Integral Points on Elliptic Curves Defined by Simplest Cubic Fields

Sylvain Duquesne

CONTENTS

Let f(X) be a cubic polynomial defining a simplest cubic field in the sense of Shanks. We study integral points on elliptic curves of the form $Y^2 = f(X)$. We compute the complete list of integral points on these curves for the values of the parameter below 1000. We prove that this list is exhaustive by using the methods of Tzanakis and de Weger, together with bounds on linear forms in elliptic logarithms due to S. David. Finally, we analyze this list and we prove in the general case the phenomena that we have observed. In particular, we find all integral points on the curve when the rank is equal to 1.

INTRODUCTION

Let m be a positive integer such that

$$\Delta := m^2 + 3m + 9$$

is squarefree. Denote by $\mathbb{K}_m$ the cubic field defined by the polynomial

$$f(X) = X^3 + mX^2 - (m+3)X + 1,$$

which is irreducible over $\mathbb{Q}$. The field $\mathbb{K}_m$ is said to be a *simplest cubic field* [Shanks 1974].

These fields have often been studied because their regulator is explicit and as small as possible, hence their class number is particularly large.

In this work, we are interested in elliptic curves defined by equation

$$E_m : Y^2 = X^3 + mX^2 - (m+3)X + 1 \qquad (0–1)$$

where m is an integer defining a simplest cubic field. We first want to find all the integral points on these curves for m below 1000. We then conjecture what should be true in general and finally we prove these conjectures. The main results are about the point $[0, 1]$: we prove that it is a generator of the Mordell–Weil group and we find all its integral multiples.

1058-6458/2001 $0.50 per page
Experimental Mathematics **10**:1, page 91

1. ELLIPTIC CURVES DEFINED BY SIMPLEST CUBIC FIELDS

The discriminant of the curve E_m defined by (0–1) is $16\Delta^2$ (recall that $\Delta = m^2{+}3m{+}9$ is assumed squarefree). If m is even, the conductor is $16\Delta^2$; if $m \equiv 1 \pmod 4$, the conductor is $8\Delta^2$; and if $m \equiv 3 \pmod 4$, it is $4\Delta^2$. Since the discriminant is always positive, the curve $E(\mathbb{R})$ has two connected components. Denote by $E^0(\mathbb{R})$ the connected component of the identity and by $E_{gg}(\mathbb{R})$ (as in "egg") the compact part of $E(\mathbb{R})$.

We first state a theorem of L. Washington.

Let Cl be the ideal class group of the simplest cubic field $\mathbb{K}_m$ and set

$$\mathrm{Cl}_2 = \{x \in \mathrm{Cl} : x^2 = 1\}$$

. The 2-rank $\mathrm{rk}_2(\mathrm{Cl}_2)$ will denote its dimension as a $\mathbb{Z}/2\mathbb{Z}$-vector space. Note that since $\mathbb{K}_m$ is a cyclic cubic field, $\mathrm{rk}_2(\mathrm{Cl}_2)$ is even. Finally, let Ш_2 denote the 2-torsion of the Tate–Shafarevitch group of $E_m(\mathbb{Q})$.

Theorem 1.1 [Washington 1987]. *The rank* $\mathrm{rk}\, E_m(\mathbb{Q})$ *is at most* $1 + \mathrm{rk}_2\, \mathrm{Cl}_2$. *In fact, there is an exact sequence*

$$1 \to E^0_m(\mathbb{Q})/2E_m(\mathbb{Q}) \to \mathrm{Cl}_2 \to \text{Ш}_2 \to 1.$$

From this theorem, Washington deduces the following corollary.

Corollary 1.2. *Let m be a positive integer such that $m^2 + 3m + 9$ is squarefree, then the rank of the elliptic curve E_m is odd, assuming that the Tate–Shafarevitch group is finite.*

Theorem 1.1 tells us that the search for such curves having large rank is equivalent to the search for simplest cubic fields whose class group has a large 2-rank. Several people have tried to find quadratic fields with large 3-rank which is the corresponding problem in degree 2. Moreover, since the class number of K_m is expected to be large, if Ш_2 is small with respect to Cl_2, we can thus also expect the rank of E_m to be large.

Proposition 1.3. *If m is a positive integer such that $m^2{+}3m{+}9$ is squarefree, the group $E_m(\mathbb{Q})$ is torsionfree.*

Proof. Easy, using the well-known fact that $E_m(\mathbb{Q})_{\mathrm{tor}}$ can be embedded in $E_m(\mathbb{F}_p)$ when p is a prime of good reduction. □

We now give a method using elliptic logarithms for searching for integral points on elliptic curves. This method was suggested by Lang [1978, Chapter VI, § 8] and Zagier [1987] and was simultaneous developed by several researchers [Stroeker and Tzanakis 1994; Gebel et al. 1994; Smart 1994]. The algorithm requires the knowledge of a basis of the Mordell–Weil group, as calculated for example by `mwrank` [Cremona 1998], and of an explicit lower bound for linear forms in elliptic logarithms, as given in [David 1995]. For a general point of view and more details, see [Smart 1998].

2. LINEAR FORMS IN ELLIPTIC LOGARITHMS

Let E be an elliptic curve given by its Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with $a_i \in \mathbb{Z}$. This curve is isomorphic over $\mathbb{Q}$ to curve of the form

$$Y^2 = 4X^3 - g_2X - g_3.$$

Let Λ be the lattice associated to E. We call ω_1 and ω_2 the periods of this lattice and $\wp$ the associated Weierstrass function. Note that we can always choose $\omega_1 \in \mathbb{R}$ and $\mathrm{Im}(\omega_1/\omega_2) > 0$.

We have the map φ from $\mathbb{C}/\Lambda$ to E defined by $\Phi(z) = \infty$ if $z \in \Lambda$ and $\varphi(z) = P = \big(x(z), y(z)\big)$ otherwise, with

$$x(z) = \wp(z) - \tfrac{1}{12}b_2, \quad y(z) = \tfrac{1}{2}(\wp'(z) - a_1x - a_3).$$

Let ψ be the inverse function of φ. It is given (modulo Λ) by

$$\psi(P) = \int_\infty^{x+b_2/12} \frac{dt}{\sqrt{4t^3 - g_2t - g_3}}.$$

This function is called the *elliptic logarithm* because it satisfies

$$\psi(P+Q) = \psi(P) + \psi(Q) \pmod \Lambda$$

for all $P, Q \in E(\mathbb{Q})$. Henceforth, we take the fundamental region

$$\{a\omega_1 + b\omega_2 : a, b \in \mathbb{R},\ 0 < a \le 1,\ 0 \le b < 1\}.$$

To compute this function, we use the link between elliptic integrals and the AGM [Cohen 1993].

We now define the canonical height in order to fix notations.

If $P = (x, y) \in E(\mathbb{Q})$ and $x = p/q$ with $(p, q) = 1$, we define

$$h(P) = h(x(P)) = \log \max\{|p|, |q|\}.$$

This height can be modified to obtain the canonical height

$$\hat{h}(P) = \tfrac{1}{2} \lim_{N\to\infty} 4^{-N} h(2^N P).$$

It is possible to bound the difference between these heights:

Lemma 2.1 [Silverman 1990]. *There exist constants e_1 and e_2 such that*

$$-e_1 \le \hat{h}(P) - \tfrac{1}{2} h(P) \le e_2.$$

In our case, we can choose

$$e_2 = 1.57 + \frac{\log(m^2+3m+9)}{4} + \frac{\log m}{2} \quad \textit{if } m \ge 9.$$

We now give a simplified version of S. David's result [1995] which allows us to give lower bounds for linear forms in elliptic logarithms.

