DESCENT BY 2-ISOGENY (AFTER CASSELS)

MARTIN BRIGHT

In this lecture we will use descent by 2-isogeny to prove the weak Mordell–Weil theorem for an elliptic curve over the rational numbers $\mathbb{Q}$ having a rational 2-torsion point. The main references are §14 of Cassels [1] and the notes on complex elliptic curves by Stevenhagen [3].

1. Introduction

Ultimately we would like to prove the following theorem.

Theorem 1 (Mordell–Weil)**.** *Let k be a number field, and let E be an elliptic curve over k. Then the group $E(k)$ is a finitely generated Abelian group.*

A full proof of this can be found, for example, in Milne [2]. Any standard proof of the Mordell–Weil theorem consists of two steps, the first of which is to prove the so-called *weak Mordell–Weil theorem*:

Theorem 2. *Under the assumptions of Theorem 1, the quotient group $E(k)/2E(k)$ is finite.*

This theorem is then combined with the theory of heights to deduce the Mordell–Weil theorem. In the context of this course, there are two barriers to presenting he complete proof of the weak Mordell–Weil theorem: firstly that it makes use of Galois cohomology, and secondly that it uses results (finiteness of the class group and structure of the unit group) from algebraic number theory. These are both fascinating and important topics, but they are not required as background for this course. To avoid needing algebraic number theory, we will stick to the case $k = \mathbb{Q}$; and, to avoid needing Galois cohomology, we will require that E have a rational 2-torsion point. These notes contain a proof of the weak Mordell–Weil theorem in that case. In fact, we get rather more than just a proof: we also obtain a practical algorithm for bounding (and, in many cases, computing exactly) the rank of the group $E(\mathbb{Q})$.

2. A historical example

To demonstrate the history behind descent, we prove the following theorem of Fermat.

Theorem 3 (Fermat)**.** *The equation $x^4 + y^4 = z^2$ has no solutions in integers with x and y both non-zero.*

Proof. The idea is to suppose that there is indeed a solution, and show that we can always produce a smaller solution – this is Fermat's method of "infinite descent". Because there is no infinite strictly decreasing sequence of positive integers, we deduce that there can be no solutions.

We will phrase the argument slightly differently, by starting with a minimal solution. So suppose that (x, y, z) is a solution with x, y non-zero and $\max\{|x|, |y|\}$ minimal. We can assume that z is positive.

Date: October 2020.

It follows that x, y, z are coprime: if some prime p were to divide all of x, y, z, then p^4 would divide z^2 and so p^2 would divide z. So we could replace (x, y, z) by $(x/p, y/p, z/p^2)$ and obtain a smaller solution, contradicting minimality. And in fact x, y, z are pairwise coprime, since any prime dividing two of them also has to divide the third.

Recall that the square of an even number is congruent to 0 (mod 4), and the square of an odd number is congruent to 1 (mod 4). So, looking at the equation modulo 4, we see that x and y cannot both be odd. As they are coprime, one must be odd and the other even. We assume that x is even and y is odd (and therefore z is also odd).

Now, rearranging the equation and factorising gives

$$x^4 = (z + y^2)(z - y^2).$$

The left-hand side is positive; since $z + y^2$ is positive, both the factors on the right-hand side must be positive. Let's consider their gcd. If a prime p divides both $(z + y^2)$ and $(z - y^2)$, then p also divides $(z + y^2) + (z - y^2) = 2z$. If p were to divide z, then p would also divide $(z + y^2) - z = y^2$; but y and z are coprime. So p can only be 2.

We thus have two positive integers, with no prime factors in common apart from possibly 2, whose product is a fourth power. Considering prime factorisations shows that $(z + y^2)$ and $(z - y^2)$ must both be of the form $2^r \times$ (fourth power). Furthermore, y^2 and z are both odd, so only one of $z \pm y^2$ is a multiple of 4. That means that one of $z \pm y^2$ is of the form $2 \times$ (fourth power), and the other is of the form $8 \times$ (fourth power).

One possibility is

$$z + y^2 = 8u^4, \qquad z - y^2 = 2v^4$$

for some integers u, v. However, eliminating z gives $y^2 = 4u^4 - v^4$ which is impossible, since y is odd (look modulo 4).

