4-descent on the elliptic curve $y^2 = x^3 + 7823$

Jennifer Balakrishnan

May 17, 2003

Abstract

We outline the refinement of the 4-descent used by Michael Stoll in [10] to find the Mordell-Weil generator of the elliptic curve $y^2 = x^3 + 7823$. In general, given a 2-covering space of an elliptic curve, the procedure yields the set of everywhere locally soluble 4-covering spaces lifting it.

1 Introduction

If E is an elliptic curve over $\mathbb{Q}$, then we know by a theorem of Mordell that its group of rational points is finitely generated. Thus, it is of interest to find the set of generators of the Mordell-Weil group, the group of rational points on the elliptic curve $E(\mathbb{Q})$.

1.1 Points of finite order

In examining the Mordell-Weil group of $y^2 = x^3 + 7823$, we know that it could potentially have nontrivial points of finite order.

However, by the Nagell-Lutz theorem, as 7823 is prime, $-7823^{\frac{1}{3}}$ is irrational, and so there are no rational points of order 2. Checking factors of the discriminant, we see that $y^2 = x^3 + 7823$ has no points of any finite order. Thus, whatever rational points $y^2 = x^3 + 7823$ has, these points have infinite order

1.2 Points of infinite order

Through the work of Kolyvagin [7] and Gross-Zagier [6], we know that since the L-series of $E = y^2 = x^3 + 7823$ has a simple zero at $s = 1$, the group $E(\mathbb{Q})$ must be isomorphic to $\mathbb{Z}$. E is thus of rank 1 and we have one rational point of infinite order generating the Mordell-Weil group.

1.3 The Mordell-Weil generator of $y^2 = x^3 + 7823$

Until January of 2002, the Mordell-Weil generators of all Mordell curves, those of the form $y^2 = x^3 + D$, for $|D| \leq 10,000$ had been found, except for $D = 7823$. A table of this information can be found at [5]. Conspicuously absent was the case $D = 7823$; finding the Mordell-Weil generator of $y^2 = x^3 + 7823$, which was known to have large height, had eluded previous methods of search. Nevertheless, Stoll's method [10] of 4-descents was successfully able to find the generator with coordinates

$$x = \frac{2263582143321421502100209233517777}{119816734100955612^2}$$
$$y = \frac{186398152584623305624837551485596770028144776655756}{119816734100955612^3}.$$

2 2-descents

2.1 Background

We first perform a 2-descent on $y^2 = x^3 + 7823$, en route to Stoll's method of 4-descent, to find a rational point on $y^2 = x^3 + 7823$.

Recall that an exact sequence of groups is a sequence of maps $\phi_i : A_i \to A_{i+1}$ between groups A_i such that im ϕ_i= ker ϕ_{i+1}. A short exact sequence is written as follows:

$$0 \to A \to B \to C \to 0.$$

In performing the 2-descent, we wish to understand the short exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to S^{(2)}(E/\mathbb{Q}) \to \text{Ш}(E/\mathbb{Q})[2] \to 0.$$

We shall explain the objects $S^{(2)}(E/\mathbb{Q})$ and $\text{Ш}(E/\mathbb{Q})[2]$ as we encounter them in the process of carrying out the 2-descent.

We begin by categorizing the *principal homogeneous spaces* associated to E: these are genus 1 (algebraic) curves D with a polynomial mapping $\phi : D \to E$, such that E is isomorphic to D over an extension of $\mathbb{Q}$. In the general 2-descent, the ϕ we consider are called *2-coverings* and they have degree 4. The curves D are might not have rational points, but when they do, these rational points map to rational points on E. Thus, we have a "descent" from $D \to E$.

A comprehensive listing of the 2-coverings can be easily computed using a program such as Cremona's `mwrank` [3]. In deciding which spaces we want to descend from to search globally (i.e., for our rational point), we should first consider the local question. Thus, we test local solubility: solubility over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every p. The set of 2-coverings which are locally soluble correspond to elements of the 2-Selmer group. For those descendants that are found to be locally soluble, we consider the global question. Indeed, local solubility does not imply global solubility; those quartics that fail to satisfy the "Hasse principle," correspond to nontrivial elements of the Shafarevich-Tate group Ш associated to the elliptic curve.

2.2 Cremona's algorithm for 2-descents

The following procedure is an implementation of the general 2-descent algorithm for elliptic curves, which can be found in more generality in Cremona's book [4]. For the underlying theory and proofs, we direct the reader to Silverman's [9]. Recall that the purpose of carrying out a 2-descent is to find the homogeneous spaces D, which are given by equations of the form

$$D : y^2 = g(x) = ax^4 + bx^3 + cx^2 + dx + e$$

with $a,b,c,d,e \in \mathbb{Q}$. These a,b,c,d,e are defined in terms of I and J:

$$I = 12ae - 3bd + c^2$$
$$J = 72ace + 9bcd - 27ad^2 - 27eb^2c^3$$

There could possibly be more than one set of (I,J). If $2^6 \nmid J$, then we have just one (I,J) pair, namely $(c_4, 2c_6)$. Otherwise, we have two (I,J) that we must consider: the original $(c_4, 2c_6)$ and also $(2^{-4}c_4, 2^{-5}c_6)$.

