Higher Descents on Elliptic Curves

J. E. Cremona

August 1997

1 Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$. Our overall goal is to find explicitly the Mordell-Weil group $E(\mathbb{Q})$, its rank r and a $\mathbb{Z}$-basis. In place of the latter we are often satisfied with a basis for $E(\mathbb{Q})/mE(\mathbb{Q})$ for some integer $m \geq 2$; computing this quotient is usually known as "doing an m-descent" on E.

In this talk we will first give some generalities on descents, before specializing to the well-known case of descent via 2-isogeny. This will be called the first descent. While often conclusive with no further work, there are curves for which this first descent proves inconclusive, in the sense that we obtain homogeneous spaces (defined below) for which we cannot decide whether they have rational points. Higher descents attempt to settle this question, and we will go on to describe in some detail how to carry out a second descent.

Finally we give a numerical example to illustrate the method.

The terminology of descents is by now classical, going back to a series of papers by Cassels (summarized in [3]), and Birch and Swinnerton-Dyer ([1] and [2]). The second descent which we will describe for general curves was used in [2] to study curves of the form $y^2 = x^3 - Dx$. It has been implemented simultaneously (but independently) by the author in `C++` as part of his program `mwrank`, and also by D. Rusin and I. Connell in Maple, as part of Connell's package `apecs`.

A longer version of this article is in preparation [6].

2 The First Descent

Since $E(\mathbb{Q})$ is a finitely-generated abelian group, we can divide our task into the following subtasks: finding the (finite) torsion subgroup, finding the rank r, usually by finding r independent points in $E(\mathbb{Q})$, by finding a basis for $E(\mathbb{Q})/mE(\mathbb{Q})$ for some integer $m \geq 2$, and finally finding a $\mathbb{Z}$-basis for $E(\mathbb{Q})$ itself. The first of these steps is easy (see [5, Section 3.5]); here we will not be concerned with the last step, and wish to determine $E(\mathbb{Q})/mE(\mathbb{Q})$ for some m. The only case worked out in detail and implemented in practice for general elliptic curves is the case $m = 2$. Hence for the purposes of this talk our more modest goal is to compute $E(\mathbb{Q})/2E(\mathbb{Q})$ explicitly, thus obtaining both the rank r and r independent rational points on E which generate a subgroup of finite index in the Mordell-Weil group $E(\mathbb{Q})$. This process is known as "doing a 2-descent".

2.1 Descent via isogeny

Let $\varphi\colon E' \to E$ be a nonzero isogeny of degree m between two elliptic curves E' and E, with both curves and the isogeny defined over $\mathbb{Q}$. "Doing a φ-descent" on E means determining the quotient $E(\mathbb{Q})/\varphi(E'(\mathbb{Q}))$. We have the exact sequence

$$0 \to E'[\varphi] \hookrightarrow E' \xrightarrow{\varphi} E \to 0,$$

where $E'[\varphi]$ denotes the kernel of φ, which is finite of order m. Applying $G_{\mathbb{Q}}$-cohomology, where $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we obtain the injection

$$0 \to E(\mathbb{Q})/\varphi(E'(\mathbb{Q})) \xrightarrow{\delta} H^1(G_{\mathbb{Q}}, E'[\varphi]). \tag{1}$$

For this to be useful computationally, we must represent elements of the group $H^1(G_{\mathbb{Q}}, E'[\varphi])$ in a concrete way, and determine which come from rational points on E. Each element gives rise to a so-called φ-covering of E: this consists of a curve $\mathcal{C}$, isomorphic to E' over $\overline{\mathbb{Q}}$ (via θ, say), and a map $\xi\colon \mathcal{C} \to E$ defined over $\mathbb{Q}$ and of degree m such that the following diagram commutes:

$$\begin{tikzcd} E' \arrow[r, "\varphi"] & E \\ \mathcal{C} \arrow[u, "\theta"] \arrow[ur, "\xi"'] & \end{tikzcd} \tag{2}$$

For each such φ-covering such that $\mathcal{C}(\mathbb{Q}) \neq \emptyset$, the image of $\mathcal{C}(\mathbb{Q})$ under ξ is a complete coset of $\varphi(E'(\mathbb{Q}))$ in $E(\mathbb{Q})$. So if we can find all such φ-coverings explicitly and determine which have rational points, we will be able to compute the order of $E(\mathbb{Q})/\varphi(E'(\mathbb{Q}))$. Repeating the process with the dual isogeny $\varphi'\colon E \to E'$, we can determine the order of $E'(\mathbb{Q})/\varphi'(E(\mathbb{Q}))$, and hence determine the rank of $E(\mathbb{Q})$. (See [8, Chapter X, Remark 4.7] for details.)

