Integral Points on Elliptic Curves Defined by Simplest Cubic Fields
Sylvain Duquesne

CONTENTS
Introduction
1. Elliptic Curves Defined by Simplest Cubic Fields
2. Linear Forms in Elliptic Logarithms
3. Computation of Integral Points
4. Tables of Results
5. General Results about Integral Points on the Elliptic Curves
y^2 = x^3 + mx^2 - (m+3)x + 1
References

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
\[ E_m : Y^2 = X^3 + mX^2 - (m+3)X + 1 \]
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.
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 $E_m(\mathbb{R})$ 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 $\text{Cl}$ be the ideal class group of the simplest cubic field $\mathbb{K}_m$ and set

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

The 2-rank $rk_2(\text{Cl}_2)$ will denote its dimension as a $\mathbb{Z}/2\mathbb{Z}$-vector space. Note that since $\mathbb{K}_m$ is a cyclic cubic field, $rk_2(\text{Cl}_2)$ is even. Finally, let $\text{III}_2$ denote the 2-torsion of the Tate–Shafarevitch group of $E_m(\mathbb{Q})$.

**Theorem 1.1** [Washington 1987]. The rank $rk E_m(\mathbb{Q})$ is at most $1 + rk_2(\text{Cl}_2)$. In fact, there is an exact sequence

$$1 \to E_m^0(\mathbb{Q})/2E_m(\mathbb{Q}) \to \text{Cl}_2 \to \text{III}_2 \to 1.$$ 

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 $\text{III}_2$ is small with respect to $\text{Cl}_2$, 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 $E_m(\mathbb{Q})_{\text{tor}}$ can be embedded in $E_m(\mathbb{F}_p)$ when $p$ is a prime of good reduction. \[\square\]

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

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

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

Let $\psi$ be the inverse function of $\varphi$. It is given (modulo $\Lambda$) by

$$\psi'(P) = \int_{\infty}^{x_{z} + b_2/12} \frac{dt}{\sqrt{4t^3 - g_2t - g_3}}.$$ 

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

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

\[
\hat{h}(P) = \frac{1}{2} \lim_{N \to \infty} 4^{-N} h(2^N P).
\]

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

\[-e_1 \leq \hat{h}(P) - \frac{1}{2} h(P) \leq e_2.\]

In our case, we can choose

\[e_2 = 1.57 + \frac{\log(m^2 + 3m + 9)}{4} + \frac{\log m}{2} \text{ if } m \geq 9.\]

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

\[Y^2 = 4X^3 - g_2X - g_3\]

with invariant \( j \) and periods \( \omega_1 \) and \( \omega_2 \) such that \( \omega_1 \in \mathbb{R} \) and \( \text{Im}(\omega_1/\omega_2) > 0 \). Let \( P_1, \ldots, P_n \) 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

\[d_1 = \frac{3\pi}{|\omega_1|^2 \text{Im}(\omega_1/\omega_2)};\]

the modified height

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

and constants \( d_2 = \max\{e h_E, h_m(P_i), \ldots, h_m(P_n)\},\)

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

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 \( L(x) \neq 0 \) and \( A \geq \exp(d_2) \), 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 \( P_1, P_2, \ldots, P_n \) 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 torsion-free, 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

\[Q_1 = 2P_1 \in E^0(\mathbb{R}),\]

\[q_1 \in \mathbb{Z} \text{ such that } p_1 = 2q_1 + r, \text{ for } r = 0 \text{ or } 1,\]

\[Q_i = P_i,\]

\[q_i = p_i \text{ for } i \neq 1,\]

\[Q_{n+1} = P_1,\]

so that

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

The points \( P, Q_1, \ldots, Q_n \) 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,

\[
\frac{1}{|x|} \leq c_1 e^{-c_2 H^2},
\]

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

\[
[\hat{h}(Q_1 + Q_2) - \hat{h}(Q_1) - \hat{h}(Q_2)]_{1 \leq i, j \leq n}.
\]

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

\[Y^2 = 4X^3 - g_2X - g_3 = g(X).\]
Let \( \gamma_1, \gamma_2, \gamma_3 \) 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
\[
|\psi(P)|^2 \leq \frac{c_5}{|x|}
\]
with \( c_5 = 8 + |\omega^2|/12 \).