Now consider the curve $E_{I,J}$ isomorphic to E:

$$E_{I,J} : Y^2 = F(X) = X^3 - 27IX - 27J.$$

This is the curve for which the descent will be used. After a point (x'', y'') has been found on H, the descent map will take it to (x', y') on $E_{I,J}$, and a simple transformation can be made to recover (x,y) on our original elliptic curve.

To find the map from D to E, we must first consider covariants g_4 and g_6 attached to our $g \in D$:

$$g_4(X,Y) = (3b^2 - 8ac)X^4 + 4(bc - 6ad)X^3Y$$
$$+2(2c^2 - 24ae - 3bd)X^2Y^2 + 4(cd - 6be)XY^3 + (3d^2 - 8ce)Y^4$$
$$g_6(X,Y) = (b^3 + 8a^2d - 4abc)X^6 + 2(16a^2e + 2abd - 4ac^2 + b^2c)X^5Y + 5(8abe + b^2d - 4acd)X^4Y^2$$
$$+20(b^2e - ad^2)X^3Y^3 - 5(8ade + bd^2 - 4bce)X^2Y^4 - 2(16ae^2 + 2bde - 4c^2e + cd^2)XY^5 - (d^3 + 8be^2 - 4cde)Y^6$$

as well as two seminvariants p and r:

$$p = g_4(1,0) = 3b^2 - 8ac$$
$$r = g_6(1,0) = b^3 + 8a^2d - 4abc.$$

Then our 2-covering map ξ takes rational points (x,y) on D to rational points on $E_{I,J}$ in the following manner:

$$\xi : (x,y) \to \left(\frac{3g_4(x,1)}{(2y)^2}, \frac{27g_6(x,1)}{(2y)^3} \right).$$

This 2-covering map ξ is a rational map of degree 4 from $D(\mathbb{Q})$ to $E_{I,J}(\mathbb{Q})$.

Now we wish to find all such D associated with $E_{I,J}$. Since the D are of degree 4, we have the following possibilities:

- Type 1: 0 real roots,
- Type 2: 4 real roots, or
- Type 3: 2 real roots.

If $\Delta < 0$, then all D are Type 3; Types 1 and 2 homogeneous spaces are encountered when $\Delta > 0$. In the case of $y^2 = x^3 + 7823$, the discriminant Δ is $-16 \cdot 27 \cdot 7823^2 < 0$ and thus all homogeneous spaces will be Type 3. For a thorough development of how one can find bounds on the coefficients of D, we refer the reader to [1]. We summarize the bounds given there for Type 3 D:

Consider the resolvent cubic $\theta^3 - 3I\theta + J = 0$, with discriminant 27Δ, $D = 4I^3 - J^2 \neq 0$. Again, since $\Delta < 0$, this cubic has one real root θ; this θ is involved in the bounds of a, b, c as follows:

$$\frac{1}{3}\theta - \sqrt{\frac{4}{27}(\theta^2 - I)} \leq a \leq \frac{1}{3}\theta + \sqrt{\frac{4}{27}(\theta^2 - I)}$$

$$-2 \mid a \mid < b \leq 2 \mid a \mid$$

$$\frac{9a^2 - 2a\theta + \frac{1}{3}(4I - \theta^2) + 3b^2}{8|a|} \leq c \cdot sign(a) \leq \frac{4a\theta + 3b^2}{8|a|}.$$

Recalling that $r = g_6(1,0) = b^3 + 8a^2d - 4abc$, we can find d and e:

$$d = \frac{r - b^3 + 4abc}{8a^2}$$

$$e = \frac{I + 3bd - c^2}{12a}.$$

Thus, given a pair (I, J), we see that all possible 2-coverings can be found by running a simple computer search for a, b, c, d, e.

2.3 Running the algorithm on mwrank

The above procedure has been implemented by Cremona in the program `mwrank` [3]. Thus, for the elliptic curve $y^2 = x^3 + 7823$, we use `mwrank` to find these coefficients a, b, c, d, e and hence, the 2-covering spaces.

