On Sums of Consecutive Squares

A. Bremner* R.J. Stroeker† N. Tzanakis‡

Abstract

In this paper we consider the problem of characterizing those perfect squares that can be expressed as the sum of consecutive squares where the initial term in this sum is k^2. This problem is intimately related to that of finding all integral points on elliptic curves belonging to a certain family which can be represented by a Weierstraß equation with parameter k. All curves in this family have positive rank, and for those of rank 1 a most likely candidate generator of infinite order can be explicitly given in terms of k. We conjecture that this point indeed generates the free part of the Mordell-Weil group, and give some heuristics to back this up. We also show that a point which is modulo torsion equal to a nontrivial multiple of this conjectured generator cannot be integral.

For k in the range $1 \leq k \leq 100$ the corresponding curves are closely examined, all integral points are determined and all solutions to the original problem are listed. It is worth mentioning that all curves of equal rank in this family can be treated more or less uniformly in terms of the parameter k. The reason for this lies in the fact that in Sinnou David's lower bound of linear forms in elliptic logarithms—which is an essential ingredient of our approach—the rank is the dominant factor. Also the extra computational effort that is needed for some values of k in order to determine the rank unconditionally and construct a set of generators for the Mordell-Weil group deserves special attention, as there are some unusual features.

1991 *Mathematics subject classification:* 11D25, 11G05

Key words and phrases: diophantine equation, elliptic curve, elliptic logarithm

*Department of Mathematics, Arizona State University, Tempe, AZ 85287-1804, USA, e-mail: abremner@math.la.asu.edu

†Econometric Institute, Erasmus University, P.O.Box 1738, 3000 DR Rotterdam, The Netherlands, e-mail: stroeker@wis.few.eur.nl

‡Department of Mathematics, University of Crete, Iraklion, Greece, e-mail: tzanakis@talos.cc.uch.gr

Contents

1 Preliminaries

1.1 Introduction

Everyone is familiar with the Pythagorean identity

$$3^2 + 4^2 = 5^2$$

and many with the identity resulting from Lucas' "Square Pyramid" problem,

$$1^2 + 2^2 + \cdots + 24^2 = 70^2.$$

The problem of determining those squares equal to the sum of consecutive squares has attracted considerable interest throughout the years: the reader is referred to Guy [5, Problem D3] for a comprehensive list of both historical and contemporary references.

We are interested in integer solutions of

$$k^2 + (k+1)^2 + \cdots + (k+n-1)^2 = t^2, \tag{1}$$

which equation may be written in the form of an elliptic curve

$$E_k : \frac{1}{3}n^3 + \left(k - \frac{1}{2}\right)n^2 + \left(k^2 - k + \frac{1}{6}\right)n = t^2. \tag{2}$$

Most authors to date have considered n as fixed and asked for corresponding pairs of integers k, t if any. It is known that there exist solutions for infinitely many n, and in particular all such $n < 1000$ have been determined. The analysis in this instance depends upon an associated Pellian equation.

Alternatively, one can consider k as fixed and ask for corresponding integer pairs n, t (when $k = 1$ this is the Lucas problem mentioned above). The analysis now depends upon the theory of elliptic curves; a few explorations have been made in this direction (Platiel & Rung [8], Rung [9]; see also Kuwata & Top [7]). The present paper offers a systematic investigation of this approach, and all integer solutions n, t of (2) are found in the range $1 \leq k \leq 100$.

Stroeker & Tzanakis [14] and Gebel, Pethö & Zimmer [4] have studied specific elliptic curves over $\mathbb{Q}$, showing that when the rational Mordell-Weil group of the curve is known, then finding all integer points can be reduced to a practicably efficient process. Both papers employ similar methods, not following the traditional well established path of solving Thue equations, but instead relying on a highly nontrivial lower bound for linear forms in elliptic logarithms recently obtained by Sinnou David [3]. Where the calculations in [4] leading to the computation of the Mordell-Weil group are based on the assumption of the Birch and Swinnerton-Dyer conjectures, the results of [14] are unconditional. This is also one of the objectives of the present paper, and our results for k in the range $1 \leq k \leq 100$ do not depend on any of the usual conjectures. However, in practice, this often means that an extensive amount of computational effort is required.

