker \overline{f}'$. Conversely, assume that $a' + \operatorname{im} \alpha \in \ker \overline{f}'$. Then $f'(a') \in \operatorname{im} \beta$, that is, $f'(a') = \beta(b)$ for some $b \in B$. Put $c = g(b)$; then $\delta(c) = a' + \operatorname{im} \alpha$ by construction, hence $\ker \overline{f}' \subseteq \operatorname{im} \delta$. □

Note that the exact 6-term sequence is an immediate consequence of the snake lemma: all you have to do is apply it to the exact and commutative diagram

$$\begin{array}{ccccccc} & & A & \xrightarrow{f} & B & \longrightarrow & \operatorname{coker} f \longrightarrow 0 \\ & & {\scriptstyle g\circ f}\downarrow & & \downarrow{\scriptstyle g} & & \downarrow \\ 0 & \longrightarrow & C & \xrightarrow{\mathrm{id}} & C & \longrightarrow & 0 \end{array}$$

3. Tate's formula

Consider the sequence

$$\mathrm{E}(\mathbb{Q}) \xrightarrow{\phi} \overline{E}(\mathbb{Q}) \xrightarrow{\psi} \mathrm{E}(\mathbb{Q}).$$

Lemma 4 then gives us the exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker \phi & \longrightarrow & \ker(\psi \circ \phi) & \longrightarrow & \ker \psi & & \\ & & & & & & \downarrow & & \\ 0 & \longleftarrow & \operatorname{coker} \psi & \longleftarrow & \operatorname{coker} (\psi \circ \phi) & \longleftarrow & \operatorname{coker} \phi & & \end{array}$$

Now $\ker \phi = \{\mathcal{O}, T\}$, $\ker(\psi \circ \phi) = \mathrm{E}(\mathbb{Q})[2]$, $\ker \psi = \{\mathcal{O}, \overline{T}\}$, $\operatorname{coker} \phi = \overline{E}/\operatorname{im} \phi \simeq \overline{E}/\ker \beta \simeq \operatorname{im} \beta$, $\operatorname{coker} (\psi \circ \phi) = \overline{E}(\mathbb{Q})/2\overline{E}(\mathbb{Q})$ and $\operatorname{coker} \psi \simeq \mathrm{E}/\ker \alpha \simeq \operatorname{im} \alpha$, so the above exact sequence becomes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \{\mathcal{O}, T\} & \longrightarrow & \mathrm{E}(\mathbb{Q})[2] & \longrightarrow & \{\mathcal{O}, \overline{T}\} & & \\ & & & & & & \downarrow & & \\ 0 & \longleftarrow & \operatorname{im} \alpha & \longleftarrow & \mathrm{E}(\mathbb{Q})/2\,\mathrm{E}(\mathbb{Q}) & \longleftarrow & \operatorname{im} \beta & & \end{array}$$

If we put $\#E(\mathbb{Q})[2] = 2^t$, then since $\mathrm{E}(\mathbb{Q})$ is finitely generated (we proved this for all elliptic curves for which $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite), then the classification theorem for finitely generated abelian groups says that $\mathrm{E}(\mathbb{Q}) = \mathrm{E}(\mathbb{Q})_{\mathrm{tors}} \oplus \mathbb{Z}^r$, where $r \in \mathbb{N}$ is called the (Mordell-Weil-) rank of $\mathrm{E}(\mathbb{Q})$. Thus $\#\,\mathrm{E}(\mathbb{Q})/2\,\mathrm{E}(\mathbb{Q}) = 2^{r+t}$, and we find $2 \cdot 2 \cdot 2^{r+t} = 2^t \cdot \#\operatorname{im} \alpha \cdot \#\operatorname{im} \beta$, that is,

$$2^r = \frac{\#\operatorname{im} \alpha \cdot \#\operatorname{im} \beta}{4}.$$

Exchanging the roles of E and $\overline{E}$ shows immediately that the 2-isogenous curves E and $\overline{E}$ have the same rank.