Let E be an elliptic curve given by the equation

$$Y^2 = 4X^3 - g_2 X - g_3$$

with invariant j and periods ω_1 and ω_2 such that $\omega_1 \in \mathbb{R}$ and $\mathrm{Im}(\omega_1/\omega_2) > 0$. Let $P_1, \dots, P_n$ denote n points on E. We define the height

$$h_E = \max(1, h_2(1, g_2, g_3), h(j)),$$

of the elliptic curve, where h_2 denotes the absolute logarithmic height on $\mathbb{P}^2_{\mathbb{Q}}$; the constant

$$d_1 = \frac{3\pi}{|\omega_1|^2 \,\mathrm{Im}(\omega_1/\omega_2)};$$

the modified height

$$h_m(P_i) = \max\{2\hat{h}(P_i), h_E, d_1 |\psi(P_i)|^2\};$$

and constants $d_2 = \max\{e h_E, h_m(P_1), \dots, h_m(P_n)\}$,

$$d_3 = \min_{1\le i\le n} \left\{ \frac{e\sqrt{h_m(P_i)}}{\sqrt{d_1}\,|\psi(P_i)|} \right\},$$

and

$$d_4 = 2.10^{8+7n} \left(\frac{2}{e}\right)^{2n^2} \times (n+1)^{4n^2+10n} (\log d_3)^{-2n-1} \prod_{i=1}^{n} h_m(P_i).$$

Theorem 2.2 [David 1995]. *Let $L(x) = \sum_{i=1}^n x_i \psi(P_i)$ with $x \in \mathbb{Z}^n$, and set $A = \max |x_i|$. If $L(x) \ne 0$ and $A \ge \exp(d_2)$, then*

$$\log |L(x)| > -d_4(\log A + \log d_3)(\log\log A + h_E + \log d_3)^{n+1}.$$

3. COMPUTATION OF INTEGRAL POINTS

Let E be an elliptic curve associated to a simplest cubic field. We assume that we have computed a basis $P_1, P_2, \dots, P_n$ for the Mordell–Weil group. Since the sum of two points in $E^0(\mathbb{R})$ is still in $E^0(\mathbb{R})$, the sum of two points in $E_{gg}(\mathbb{R})$ is in $E^0(\mathbb{R})$ and $[0, 1] \in E_{gg}(\mathbb{R})$, we shall assume that P_1 and only P_1 belongs to $E_{gg}(\mathbb{R})$.

Let P be an integral point. Since $E(\mathbb{Q})$ is torsionfree, we have $P = p_1 P_1 + \cdots + p_n P_n$ for some $p_i \in \mathbb{Z}$. It is easy to compute integral points in $E_{gg}(\mathbb{Q})$. Hence we now assume that the point P belongs to $E^0(\mathbb{R})$. Set

$$\begin{aligned} Q_1 &= 2P_1 \in E^0(\mathbb{R}), \\ q_1 &\in \mathbb{Z} \text{ such that } p_1 = 2q_1 + r, \text{ for } r = 0 \text{ or } 1, \\ Q_i &= P_i, \\ q_i &= p_i \text{ for } i \ne 1, \\ Q_{n+1} &= P_1, \end{aligned}$$

so that

$$P = q_1 Q_1 + \cdots + q_n Q_n + r Q_{n+1}.$$

The points $P, Q_1, \dots, Q_n$ being in $E^0(\mathbb{R})$, their sum also belongs to $E^0(\mathbb{R})$, hence $r = 0$.

Now set $H = \max |q_i|$. Our purpose is to find an upper bound for H. We first need to link H with the x-coordinate of P.

Proposition 3.1. *If $P = (x, y)$ is an integral point,*

$$\frac{1}{|x|} \le c_1 e^{-c_2 H^2},$$

where $c_1 = \exp e_2$ (see Lemma 2.1) and c_2 is the smallest eigenvalue of the regulator matrix

$$[\hat{h}(Q_i + Q_j) - \hat{h}(Q_i) - \hat{h}(Q_j)]_{1\le i,j\le n}.$$

We now need to link the x-coordinate of P with its elliptic logarithm. As we have seen before, the curve E is isomorphic to a curve of the form

$$Y^2 = 4X^3 - g_2 X - g_3 = g(X).$$

Let γ_1, γ_2, γ_3 denote the roots of $g(X)$. Set $c_4 = 2\max|\gamma_i|$.

Proposition 3.2. *If $P=(x,y)\in E^0(\mathbb{R})$ and $|x+b_2/12|> c_4$, then*

$$|\psi(P)|^2 \le \frac{c_5}{|x|}$$

with $c_5 = 8 + |\omega_1^2|/12$.

Using the elliptic logarithm property and since iQ_i lies in $E^0(\mathbb{R})$ for all i, we have

$$\psi(P) - q_1\psi(Q_1) - \cdots - q_n\psi(Q_n) = m\omega_1$$

with $|m| \le nH+1$. We have $\omega_1 = \psi(\infty)$, hence $q_1\psi(Q_1)+\cdots+q_n\psi(Q_n)+m\omega_1$ is a linear form in elliptic logarithms. David's result allows us to obtain a lower bound for $\psi(P)$. Comparing this bound with the upper bound obtained by Propositions 3.1 and 3.2, we deduce a very large upper bound H_0 for H. We now seek to reduce this bound. For this, we consider the following problem: suppose we are given n real numbers $\alpha_1,\ldots,\alpha_n$, two positive real constants c_6 and c_7 and a linear form

$$L(x) = \sum_{i=1}^{n} x_i\alpha_i$$

where the x_i are integers bounded by nH_0+1.

We would like to deduce from the inequality

$$|L(x)| \le c_6 e^{-c_7 H^2}$$

a bound for H. In other words, we would like to show that the linear form cannot become too small if its coefficients are bounded.

This problem was studied by Baker and Davenport [1969] in the case $n=2$. There exist several ways to generalize their method. We give here the one most used in recent years.

The basic idea (due to de Weger) is to approximate the linear form by an approximation lattice and to find a reduced basis for this lattice. The first vector of this new basis gives an approximation to the smallest vector in the lattice. So it tells us when the linear form is small.

Consider the lattice Λ generated by the columns of the matrix

$$A = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ 0 & & 1 & 0 \\ \lfloor C\alpha_1\rfloor & \cdots & \lfloor C\alpha_{n-1}\rfloor & \lfloor C\alpha_n\rfloor \end{pmatrix} \in \mathcal{M}_{n,n}(\mathbb{Z}).$$

We choose the constant C approximately equal to $(nH_0)^n$. Thus the determinant of A will be of the order of $(nH_0)^n$ and we hope that the first basis element in an LLL-reduced lattice will be of order nH_0.

Proposition 3.3. *Let $B=(b_1,\ldots,b_n)$ be a reduced basis for the lattice, B^* the associated Gram-Schmidt basis, $c_8 = \min\{\|b_i^*\| : 1\le i\le n\}$, $S=\sum_{i=1}^{n-1} X_i^2$ and $T = \frac{1}{2}\sum_{i=1}^{n} X_i$. If $c_8^2 \ge T^2+S$ and $x = {}^t(x_1,\ldots,x_n)\ne 0$ then*

$$H \le \sqrt{\bigl(\log(Cc_6) - \log\bigl(\sqrt{c_8^2 - S} - T\bigr)\bigr)/c_7}.$$

Remark. If the bound for H exists, it is of the form $O\bigl(\sqrt{\log H_0}\bigr)$. If the method fails (i.e., if the condition on c_8 is not satisfied), we increase the constant C and repeat the algorithm.