In [13] Stroeker takes the elliptic logarithm method one step further and examines the parametrized family of elliptic curves that arises from demanding that the sum of consecutive *cubes* be a square. He is able systematically to treat the first 50 curves of the family, showing that certain aspects of the computations can be successfully carried through uniformly in terms of the parameter. The current paper is modelled on this latter, though with some extra features. First, to determine the Mordell-Weil rank unconditionally in eleven cases required an extra argument; in particular for $k = 68$, it was found necessary to invoke the arithmetic of a number field with class-group of order 16128. A detailed discussion is devoted to this exceptional case, because it is rather surprising that the nontrivial structure of this class-group ultimately clinches the argument. Some of the curves in our range have generators of large height, and an extra descent was necessary in order to compute the corresponding Mordell-Weil groups. Second, the curve (2) possesses an 'obvious' integer solution for each k, namely $(n, t) = (1, k)$. It turns out that the point Q_k on the corresponding elliptic curve has infinite order, and one might reasonably ask two associated questions in the case that the curve has rank 1:

(i) Is Q_k always a generator, and

(ii) Can any multiple of Q_k modulo torsion give rise (on specialization) to a nontrivial integer solution of equation (2)?

In the range $1 \leq k \leq 100$, question (i) can be answered in the affirmative, and we offer some suggestions as to the reason why the answer should be yes for all sufficiently large

k. We answer question (ii) in the negative by means of a p-adic approach ($p = 2, 3$), involving straightforward but intricate double induction arguments.

1.2 The family of curves

Under the substitution

$$(x, y) = (12n + 12k - 6, 72t) \tag{3}$$

with inverse

$$(n, t) = \left(\frac{1}{12}(x + 6) - k, \frac{1}{72}y\right)$$

the curve E_k at (2) transforms into the following Weierstraß form

$$E_k : y^2 = x^3 - 36x - 864k(k - 1)(2k - 1). \tag{4}$$

We shall denote by $E_k(\mathbb{Q})$ the rational Mordell-Weil group of this curve. There is a rational point T_k on E_k of order 2, namely

$$T_k = (6(2k - 1), 0), \tag{5}$$

and with the substitution

$$(X, Y) = (x - 6(2k - 1), y) \tag{6}$$

(4) transforms to

$$Y^2 = X(X^2 + 18(2k - 1)X + 72(6k^2 - 6k + 1)) \tag{7}$$

with T_k transforming to $(0, 0)$. For $P \in E_k(\mathbb{Q})$, the coordinates $(x(P), y(P))$ will always be relative to (4), and the coordinates $(X(P), Y(P))$ will always be relative to (7).

The discriminant Δ_k of E_k is given by

$$\Delta_k = -2^{12}3^6(12k^2 - 12k - 1)(6k^2 - 6k + 1)^2$$

and the j-invariant j_k by

$$j_k = -2^6 3^3/(12k^2 - 12k - 1)(6k^2 - 6k + 1)^2.$$

Some simple facts are easy to establish.

Lemma 1. (i) $E_1(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *and* $E_k(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$ *for* $k \geq 2$,
(ii) *The rank* r_k *of* $E_k(\mathbb{Q})$ *satisfies* $r_k \geq 1$ *for* $k \geq 1$.

Proof. (i) For $k = 1$, the torsion statement follows from Silverman [10, p. 311]. For $k \geq 2$, we use the well-known fact (Silverman [10, p. 176]) that if a prime p does not divide the discriminant Δ_k of E_k, then $E_k(\mathbb{Q})_{\text{tors}}$ injects in $E_{k,p}(\mathbb{F}_p)$ where $E_{k,p}$ is the reduction mod p of E_k. With $p = 5$, we have

$$E_{k,5}(\mathbb{F}_5) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{for } k \equiv 0, 1, 3 \bmod 5, \\ \mathbb{Z}/8\mathbb{Z} & \text{for } k \equiv 2, 4 \bmod 5. \end{cases}$$