Let me also recall the description of the image of α again. Starting with a rational point $P = (x, y) \in E(\mathbb{Q})$, we have constructed an integral point (N, M, e) on one of the torsors $\mathcal{T}_{b_1}^{(\psi)}$; given (N, M, e), we can compute x from $x = b_1(M/e)^2$.

Thus (x,y) leads to a point on $\mathcal{T}_{b_1}^{(\psi)}$, where b_1 is determined by $b_1\mathbb{Q}^{\times 2} = x\mathbb{Q}^{\times 2}$. The map α was defined by $\alpha(P) = x\mathbb{Q}^{\times 2}$: an element $b_1\mathbb{Q}^{\times 2}$ is in the image of α if and only if $\mathcal{T}_{b_1}^{(\psi)}$ has a rational (and therefore integral) point.

4. Tate's Method

In this section we want to describe Tate's method for computing the rank of (certain) elliptic curves $E : y^2 = x(x^2 + ax + b)$. The idea is to consider E simultaneously with the 2-isogenous curve $\overline{E} : y^2 = x(x^2 + \overline{a}x + \overline{b})$, where $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$. Here's what to do:

(1) List all torsors $\mathcal{T}^{(\psi)}(b_1) : N^2 = b_1M^4 + aM^2e^2 + b_2e^4$, where b_1 runs through the squarefree divisors of $b = b_1b_2$; the number of such torsors that have a rational point $\neq (0,0,0)$ is a power of 2, say 2^w.
(2) List all torsors $\mathcal{T}^{(\phi)}(b_1) : N^2 = b_1M^4 + \overline{a}M^2e^2 + b_2e^4$, where b_1 runs through the squarefree divisors of $\overline{b} = b_1b_2$; the number of such torsors that have a rational point $\neq (0,0,0)$ is a power of 2, say $2^{\overline{w}}$.
(3) The rank of E (and of $\overline{E}$) is given by $r = w + \overline{w} - 2$.

Example. 1. Consider $E : y^2 = x(x^2 + 1)$. There are only two squarefree divisors of $b = 1$, but only $\mathcal{T}^{(\psi)}(1)$ has a rational point:

b_1	$\mathcal{T}^{(\psi)}(b_1)$	(N,M,e)	P
1	$N^2 = M^4 + e^4$	$(1,1,0)$	$\mathcal{O}$
-1	$N^2 = -M^4 - 5e^4$		

Thus $w = 0$.

2. Consider $\overline{E} : y^2 = x(x^2 - 4)$. Here we find four torsors:

b_1	$\mathcal{T}^{(\phi)}(b_1)$	(N,M,e)	P
1	$N^2 = M^4 - 4e^4$	$(1,1,0)$	$\mathcal{O}$
-1	$N^2 = -M^4 + 4e^4$	$(2,0,1)$	$(0,0)$
2	$N^2 = 2M^4 - 2e^4$	$(0,1,1)$	$(2,0)$
-2	$N^2 = -2M^4 + 2e^4$	$(0,1,1)$	$(-2,0)$

Thus $\overline{w} = 2$.

3. Now Tate's formula gives $r = 0 + 2 - 2 = 0$, that is, $E(\mathbb{Q}) = E(\mathbb{Q})_{\rm tors}$ and $\overline{E}(\mathbb{Q}) = \overline{E}(\mathbb{Q})_{\rm tors}$. Determining these torsion groups using Nagell-Lutz is left as an exercise.

As we will see, the main problem with this method is that we do not have an algorithm for deciding which of the torsors $\mathcal{T}(b_1)$ have rational points and which don't.