The following is the `mwrank` output:

```
Enter curve:  [0,0,0,0,7823]
Curve [0,0,0,0,7823] :
Basic pair:  I=0, J=-211221 disc=-44614310841
Two (I,J) pairs Looking for quartics with I = 0, J = -211221
Looking for Type 3 quartics:
Trying positive a from 1 up to 17
Trying negative a from -1 down to -11
Finished looking for Type 3 quartics.
Looking for quartics with I = 0, J = -13518144
Looking for Type 3 quartics:
Trying positive a from 1 up to 68
(30,-12,48,116,-18) --nontrivial...--new (B) #1
(41,-16,-6,112,-11) --nontrivial...--equivalent to (B) #1
```

```
Trying negative a from -1 down to -45
(-11,-20,408,1784,2072) --nontrivial...--equivalent to (B) #1
(-18,-28,312,996,838) --nontrivial...--equivalent to (B) #1
Finished looking for Type 3 quartics.
```

As seen above, `mwrank` finds that, up to equivalence, there is one 2-covering space:

$$D : y^2 = -18x^4 + 116x^3 + 48x^2 - 12x + 30.$$

Now, to find a find a rational point on D, we first check for local solubility. `mwrank` verifies that D is locally soluble. Nevertheless, local solubility does not imply global solubility, and this check must be performed as well. However, even if a rational point exists on D, it could be of rather large height, and hence, difficult to find in a limited search region. In practice,when running a search over a fixed region, we cannot tell the difference between a quartic that has a large rational solution and one that does not have any rational solutions. This poses computational obstacles. The former challenge is precisely the situation encountered with $y^2 = x^3 + 7823$: the Gross-Zagier theorem tells us that the canonical height of the Mordell-Weil generator should be about 77.6. Thus, even though a 2-descent allows us to consider a smaller search region on the covering space, as we have a degree 4 map taking a point on D to a point on E, points on D might not be small enough, computationally speaking. Thus we must take another descent, hopefully resulting in a practical computation to find the Mordell-Weil generator.

3 4-descents

3.1 Background

In the 2-descent, we considered the short exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to S^{(2)}(E/\mathbb{Q}) \to \text{Ш}(E/\mathbb{Q})[2] \to 0.$$

Similarly, with the 4-descent we have the sequence

$$0 \to E(\mathbb{Q})/4E(\mathbb{Q}) \to S^{(4)}(E/\mathbb{Q}) \to \text{Ш}(E/\mathbb{Q})[4] \to 0.$$

Recall that the purpose of the 2-descent was to find the locally soluble principle homogeneous spaces D that lifted the elliptic curve E, resulting in maps $\phi : D \to E$. These D, members of $S^{(2)}(E/\mathbb{Q})$, were found to be quartics. Thus, in carrying out the 4-descent, we wish to find the locally soluble principle homogeneous spaces C lifting D, ultimately resulting in the map $\phi' : C \to D \to E$.

We are curious as to what these elements of $S^{(4)}(E/\mathbb{Q})$ look like.[1] We begin with an element D' of $S^{(2)}(E/\mathbb{Q})$,homogenize, and make a change of variables so that our 2-covering is of the form $D : aY^2 = G(X,Z)$, with $G(X,Z)$ a binary quartic form with coefficients in $\mathbb{Z}$, $G(1,0) = 1$ and $a \in \mathbb{Q}^*$ the coefficient of the quartic term of our original g.

We find our 4-covering from the following equation:

$$X - \theta Z = \varepsilon(x_0 + x_1\theta + x_2\theta^2 + x_3\theta^3)^2,$$

[1] For a more rigorous approach to this investigation, see [8] and [10].

for, equating coefficients of θ^j yields that

$$X = Q_3(x), Z = Q_4(x), 0 = Q_1(x), 0 = Q_2(x),$$

where the Q_j are quadratic forms, given in terms of the variables $x_1, \ldots, x_4$. Now, since $Q_1(x) = Q_2(x) = 0$, we have an intersection of two quadric surfaces in $\mathbb{P}^3$ as our 4-covering C. We shall represent these two quadric surfaces Q_1 and Q_2 by 4-by-4 matrices M_1 and M_2.

Now consider the mapping from C to D. Given the matrices M_1 and M_2, consider $M_1' = \mathrm{adj}(M_1)$ and $M_2' = \mathrm{adj}(M_2)$. Let d_1 and d_2 be the symmetric matrices determined by $\mathrm{adj}(t_1 M_1' + t_2 M_2') = t_1^3 \sigma_0^2 M_1' + t_1^2 t_2 \sigma_0 d_1 + t_1 t_2^2 \sigma_4 d_2 + t_2^3 \sigma_4^2 M_2'$. If $F_1(x)$ and $F_2(x)$ are quadratic forms such that $F_1(x) = x^t d_1 x$ and $F_2(x) = x^t d_2 x$, and x is a point where the two quadrics intersect, then we have the syzygy

$$G^2 = \sigma_0 F_1^4 - F_1^3 F_2 \sigma_1 + F_1^2 F_2^2 \sigma_2 - F_1 F_2^3 \sigma_3 + F_2^4 \sigma_4$$

and a map ψ from C onto D given by

$$(x,y) \to \left(\frac{-F_1(x)}{F_2(x)}, \frac{G(x)}{F_2(x)} \right).$$

It is simple to check that $\det(Q_1(x)t_1 + Q_2(x)t_2) = aG(t_1, t_2)$, and thus we have a 4-descent extending the 2-descent.