The covering curves $\mathcal{C}$ are also known as homogeneous spaces, since they can be given the structure of principal homogeneous spaces for E, via (2). The φ-Selmer group $S^{(\varphi)}(E'/\mathbb{Q})$ is the subgroup of $H^1(G_{\mathbb{Q}}, E'[\varphi])$ consisting of elements represented by homogeneous spaces $\mathcal{C}$ which have points everywhere locally, *i.e.* for which $\mathcal{C}(\mathbb{Q}_p) \neq \emptyset$ for all primes p (including $\mathbb{Q}_\infty = \mathbb{R}$). This group is finite and effectively computable (for suitable φ), and contains $E(\mathbb{Q})/\varphi(E'(\mathbb{Q}))$, giving the exact sequence

$$0 \to E(\mathbb{Q})/\varphi(E'(\mathbb{Q})) \hookrightarrow S^{(\varphi)}(E'/\mathbb{Q}) \to Ш(E'/\mathbb{Q})[\varphi] \to 0$$

where $Ш(E'/\mathbb{Q})$ is the Tate-Shafarevich group of E' over $\mathbb{Q}$.

Theoretically, then, it is the possible existence of non-trivial elements of $Ш(E'/\mathbb{Q})$ which provides the obstacle to the φ-descent, since if such elements exist then we will encounter homogeneous spaces which are everywhere locally soluble (ELS) but which contain no global rational point. However, an obstacle which can also arise in practice is that some homogeneous space which does possess rational points may not have any small points (in the sense that the naive or Weil height of the coordinates is small), so that we may be unable to find rational points even when they exist.

Performing a second descent can help circumvent both these obstacles, either by producing large rational points as the images of small points on further curves, which we call descendants of $\mathcal{C}$, or by proving that no such descendants exist. We give some explicit examples of this below, together with an example where we find a further obstacle, this time to the second descent: $\mathcal{C}$ may have ELS descendants on none of which are we able to find rational points. In such a case, a third descent would be necessary, but it is not clear how to do this in general.

One can also use φ-coverings to find rational points on E, given explicit equations for $\mathcal{C}$ and ξ. Since ξ has degree $m \geq 2$, rational points on $\mathcal{C}$ will have smaller height than rational points on E itself, and so should be easier to find. It might appear, then, that it would be best to use an isogeny φ of large degree; however, the only isogenies for which a well worked out theory exists (in a form suitable for implementation for general curves) are the multiplication by 2 map (denoted [2]), of degree 4, and 2-isogenies (of degree 2).

Taking $\varphi = [2]$ is a practical possibility for all curves. In this case, the curves $\mathcal{C}$ have equations for the form $y^2 = g(x)$ where $g(x) \in \mathbb{Z}[x]$ is a polynomial of degree 4. There are efficient procedures for finding all such 2-coverings $\mathcal{C}$, though this is time-consuming when the discriminant Δ of E is large. See [5, Section 3.6] for details of this 2-descent process, which is implemented in our program `mrank`. A second descent then involves considering 4-coverings. The theory of these is currently under development: see [9] for a recent account, and [4] for a method of determining whether a given 2-descent has descendants.

When E has a rational point of order 2, there is a 2-isogeny defined over $\mathbb{Q}$ which we may use to do a descent via 2-isogeny. Now the second descent curves are 2-coverings, which we can determine explicitly.