5. Selmer and Tate-Shafarevich Groups

For computing the rank of an elliptic curve E : $y^2 = x(x^2 + ax + b)$ we have to decide whether certain torsors have rational points or not, that is, we have to compute $\#\operatorname{im}\alpha$ and $\#\operatorname{im}\beta$. This is a difficult problem. On the other hand, it is relatively easy to decide whether these torsors have local solutions everywhere,

that is, whether they have solutions modulo all prime powers and in the reals. The classes $b_1\mathbb{Q}^{\times 2}$ corresponding to such everywhere locally solvable torsors $\mathcal{T}^{(\psi)}(b_1)$ (these are the torsors that have solutions modulo every prime power as well as real solutions) form a group $\mathrm{Sel}^{(\psi)}(\overline{E}/\mathbb{Q})$ containing $W(\overline{E}/\mathbb{Q}) := \mathrm{im}\ \alpha$ as a subgroup.

The group structure can be explained as follows: if $\mathcal{T}^{(\psi)}(b_1)$ and $\mathcal{T}^{(\psi)}(b_1')$ have points over some field K containing $\mathbb{Q}$ (we only use $\mathbb{Q}$ itself as well as the p-adic completions $\mathbb{Q}_p$), then these give rise to points $P, P' \in E(K)$; the point $P'' = P + P'$ will come from some K-rational point on the torsor $\mathcal{T}^{(\psi)}(b_1'')$, where $b_1''\mathbb{Q}^{\times 2} = \alpha(P'') = \alpha(P)\alpha(P') = b_1 b_1'\mathbb{Q}^{\times 2}$.

The following exact sequence then defines the ψ-part of the Tate-Shafarevich group of $\overline{E}$:

$$0 \longrightarrow W(\overline{E}/\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(\psi)}(\overline{E}/\mathbb{Q}) \longrightarrow \text{Ш}(\overline{E}/\mathbb{Q})[\psi] \longrightarrow 0$$

Note that both $W(\overline{E}/\mathbb{Q})$ and $\mathrm{Sel}^{(\psi)}(\overline{E}/\mathbb{Q})$ are finite elementary-abelian 2-groups, hence so is their quotient $\text{Ш}(\overline{E}/\mathbb{Q})[\psi]$. Using Galois cohomology one can define the full Tate-Shafarevich group $\text{Ш}(\overline{E}/\mathbb{Q})$; the conjecture that this group is always finite is an important part of the Birch–Swinnerton-Dyer conjecture.

Of course there is a 'dual' sequence

$$0 \longrightarrow W(\mathrm{E}/\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(\phi)}(\mathrm{E}/\mathbb{Q}) \longrightarrow \text{Ш}(\mathrm{E}/\mathbb{Q})[\phi] \longrightarrow 0;$$

note that although $\mathrm{E}(\mathbb{Q})$ and $\overline{E}(\mathbb{Q})$ have the same rank r, their torsion subgroups, Selmer groups, and Tate-Shafarevich groups are in general different.

6. Local Solvability

Let us now discuss how we can test a torsor $\mathcal{T}^{(\psi)}(b_1)$ for local solvability. Such a test consists of two parts: checking solvability modulo p, and then checking whether solutions modulo p can be lifted to $\mathbb{Q}_p$.

A theorem due to F.K. Schmidt says that any smooth curve of genus 1 has an $\mathbb{F}_p$-rational point. Thus $\mathcal{T}^{(\psi)}(b_1)$ is solvable modulo p for all primes $p \nmid 2b(a^2 - 4b)$. Let me now explain an elementary way to prove this result.

Theorem 6. *The quartic $\mathcal{T}_{b_1} : Y^2 = b_1X^4 + aX^2 + b_2$ has nontrivial solutions modulo every prime p not dividing $2(a^2 - 4b_1b_2)$.*

For the proof of this result we need some preparations. We start with

Lemma 7. *Let $f, g \in \mathbb{F}_p[X]$ be quadratic polynomials over $\mathbb{F}_p$. If $f(t)^n = g(t)^n$ for all $t \in \mathbb{F}_p$ and some integer $n \le \frac{p-1}{2}$, then there exists a constant $c \in \mathbb{F}_p$ such that $f = c \cdot g$.*

Proof. Clearly $\deg f^n = n \deg f \le p - 1$, hence the polynomial $f^n - g^n$ has degree $\le p - 1$ and at least p roots 0, 1, …, $p - 1$. Since $\mathbb{F}_p$ is a field, polynomials of degree m have at most m roots; hence we conclude that $f^n = g^n$.