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 \( |m| \leq nH + 1 \). 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
\[
|L(x)| \leq c_6 e^{-c_7 H^2}
\]
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 \( \Lambda \) generated by the columns of the matrix
\[
A = \begin{pmatrix}
1 & \cdots & 0 \\
0 & \ddots & \vdots \\
[\alpha_1] & \cdots & [\alpha_{n-1}] & [\alpha_n]
\end{pmatrix} \in \mathbb{M}_{n,n}(\mathbb{Z}).
\]

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, \( c_8 = \min \{ \| b_i^* \| : 1 \leq i \leq n \} \), \( S = \sum_{i=1}^{n} X_i^2 \) and \( T = \frac{1}{2} \sum_{i=1}^{n} X_i \). If \( c_8^2 \geq T^2 + S \) and \( x = (x_1, \ldots, x_n) \neq 0 \) then
\[
H \leq \sqrt{\left( \log(Cc_8) - \log \left( \sqrt{c_8^2 - S - T} \right) \right) / c_7}.
\]

**Remark.** If the bound for \( H \) exists, it is of the form \( O(\sqrt{\log H_0}) \). 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 \( O(\log H_0) \). 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 \( m \leq 1000 \) such that \( m^3 + 3m + 9 \) is square-free, we found the rank \( \operatorname{rk} E_m(\mathbb{Q}) \). Where possible, the basis of the Mordell–Weil group was computed using \texttt{mrank} [Cremona 1998]. In some cases, distinguished in the tables by an underlined value of the parameter \( m \), \texttt{mrank} 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 other integral point 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 always be a generator. (This last remark is valid only if the parameter \( m \) defines a simplest cubic field, as we have assumed;
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 [Pethö 1991; Niklass and Smar 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, 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 $p$.

<table>
<thead>
<tr>
<th>$m$</th>
<th>$x$-coordinate of integral points when the rank is 5, as determined by mwrank</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>-124, -124, -105, -81, -64, -33, -28, -4, -1, 0, 2, 6, 30, 90, 114, 182, 290, 846, 854, 4182, 5186, 17342, 414290</td>
</tr>
<tr>
<td>347</td>
<td>-345, -292, -225, -84, -64, -12, -4, 0, 6, 26, 98, 1190, 5070, 14930, 30278</td>
</tr>
<tr>
<td>419</td>
<td>-420, 280, -225, -196, -64, -33, -1, 0, 2, 6, 14, 366, 482, 594, 44102</td>
</tr>
<tr>
<td>430</td>
<td>-408, -276, -105, -9, 0, 42, 54, 222, 270, 966, 300990, 48402</td>
</tr>
<tr>
<td>473</td>
<td>-456, -364, -240, -60, -16, -4, 0, 27, 51, 107, 899, 2315, 56171</td>
</tr>
<tr>
<td>611</td>
<td>-612, -537, -324, -289, -280, -184, -9, -1, 0, 2, 74, 266, 546, 686, 1650, 8502, 93638, 1313274</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>16</td>
<td>18</td>
</tr>
<tr>
<td>23</td>
<td>25</td>
</tr>
<tr>
<td>26</td>
<td>28</td>
</tr>
<tr>
<td>39</td>
<td>41</td>
</tr>
</tbody>
</table>

TABLE 3. Parameter $m$ and $x$-coordinate of integral points when the rank is 3 (as determined by $m_{\text{rank}}$ 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 \( p \equiv 1 \) (mod 4).

Assume now that \( a \) is even, so that \( b \) is odd. Then, when \( a \equiv 2 \) (mod 4), \( b \) is always a square modulo 2. When \( a \equiv 4 \) (mod 8), we have \( x^2 - x \equiv 0 \) (mod 4) so either \( x \) is even, hence \( b \equiv 1 \) (mod 4), so \( b \) is a square modulo 4. Or \( x \) is odd, hence \( x \equiv 3 \) (mod 4), so \( x^2 - x \equiv 2 \) (mod 4) which is a contradiction. When \( a \equiv 0 \) (mod 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 \( b \equiv 1 \) (mod 8). Thus, when \( x \equiv 0 \) (mod 4) then \( b \equiv 1 \) (mod 8), so \( b \) is a square modulo \( 2^n \). The case \( x \equiv 1 \) (mod 4) is not possible by hypothesis. Finally, if \( x \equiv 2 \) or 3 (mod 4), then \( a \equiv x^2 - x \equiv 2 \) (mod 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 \( x \equiv 2 \) (mod 4) or \( x \equiv 3 \) (mod 8), while if \( x < 1 \) we have \( x \equiv 0 \) (mod 4) or \( x \equiv 7 \) (mod 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
\[
x - 1 = 2 \prod_{p \mid x-1 \atop p \neq 2} p \equiv 2 \pmod{8}.
\]
The proof is similar when \( x < 1 \). \( \square \)