Hence, this method allows us to reduce the bound to $O\bigl(\sqrt{\log H_0}\bigr)$. The new bound is generally small enough to enumerate all the possibilities for integral points. However, if this bound seems to large, we repeat the algorithm.

4. TABLES OF RESULTS

Tables 1–3 show results obtained by this method. For all $m \le 1000$ such that m^3+3m+9 is squarefree, we found the rank $\operatorname{rk} E_m(\mathbb{Q})$. Where possible, the basis of the Mordell–Weil group was computed using `mwrank` [Cremona 1998]. In some cases, distinguished in the tables by an underlined value of the parameter m, `mwrank` cannot conclude about the rank; we then computed the rank using the Birch and Swinnerton-Dyer conjecture.

The tables are separated by rank. Tables 2 and 3 list the x-coordinate of each integral point in $E_0(\mathbb{R})$. Examination shows that there are always integral points in $E_0(\mathbb{R})$ with a positive x-coordinate when m is odd and never when m is even.

When the rank is 1, the point $[0,1]$ seems to be a basis for the Mordell–Weil group and there does not exist any integral point other than $[0,1]$ and its double when m is odd. So Table 1 gives only the list of the values of the parameter m when the rank is 1. More generally, $[0,1]$ seems to be always a generator. (This last remark is valid only if the parameter m defines a simplest cubic field, as we have assumed;

000 +	1 2 4 7 8 10 13 14 16 19 20 22 28 31 32 34 35 37 38 40 43 46 47 49 50 52 53 56 58 61 62 65 68 70 73 74 76 77 79 80 82 86 88 89 91 92 94 97 98
100 +	4 6 7 9 10 12 15 16 19 21 22 24 25 28 31 34 40 45 48 55 58 60 61 64 67 $\underline{70}$ 72 73 75 78 82 $\underline{84}$ 85 90 93 96 97 99
200 +	0 2 3 5 6 8 9 11 12 14 15 17 21 24 26 32 33 38 39 41 44 45 47 51 53 54 56 57 59 60 $\underline{62}$ 65 66 68 72 78 $\underline{80}$ 81 $\underline{84}$ 89 $\underline{90}$ 93 95 96 98
300 +	$\underline{1}$ 2 4 10 13 14 16 17 19 20 22 23 25 26 28 31 $\underline{32}$ $\underline{34}$ 37 38 40 43 44 46 49 $\underline{52}$ 53 55 61 62 64 67 68 $\underline{70}$ 73 76 79 80 $\underline{82}$ 83 85 86 88 92 94
400 +	1 3 9 10 $\underline{12}$ 13 15 16 $\underline{18}$ 21 22 24 25 $\underline{27}$ 30 31 36 37 43 45 48 $\underline{49}$ 51 52 $\underline{54}$ 55 $\underline{60}$ 63 64 66 67 69 76 78 81 84 85 87 88 90 93 $\underline{96}$ 97
500 +	$\underline{2}$ $\underline{5}$ 6 8 9 $\underline{14}$ 18 20 21 $\underline{24}$ 26 27 29 30 36 39 41 $\underline{47}$ 50 51 53 54 $\underline{56}$ $\underline{60}$ 62 63 66 68 69 72 74 81 86 87 89 90 92 95 96 98 99
600 +	1 4 5 8 10 13 $\underline{14}$ 20 22 23 28 31 32 34 35 38 40 43 $\underline{46}$ 47 50 52 56 58 59 61 62 64 65 67 70 73 74 76 77 79 80 $\underline{82}$ 85 86 88 89 92 94 95 97
700 +	0 3 6 7 13 15 18 21 25 28 30 31 33 $\underline{34}$ 36 39 43 46 $\underline{48}$ 49 51 52 54 55 57 60 61 63 64 66 67 69 70 $\underline{72}$ 75 78 79 81 82 85 87 88 90 $\underline{94}$ 97 99
800 +	2 $\underline{5}$ 11 12 14 17 18 $\underline{20}$ 21 23 26 27 29 $\underline{32}$ 33 36 41 $\underline{42}$ 47 50 51 53 54 57 59 60 62 63 65 66 68 69 71 72 77 81 83 84 86 89 90 $\underline{92}$ 93 $\underline{95}$ 96 98
900 +	1 2 5 7 8 10 13 16 17 19 20 $\underline{22}$ 25 29 31 32 35 $\underline{37}$ 40 $\underline{44}$ 46 47 49 50 52 53 55 $\underline{62}$ $\underline{64}$ 65 67 68 $\underline{71}$ 73 74 76 79 80 86 88 94 97 98
1000	

TABLE 1. Values of $m \leq 1000$ such that $\mathbb{K}_m$ is a simplest cubic field and for which the rank of $E_m(\mathbb{Q})$ equals 1, as computed by `mwrank` [Cremona 1998], or, in the underlined cases, by the use of the Birch–Swinnerton-Dyer conjecture. Each row represents a range $100k \leq m < 100(k+1)$. In all these cases the point $[0, 1]$ is a generator, so the integral points are given by Theorem 5.8.

it is false for $m = 5$, for instance.)

The remainder of this paper is devoted to proving these and other general results for the curves E_m defined by simplest cubic fields. In particular, we prove that $[0, 1]$ is always a generator (Theorem 5.7 below) and that there are no other integral points on E_m that are positive multiples of $[0, 1]$, apart from $2[0, 1]$ when m is odd (Theorem 5.8).

5. GENERAL RESULTS ABOUT INTEGRAL POINTS ON THE ELLIPTIC CURVES $y^2 = x^3 + mx^2 - (m+3)x + 1$

Several papers have considered the problem of solving parametrized Diophantine equations. In particular for Thue equations see [Pethő 1991; Niklasch and Smart 1998]. In this paper, we obtain some interesting results on parametrized elliptic curves. All the curves in our family have the integral point $[0, 1]$ however, and this is essential in the following. Hence it should be possible to extend our method to other parametrized curves having a fixed nontorsion point.

5A. Arithmetic Study of Integral Points

First we show that when the parameter m is even there is no integral point in the non-compact part of the curve E_m.

Lemma 5.1. *If m is even and if $[x, y]$ is an integral point, then $x \equiv 0 \pmod 8$.*

Proof. Set $m = 2k$, so that we have $y^2 = x^3 + 2kx^2 - (2k+3)x + 1$. Then, if x is even then y^2 is odd. The only odd square modulo 8 is 1, so $(2k + 3)x \equiv 0 \pmod 8$. Since $2k+3$ is invertible modulo 8, we obtain $x \equiv 0 \pmod 8$. If x is odd, a similar argument leads to a contradiction. □

Lemma 5.2. *If m is odd and $[x, y]$ is an integral point, then 4 does not divide $|x - 1|$.*

Proof. Similar to the previous proof. □

Theorem 5.3. *Let x be an integer. Set $a = x^2 - x$ and $b = x^3 - 3x + 1$. There exists m such that $am + b$ is a square if and only if every odd prime dividing $|x - 1|$ is congruent to 1 modulo 4 and if in addition 4 does not divide $|x - 1|$.*

Proof. Note that b is coprime to x and to $x - 1$, hence to a. Thus, there exists m such that $am + b$ is a square if and only if b is a square modulo a; that is, if and only if for all prime divisor p of a, b is a square modulo $p^{v_p(a)}$ (where as usual $v_p(a)$ denotes the p-adic valuation of the nonzero integer a).

Using Hensel's lemma, if $p \neq 2$, we know that b is a square modulo p^n for every integer n if and only if b is a square modulo p.