Therefore the other possibility holds:

$$z + y^2 = 2u^4, \qquad z - y^2 = 8v^4,$$

where u, v are coprime integers with u odd. Eliminating z gives

$$y^2 = u^4 - 4v^4.$$

This is the halfway point of the proof. We treat this equation in the same way as the original one: factorising gives

$$4v^4 = (u^2 + y)(u^2 - y)$$

and it follows that both $u^2 \pm y$ must be of the form $2 \times$ (fourth power). Setting $u^2 + y = 2r^4$ and $u^2 - y = 2s^4$ and eliminating y gives

$$r^4 + s^4 = u^2,$$

and so (r, s, u) is a new solution to our original equation. Going back through the substitutions shows $x^4 = 16u^4v^4 = 16u^4r^4s^4$; so r, s are non-zero and smaller than x, contradicting minimality of the original solution. □

What is going on in this proof? We have two curves

$$E: \quad X^4 + Y^4 = Z^2 \quad \text{and} \quad E': \quad U^4 - 4V^4 = W^2,$$

together with two morphisms between them:

$$\phi\colon E \to E', \quad (u, v, w) = (z, xy, x^4 - y^4)$$
$$\psi\colon E' \to E, \quad (x, y, z) = (2uv, w, u^4 + 4v^4).$$

These curves are both elliptic curves (though they look a little unusual since they are not in Weierstrass form), and the morphisms ϕ, ψ are isogenies. In fact, the composition $\psi \circ \phi\colon E \to E$ is multiplication by 2 in the group of E. In the proof, we started with a point $P = (x, y, z) \in E(\mathbb{Q})$ and we showed that P was of the form $\psi(P')$ for some $P' = (u, v, w) \in E'(\mathbb{Q})$. Then we showed that P' was of the form $\phi(Q)$ for some $Q = (r, s, u) \in E(\mathbb{Q})$. The fact that Q had smaller coefficients than P (in fact, $2Q = P$ in the group $E(\mathbb{Q})$) led to a contradiction.

The idea of descent by 2-isogeny is to replicate this method on more general elliptic curves. In this particular example, the map $\psi\colon E'(\mathbb{Q}) \to E(\mathbb{Q})$ was not quite surjective: we had to assume x odd, y even and z positive in order to lift the point P. In the second step, the map $\phi\colon E(\mathbb{Q}) \to E'(\mathbb{Q})$ turned out to be surjective. The important general result will be that each of these homomorphisms has finite cokernel.

3. Constructing a 2-isogeny

We begin with an elliptic curve E defined over $\mathbb{Q}$, having a rational 2-torsion point. If E is in short Weierstrass form and the 2-torsion point is $(\alpha, 0)$, then the substitution $X \mapsto X + \alpha$ translates the 2-torsion point to $(0, 0)$ and the equation of E becomes

$$E: \quad y^2 = x(x^2 + ax + b)$$

and, after a suitable change of variables, we can assume $a, b \in \mathbb{Z}$. Because E is non-singular, the cubic on the right-hand side has three distinct roots: so we have $b \neq 0$ and $a^2 - 4b \neq 0$.

Lemma 4. *There is a second elliptic curve E' over $\mathbb{Q}$ and an isogeny $\phi\colon E \to E'$ having kernel $\{O, (0, 0)\}$. Specifically, E' is given by*

$$E': \quad v^2 = u(u^2 + a'u + b')$$

with $a' = -2a$ and $b' = a^2 - 4b$; and ϕ is given by

$$\phi(x, y) = \begin{cases} (x + a + b/x, y - by/x^2) & \text{if } x \neq 0; \\ O & \text{if } (x, y) = (0, 0). \end{cases}$$

Proof. Of course, the easiest way to prove this lemma is simply to verify that the given E' and ϕ have the claimed properties. However, it is interesting to see how we might have found them in the first place.

One method is to view E as an elliptic curve over $\mathbb{C}$. Then there is an isomorphism (of Riemann surfaces) $\pi\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$, for some lattice $\Lambda = \langle \lambda_1, \lambda_2 \rangle \subset \mathbb{C}$, and the 2-torsion point can be taken to be $\pi(\lambda_1/2)$. Then E' and ϕ need to fit into the commutative diagram

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow[\sim]{\pi} & E(\mathbb{C}) \\ {\scriptstyle 2:1}\downarrow & & {\scriptstyle 2:1}\downarrow \\ \mathbb{C}/\langle \frac{1}{2}\lambda_1, \lambda_2 \rangle & \xrightarrow[\sim]{} & E'(\mathbb{C}) \end{array}.$$

For details of how this approach can be used to calculate E' and ϕ, see Example 3.10 of [3].