**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. \( \square \)

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. \( y \equiv \pm 1 \pmod{p^\nu(x)} \) for every odd prime \( p \) dividing \( x \);
2. \( y \equiv \pm \sqrt{\mathbb{Q}} \pmod{p^\nu(x)} \) for every odd prime \( p \) dividing \( x-1 \);
3. \( y \) is odd;
4. if \( x < 1 \) and \( x \equiv 0 \pmod{8} \), then
\[
y \equiv \pm 1 \pmod{2^{\nu(x)-1}}.
\]

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:
\[
x = u + 1,
\]
\[
y = tu + t - u,
\]
\[
m = t^2 - 2t - u - 1 + \frac{t^2 + 1}{u}.
\]

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

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

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 $\omega_1$ and $\omega_2$**

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

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

with

$$f(x) = x^3 - (\frac{3}{4}m^2 + m + 3)x + \frac{2}{27}m^3 + \frac{1}{3}m^2 + m + 1.$$ 

Let $e_1 \leq e_2 \leq e_3$ be the real roots of $f$ (the discriminant is always positive). The periods $\omega_1$ and $\omega_2$ 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:

$$-\frac{2m}{3} - 1 - \frac{m}{2} \leq e_1 \leq -\frac{2m}{3} - 1 - \frac{1}{m} \quad \text{if} \quad m \geq 2,$$

$$m \leq e_2 \leq \frac{m}{3} + \frac{1}{m}.$$ 

We start with an approximation for $\omega_2$ 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 $m + 1 + 1/m \leq x - e_1 \leq m + 2 + 3/m$, so

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

and

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

Finally, we have

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

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

We now consider the case of $\omega_1$.

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 $\omega_1^-$, the roots $e_2$ and $e_3$ are far from the endpoints of the domain of integration. We thus have, for $x \in [e_1, 0]$:

$$m/3 \leq e_2 - x \leq m + 1 + 3/m,$$

$$m/3 + 1 \leq e_3 - x \leq m + 2 + 3/m.$$
So
\[
\omega_1^+ \geq \frac{1}{\sqrt{(m+1+3/m)(m+2+3/m)}} \int_{\epsilon_1}^{0} \frac{dx}{\sqrt{x - e_1}},
\]
\[
\omega_1^- \leq \frac{1}{\sqrt{(m/3)(m+3+1)}} \int_{\epsilon_1}^{0} \frac{dx}{\sqrt{x - e_1}},
\]
\[
\omega_1^+ \geq \frac{2\sqrt{-e_1}}{\sqrt{(m+1+3/m)(m+2+3/m)}},
\]
\[
\omega_1^- \leq \frac{2\sqrt{-e_1}}{\sqrt{(m/3)(m+3+1)}},
\]
\[
\omega_1^+ \geq \frac{2\sqrt{2m/3+1+1/m}}{\sqrt{(m+1+3/m)(m+2+3/m)}},
\]
\[
\omega_1^- \leq \frac{2\sqrt{2m/3+1+2/m}}{\sqrt{(m/3)(m+3+1)}}.
\]

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 \(\omega_1^+\). 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
\[
\frac{I}{m+1+3/m} \leq \omega_1^+ \leq \frac{I}{2m/3+1+1/m}
\]
with
\[
I = \int_{\epsilon_2}^{e_2} \frac{dx}{\sqrt{(x - e_2)(x - e_3)}} = \log \frac{\sqrt{e_2} + \sqrt{e_2}}{\sqrt{e_3} - \sqrt{e_2}}
\]
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
\[
\omega_1^+ \geq \frac{1}{\sqrt{m+1+3/m}} \log \frac{4m}{3(1+1/m)},
\]
\[
\omega_1^+ \leq \frac{1}{\sqrt{2m/3+1+1/m}} \log \frac{4(m+3+3/m)}{3(1-1/m)},
\]
\[
\omega_1^+ \geq \frac{\log m}{\sqrt{m+1+3/m}} + \frac{\log m}{\sqrt{m+1+3/m}},
\]
\[
\omega_1^+ \leq \frac{\log m}{\sqrt{2m/3+1+1/m}} + \frac{\log (m+3+3/m)}{\sqrt{2m/3+1+1/m}}.
\]

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,
\[
\hat{h}(P) - \frac{1}{2}\hat{h}(P) \leq 1.57 + \frac{1}{4} \log (m^2+3m+9) + \frac{1}{2} \log m.
\]