143	$-144, -124, -105, -81, -64, -33, -28, -4, -1, 0, 2, 6, 30, 90, 114, 182, 290, 846, 854, 4182, 5186, 17342, 414290$
347	$-345, -292, -225, -84, -64, -12, -4, 0, 6, 26, 98, 1190, 5070, 14930, 30278$
419	$-420, -280, -225, -196, -64, -33, -1, 0, 2, 6, 14, 366, 482, 594, 44102$
439	$-408, -276, -105, -9, 0, 42, 54, 222, 270, 966, 30090, 48402$
473	$-456, -364, -240, -60, -16, -4, 0, 27, 51, 107, 899, 2315, 56171$
611	$-612, -537, -324, -289, -280, -184, -9, -1, 0, 2, 74, 266, 546, 686, 1650, 8502, 93638, 1313274$

TABLE 2. Parameter m and x-coordinate of integral points when the rank is 5, as determined by `mwrank`.

11	−12, −9, −4, −1, 0, 2, 6, 26, 30, 38, 3170, 7502
17	−12, −4, 0, 3, 35, 83
23	−24, −16, −9, −1, 0, 2, 14, 42, 146
25	−12, 0, 3, 51, 171
26	−24, −16, 0
29	−28, −4, 0, 11, 227
44	−40, −16, 0
55	−12, 0, 6, 126, 786
59	−60, −36, −25, −1, 0, 2, 42, 86, 902
64	−24, 0
67	−57, −9, 0, 6, 1158
71	−52, −4, 0, 14, 1298
83	−84, −49, −36, −1, 0, 2, 62, 114, 1766
85	−24, 0, 3, 1851
95	−84, −4, 0, 30, 2306
101	−40, 0, 3, 2603
113	−84, −4, 0, 35, 3251
118	−96, 0
127	−60, 0, 186, 4098
130	−72, 0
133	−24, 0, 4491
136	0
137	−40, 0, 3, 4763
142	−72, 0
146	−40, 0
149	−136, −16, 0, 11, 5627
151	0, 66, 5778
157	−84, −60, −12, 0, 3, 6243
163	−156, −36, 0, 6726
166	−24, 0
169	−168, −144, 0, 7227
176	−88, 0
179	−180, −100, −81, −1, 0, 2, 146, 222, 8102
181	−96, 0, 8283
187	−177, −9, 0, 18, 8838
191	−28, 0, 6, 9218
194	0
218	−88, 0
220	0
223	−33, 0, 6, 12546
227	−172, −4, 0, 66, 12998
229	0, 75, 13227
230	0
236	0
242	−64, 0
248	−88, 0
263	−264, −144, −121, −1, 0, 2, 222, 314, 17426
274	0
275	−12, 0, 26, 3770, 12630, 19046
277	−84, 0, 3, 19323
283	0, 174, 20166
287	−129, 0, 20738
292	−240, 0
305	−112, 0, 3, 23411
307	−57, 0, 6, 23718
308	0
311	−312, −169, −144, −1, 0, 2, 266, 366, 24338
329	0, 35, 627, 27227
341	−28, 0, 11, 29243
350	−24, 0
358	0
359	0, 114, 32402
365	−112, 0, 3, 33491
371	−24, 0, 14, 34598
377	−12, 0, 35, 35723
389	−376, −16, 0, 27, 38027
391	−84, 0, 34146, 38418
395	−60, 0, 1890, 39206
400	−192, 0
406	−168, 0
407	−385, −25, 0, 18, 41618
428	−24, 0
434	0
440	−40, 0
442	0
457	−240, 0, 52443
458	−40, 0
461	−12, 0, 35, 53363
470	0
472	0
475	−57, 0, 56646
479	−480, −256, −225, −1, 0, 2, 422, 546, 57602
491	−465, −25, 0, 18, 60518
494	−456, −16, 0
499	0, 30, 62502
500	0
503	−33, 0, 14, 63506
511	0, 102, 65538
512	0
517	−12, 0, 67083
523	−108, 0, 68646
532	−504, 0
533	−444, −4, 0, 147, 71291
535	0, 66, 71826
538	0
542	−280, 0
545	−40, 0, 74531
548	0
557	0, 555, 77843
559	−33, 0, 78402
571	−564, −36, 0, 81798
575	−444, −4, 0, 158, 82946
578	0
583	−105, 0, 6, 85266
584	0
616	−504, 0
617	−220, −52, 0, 3, 11, 95483
619	−96, 0, 6, 96102
625	0, 97971
626	−616, 0
637	−24, 0, 101763
641	−532, −4, 0, 147, 103043
644	−304, 0
649	0, 105627
653	−28, 0, 106931
655	−12, 0, 107586
668	−264, 0
671	−364, 0, 1470, 112898
683	−684, −361, −324, −1, 0, 2, 614, 762, 116966
698	−184, 0
701	−220, 0, 3, 123203
704	−688, −64, 0
709	0, 151, 126027
710	0
712	−24, 0
719	−633, −9, 0, 74, 129602
722	−304, 0
724	−288, 0
737	−72, 0, 11, 136163
745	−264, 0, 3, 139131
758	−240, 0
773	−348, 0, 149771
784	0
791	0, 156818
793	−156, 0, 3771, 157611
796	−336, 0
800	0, −112, 0
803	−744, −16, 0, 54, 161606
806	−480, 0
808	0
809	−628, −4, 0, 219, 164027
815	−145, 0, 6, 166466
824	0
830	−184, −40, 0
835	−792, 0, 174726
839	−840, −441, −400, 0, −1, 2, 762, 926, 176402
845	−72, 0, 11, 178931
848	−280, 0
856	−24, 0
875	−52, 0, 18, 10626, 191846
878	−168, 0
880	−240, 0
899	0, 202502
904	0
914	−376, 0
928	0
934	0
938	0
941	−732, −4, 0, 219, 221843
943	−660, −129, −24, 0, 42, 222786
956	0
958	−264, 0
959	−73, 0, 14, 230402
961	−12, 0, 75, 291, 231363
970	−792, 0
977	0, 203, 10131, 239123
982	−840, 0
983	−33, 0, 242066
989	−168, 0, 245027
991	−156, 0, 6, 246018
995	−52, 0, 18, 248006

TABLE 3. Parameter m and x-coordinate of integral points when the rank is 3 (as determined by `mwrank` or, for underlined values of m, using the Birch–Swinnerton-Dyer conjecture.)

Thus, let p be an odd prime divisor of a. Then either p divides x, so

$$\left(\frac{b}{p}\right) = \left(\frac{1}{p}\right) = 1,$$

so b is a square modulo p; or p divides $x - 1$, hence

$$\left(\frac{b}{p}\right) = \left(\frac{(x^2-2)(x-1)-1}{p}\right) = \left(\frac{-1}{p}\right).$$

It follows that b is a square if and only if $p \equiv 1 \pmod 4$.