Thus $|E_k(\mathbb{Q})_{\text{tors}}|$ divides 8. Certainly $E_k(\mathbb{Q})$ has precisely the one point T_k of order 2, since $6(2k-1)$ is the only real zero of the right-hand side of (4). Furthermore, $E_k(\mathbb{Q})$ possesses no point of order 4, for such a point $P(x, y)$ satisfies $2P = (6(2k-1), 0)$, implying

$$6(2k-1) = \frac{(x^2+36)^2 + 6912k(k-1)(2k-1)x}{4y^2}.$$

But this forces x to be exactly divisible by 2, and hence $6(2k-1)$ should be exactly divisible by an even power of 2, which is clearly absurd. This shows (i), with the immediate consequence that the point $Q_k = (12k+6, 72k)$ on (4), corresponding to $(n, t) = (1, k)$ on (2), cannot be of finite order, which shows $r_k \geq 1$. $\square$

Our goal is to determine all integer solutions of (2) in the range $1 \leq k \leq 100$. We shall actually do more and determine all integer solutions of (4) in the range $1 \leq k \leq 100$; integer solutions of (2) correspond via the transformation (3) and its inverse to a subset of integer solutions of (4). The attack falls into two distinct parts: determination of the Mordell-Weil groups and subsequent determination of the integer points.

2 The Mordell-Weil groups

In this part the Mordell-Weil groups for k in the range $1 \leq k \leq 100$ will be computed completely and unconditionally. As the torsion subgroups have been determined in the previous part, that leaves the rank and the generators of infinite order.

2.1 Rank calculations

The first step is to compute the rank of each curve in the family. Connell's Apecs program was able to determine rank unconditionally in the range $1 \leq k \leq 100$ except in the 11 cases $k = 29, 40, 49, 51, 53, 57, 68, 77, 84, 93, 99$. To fill in these gaps we used the following descent arguments.

At a rational point of (7), put $X = \Delta A^2/B^2$, Δ squarefree, $A, B \in \mathbb{Z}$, $(A,B) = 1$. There results a quartic of type

$$c_0A^4 + c_1A^2B^2 + c_2B^4 = C^2 \tag{8}$$

on which we seek points. John Cremona's algorithm "mwrank" (see [2]) will quickly sieve out all quartics (8) locally unsolvable for some prime p (including ∞). Therefore we can safely assume that (8) is everywhere locally solvable. Then the associated quadric

$$c_0\mathcal{X}^2 + c_1\mathcal{X}\mathcal{Y} + c_2\mathcal{Y}^2 = \mathcal{Z}^2 \tag{9}$$

is everywhere locally solvable, and hence globally solvable. Let (α, β, γ) be a point of (9); then (9) may be rationally parametrized as follows:

$$\begin{aligned}&\mathcal{X} : \mathcal{Y} : \mathcal{Z} = \\ &\quad \alpha W^2 - 2\gamma WV + (\alpha c_0 + \beta c_1)V^2 : \beta(W^2 - c_0V^2) : \gamma W^2 - (2c_0\alpha + c_1\beta)WV + c_0\gamma V^2.\end{aligned}$$

It follows from (8) that

$$\begin{aligned} hA^2 &= \alpha W^2 - 2\gamma WV + (\alpha c_0 + \beta c_1)V^2 \\ hB^2 &= \beta(W^2 - c_0V^2), \end{aligned} \tag{10}$$

where the squarefree part of h is a divisor of the resultant of the two quadratics in W, V, namely, $\beta^4(c_1^2 - 4c_0c_2)$. That is, the squarefree part of h divides $\beta(c_1^2 - 4c_0c_2)$. The possibilities for h can be tested in (10), discarding those for which the pair of quadrics is not everywhere locally solvable. For a remaining value of h, the second quadric at (10) being locally solvable implies it is globally solvable, and so rationally parametrizable. Substituting into the first quadric at (10) results in a homogeneous quartic in two variables being a square. In ten of the eleven exceptional cases listed above, all the resulting quartics turn out to be locally unsolvable. The rather tedious but straightforward details of these cases are omitted; verification should not pose any serious problems. However, for $k = 68$ everywhere locally solvable quartics remain, so that we are still uncertain about the expected non-existence of global solutions. We had to do some rethinking at this point, and the proof we found in the end to show that these quartics can possess no global solution is interesting enough in itself to justify a detailed description. Moreover, it clearly shows the power that sophisticated software like PARI/GP puts at one's fingertips.