2.2 Descent via 2-isogeny

Let E be an elliptic curve defined over $\mathbb{Q}$ with a rational point of order 2. Then there is an isogenous curve E', also defined over $\mathbb{Q}$, and dual 2-isogenies $\varphi \colon E' \to E$ and $\varphi' \colon E \to E'$, defined over $\mathbb{Q}$, and we can use descent to determine both $E(\mathbb{Q})/\varphi(E'(\mathbb{Q}))$ and $E'(\mathbb{Q})/\varphi'(E(\mathbb{Q}))$, and hence $E(\mathbb{Q})/2E(\mathbb{Q})$. Explicitly, we can choose coordinates so that E and E' have equations of the form

$$E: \quad y^2 = x(x^2 + cx + d) \tag{3}$$

$$E': \quad y^2 = x(x^2 + c'x + d') \tag{4}$$

where c, d, c', d' are integers related by $c' = -2c$, $d' = c^2 - 4d$, and $dd' \neq 0$. The kernels of φ and φ' are generated by the points $(0,0)$ on E' and E respectively. The connecting map δ in (1) now maps $E(\mathbb{Q})/\varphi(E'(\mathbb{Q}))$ to

$$H^1(G_{\mathbb{Q}}, E'[\varphi]) = \mathrm{Hom}(G_{\mathbb{Q}}, \{\pm 1\}) \simeq \mathbb{Q}^*/(\mathbb{Q}^*)^2,$$

and is given by mapping $P = (x,y) \in E(\mathbb{Q})$ to $x \pmod{(\mathbb{Q}^*)^2}$ (if $x \neq 0$) and $(0,0)$ to $d \pmod{(\mathbb{Q}^*)^2}$. Moreover, the image is contained in the finite subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by the divisors of d. For each factorization $d = d_1 d_2$ with $d_1, d_2 \in \mathbb{Z}$ one has the homogeneous space

$$\mathcal{C}_{d_1}: \quad v^2 = d_1 u^4 + cu^2 + d_2, \tag{5}$$

which is a φ-covering of E with associated map $\xi \colon \mathcal{C}_{d_1} \to E$ given by $\xi((u,v)) = (d_1 u^2, d_1 uv)$.

Hence the algorithm **Descent via 2-isogeny** may be summarized as follows, given a curve with a rational point of order 2:

1. Transform the equation of the given curve into the form (3), mapping the given point of order 2 to $(0,0)$;
2. For each square-free divisor d_1 of d, determine whether $\mathcal{C}_{d_1}$ has rational points;
3. The points $\xi(P)$ for $P \in \mathcal{C}_{d_1}$ generate $E(\mathbb{Q})/\varphi(E'(\mathbb{Q}))$;
4. Repeat with E' to find $E'(\mathbb{Q})/\varphi(E(\mathbb{Q}))$, and so determine $E(\mathbb{Q})/2E(\mathbb{Q})$.

In step 2, we will first determine the subgroup of square-free divisors d_1 of d such that $\mathcal{C}_{d_1}$ is ELS (hence determining the Selmer group $S^{(\varphi)}(E'/\mathbb{Q})$), and then proceed to search for rational points on these $\mathcal{C}_{d_1}$, remembering that those which have rational points again form a subgroup. If we fail to find a rational point on some ELS curve $\mathcal{C}_{d_1}$, there are two possibilities:

either $\mathcal{C}_{d_1}$ has rational points, but they are too large to have been found in the search;

or $\mathcal{C}_{d_1}$ has no rational points.

To distinguish between these, we now carry out the second descent.

3 The Second Descent

3.1 Theoretical background

We continue with the notation of the previous section. Given a φ-covering $\mathcal{C}$ of the elliptic curve E as in (2), we attempt to extend it to a 2-covering $\mathcal{D}$ so that we have a larger commutative diagram

$$\begin{tikzcd} E \arrow[r, "\varphi'"] & E' \arrow[r, "\varphi"] & E \\ \mathcal{D} \arrow[u] \arrow[r, "\eta"'] & \mathcal{C} \arrow[u] \arrow[ur, "\xi"'] & \end{tikzcd} \tag{6}$$

Both vertical maps are isomorphism defined over $\overline{\mathbb{Q}}$; the other maps are all of degree 2 and defined over $\mathbb{Q}$. In general there will be several inequivalent ways of doing this for a given $\mathcal{C}$, but the number is finite. We call the homogeneous spaces $\mathcal{D}$ *descendants* of $\mathcal{C}$. If one succeeds in finding a single rational point on just one descendant, then the image of this point under η will give the desired point on $\mathcal{C}$, and hence (via ξ) a rational point on E itself. In principal, finding points on the descendants should be easier than on the first descent curves, since they will have smaller height, approximately by a factor of 2 (see examples in section 4 below).