Assume now that a is even, so that b is odd. Then, when $a \equiv 2 \pmod 4$, b is always a square modulo 2. When $a \equiv 4 \pmod 8$, we have $x^2 - x \equiv 0 \pmod 4$ so either x is even, hence $b \equiv 1 \pmod 4$, so b is a square modulo 4. Or x is odd, hence $x \equiv 3 \pmod 4$, so $x^2 - x \equiv 2 \pmod 4$ which is a contradiction. When $a \equiv 0 \pmod 8$, b is odd and it is trivial to prove by induction that for all n, b is a square modulo 2^n if and only if $b \equiv 1 \pmod 8$. Thus, when $x \equiv 0 \pmod 4$ then $b \equiv 1 \pmod 8$, so b is a square modulo 2^n. The case $x \equiv 1 \pmod 4$ is not possible by hypothesis. Finally, if $x \equiv 2$ or $3 \pmod 4$, then $a \equiv x^2 - x \equiv 2 \pmod 4$, which is a contradiction. □

Corollary 5.4. *Let $P = [x, y]$ be an integral point on the curve E_m. Then, if $x > 1$ we have $x \equiv 2 \pmod 4$ or $x \equiv 3 \pmod 8$, while if $x < 1$ we have $x \equiv 0 \pmod 4$ or $x \equiv 7 \pmod 8$.*

Proof. Assume first that $x > 1$. If $[x, y]$ is an integral point, $x^3 + mx^2 - (m+3)x + 1$ is a square. Theorem 5.3 implies that every odd prime dividing $x - 1$ is congruent to 1 modulo 4. If x is even, we deduce that $x - 1$ is congruent to 1 modulo 4. If x is odd, we know that 4 does not divide $|x-1|$ by Lemma 5.2 and so

$$x - 1 = 2 \prod_{\substack{p \mid x-1 \\ p \neq 2}} p \equiv 2 \pmod 8.$$

The proof is similar when $x < 1$. □

Corollary 5.5. *If m is even, there is no integral point on $E_m^0(\mathbb{Q})$ (i.e., with a positive x-coordinate).*

Proof. The point $[1, y]$ is never on the curve. If $x > 1$, there is a contradiction between the previous corollary and Lemma 5.1. □

These corollaries can be summarized as follows:

Proposition 5.6. *There exists m (not necessary defining a simplest cubic field) such that the point $[x, y]$ is on $E_m(\mathbb{Z})$ if and only if the following conditions are satisfied:*

1. *$y \equiv \pm 1 \pmod{q^{v_q(x)}}$ for every odd prime q dividing x;*
2. *$y \equiv \pm\sqrt{-1} \pmod{p^{v_p(x)}}$ for every odd prime p dividing $x-1$;*
3. *y is odd;*
4. *if $x < 1$ and $x \equiv 0 \pmod 8$, then*

$$y \equiv \pm 1 \pmod{2^{v_2(x)-1}}.$$

This proposition allows us to do a "faster" systematic search for integral points. Before proving the announced results, we look for some parametrized solutions of equation (0–1).

5B. Parametrized Solutions of $y^2 = x^3 + mx^2 - (m+3)x + 1$

In this section, we consider the equation (0–1) as an affine surface in $\mathbb{R}^3$. We set $x = u+1$. Since $(0, 1, m)$ is always on the surface, we can set $y - 1 = (t-1)x$. Thanks to the linearity in m of the equation, we obtain a rational parametrization of our surface:

$$\begin{aligned} x &= u + 1, \\ y &= tu + t - u, \\ m &= t^2 - 2t - u - 1 + \frac{t^2+1}{u}. \end{aligned}$$

In order to find parametrized integral solutions of our equation, we set

$$k = \frac{t^2+1}{u},$$

and we denote by $P(k)$ the parametrized solution thus obtained. For example:

$$P(1) = \begin{cases} x = t^2 + 2, \\ y = -t^3 - 2t - t^2 - 1, \\ m = 2t - 1 \end{cases}$$

The solution obtained is the point $2[0, 1]$ when m is odd. This remark has already been made.

The equations for $P(-1)$ give an integral point when $m = 2t^2 + 2t - 1$. In this case the points $P_0 = [-1, 2t+1]$, $P_1 = [0, 1]$ and $P_2 = [2, 2t+1]$ are independent on $E_m(\mathbb{Q}(t))$ (this can be shown using the Néron–Tate height pairing [Shioda 1990]). Moreover $2P_1$, $P_0 + P_1$, $P_0 - P_1$, $P_2 + P_1$, $P_0 + P_2$ and $P_2 - P_1$ are integral points. Note that this last one is the point given by $P(-1)$. So finally in this case, we obtain at least 9 integral points on the curve E_m. The numerical data suggest this phenomenon.

Similar considerations with $k = -5$ give (after replacing t by $-\frac{5}{2}t + 2$) an integral point for $m = 5t^2 - 3t + 3$ and we find on this curve 3 independent integral points.

We can hope to find some m such that E_m has high rank if m satisfy both of the two previous equations, in other words if

$$m = 2t_1^2 + 2t_1 - 1 = 5t_2^2 - 3t_2 + 3.$$

Set $T_1 = 2t_1 + 1$ and $T_2 = 10t_2 - 3$, we have to solve $T_2^2 - 10T_1^2 = -81$ with the conditions T_1 odd, $T_2 \equiv -3 \pmod{10}$, T_1 and T_2 not multiples of 3. An easy argument in the field $\mathbb{Q}(\sqrt{10})$ shows that the general solution is

$$T_2 + T_1\sqrt{10} = (-1)^{k+1}(3 + \sqrt{10})^{2k+1}(11 + 2\sqrt{10}).$$

with $k \in \mathbb{Z}$. If $k = 0$, we obtain $m = 11$ which is the smallest value of m for rank 3. If $k = -1$, we obtain $m = 143$ which is the smallest value for rank 5. If $k = 1$, we obtain $m = 14963$ and E_m is of rank at least 7 (the points $[0, 1]$, $[-1, 173]$, $[2, 173]$, $[-4, 547]$, $[-11884, 659563]$ are given by our parametrization and the additional generators

$$[-64, 7873] \quad \text{and} \quad [90, 10981]$$

are found by a systematic search. All these points are independent). Note that this is not the smallest rank 7 curve in our family, since E_m is of rank 7 also for $m = 12563$, which may well be the smallest m.

We now prove results concerning the point $[0, 1]$. For this purpose, we must find approximations for the height of a point on E_m. For this, we need in particular to know the asymptotic behavior of the periods associated to the curve E_m in terms of the parameter m.

5C. Approximating the periods ω_1 and ω_2

The curve E_m defined by (0–1) is isomorphic to the curve

$$y^2 = 4f(x)$$

with

$$f(x) = x^3 - \left(\tfrac{1}{3}m^2 + m + 3\right)x + \tfrac{2}{27}m^3 + \tfrac{1}{3}m^2 + m + 1.$$

Let $e_1 \le e_2 \le e_3$ be the real roots of f (the discriminant is always positive). The periods ω_1 and ω_2 are given by

$$\omega_1 = \int_{e_1}^{e_2} \frac{dx}{\sqrt{f(x)}} \quad \text{and} \quad \omega_2 = -\int_{e_2}^{e_3} \frac{dx}{\sqrt{f(x)}}.$$

A straightforward study of the function f gives the inequalities:

$$\begin{gathered} -\frac{2m}{3} - 1 - \frac{2}{m} \le e_1 \le -\frac{2m}{3} - 1 - \frac{1}{m} \quad \text{if } m \ge 2, \\ \frac{m}{3} \le e_2 \le \frac{m}{3} + \frac{1}{m}, \\ \frac{m}{3} + 1 \le e_3 \le \frac{m}{3} + 1 + \frac{1}{m}. \end{gathered}$$

We start with an approximation for ω_2 given by

$$\omega_2 = i\int_{e_2}^{e_3} \frac{dx}{\sqrt{(x-e_1)(x-e_2)(e_3-x)}} \in i\mathbb{R}.$$

If $x \in [e_2, e_3]$, then $m + 1 + 1/m \le x - e_1 \le m + 2 + 3/m$, so

$$\frac{1}{\sqrt{m+2+3/m}} \le \frac{1}{\sqrt{x - e_1}} \le \frac{1}{\sqrt{m+1+1/m}}$$

and

$$\frac{I}{\sqrt{m+2+3/m}} \le \frac{\omega_2}{i} \le \frac{I}{\sqrt{m+1+1/m}}$$

with

$$I = \int_{e_2}^{e_3} \frac{dx}{\sqrt{(x-e_2)(e_3-x)}} = \int_{-1}^{1} \frac{dt}{\sqrt{1-t^2}} = \pi.$$

Finally, we have

$$\frac{\pi}{\sqrt{m+2+3/m}} \le \frac{\omega_2}{i} \le \frac{\pi}{\sqrt{m+1+1/m}}.$$

So $\omega_2 \sim i\pi/\sqrt{m}$ and $\omega_2/i \ge 3.13/\sqrt{m}$ if $m \ge 500$.