Now factor f and g into linear factors over some finite extension of $\mathbb{F}_p$; then every root α with multiplicity m is a root of multiplicity mn of f^n, thus of g^n, hence a root of multiplicity m of g. Thus f and g have the same roots (with multiplicity) over some extension of $\mathbb{F}_p$, hence they are equal up to some constant c (which necessarily is an element of the base field $\mathbb{F}_p$ since the coefficients of f and g are). □

Proposition 8. *Assume that $f, g \in \mathbb{F}_p[X]$ are quadratic polynomials over $\mathbb{F}_p$ such that $(\frac{f(t)}{p}) = (\frac{g(t)}{p})$ for all $t \in \mathbb{F}_p$. Then there exists a constant $c \in \mathbb{F}_p$ such that $f = c \cdot g$.*

Proof. By Euler's criterion we know that $(\frac{f(t)}{p}) \equiv f(t)^n \pmod p$ with $n = \frac{p-1}{2}$; thus the assumptions imply that $f(t)^n \equiv g(t)^n \pmod p$ for all $t \in \mathbb{F}_p$, so the claim follows from Lemma 7. □

Corollary 9. *We have $\left(\frac{(x_0t-y_0)^2-b_2}{p}\right) = \left(\frac{t^2-b_1}{p}\right)$ for $t = 0, 1, \dots, p-1$ if and only if $y_0 = 0$ and $b_2 = b_1x_0^2$.*

Proof. If $y_0 = 0$ and $b_2 = b_1x_0^2$, the claim is obvious. If $\left(\frac{(x_0t-y_0)^2-b_2}{p}\right) = \left(\frac{t^2-b_1}{p}\right)$ for $t = 0, 1, \dots, p-1$, on the other hand, then applying Prop. 8 shows that $f(X) = (x_0X-y_0)^2-b_2$ and $g(X) = X^2-b_1$ differ by a constant factor c; comparing the coefficients of the leading term shows that $c = x_0^2$ whereas comparing linear terms gives $y_0 = 0$. Finally, comparing constant terms shows that $b_2 = b_1x_0^2$. □

Now we are ready to give the

Proof of Theorem 6. If $e = 0$ gives rise to a solution (N, M, e), then we have $N^2 \equiv b_1M^4 \bmod p$, and this implies that b_1 is a square modulo p (possibly 0). Conversely, if b_1 is a square modulo p, then there exists an $\mathbb{F}_p$-rational point (N, M, e) with $e = 0$ (and $M \neq 0$).

If b_1 is a square modulo p we are done, so from now on we will assume that $(b_1/p) = -1$. In this case we can't have solutions with $e = 0$, so we might as well divide through by e^4, put $y = N/e^2$ and $X = M/e$, and get

$$y^2 = b_1X^4 + aX^2 + b_2. \tag{3}$$

Now the substitution $X^2 = x$ transforms (3) into the conic

$$\mathcal{C} : y^2 = b_1x^2 + ax + b_2. \tag{4}$$

Our aim is to find an $\mathbb{F}_p$-rational point (x, y) on $\mathcal{C}$ such that $x = X^2$ is a square. The proof proceeds in several steps:

1. The conic $\mathcal{C}$ has an $\mathbb{F}_p$-rational point.

Proposition 10. *Let $\mathcal{C} : Y^2 = aX^2 + bX + c$ be a conic defined over $\mathbb{F}_p$, where p is an odd prime, and assume that $a \neq 0$. Then $\mathcal{C}(\mathbb{F}_p) \neq \varnothing$.*

Proof. Assume not; then the values of the polynomial $f(X) = aX^2 + bX + c$ are nonsquares for every $x \in \mathbb{F}_p$. Thus, by Euler's criterion, $f(X) = (aX^2 + bX + c)^{(p-1)/2} + 1 \in \mathbb{F}_p[X]$ is a polynomial of degree $p-1$ (here we use that $a \neq 0$) with $f(x) = 0$ for all $x \in \mathbb{F}_p$: this is a contradiction because polynomials f over fields have at most $\deg f$ roots.