Another approach is to use Galois theory, as in [1]. Suppose that there is such a morphism ϕ; then ϕ induces a pull-back map $\phi^*\colon \mathbb{Q}(E') \to \mathbb{Q}(E)$, which realises $\mathbb{Q}(E')$ as a subfield of $\mathbb{Q}(E)$, and the degree $[\mathbb{Q}(E) : \phi^*\mathbb{Q}(E')]$ is 2. Since ϕ maps a point $P \in E$ and $P + (0, 0)$ to the same image, any rational function in $\phi^*\mathbb{Q}(E')$ must be invariant under the automorphism of E induced by taking P to $P + (0, 0)$. Let us find such functions directly.

If $P = (x, y)$ is a point of E, then we can calculate $P + (0, 0) = (b/x, -by/x^2)$. One function which is obviously invariant under replacing P with $P + (0, 0)$ is the function $x + b/x$; it turns out to be slightly better to instead use the function $\lambda = x + a + b/x$, which the equation for E shows is equal to $(y/x)^2$. Similarly, adding the y-coordinates of P and $P + (0, 0)$ gives the function $\mu = y - by/x^2$. These functions (λ, μ) certainly define a morphism ψ from E to somewhere, which satisfies $\psi(P) = \psi(P + (0, 0))$ for all points P of E.

Now check that λ, μ satisfy the equation

$$\mu^2 = \lambda(\lambda^2 + a'\lambda + b')$$

with $a' = -2a$ and $b' = a^2 - 4b$. That means that the image of ψ is contained in the elliptic curve E' defined by that equation. If we can show that ψ has degree 2, then ψ will indeed be the ϕ that we have been looking for. The subfield $\psi^*\mathbb{Q}(E')$ of $\mathbb{Q}(E)$ is generated by λ and μ; and both x and y can be written as rational expressions in λ, μ and $\sqrt{\lambda} = y/x$. Since x and y generate $\mathbb{Q}(E)$, we have

$$\psi^*\mathbb{Q}(E') = \mathbb{Q}(\lambda, \mu) \subsetneq \mathbb{Q}(E) \subset \mathbb{Q}(\lambda, \mu, \sqrt{\lambda})$$

and the total extension here has degree 2; so ψ does indeed have degree 2. □

The new curve E' also has a 2-torsion point at $(0, 0)$, and this was the reason for choosing λ rather than $x + b/x$ for the coordinate on E'. It is natural to ask what happens if we apply the same construction again, starting with E'. We obtain an isogeny $\phi' \colon E' \to E''$, where E'' is defined by

$$E'' : \quad Y^2 = X(X^2 + a''X + b'')$$

and we calculate

$$a'' = -2a' = 4a, \quad b'' = (a')^2 - 4b' = 4a^2 - 4(a^2 - 4b) = 16b.$$

Now the substitution $X \mapsto 4x, Y \mapsto 8y$ gives an isomorphism from E'' to E. So applying the construction of Lemma 4 twice takes us back to where we started. More precisely, we can check that the following holds:

Lemma 5. *Under the conditions of Lemma 4, there is a second isogeny $\hat{\phi} \colon E' \to E$, defined by*

$$\hat{\phi}(u, v) = \begin{cases} \left(\frac{1}{4}(u + a' + b'/u), \frac{1}{8}(v - b'v/u^2)\right) & \text{if } x \neq 0; \\ O & \text{if } (u, v) = (0, 0). \end{cases}$$

The kernel of $\hat{\phi}$ consists of $\{O, (0, 0)\} \subset E'(\mathbb{Q})$, and the composite $\hat{\phi} \circ \phi \colon E \to E$ is equal to multiplication by 2 in the group law of E.

Remark. The isogeny $\hat{\phi}$ is called the *dual isogeny* to ϕ. This is a special case of a more general phenomenon: for every isogeny ϕ of degree n, there is a dual isogeny $\hat{\phi}$ in the opposite direction such that $\hat{\phi} \circ \phi$ is multiplication by n.