3.2 Result, sans Stoll's improvements

Again, finding a finite list of ψ and C is merely a computational task, but the resulting equations can be quite cumbersome. If these 4-coverings have large coefficients, then we run into the same problem we encountered with the 2-descent, searching for points remains a difficulty.

For example, the 4-descent carried out on $E : y^2 = x^3 + 7823$ results in the following matrices M_1 and M_2:

$$M_1 = \begin{pmatrix} -22181252 & -12522843 & 485492211 & 2218020408 \\ -12522843 & 485492211 & 2218020408 & -2954387682 \\ 485492211 & 2218020408 & -2954387682 & -65148580179 \\ 2218020408 & -2954387682 & -65148580179 & -185865980697 \end{pmatrix}$$

$$M_2 = \begin{pmatrix} 383480 & 60588 & -9008739 & -37014651 \\ 60588 & -9008739 & -37014651 & 71170650 \\ -9008739 & -37014651 & 7117650 & 1173510018 \\ -37014651 & 71170650 & 1173510018 & 2915000865 \end{pmatrix}$$

4 Stoll's method of 4-descent

Stoll begins his explanation with the caveat that it is "rather *ad hoc* and with no theoretical underpinnings," but nevertheless "seems to work reasonably well in practice." Let the reader be forewarned.

The goal is to find matrices M_1' and M_2' with smaller entries, satisfying $\det(xM_1' + M_2') = g(x)$. The procedure begins with M_1: sending $x_j \to \sum_{i \neq j} a_i x_j$. This process is carried out for $x_1, \dots, x_4$, until we end up with a satisfactorily smaller matrix. The same is done for M_2. Swapping M_1 and M_2 until no further improvements can be made, this procedure terminates. Next, a set of generators of $SL_4(\mathbb{Z})$ is chosen and applied to each of these matrices. If one of the matrices is made smaller, the above process is repeated for the smaller matrix.

This process, carried out on $E : y^2 = x^3 + 7823$ results in the reduced 4-covering, given by the simultaneous equations as follows:

$$\begin{aligned} {x_1}^2 + 4x_1x_2 - 2x_1x_3 - 2x_1x_4 - 2{x_2}^2 - 3{x_3}^2 + 4x_3x_4 + {x_4}^2 &= 0 \\ {x_1}^2 - 6x_1x_4 + 2{x_2}^2 + 4x_2x_3 + 3{x_3}^2 + 2x_3x_4 + {x_4}^2 &= 0 \end{aligned}$$

5 Finding the Mordell-Weil generator

As we found in section 2, carrying out a 2-descent on the curve $y^2 = x^3 + 7823$ yields the following 2-covering space:

$$C : y^2 = -18x^4 + 116x^3 + 48x^2 - 12x + 30.$$

The 4-covering space C lifting it, given by the following two equations:

$$\begin{aligned} {x_1}^2 + 4x_1x_2 - 2x_1x_3 - 2x_1x_4 - 2{x_2}^2 - 3{x_3}^2 + 4z_3x_4 + {x_4}^2 &= 0 \\ {x_1}^2 - 6x_1x_4 + 2{x_2}^2 + 4x_2x_3 + 3{x_3}^2 + 2x_3x_4 + {x_4}^2 &= 0 \end{aligned}$$

has the point $P = (-681 : 116 : 125 : -142)$, from which we can find the point

$$Q = \left(\frac{53463613}{32109353}, \frac{239633346820191122}{32109353^2} \right)$$

on D. This results in the Mordell-Weil generator on E, with coordinates

$$\begin{aligned} x &= \frac{2263582143321421502100209233517777}{11981673410095561^2} \\ y &= \frac{186398152584623305624837551485596770028144776655756}{11981673410095561^3}. \end{aligned}$$

All of these computations were carried out with the MAGMA computer algebra system [2].

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] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[3] J. E. Cremona, `mwrank` *(computer software)*,
`http://www.maths.nott.ac.uk/personal/jec/ftp/progs/`.

[4] ______, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[5] J. Gebel, A. Pethö, and H. G. Zimmer, *Data on Mordell's curve*,
`http://diana.math.uni-sb.de/ simath/mordell/`.

[6] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[7] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

[8] Siksek S. Merriman, J. R. and N. P. Smart, *Explicit 4-descents on an elliptic curve*, Acta. Arith. **77** (1996), 385–404.

[9] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[10] M. Stoll, *Explicit 4-descent on an elliptic curve*,
`http://www.faculty.iu-bremen.de/stoll/papers/4-descent.pdf`.