Since \(P\) is integral, \(\hat{h}(P) = \log \max\{1, |x_P|\}\). So
\[
\hat{h}(P) \leq \frac{2m}{25} \log m + \frac{1}{4} \log \max\{1, |x_P|\} \quad \text{if} \quad m \geq 500.
\]

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 \(P = [\alpha/\delta^2, \beta/\delta^3] \in E_m(\mathbb{Q})\) with \((\alpha, d) = (\beta, d) = 1\). We first compute the non-Archimedean contributions. We use the algorithm described in [Silverman 1988; Cohen 1993, Section 7.5.2]. We have \(\beta^2 = \alpha^3 + m\delta^2 \alpha - (m+3)\delta \alpha + 1\). 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
\[
\Delta = m^2+3m+9;
\]
\[
A = 3\alpha^2 + 2m\delta^2 \alpha - (m+3)\delta^4 \quad \text{(the numerator of} \quad 3\alpha^2/\delta^4 + 2m\alpha/\delta^2 - (m+3));
\]
\[
B = 2\beta \quad \text{(the numerator of} \quad 2\beta/\delta^4);\]
\[
C = 3\alpha^4 + 4m\delta^2 \alpha - (6m+18)\alpha^2 \delta^2 + 12\alpha d^3 - \Delta \delta^4 \quad \text{(the numerator of} \quad 3\alpha^4/\delta^4 + 4m\alpha^3 \delta^2 - (6m+18) \times \alpha^2/\delta^4 + 12\alpha/\delta^2 - \Delta);\]
\[
D = \gcd(A, B).
\]

We prove that the only prime giving any local contribution is 2. Let \(p\) be an odd prime dividing \(D\). Because
\[
4A^2 = (9\alpha^2+3\delta^2m)B^2 + 4\Delta \delta^4 \alpha^2 \delta d - d^4 \alpha \delta,
\]
p divides \(4\Delta \delta^4 \alpha^2 \delta d + d^4 \alpha \delta^2\). On the other hand \(p\) does not divide \(d\) (because \(p\) divides \(\beta\)) and \(\Delta\)
is squarefree, so $p$ divides $(\alpha^2 - d^2 \alpha + d^2)$. Next, because

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

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

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

$p^2$ divides $d^2 (2m+3) \Delta$, so $p$ divides $2m+3$. And since $4\Delta = (2m+3)^2 + 27$, we conclude that $p = 3$; but then $3$ divides $m$ and $\Delta$ 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 $m \equiv 1 \pmod{4}$, $C_2 = \log d - \frac{1}{4}\log 2$.
- If $m \equiv 3 \pmod{4}$, $C_2 = \log d - \frac{3}{4}\log 2$.

In all cases, $C_2 \geq \log d - \frac{1}{2}\log 2$.

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

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

Then the Archimedean contribution is

$$C_\infty = \frac{1}{\sqrt{2}} \log \left| \frac{16\Delta^2}{q} - \frac{1}{4} \log |\theta| \right| + \frac{1}{8} \log \left( \frac{\alpha \alpha^3 + \alpha + d^2 - (3\alpha + d^2 m + 1)}{\lambda} \right).$$

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 $C_\infty$, we need an upper bound for $q$. Using approximations to the periods, we deduce

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

if $m \geq 500$, so

$$q \leq \exp \left( -\frac{9.47}{\log m} \right) \leq 1 - \frac{4.86}{\log m},$$

if $m \geq 500$.

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

$$\frac{1}{\sqrt{2}} \log \left| \frac{16\Delta^2}{q} \right| \geq \frac{1}{8} \log m + \frac{1}{8} \log 2,$$

$$\frac{1}{\sqrt{2}} \log \left| 1/q \right| \geq \frac{1}{8} \log \exp \frac{9.47}{\log m} \geq \frac{9.47}{32 \log m},$$

$$-\frac{1}{4} \log |\theta| \geq -\frac{1}{4} \log \frac{1}{1-q} \geq -\frac{1}{4} \log \frac{\log m}{4.86} \geq \frac{1}{4} \log 4.86 - \frac{1}{6} \log m.$$