On the other hand, it may happen that an ELS first descent curve $\mathcal{C}$ may have no ELS descendants. In this case, $\mathcal{C}$ certainly has no rational points; it represents an element of the Selmer group $S^{(\varphi)}(E'/\mathbb{Q})$ which is not the image of an element of $S^{(2)}(E/\mathbb{Q})$, and so represents a non-trivial element of $\text{Ш}(E'/\mathbb{Q})$.

The situation is illustrated by the following commutative diagram:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & K \arrow[r] \arrow[d] & E'(\mathbb{Q})/\varphi'(E(\mathbb{Q})) \arrow[r, "\varphi"] \arrow[d, "\delta"] & E(\mathbb{Q})/2E(\mathbb{Q}) \arrow[r] \arrow[d, "\delta"] & E(\mathbb{Q})/\varphi(E'(\mathbb{Q})) \arrow[r] \arrow[d, "\delta"] & 0 \\
0 \arrow[r] & K \arrow[r] \arrow[d] & S^{(\varphi')}(E/\mathbb{Q}) \arrow[r] \arrow[d] & S^{(2)}(E/\mathbb{Q}) \arrow[r, "\varphi'"] \arrow[d] & S^{(\varphi)}(E'/\mathbb{Q}) \arrow[d] & \\
 & 0 \arrow[r] & \text{Ш}(E/\mathbb{Q})[\varphi'] \arrow[r] \arrow[d] & \text{Ш}(E/\mathbb{Q})[2] \arrow[r, "\varphi'"] \arrow[d] & \text{Ш}(E'/\mathbb{Q})[\varphi] \arrow[d] & \\
 & & 0 & 0 & 0 &
\end{tikzcd}$$

In this diagram, the group K has order 2, unless d' is a square in which case it is trivial. The ELS first descent curves $\mathcal{C}$ represent elements of $S^{(\varphi)}(E'/\mathbb{Q})$, and their ELS descendants (if they exist) represent their preimages in $S^{(2)}(E/\mathbb{Q})$. Of course it is still possible to have descendants which are ELS but with no rational point; this will happen if $\mathcal{C}$ represents an element of $\text{Ш}(E'/\mathbb{Q})[\varphi]$ which is the image under φ' of an element of $\text{Ш}(E/\mathbb{Q})[2]$. So the obstruction has been reduced from the group $\text{Ш}(E'/\mathbb{Q})[\varphi]$ to its subgroup $\varphi'(\text{Ш}(E/\mathbb{Q})[2])$. If ELS descendants do exist, they form a coset of $S^{(\varphi')}(E/\mathbb{Q})/K$ in $S^{(2)}(E/\mathbb{Q})$, so are parametrized by the first descents on the isogenous curve E'; this will be made explicit below.

This is a sketch of the theory behind the second descent algorithm. Now we explain how to carry out the second descent in practice.

3.2 The second descent in practice

Our starting point is a curve $\mathcal{C}$ given by an (affine) equation of the form (5), where $d_1, c, d_2 \in \mathbb{Z}$, $d = d_1 d_2 \neq 0$, $d' = c^2 - 4d \neq 0$, and we desire either to find a rational point on $\mathcal{C}$ or show that no such point exists. We may assume that d_1 is non-square (otherwise $\mathcal{C}$ represents the trivial class) so that $\mathcal{C}$ has no rational points at infinity, and we seek a rational solution (u, v) to (5). We also assume that $\mathcal{C}$ is ELS, so that (5) has real solutions and p-adic solutions for all primes p.

3.2.1 Step 1: solving the conic

Let $\mathcal{C}_0$ be the curve

$$\mathcal{C}_0 : \quad Y^2 = d_1 X^2 + cXZ + d_2 Z^2, \tag{7}$$

which is a conic (curve of genus 0). There is an obvious map $\mathcal{C} \longrightarrow \mathcal{C}_0$, and rational points on $\mathcal{C}$ correspond to rational points on $\mathcal{C}_0$ such that X/Z is a square. Since $\mathcal{C}$ is ELS, so is $\mathcal{C}_0$, and hence by the Hasse principle, $\mathcal{C}_0$ has a rational point $P_0 = (X_0 : Y_0 : Z_0) \in \mathbb{P}^2(\mathbb{Q})$. Our first step is to find such a point P_0, so we need as a sub-algorithm an efficient way of solving an equation such as (7).