4. The cokernel of the 2-isogeny

The next step is to understand the image of $E(\mathbb{Q})$ inside $E'(\mathbb{Q})$. To do this, we define a map from $E'(\mathbb{Q})$ to the quotient group $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. This quotient group consists of equivalence classes of non-zero rational numbers, where α and $\alpha\beta^2$ are considered equivalent. It follows that each equivalence class contains exactly one element that is a square-free integer.

Lemma 6. *Define a function* $q\colon E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ *as follows.*

$$q((u,v)) = [u] \quad \text{if } u \neq 0;$$
$$q((0,0)) = [a^2 - 4b];$$
$$q(O) = [1].$$

Then q *is a homomorphism of groups, and the sequence*

$$E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{q} \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

is exact.

Proof. To see that q is a homomorphism of groups, consider two points $P, Q \in E(\mathbb{Q})$ and suppose that $P \neq \pm Q$ and that neither is equal to $(0,0)$. Then the line L through P and Q is defined by $v = cu + d$, and L meets E' in the three points $P, Q, -(P+Q)$. Substituting the equation of L into the equation for E' gives

$$(cu+d)^2 = u(u^2 + a'u + b')$$

and so

$$u^3 + (a' - c^2)u^2 + (b' - 2cd)u - d^2 = 0.$$

The three roots of this equation correspond to the u-coordinates of $P, Q, P+Q$, and the product of the three roots is d^2, a square. This gives $u(P)u(Q)u(P+Q) = d^2$, or equivalently $u(P+Q) = u(P)u(Q)(d/u(P)u(Q))^2$. The remaining cases when one of $P, Q, P+Q$ is equal to O, or when either $u(P)$ or $u(Q)$ is 0, can be checked separately.

Now let us show that the kernel of q contains $\phi(E(\mathbb{Q}))$. First suppose that $(x,y) \neq (0,0)$ lies in $E(\mathbb{Q})$; then $q(\phi(x,y))$ is equal to $x + a + b/x = (y/x)^2$ so is a non-zero square, unless $y = 0$. The case $y = 0$ can only happen when E has a rational 2-torsion point other than $(0,0)$, in which case the discriminant $a^2 - 4b$ must be a square; then we have $q(\phi(x,y)) = q((0,0)) = a^2 - 4b$. Finally, we also have $q(\phi((0,0))) = q(O) = 1$ and $q(\phi(O)) = q(O) = 1$. In all cases, for $P \in E(\mathbb{Q})$, we have $q(\phi(P)) \in (\mathbb{Q}^\times)^2$, that is, $\phi(P)$ lies in the kernel of q.

Finally, we show that the kernel of q is contained in $\phi(E(\mathbb{Q}))$. Suppose that $(u,v) \in E'(\mathbb{Q})$ lies in $\ker q$, with $u \neq 0$; then u is a square. The point (x,y) with $x = \frac{1}{2}(u + \sqrt{u}v - a)$ and $y = \sqrt{u}x$ lies in $E(\mathbb{Q})$, and it is easy to check that $\phi(x,y)$ is equal to (u,v). Now suppose $(u,v) = (0,0)$. Any point (x,y) satisfying $\phi(x,y) = (0,0)$ satisfies $x + a + b/x = 0$, or equivalently $x^2 + ax + b = 0$; this has rational solutions if and only if $q((0,0)) = a^2 - 4b$ is a square. Also O always lies in the image of $E(\mathbb{Q})$. Thus $\phi(E(\mathbb{Q}))$ contains $\ker q$. □

Remark. For experts in Galois cohomology, this lemma is a very explicit version of the following fact. The short exact sequence

$$0 \to \ker\phi \to E(\bar{\mathbb{Q}}) \xrightarrow{\phi} E'(\bar{\mathbb{Q}}) \to 0$$

gives rise to a long exact sequence in Galois cohomology, part of which is

$$E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{\partial} \mathrm{H}^1(\mathbb{Q}, \ker\phi).$$

We know that $\ker\phi = \{O, (0,0)\}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and a standard calculation gives $\mathrm{H}^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. The map q is then identified with the boundary map ∂.

The isomorphism theorem shows that $\operatorname{coker}\phi = E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ is isomorphic to the image $\operatorname{im} q$. The following lemma helps us to identify which elements of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ lie in $\operatorname{im} q$.

Lemma 7. *Let r be a square-free integer. The class $[r] \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ lies in the image of q if and only if the equation*

$$r^2\ell^4 + a'r\ell^2m^2 + b'm^4 = rn^2$$

has a non-zero solution (ℓ, m, n) with $\ell, m, n \in \mathbb{Z}$. Furthermore, this can only happen if r divides b'.