The argument above goes back to Lagrange; a different proof starts with the observation that the polynomial $f(X) = aX^2+bX+c$ attains exactly $\frac{p+1}{2}$ different values (by completing the square the claim can be reduced to counting values of $f(X) = X^2$). Since there are only $\frac{p-1}{2}$ nonsquares in $\mathbb{F}_p$, the claim follows. □

2. Parametrize the conic $\mathcal{C}$ using lines through the known point (x_0, y_0).

Proposition 11. *Let $\mathcal{C} : Y^2 = aX^2 + bX + c$ be a nonsingular conic defined over $\mathbb{F}_p$, and let $P = (x_0, y_0)$ be a point in $\mathcal{C}(\mathbb{F}_p)$. Then the $\mathbb{F}_p$-rational points $\neq P$ are given by*

$$x = \frac{t^2x_0 - 2ty_0 + ax_0 + b}{t^2 - a}, \tag{5}$$

$$y = \frac{-t^2y_0 + t(2ax_0 + b) - ay_0}{t^2 - a}. \tag{6}$$

Since we assumed that b_1 is a nonsquare modulo p, every $t \in \mathbb{F}_p$ gives rise to a point on $\mathcal{C}$ over $\mathbb{F}_p$. If $x_0 = 0$, then x_0 is a square and we are done. If $x_0 \neq 0$, then we can multiply the numerator and denominator in (5) by x_0 and get

$$x = \frac{(x_0t - y_0)^2 - b_2}{x_0(t^2 - b_1)}. \tag{7}$$

3. Assume that there is no point $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ on $\mathcal{C}$ with $x \in \mathbb{F}_p^2$; then we must have $(x/p) = -1$ for all x, in particular $(x_0/p) = -1$ and therefore $\left(\frac{(x_0t-y_0)^2-b_2}{p}\right) = \left(\frac{t^2-b_1}{p}\right)$ for all $t \in \mathbb{F}_p$.

By Corollary 9 we have $y_0 = 0$ and $b_2 = x_0^2b_1$. This gives $0 = y_0^2 = b_1x_0^2 + ax_0 + b_2 = b_1x_0^2 + ax_0 + b_1x_0^2$, hence $a = -2b_1x_0$. But then $a^2 - 4b_1b_2 = 0$ contradicting the assumption. □

This criterium allows us to decide in a finite number of steps for which primes a given quartic has an $\mathbb{F}_p$-rational point. If such a point exists, it is easy to transform the quartic into an elliptic curve in Weierstrass form, for which the bounds of Hasse apply.

As a first step in deciding whether $\mathcal{T}_{b_1} : Y^2 = b_1X^4 + aX^2 + b_2$ has a nontrivial rational solution, one checks whether $\mathcal{T}_{b_1}$ has solutions in all completions $\mathbb{Q}_p$ of the rationals. Fortunately, it is sufficient to test solvability only for a finite number of 'bad' primes. Here is what we know so far: $\mathcal{T}(b_1)$ has $\mathbb{F}_p$-rational points for every prime $p \nmid 2(a^2 - 4b)$, where $b = b_1b_2$. Note that $a^2 - 4b = \operatorname{disc} g$, where $g(X) = b_1X^2 + aX + b_2$.

Now the polynomial $f(X) = b_1X^4 + aX^2 + b_2$ has discriminant $\operatorname{disc} f = 16b(a^2 - 4b)^2 = 16b(\operatorname{disc} g)^2$. Although $p \nmid 2 \operatorname{disc} g$ was sufficient to guarantee solvability modulo p, for lifting these solutions to the completions via Hensel's Lemma we need the stronger condition $p \nmid \operatorname{disc} f$. Thus we have proved the following

Theorem 12. *The quartic $\mathcal{T}(b_1)$ has a solution in $\mathbb{Z}_p$ for all primes p not dividing $2b(a^2 - 4b)$.*