3.2.2 Step 2: parametrizing the conic

Given one solution P_0 of (7) it is simple to parametrize all solutions:

$$X = q_1(\alpha,\beta), \quad Y = q_2(\alpha,\beta), \quad Z = q_3(\alpha,\beta) \tag{8}$$

where the q_i are quadratic polynomials with integer coefficients, which determine a birational map.

$$\begin{aligned}\theta\colon \mathbb{P}^1(\mathbb{Q}) &\longrightarrow \mathcal{C}_0(\mathbb{Q})\\ (\alpha:\beta) &\mapsto (q_1(\alpha,\beta) : q_2(\alpha,\beta) : q_3(\alpha,\beta)).\end{aligned}$$

It will be important to keep this parametrization as simple as possible; we can arrange that q_1 and q_3 have discriminants $16d_2$ and $16d_1$ respectively, with resultant $\mathrm{Res}_u(q_1(u,1), q_3(u,1)) = 16d'$, all independent of P_0.

3.2.3 Step 3: parametrizing the set of descendants

For $\theta(\alpha,\beta)$ to give a point in $\mathcal{C}(\mathbb{Q})$ and not just on $\mathcal{C}_0(\mathbb{Q})$, we require

$$\frac{X}{Z} = \frac{q_1(\alpha,\beta)}{q_3(\alpha,\beta)} = \text{square}.$$

Hence we require a solution in integers α,β,s,t to the equations

$$q_1(\alpha,\beta) = d_3 s^2 \tag{9}$$

$$q_3(\alpha,\beta) = d_3 t^2 \tag{10}$$

where d_3 is a square-free divisor of the resultant $16d'$. Each of the finite number of possible d_3 for which the equations (9), (10) are soluble (separately) will give rise to a descendant curve $\mathcal{D}$. The following steps are now carried out for each such d_3.

Note that these d_3, which form a group H_0 modulo squares, are precisely the integers which parametrize the first descent curves $\mathcal{C}'_{d_3}$ for the curve E'. Assuming that we have already carried out the first descent on E', we will have already identified a subgroup H_1 of H_0 consisting of those d_3 for which $\mathcal{C}'_{d_3}$ is ELS (so H_1 is isomorphic to the Selmer group $S^{(\varphi')}(E/\mathbb{Q})$). The set of values of d_3 which give ELS descendants of our first descent curve $\mathcal{C}$ is either empty, or one complete coset of H_1 in H_0. We can use this to make the algorithm more efficient, as in looking for descendants, we do not need to test all $d_3 \in H_0$, but only one in each H_1-coset. If none of the cosets gives rise to an ELS descendant (see the later steps for how to determine this) then we will have successfully proved that $\mathcal{C}(\mathbb{Q}) = \emptyset$.

Suppose now that there is an ELS descendant $\mathcal{D}$ coming from one value of d_3. If we find a rational point on $\mathcal{D}$, then we map it to a rational point on $\mathcal{C}$, and again we are successful. If we fail to find a rational point on $\mathcal{D}$, then we loop through the rest of the coset d_3H_1, construct each of the other ELS descendants, and search for rational points on each until we find one (in which case we can exit from the loop). Finally, if we fail to find rational points on any of the ELS descendants, we admit defeat, and either restart the algorithm with a larger search bound for rational points on the descendants, or attempt a third descent.

We now turn to the construction of the descendant curves themselves, for a fixed value of d_3 in (9), (10).

3.2.4 Step 4: constructing the descendants

To solve (9), (10) we first verify that each is soluble separately, using the standard criterion of Legendre. If either fails, we continue to the next value of d_3. Assuming both are soluble, we find a solution to (9) using the same algorithm as in Step 1, and hence parametrize the solutions:

$$\alpha = Q_1(\lambda, \mu), \quad \beta = Q_3(\lambda, \mu), \quad \text{and} \quad s = Q_2(\lambda, \mu) \tag{11}$$