We now consider the case of ω_1.

We split the integral into two parts: $\omega_1 = \omega_1^+ + \omega_1^-$, with

$$\omega_1^- = \int_{e_1}^{0} \frac{dx}{\sqrt{f(x)}} \quad \text{and} \quad \omega_1^+ = \int_{0}^{e_2} \frac{dx}{\sqrt{f(x)}}.$$

For ω_1^-, the roots e_2 and e_3 are far from the endpoints of the domain of integration. We thus have, for $x \in [e_1, 0]$:

$$\begin{gathered} m/3 \le e_2 - x \le m + 1 + 3/m, \\ m/3 + 1 \le e_3 - x \le m + 2 + 3/m. \end{gathered}$$

So

$$\omega_1^- \geq \frac{1}{\sqrt{(m+1+3/m)(m+2+3/m)}} \int_{e_1}^{0} \frac{dx}{\sqrt{x-e_1}},$$

$$\omega_1^- \leq \frac{1}{\sqrt{(m/3)(m/3+1)}} \int_{e_1}^{0} \frac{dx}{\sqrt{x-e_1}},$$

$$\omega_1^- \geq \frac{2\sqrt{-e_1}}{\sqrt{(m+1+3/m)(m+2+3/m)}},$$

$$\omega_1^- \leq \frac{2\sqrt{-e_1}}{\sqrt{(m/3)(m/3+1)}},$$

$$\omega_1^- \geq \frac{2\sqrt{2m/3+1+1/m}}{\sqrt{(m+1+3/m)(m+2+3/m)}},$$

$$\omega_1^- \leq \frac{2\sqrt{2m/3+1+2/m}}{\sqrt{(m/3)(m/3+1)}}.$$

We deduce the inequalities $\omega_1^- \leq 4.9/\sqrt{m}$ and $\omega_1^- \geq 1.63/\sqrt{m}$ if $m \geq 500$.

Now consider the case of ω_1^+. Here only e_1 is sufficiently far from the domain of integration. For $x \in [0, e_2]$,

$$\frac{2m}{3}+1+\frac{1}{m} \leq x-e_1 \leq m+1+\frac{3}{m},$$

so

$$\frac{I}{\sqrt{m+1+3/m}} \leq \omega_1^+ \leq \frac{I}{\sqrt{2m/3+1+1/m}}$$

with

$$I = \int_0^{e_2} \frac{dx}{\sqrt{(x-e_2)(x-e_3)}} = \log \frac{\sqrt{e_3}+\sqrt{e_2}}{\sqrt{e_3}-\sqrt{e_2}}$$

and

$$\frac{4m/3}{1+1/m} \leq \frac{\sqrt{e_3}+\sqrt{e_2}}{\sqrt{e_3}-\sqrt{e_2}} \leq \frac{4\,(m/3+1+1/m)}{1-1/m}.$$

We can thus write

$$\omega_1^+ \geq \frac{1}{\sqrt{m+1+3/m}} \log \frac{4m}{3\,(1+1/m)},$$

$$\omega_1^+ \leq \frac{1}{\sqrt{2m/3+1+1/m}} \log \frac{4(m+3+3/m)}{3(1-1/m)},$$

$$\omega_1^+ \geq \frac{\log \dfrac{4}{3\,(1+1/m)}}{\sqrt{m+1+3/m}} + \frac{\log m}{\sqrt{m+1+3/m}},$$

$$\omega_1^+ \leq \frac{\log \dfrac{4}{3\,(1-1/m)}}{\sqrt{2m/3+1+1/m}} + \frac{\log\,(m+3+3/m)}{\sqrt{2m/3+1+1/m}}.$$

Finally, we have, for $m \geq 500$,

$$\frac{0.28}{\sqrt{m}} + \frac{0.99\log m}{\sqrt{m}} \leq \omega_1^+ \leq \frac{5.26}{\sqrt{m}} + \frac{1.23\log m}{\sqrt{m}},$$

$$\frac{1.91}{\sqrt{m}} + \frac{0.99\log m}{\sqrt{m}} \leq \omega_1 \leq \frac{5.26}{\sqrt{m}} + \frac{1.23\log m}{\sqrt{m}}.$$

Remark. In fact we can easily prove that

$$\omega_1 = \frac{\log m + 4\log 2 + o(1)}{\sqrt{m}},$$

but we do not need this.

5D. Approximating the Canonical Height

First, we find an upper bound for the canonical height of an integral point P on E_m. By Lemma 2.1,

$$\hat{h}(P) - \tfrac{1}{2}h(P) \leq 1.57 + \tfrac{1}{4}\log(m^2+3m+9) + \tfrac{1}{2}\log m.$$

Since P is integral, $h(P) = \log\max\{1, |x_P|\}$. So

$$\hat{h}(P) \leq \tfrac{32}{25}\log m + \tfrac{1}{2}\log\max\{1, |x_P|\} \quad \text{if } m \geq 500. \tag{5–1}$$

To find a lower bound for the canonical height of a rational point on E, we write it as the sum of local contributions.

Let $P = \left[\alpha/d^2,\, \beta/d^3\right] \in E_m(\mathbb{Q})$ with $(\alpha, d) = (\beta, d) = 1$. We first compute the non-Archimedean contribution. We use the algorithm described in [Silverman 1988; Cohen 1993, Section 7.5.2]. We have $\beta^2 = \alpha^3 + md^2\alpha^2 - (m+3)d^4\alpha + 1$. So $\beta \equiv \alpha + 1 \pmod 2$ and d cannot be even. A similar argument shows that d is not a multiple of 3. Set

- $\Delta = m^2+3m+9$;
- $A = 3\alpha^2 + 2md^2\alpha - (m+3)d^4$ (the numerator of $3\alpha^2/d^4 + 2m\alpha/d^2 - (m+3)$);
- $B = 2\beta$ (the numerator of $2\beta/d^3$);
- $C = 3\alpha^4 + 4m\alpha^3d^2 - (6m+18)\alpha^2d^4 + 12\alpha d^6 - \Delta d^8$ (the numerator of $3\alpha^4/d^8 + 4m\alpha^3/d^6 - (6m+18) \times \alpha^2/d^4 + 12\alpha/d^2 - \Delta$); and
- $D = \gcd(A, B)$.

We prove that the only prime giving any local contribution is 2. Let p be an odd prime dividing D. Because

$$4A^2 = (9\alpha+3d^2m)B^2 + 4\Delta d^4(\alpha^2-d^2\alpha+d^4),$$

p^2 divides $4\Delta d^4(\alpha^2-d^2\alpha+d^4)$. On the other hand p does not divide d (because p divides β) and Δ

is squarefree, so p divides $(\alpha^2-d^2\alpha+d^4)$. Next, because

$$B^2=4(\alpha+d^2(m+1))(\alpha^2-d^2\alpha+d^4)-4d^4(3\alpha+d^2m),$$

p divides $3\alpha+d^2m$. Moreover the resultant of A and B is $d^{12}\Delta^2$, so p divides Δ and hence p divides $(3\alpha+d^2m-3d^4\Delta)$. Because

$$27B^2=4(3\alpha+d^2m-3d^4\Delta)(3\alpha+d^2m)+4d^6(2m+3)\Delta,$$

p^2 divides $d^6(2m+3)\Delta$, so p divides $2m+3$. And since $4\Delta=(2m+3)^2+27$, we conclude that $p=3$; but then 3 divides m and Δ is not squarefree. We have thus proved 2 is the only prime dividing D.