As for $-\frac{1}{8} \log \lambda = \frac{1}{8} \log (\omega_1/2\pi)$, it is greater than or equal to

$$-\frac{1}{8} \log (2\pi) + \frac{1}{8} \log \frac{1.91 + 0.99 \log m}{\sqrt{m}} \geq \frac{1}{8} \log \frac{1}{\sqrt{m}} - \frac{1}{8} \log (2\pi) + \frac{1}{8} \log (1.91 + 0.99 \log m) \geq -\frac{1}{10} \log m - \frac{1}{8} \log (2\pi) + \frac{1}{8} \log \left( \frac{0.99 + 1.91}{\log m} \right) + \frac{1}{8} \log \log m,$$

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 $C_\infty$:

$$\frac{1}{16} \log m + \frac{9.47}{32 \log m} + \frac{1}{4} \log (\beta/d^3)$$

$$+ \frac{1}{8} \log (0.99 + 1.91/\log m) - \frac{1}{8} \log \log m + 0.252.$$

Adding the non-Archimedean contribution, we obtain

$$\tilde{h}(P) \geq \frac{1}{16} \log m + \frac{9.47}{32 \log m} + \frac{1}{4} \log (\beta/d^3)$$

$$+ \frac{1}{8} \log (0.99 + 1.91/\log m)$$

$$- \frac{1}{8} \log \log m + \log d - \frac{1}{8} \log 2 + 0.252.$$  

Hence, we obtain a lower bound for $\tilde{h}(P)$:

$$\tilde{h}(P) \geq \frac{1}{16} \log m + \frac{9.47}{32 \log m} + \frac{1}{4} \log (\beta d)$$

$$+ \frac{1}{8} \log (0.99 + 1.91/\log m) - \frac{1}{8} \log \log m + 0.02. \ (5.2)$$

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 $E_0(Q)$ is still in $E_0(Q)$, $P$ belongs to $E_{gg}(Q)$. 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)

\[
\hat{h}(P) \geq \frac{1}{10} \log m + \frac{1}{4} \log \sqrt{2m + 3} + \frac{1}{8} \log 0.99 - \frac{1}{8} \log \log m + 0.02,
\]

\[
\hat{h}(P) \geq \frac{3}{10} \log m - \frac{1}{8} \log \log m + 0.1,
\]

\[
\hat{h}(P) \geq \frac{1}{9} \log m.
\]

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

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

Moreover $2P \in E_0(Q)$ 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)

\[
\hat{h}(P) \geq \frac{1}{10} \log m + \frac{1}{4} \log 0.99 - \frac{1}{8} \log \log m + \frac{1}{4} \log 5,
\]

\[
\hat{h}(P) \geq \frac{1}{17} \log m.
\]

As in the previous case, we obtain

\[
n^2 \leq 17 \frac{32}{25} \leq 22.
\]

The points $2P$ and $4P$ are in $E_0(Q)$. 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. \qed

**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 $[0, 1] \in E_{gg}(Q)$, $P \in E_{gg}(Q)$. We then have $|x_P| \leq m + 1$ and, by (5–1) and (5–2),

\[
\hat{h}(P) \leq \frac{32}{25} \log m + \frac{1}{2} \log (m + 1),
\]

\[
\hat{h}(P) \leq \frac{42}{25} \log m,
\]

\[
\hat{h}([0, 1]) \geq \frac{1}{10} \log m + \frac{1}{8} \log (0.99 + 1.91/\log m)
\]

\[
+ \frac{9.47}{32 \log m} - \frac{1}{8} \log \log m + 0.02,
\]

\[
\hat{h}([0, 1]) \geq \frac{1}{25} \log m.
\]

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

\[
\frac{1}{4} \log m + C_2 + o(1),
\]

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

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

\[
|x(3[0, 1])| < 1 \text{ when } m \geq 8, \text{ so } 3[0, 1] \text{ is not integral.}
\]

The same reasoning with $m \geq 29$ implies that $5[0, 1]$ is not integral. \qed

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

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

\[
\frac{m^n + 8m^5 + 46m^4 + 280m^3 + 1156m^2 + 3320m + 17868m + 11368}{m^n + 2m^3 + 460m^2 + 460m + 4760}.
\]

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

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

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 $v(k) = -128k^2 - 640k^6 - 1408k^5 - 1584k^4 - 648k^3 + 596k^2 + 908k + 401$. It follows that $4[0, 1]$ is never integral as claimed. \qed
Lemma 5.11. $P \not\in E(\mathbb{Z}) \implies 2P \not\in E(\mathbb{Z})$.

Proof. Let $P = [a/d^2, b/d^4]$, 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, $d^8$ divides the denominator of $x_{2P}$. □

Remark. In general if $P$ is not integral then $|m|P$ 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 $P = 2m[0,1]$ 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


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