where the Q_j are integer quadratics such that

$$q_1(Q_1(\lambda, \mu), Q_3(\lambda, \mu)) = d_3 Q_2(\lambda, \mu)^2 \tag{12}$$

identically in λ and μ. Substituting in (10) we obtain the equation

$$\mathcal{D}: \quad g(\lambda, \mu) = d_3 t^2 \tag{13}$$

where $g(\lambda, \mu)$ is the quartic $q_3(Q_1(\lambda, \mu), Q_3(\lambda, \mu))$. We check that $\mathcal{D}$ is ELS, using the algorithm in [5] or Siksek's improvement for large primes (see [9]). Now $\mathcal{D}$ is the required descendant, which is a 2-covering of E. Equations (11) and (8) give an explicit rational map from a rational point (λ, μ, t) on $\mathcal{D}$ via $(\alpha, \beta, s) = (Q_1(\lambda, \mu), Q_3(\lambda, \mu), Q_2(\lambda, \mu))$ to $(X, Y, Z) = (q_1(\alpha, \beta), q_3(\alpha, \beta))$ on $\mathcal{C}_0$ with X/Z square, and hence to a rational point $(u, v) = \left(\frac{s}{t}, \frac{Y}{d_3 t^2}\right) = \left(\frac{Q_2(\lambda,\mu)}{t}, \frac{q_2(Q_1(\lambda,\mu), Q_3(\lambda,\mu))}{d_3 t^2}\right)$ on the first descent curve $\mathcal{C}$.

3.2.5 Step 5: simplifying the descendants

Before we can go about searching for a rational point on the descendant curve $\mathcal{D}$, it is essential to simplify its equation, replacing the quartic $g(\lambda, \mu)$ with an equivalent one (defining the same curve $\mathcal{D}$ up to birational isomorphism), since the preceding steps will usually lead to quartics with huge integer coefficients. This simplification is a major part of our algorithm, and is essential for the algorithm to be practical. It takes place in two stages, which we call *minimizing* and *reducing* the quartic. The minimization stage replaces g by a projectively equivalent integer quartic g^* whose invariants I^*, J^* are of the form $I^* = w^{-4}I(g)$, $J^* = w^{-4}I(g)$, where $w \in \mathbb{Z}$ is as large as possible. Our algorithm for this, which is in some respects a quartic analogue of Tate's algorithm for reducing elliptic curves, is based on ideas from Serf's thesis [7] which in turn follow [1]. Secondly, the reduction stage uses a unimodular transformation to reduce the size of the coefficients of g^* (while keeping I and J unchanged). Here we use a reduction theory for quartics similar to that in [1] (though slightly improved in the case of negative discriminant).

Finally, we use a sieve-assisted search to look for rational points on the transformed equation (13), as described in [5, Section 3.6].

Our algorithms for minimizing and reducing quartics will be described elsewhere. These, and the efficient algorithm for finding a small point on a conic (which we use to solve both (7) and (9)), are the crucial basic number-theoretical algorithms without which the second descent procedure described here could not be made to work effectively in practice.

4 Example

Rusin was interested in the elliptic curve E with standard Weierstrass coefficients $[a_1, a_2, a_3, a_4, a_6] = [0, -1, 0, -1250000000083, -10000000000088]$. Using the point $(-8, 0)$ of order 2 this can be put in the form (3) with $c = -25$ and $d = 3^2 \cdot 5^3 \cdot 11 \cdot 41 \cdot 271 \cdot 9091$. The 128 square-free divisors d_1 of d give 32 ELS first descent curves $\mathcal{C}_{d_1}$ (generated by $d_1 = d$ and $d_1 = -1$, $55 = 5 \cdot 11$, $451 = 11 \cdot 41$ and $11111 = 41 \cdot 271$). Here $\mathcal{C}_d$ comes from the rational 2-torsion point on E and so has a trivial rational point.

A simple search finds the rational point $(u, v) = (20, 26565)$ on $\mathcal{C}_{-1355}$, which maps to the point $P_1 = (-542000, -719911500)$ on E. There is also a small rational point on $\mathcal{C}_{4100041}$, with $u = 3/4$, (which we can ignore since $4100041 \equiv -1355d$ modulo squares), but none on the 28 other non-trivial first descent curves $\mathcal{C}_{d_1}$. (In fact we do not search all 28, since we only look at one in each coset of the subgroup which is known to have rational points.) So the φ-Selmer rank of E is 5, of which at least 2 comes from rational points on E.