We now compute the local contribution $C_2=C_l$ at $l=2$. We have $v_2(B)=1$ and $C\equiv-(2m+2) \pmod 8$, so we obtain:

- If m is even, $C_2=\log d$.
- If $m\equiv 1 \pmod 4$, $C_2=\log d-\frac14\log 2$.
- If $m\equiv 3 \pmod 4$, $C_2=\log d-\frac13\log 2$.

In all cases, $C_2\geq \log d-\frac13\log 2$.

We consider now the Archimedean contribution C_∞ of the point P. Denote by z the elliptic logarithm of P. Set $\lambda=2\pi/\omega_1$, $t=\lambda\operatorname{Re} z$, $q=\exp(2i\pi\omega_2/\omega_1)$ and

$$\theta=\sum_{n=0}^{\infty}\sin((2n+1)t)(-1)^n q^{n(n+1)/2}.$$

Then the Archimedean contribution is

$$C_\infty=\tfrac{1}{32}\log\left|16\Delta^2/q\right|-\tfrac14\log|\theta| + \tfrac18\log\left(\frac{(\alpha/d^2)^3+m(\alpha/d^2)^2-(m+3)\alpha/d^2+1}{\lambda}\right).$$

The discriminant $16\Delta^2$ of the curve is greater than $16m^4$. On the other hand,

$$|\theta|\leq\sum_{n=0}^{\infty}q^{n(n+1)/2}\leq\frac{1}{1-q}.$$

To find a lower bound for C_∞, we need an upper bound for q. Using approximations to the periods, we deduce

$$2i\pi\frac{\omega_2}{\omega_1}\leq\frac{-3.13\ 2\pi}{5.26+1.23\log m}\leq-\frac{9.47}{\log m}$$

if $m\geq 500$, so

$$q\leq\exp\Bigl(-\frac{9.47}{\log m}\Bigr)\leq 1-\frac{4.86}{\log m}$$

if $m\geq 500$.

We are now able to minimize each part of C_∞ for $m\geq 500$:

$$\begin{aligned}
&\tfrac{1}{32}\log\left|16\Delta^2\right|\geq\tfrac18\log m+\tfrac18\log 2,\\
&\tfrac{1}{32}\log|1/q|\geq\tfrac{1}{32}\log\exp\frac{9.47}{\log m}\geq\frac{9.47}{32\log m},\\
&-\tfrac14\log|\theta|\geq-\tfrac14\log\frac{1}{1-q}\geq-\tfrac14\log\frac{\log m}{4.86}\\
&\qquad\geq\tfrac14\log 4.86-\tfrac14\log\log m.
\end{aligned}$$

As for $-\frac18\log\lambda=\frac18\log(\omega_1/2\pi)$, it is greater than or equal to

$$\begin{aligned}
&-\tfrac18\log(2\pi)+\tfrac18\log\frac{1.91+0.99\log m}{\sqrt{m}}\\
&\quad\geq\tfrac18\log\frac{1}{\sqrt{m}}-\tfrac18\log(2\pi)+\tfrac18\log(1.91+0.99\log m)\\
&\quad\geq-\tfrac{1}{16}\log m-\tfrac18\log(2\pi)+\tfrac18\log\Bigl(0.99+\frac{1.91}{\log m}\Bigr)\\
&\qquad\qquad+\tfrac18\log\log m,
\end{aligned}$$

Moreover

$$\frac{\log 2}{8}-\frac{8}{\log(2\pi)}+\frac{\log 4.86}{4}\geq 0.252.$$

Finally, we obtain the following lower bound for C_∞:

$$\begin{aligned}
&\tfrac{1}{16}\log m+\frac{9.47}{32\log m}+\tfrac14\log(\beta/d^3)\\
&\quad+\tfrac18\log(0.99+1.91/\log m)-\tfrac18\log\log m+0.252.
\end{aligned}$$

Adding the non-Archimedean contribution, we obtain

$$\begin{aligned}
\hat h(P)\geq{}&\tfrac{1}{16}\log m+\frac{9.47}{32\log m}+\tfrac14\log(\beta/d^3)\\
&+\tfrac18\log(0.99+1.91/\log m)\\
&-\tfrac18\log\log m+\log d-\tfrac13\log 2+0.252.
\end{aligned}$$

Hence, we obtain a lower bound for $\hat h(P)$:

$$\begin{aligned}
&\hat h(P)\geq\tfrac{1}{16}\log m+\frac{9.47}{32\log m}+\tfrac14\log(\beta d)\\
&+\tfrac18\log(0.99+1.91/\log m)-\tfrac18\log\log m+0.02. \qquad (5\text{–}2)
\end{aligned}$$

5E. About the Special Point $[0,1]$

Theorem 5.7. *The point* $[0,1]$ *is always a generator.*

Proof. If $m\leq 500$, we have computed the Mordell–Weil group and all the integral points (see Tables on pages 95 and 96) and the assertion of the theorem is satisfied. If $m\geq 500$, we use the above approximations. Let P be a point (with positive y-coordinate) on E such that $[0,1] = nP$. Since the sum of two points in $E_0(\mathbb{Q})$ is still in $E_0(\mathbb{Q})$, P belongs to $E_{gg}(\mathbb{Q})$. We assume first that P is integral and not equal to $[0,1]$. The y-coordinate of such a point is greater than $\sqrt{2m+3}$, so by (5–2)

$$\hat{h}(P) \geq \tfrac{1}{16}\log m + \tfrac{1}{4}\log\sqrt{2m} + \tfrac{1}{8}\log 0.99 - \tfrac{1}{8}\log\log m + 0.02,$$
$$\hat{h}(P) \geq \tfrac{3}{16}\log m - \tfrac{1}{8}\log\log m + 0.1,$$
$$\hat{h}(P) \geq \tfrac{1}{6}\log m.$$

On the other hand, $\hat{h}([0,1]) \leq \frac{32}{25}\log m$ by (5–1), so

$$n^2 = \frac{\hat{h}([0,1])}{\hat{h}(P)} \leq 6\ \tfrac{32}{25} \leq 8.$$

Moreover $2P \in E_0(\mathbb{Q})$ and hence P cannot exist.

We now assume that $P = [\alpha/d^2, \beta/d^3]$ is not integral. We have seen that d is odd and not a multiple of 3, so $\beta d \geq 5$. We have by (5–2)

$$\hat{h}(P) \geq \tfrac{1}{16}\log m + \tfrac{1}{8}\log 0.99 - \tfrac{1}{8}\log\log m + \tfrac{1}{4}\log 5,$$
$$\hat{h}(P) \geq \tfrac{1}{17}\log m.$$

As in the previous case, we obtain

$$n^2 \leq 17\ \tfrac{32}{25} \leq 22.$$

The points $2P$ and $4P$ are in $E_0(\mathbb{Q})$. By an explicit computation, it is easy to show that d^2 divides the denominator of the x-coordinate of $3P$. Hence $[0,1]$ is a generator. $\square$

Theorem 5.8. *The only integral points on E_m which are positive multiples of the point $[0,1]$ are:*

- $[0,1]$ *if m is even.*
- $[0,1]$ *and* $2[0,1]$ *if m is odd.*

Proof. If $m \leq 500$, the assertion of the theorem is satisfied (see Section 4). If $m \geq 500$ we use the previous approximations. We first prove three lemmas. We only consider positive multiples.