Proof. For $r = 1$ the equation always has the solution $(1, 0, 1)$, so $[1]$ always lies in the image of q. Similarly, b' lies in the image of q because for $r = b'$ there is the solution $(0, 1, 1)$. Suppose now that $r \neq 1, b'$ and that there exists $(u, v) \in E'(\mathbb{Q})$ with $q((u, v)) = r$. Then we have $u \neq 0$, and $[u] = [r]$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Looking at the equation of E', we see that $u(u^2 + a'u + b')$ is a square, and so furthermore $[u^2 + a'u + b'] = [u] = [r]$. Equivalently, there are rational numbers s, t satisfying $u = rt^2$ and $u^2 + a'u + b' = rs^2$. Substituting the first into the second gives

$$r^2t^4 + a'rt^2 + b' = rs^2.$$

Writing $t = \ell/m$ with ℓ, m coprime integers, and clearing denominators, we obtain

$$r^2\ell^4 + a'r\ell^2m^2 + b'm^4 = r(sm^2)^2;$$

The left-hand side is an integer. If sm^2 were not an integer, then the right-hand side would not be an integer (because r is square-free); so we can write $sm^2 = n$ with $n \in \mathbb{Z}$. We have proved: if r lies in the image of q, then the equation

$$r^2\ell^4 + a'r\ell^2m^2 + b'm^4 = rn^2 \tag{1}$$

has a solution with $\ell, m, n \in \mathbb{Z}$, and with ℓ, m coprime. Conversely, it is easy to verify that any solution to (1) with $\ell, m, n \in \mathbb{Z}$ gives rise to a (u, v) satisfying $q((u, v)) = [r]$.

Next, we show that this can only happen if r divides b'. Suppose that we have a solution $(\ell, m, n) \in \mathbb{Z}^3$, and that there is a prime p satisfying $p \mid r$ but $p \nmid b'$. Then p must divide $b'm^4$, and therefore $p \mid m$. Now every term on the left-hand side is divisible by p^2; so rn^2 is divisible by p^2; since r is square-free, it follows that p divides n. Now every term except possibly the first one is divisible by p^3; therefore $r^2\ell^4$ is also divisible by p^3, and (again since r is square-free) it follows that p divides ℓ. But ℓ and m were coprime, giving a contradiction. □

Remark. Once it is known that r divides b', the equation (1) is equivalent to

$$r\ell^4 + a'\ell^2m^2 + (b'/r)m^4 = n^2. \tag{2}$$

Corollary 8. *The quotient $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ is finite.*

Proof. Lemma 7 shows that the image of q is finite, since there are only finitely many integers dividing b'. By the isomorphism $E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \cong \operatorname{im} q$, it follows that $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ is finite. □

Remark. To explicitly calculate $\operatorname{im} q$, we can list the r dividing b' and (try to) test whether (2) has integer solutions for each such r. We often also want to do the same calculation with $\hat{\phi}$ in place of ϕ. In that case, Lemma 7 states that we have to check every r satisfying $r \mid ((a')^2 - 4b') = 16b$. A closer look at the proof shows that it is actually sufficient to consider r dividing b.

5. The weak Mordell–Weil theorem

In this section we deduce Theorem 2 in the case that $k = \mathbb{Q}$ and E has a rational 2-torsion point. We begin with a standard lemma from homological algebra.

Lemma 9 (Kernel-cokernel sequence)**.** *Let $A \xrightarrow{f} B \xrightarrow{g} C$ be two homomorphisms of Abelian groups. Then the sequence*

$$0 \to \ker(f) \xrightarrow{\mathrm{id}} \ker(g \circ f) \xrightarrow{f} \ker(g) \xrightarrow{\mathrm{id}} \operatorname{coker}(f) \xrightarrow{g} \operatorname{coker}(g \circ f) \xrightarrow{\mathrm{id}} \operatorname{coker}(g) \to 0$$

is exact.