After this the rank will have been determined unconditionally for all k in the range $1 \leq k \leq 100$. The rank values are listed in Table 1; here we just indicate their distribution, namely 31 cases of rank 1, 52 cases of rank 2, 14 cases of rank 3, and 3 cases of rank 4.

2.2 The exceptional case $k = 68$

Details are provided here that show the rank r_{68} of (4) for $k = 68$

$$E_{68} : y^2 = x(x^2 + 2430x + 1968264) \tag{11}$$

is unconditionally equal to 2. We refer to [2, Chapter III, 3.6] and [10, Chapter III] for background and notational conventions. For the computation of the rank we also need the isogenous curve

$$E'_{68} : y^2 = x(x^2 - 4860x - 1968156) \tag{12}$$

and the standard 2-isogenies $\phi : E_{68} \to E'_{68}$ and $\hat{\phi} : E'_{68} \to E_{68}$. It is well-known that

$$|E_{68}(\mathbb{Q})/\hat{\phi}(E'_{68}(\mathbb{Q}))| \cdot |E'_{68}(\mathbb{Q})/\phi(E_{68}(\mathbb{Q}))| = 2^{r+2},$$

and we will show that

$$|E_{68}(\mathbb{Q})/\hat{\phi}(E'_{68}(\mathbb{Q}))| = |E'_{68}(\mathbb{Q})/\phi(E_{68}(\mathbb{Q}))| = 2^2.$$

Putting $x = \delta a^2/b^2$, $\delta, a, b \in \mathbb{Z}$, δ squarefree, $(\delta, b) = 1$, $(a, b) = 1$ in (11) gives

$$\delta a^4 + 2430a^2b^2 + \frac{1968264}{\delta}b^4 = c^2, \qquad \delta \mid 2 \cdot 3 \cdot 27337. \tag{13}$$

Moreover, the group $E_{68}(\mathbb{Q})/\hat{\phi}(E'_{68}(\mathbb{Q}))$ is isomorphic to the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by the factors δ for which the diophantine equation (13) has an integer solution. Cremona's "mrank" tells us that global solutions exist at $\delta = 1,\ 3,\ 2 \cdot 27337,\ 6 \cdot 27337$, and the remaining four values of δ, $\delta = 2,\ 6,\ 27337,\ 3 \cdot 27337$ give everywhere locally solvable curves, but the existence of a global solution for these values remains undecided. However it is easy to see that $|E_{68}(\mathbb{Q})/\hat{\phi}(E'_{68}(\mathbb{Q}))| = 2^2$ or 2^3, depending, respectively, on the existence or non-existence of a solution for $\delta = 2$.

When $\delta = 2$,

$$2a^4 + 2430a^2b^2 + 984132b^4 = c^2$$

with parametrization

$$a^2 : b^2 : c = -639u^2 - 996uv + 1152v^2 : u^2 - 2v^2 : 498u^2 + 126uv + 996v^2$$

so that for coprime integers U, V, there exist integers h, α_0, β satisfying

$$\begin{aligned} -639U^2 - 996UV + 1152V^2 &= h\alpha_0^2 \\ U^2 - 2V^2 &= h\beta^2, \end{aligned} \tag{14}$$

where h is a squarefree divisor of the resultant of the two polynomials in the left-hand side; so $h \mid 2\cdot 3\cdot 23\cdot 2377$. However, $3|h$ implies $U^2 \equiv 2V^2 \bmod 3$, which is impossible. Thus $h \mid 2\cdot 23\cdot 2377$. From (14), $3|h\alpha_0^2$, so $\alpha_0 = 3\alpha$, and

$$-213U^2 - 332UV + 384V^2 = 3h\alpha^2 \qquad (15)$$

$$U^2 - 2V^2 = h\beta^2. \qquad (16)$$

The quadrics (15) and (16) are locally solvable for precisely the following eight values of h:

$$h = 1,\ -2,\ -23,\ 46,\ 2377,\ -2\cdot 2377,\ -23\cdot 2377,\ 46\cdot 2377. \qquad (17)$$