Similarly, the first descent on E' shows that its φ'-Selmer rank is 2, generated by d' and 5, but we do not find rational points except the trivial one on $\mathcal{C}'_{d'}$ coming from the rational 2-torsion on E'.

Hence we find from the first descent that the rank is between 1 $(= 2 + 1 - 2)$ and 5 $(= 5 + 2 - 2)$. Rerunning the first descent with higher (reasonable) search bounds does not change this estimate.

When we do the second descent, two things happen: we increase the lower bound, by successfully finding more rational points on certain first descent curves, and we also decrease the upper bound, by successfully proving that certain others have no rational points. Specifically, we find rational points on $\mathcal{C}_{-55}$ and on $\mathcal{C}'_5$. This shows that the number of first φ-descent curves $\mathcal{C}_{d_1}$ with rational points is at least 8, and that all 4 first φ'-descent curves have points. Secondly, the remaining 24 curves $\mathcal{C}_{d_1}$ have no ELS descendants, so do not have rational points. This proves unconditionally that $E(\mathbb{Q})$ has rank 3 (as does $E'(\mathbb{Q})$), that the 2-rank of $Ш(E/\mathbb{Q})$ is 0, while the 2-rank of $Ш(E'/\mathbb{Q})$ is exactly 2.

We also obtain three explicit points on $E(\mathbb{Q})$ which generate a subgroup of finite index, namely $P_1 = (-542000, -719911500)$ (as above) and

$$P_2 = \left(\frac{-12123886930631252087108}{111060601^2}, \frac{-723566398176234298022167437626250}{111060601^3} \right),$$

$$P_3 = \left(\frac{1651941110876982226534320892}{10864887323^2}, \frac{669269975097446793658932928791700972130 82}{10864887323^3} \right).$$

These points have approximate canonical heights 8.9, 46.5 and 61.6 respectively.

The point P_2 comes from a descendant $\mathcal{D}$ of $\mathcal{C}_{-55}$. The parametrization of the associated conic $\mathcal{C}_0$ is given by

$$q_1(\alpha, \beta) = 1104305\alpha^2 + 9953711567910\alpha\beta + 22429576515805186725\beta^2$$
$$q_3(\alpha, \beta) = 88\alpha^2 + 793192620\alpha\beta + 1787370830745640\beta^2.$$

Using $d_3 = 13$, the first equation we obtain for the descendant $\mathcal{D}$ involves a quartic with 60-digit coefficients. Minimizing this removes a factor $w =$

45382656538986, after which the reduction step produces the more manageable quartic $g(\lambda,\mu) = 50125\lambda^4 - 1250\lambda^3\mu + 950\lambda^2\mu^2 - 124075\lambda\mu^3 + 6235186\mu^4$. Now a small search reveals that $g(505, 198)$ is a square, so we have a rational point on $\mathcal{D}$, which maps to the point

$$(u,v) = \left(\frac{14846969850}{111060601}, \frac{886090079459099250015}{111060601^2}\right)$$

on $\mathcal{C}_{-55}$, and finally to P_2 as above.

Similarly, P_3 comes from a descendant $\mathcal{D}'$ of $\mathcal{C}'_5$, via $\mathcal{C}'_5$ and E'; the map from $\mathcal{D}'$ to E has degree 8. Here we had to compute 15 descendants before we found one with a rational point.

More examples will appear in [6].

References

[1] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves I*, J. Reine Angew. Math. **212** (1963), 7–25.

[2] ———, *Notes on elliptic curves II*, J. Reine Angew. Math. **218** (1965), 79–108.

[3] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. (2) **41** (1966), 193–291.

[4] ———, *Second descents for elliptic curves*, preprint, 1997.

[5] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, 1997.

[6] J. E. Cremona and D. Rusin, *Higher descents on elliptic curves*, In preparation, 1997.

[7] P. Serf, *The rank of elliptic curves over real quadratic number fields of class number 1*, Ph.D. thesis, Universität des Saarlandes, 1995.

[8] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106, Springer-Verlag, 1986.

[9] N. P. Smart, S. Siksek, and J. R. Merriman, *Explicit 4-descents on an elliptic curve*, Acta Arith. **LXXVII.4** (1996), 385–404.