Lemma 5.9. *The odd multiples of the point $[0,1]$ are never integral, except of course for $[0,1]$ itself.*

Proof. Let $P = (2n+1)[0,1]$ be an integral point. Since $[0,1] \in E_{gg}(\mathbb{Q})$, $P \in E_{gg}(\mathbb{Q})$. We then have $|x_P| \leq m+1$ and, by (5–1) and (5–2),

$$\hat{h}(P) \leq \tfrac{32}{25}\log m + \tfrac{1}{2}\log(m+1),$$
$$\hat{h}(P) \leq \tfrac{45}{25}\log m,$$
$$\hat{h}([0,1]) \geq \tfrac{1}{16}\log m + \tfrac{1}{8}\log\left(0.99 + 1.91/\log m\right) + \frac{9.47}{32\log m} - \tfrac{1}{8}\log\log m + 0.02,$$
$$\hat{h}([0,1]) \geq \tfrac{1}{25}\log m.$$

Remark. $\hat{h}([0,1])$ is experimentally equal to

$$\tfrac{1}{4}\log m + C_2 + o(1),$$

where C_2 is as above with $d=1$. This should not be difficult to prove.

Finally, if $m \geq 500$, we have

$$(2n+1)^2 \leq 45.$$

To complete the proof, we have to look at the points $3[0,1]$ and $5[0,1]$. We have

$$x(3[0,1]) = -\frac{8m^3 + 40m^2 + 120m + 152}{m^4 + 4m^3 + 22m^2 + 36m + 81},$$

$|x(3[0,1])| < 1$ when $m \geq 8$, so $3[0,1]$ is not integral. The same reasoning with $m \geq 29$ implies that $5[0,1]$ is not integral. $\square$

Lemma 5.10. *The point $4[0,1]$ is never integral.*

Proof. We have the following expression for $x(4[0,1])$:

$$\frac{m^8+8m^7+60m^6+280m^5+1158m^4+3320m^3+7868m^2+11368m+12033}{(4m^3+20m^2+60m+76)^2}$$

If m is even, the numerator is odd whereas the denominator is even, so that $4[0,1]$ is not integral in this case.

If $m \equiv 1 \pmod 4$, we set $m = 4k+1$ and replace in $x(4[0,1])$; the same reasoning then implies that $4[0,1]$ is not integral.

If $m \equiv 3 \pmod 4$, we set $m = 4k+3$, expand, and eliminate common factors of 2, writing

$$x(4[0,1]) = \frac{p(k)}{q(k)^2}.$$

Then $p(k)$ and $q(k)$ are coprime for all values of k; in fact, we have $u(k)p(k)+v(k)q(k) = 1$ with $u(k) = 16k^2+8k-16$ and $v(k) = -128k^7 - 640k^6 - 1408k^5 - 1584k^4 - 648k^3 + 596k^2 + 908k + 401$. It follows that $4[0,1]$ is never integral as claimed. $\square$

Lemma 5.11. $P \notin E(\mathbb{Z}) \Longrightarrow 2P \notin E(\mathbb{Z})$.

Proof. Let $P = [a/d^2, b/d^3]$, with $(a,d) = (b,d) = 1$. Using the duplication formula we obtain

$$x_{2P} = \frac{a^4 - 2(m+3)a^2d^4 - 8ad^6 + (m^2+2m+9)d^8}{4b^2d^2}.$$

Since a and d are coprime, d^2 divides the denominator of x_{2P}. □

Remark. In general if P is not integral them $[m]P$ is not integral for any integer m. This follows from standard facts about the p-adic filtration of an elliptic curve over $\mathbb{Q}_p$ [Husemoller 1987].

We now complete the proof of the theorem. We have

$$x(2[0,1]) = \left(\frac{m+1}{2}\right)^2 + 2,$$

so the point $2[0,1]$ is integral if and only if m is odd.

Let $P = 2^p m[0,1]$ with m odd and $p \geq 0$. If $m = 1$, then either $p = 0$ (and $P = [0,1]$ is integral), or $p = 1$ (and $P = 2[0,1]$ is integral if and only if m is odd), or $p \geq 2$ and then P is not integral by Lemmas 5.10 and 5.11. If $m > 1$, $m[0,1]$ is not integral by Lemma 5.9, so P is not integral by Lemma 5.11. □

Corollary 5.12. *When the rank is* 1, *these theorems give us all integral points on the curve.*

REFERENCES

[Baker and Davenport 1969] A. Baker and H. Davenport, "The equations $3x^2-2=y^2$ and $8x^2-7=z^2$", *Quart. J. Math. Oxford Ser.* (2) **20** (1969), 129–137.

[Cohen 1993] H. Cohen, *A course in computational algebraic number theory*, Springer, Berlin, 1993.

[Cremona 1998] J. E. Cremona, "`mwrank`, a program for 2-descent on elliptic curves over $\mathbb{Q}$", last major update 1998. See http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs.

[David 1995] S. David, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. France (N.S.) **62**, Soc. math. France, Paris, 1995.

[Gebel et al. 1994] J. Gebel, A. Pethő, and H. G. Zimmer, "Computing integral points on elliptic curves", *Acta Arith.* **68**:2 (1994), 171–192.

[Husemoller 1987] D. Husemoller, *Elliptic curves*, Graduate Texts in Math. **111**, Springer, New York, 1987.

[Lang 1978] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der math. Wissenschaften **231**, Springer, Berlin, 1978.

[Niklasch and Smart 1998] G. Niklasch and N. P. Smart, "Exceptional units in a family of quartic number fields", *Math. Comp.* **67**:222 (1998), 759–772.

[Pethő 1991] A. Pethő, "Complete solutions to families of quartic Thue equations", *Math. Comp.* **57**:196 (1991), 777–798.

[Shanks 1974] D. Shanks, "The simplest cubic fields", *Math. Comp.* **28** (1974), 1137–1152.

[Shioda 1990] T. Shioda, "On the Mordell-Weil lattices", *Comment. Math. Univ. St. Paul.* **39**:2 (1990), 211–240.

[Silverman 1988] J. H. Silverman, "Computing heights on elliptic curves", *Math. Comp.* **51**:183 (1988), 339–358.

[Silverman 1990] J. H. Silverman, "The difference between the Weil height and the canonical height on elliptic curves", *Math. Comp.* **55**:192 (1990), 723–743.

[Smart 1994] N. P. Smart, "S-integral points on elliptic curves", *Math. Proc. Cambridge Philos. Soc.* **116**:3 (1994), 391–399.

[Smart 1998] N. P. Smart, *The algorithmic resolution of Diophantine equations*, London Math. Soc. student texts **41**, Cambridge University Press, Cambridge, 1998.

[Stroeker and Tzanakis 1994] R. J. Stroeker and N. Tzanakis, "Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms", *Acta Arith.* **67**:2 (1994), 177–196.

[Washington 1987] L. C. Washington, "Class numbers of the simplest cubic fields", *Math. Comp.* **48**:177 (1987), 371–384.

[Zagier 1987] D. Zagier, "Large integral points on elliptic curves", *Math. Comp.* **48**:177 (1987), 425–436. Addendum in **51** (1988), 375.

Sylvain Duquesne, Université Bordeaux I, Laboratoire A2X, 351 Cours de la Libération, 33405 Talence, France (duquesne@math.u-bordeaux.fr)

Received July 9, 1999; accepted in revised form April 3, 2000