Proof. This is an easy verification (or see any homological algebra textbook). □

Proof of Theorem 2 in the special case. Suppose that E is an elliptic curve over $\mathbb{Q}$ having a rational 2-torsion point P. By Lemma 4 there is another elliptic curve E' over $\mathbb{Q}$ and an isogeny $\phi\colon E \to E'$ with kernel $\{O, P\}$. By Lemma 5, there is a dual isogeny $\hat{\phi}\colon E' \to E$, and the compostion $\hat{\phi} \circ \phi$ is equal to multiplication by 2. By Corollary 8 applied to ϕ and $\hat{\phi}$ respectively, both of $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ and $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$ are finite. Now the kernel-cokernel sequence for the composition $E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{\hat{\phi}} E(\mathbb{Q})$ contains

$$E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\hat{\phi}} E(\mathbb{Q})/2E(\mathbb{Q}) \to E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \to 0$$

and therefore $E(\mathbb{Q})/2E(\mathbb{Q})$ is also finite. □

Remark. Using the kernel-cokernel sequence, it is easy to compute the order of $E(\mathbb{Q})/2E(\mathbb{Q})$ in terms of the orders of the other groups. This is because all the groups are finite-dimensional vector spaces over $\mathbb{F}_2$, and in any exact sequence of finite-dimensional vector spaces the alternating sum of the dimensions is zero. (This is an easy generalisation of the rank-nullity theorem.)

6. An example

We finish by going through an example, which is Example 1 of [1, §14]. Let E be the curve

$$E: \quad y^2 = x(x^2 - x + 6).$$

Then E' is the curve

$$E': \quad v^2 = u(u^2 + 2u - 23).$$

According to Lemma 7, to compute $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ we must go through all square-free r satisfying $r \mid -23$ and decide whether the equation (2) has integer solutions. There are only four choices for r, being ± 1 and ± 23. We already know $q((0,0)) = [-23]$, so we just have to decide whether $\mathrm{im}(q)$ is the subgroup $\{\pm 1, \pm 23\} \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, of order 4, or the subgroup $\{1, -23\} \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, of order 2. To do so, it is enough to check either $r = -1$ or $r = 23$, and we'll check $r = -1$.

This corresponds to the equation

$$-\ell^4 + 2\ell^2 m^2 + 23m^4 = n^2.$$

Completing the square allows us to write this as

$$-(\ell^2 - m^2)^2 + 24m^4 = n^2$$

which has no solutions modulo 9. Therefore $r = -1$ does not lie in $\mathrm{im}(q)$, and we have calculated that $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ has order 2 and is generated by the class of $(0,0)$.

To compute $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$, we have to look at all square-free r dividing 6. These are $r = \pm 1, \pm 2, \pm 3, \pm 6$. We already know that the class $[6] \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ corresponds to the point $(0,0)$. A negative r is never going to work, since it results in the left-hand side of (2) being negative definite. So we are down to two options for $\mathrm{im}(q)$: either $\{1, 2, 3, 6\}$ or $\{1, 6\}$. To decide, we can choose to check either 2 or 3. Taking $r = 2$ in (2) gives the equation

$$2\ell^4 - \ell^2 m^2 + 3m^4 = n^2,$$

which has the easy solution $(\ell, m, n) = (1, 1, 2)$. Therefore $\mathrm{im}(q)$ is the group $\{1, 2, 3, 6\}$. To explicitly write down generators for $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$, we work backwards through the substitutions of Lemma 7 to turn our solution (ℓ, m, n) into the point $(2, 4) \in E(\mathbb{Q})$. So $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$ has order 4, generated by the classes of $(0, 0)$ and $(2, 4)$.

Finally, we can find generators for $E(\mathbb{Q})/2E(\mathbb{Q})$. According to the kernel-cokernel lemma, we should take generators for $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$, together with the images under $\hat{\phi}$ of generators for $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$. The former gives $(0, 0)$ and $(2, 4)$, while the latter gives $\hat{\phi}((0, 0)) = O$ which does not contribute anything. So $E(\mathbb{Q})/2E(\mathbb{Q})$ has rank 2 (that is, order 4) and is generated by the classes of $(0, 0)$ and $(2, 4)$.

Acknowledgements. Thank you to Ronald van Luijk, Arshay Sheth and Anneloes Viergever for corrections to previous versions.

References

[1] J. W. S. Cassels, *Lectures on Elliptic Curves*, No. 24 of LMS Student Texts, Cambridge University Press, 1991.
[2] J. S. Milne, *Elliptic Curves*, BookSurge Publishers, 2006.
[3] P. Stevenhagen, *Complex Elliptic Curves*, on the course web site.