Write (15), (16) in the form

$$(-213+t)U^2 - 332UV + (384-2t)V^2 = h(3\alpha^2 + t\beta^2) \qquad (18)$$

where t is chosen so that the left-hand side is a *singular* quadratic; this demands $t = 202+\theta$, where $\theta^2 - \theta + 13668 = 0$, and (18) may then be written

$$-2(83U + (10+\theta)V)^2 = h(10+\theta)(3\alpha^2 + (202+\theta)\beta^2)$$

or, equivalently,

$$9\alpha^2 + (606+3\theta)\beta^2 = -6(83U + (10+\theta)V)^2/(h(10+\theta)).$$

Define the number field $\mathbb{K} = \mathbb{Q}(\varphi)$ where $\varphi^2 = -606-3\theta$, so that $\varphi^4 + 1215\varphi^2 + 492066 = 0$. Further, let $\mathbb{L} = \mathbb{Q}(\theta)$. Then

$$\mathrm{Norm}_{\mathbb{K}/\mathbb{L}}(3\alpha + \beta\varphi) = -6(83U + (10+\theta)V)^2/h(10+\theta). \qquad (19)$$

The following arithmetic information about $\mathbb{K}, \mathbb{L}$ was obtained by use of PARI/GP. In $\mathbb{L}$ there are the prime factorizations $(2) = \mathfrak{p}_2\mathfrak{p}_2'$, $(3) = \mathfrak{p}_3\mathfrak{p}_3'$, $(83) = \mathfrak{p}_{83}\mathfrak{p}_{83}'$, $(23) = \mathfrak{p}_{23}^2$, $(2377) = \mathfrak{p}_{2377}^2$, $(10+\theta) = \mathfrak{p}_2'\mathfrak{p}_{83}'^2$. A $\mathbb{Z}$-basis for the ring of integers $\mathfrak{O}_{\mathbb{L}}$ is $\{1, \theta\}$; and the following congruences hold:

mod	$\mathfrak{p}_2$	$\mathfrak{p}_2'$	$\mathfrak{p}_3$	$\mathfrak{p}_3'$	$\mathfrak{p}_{83}$	$\mathfrak{p}_{83}'$
θ	1	0	1	0	11	-10

In $\mathbb{K}$, $\mathfrak{p}_2 = \mathfrak{q}_2^2$, $\mathfrak{p}_2' = \mathfrak{q}_2'^2$, $\mathfrak{p}_3 = \mathfrak{q}_3^2$, $\mathfrak{p}_3' = \mathfrak{q}_3'^2$, $(\varphi) = \mathfrak{q}_2'\mathfrak{q}_3\mathfrak{q}_3'\mathfrak{q}_{27337}$, $(1+\varphi) = \mathfrak{q}_2\mathfrak{q}_{246641}$; a $\mathbb{Z}$-basis for the ring of integers $\mathfrak{O}_{\mathbb{K}}$ is $\{1, \varphi, \frac{1}{3}\varphi^2, \frac{1}{3}\varphi^3\}$; and the class-group is of order 16128 and of type $\mathbb{Z}_{504}\times\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$.

The following congruences hold:

mod	$\mathfrak{q}_2$	$\mathfrak{q}_2'$	$\mathfrak{q}_3$	$\mathfrak{q}_3'$
φ	1	0	0	0
$\frac{1}{3}\varphi^2$	1	0	1	2
$\frac{1}{3}\varphi^3$	1	0	0	0

Now at (19), the greatest ideal common factor of $(3\alpha+\beta\varphi)$ and $(3\alpha-\beta\varphi)$ divides $(6\alpha, 2\beta\varphi, 3\alpha+\beta\varphi)$. Since $\beta \equiv 0(2) \Rightarrow U \equiv 0(2) \Rightarrow V \equiv 0(2)$ at (16), we have $(\beta, 2) = 1$; and certainly $(\beta, 3) = 1$. Further, $(\alpha, \beta) = 1$, for any common prime divisor π divides the resultant at (15), (16), so $\pi \in \{2, 23, 2377\}$, that is, $\pi \in \{23, 2377\}$ (β odd). But then (15), (16) force $U \equiv V \equiv 0 \bmod \pi$. Thus $(6\alpha, \beta) = 1$, and the above g.c.d. divides $(6\alpha, 2\varphi, 3\alpha+\beta\varphi)$. Further, $\alpha \equiv 0 \bmod \mathfrak{q}_{27337} \Rightarrow \alpha \equiv 0 \bmod 27337$, and from (15), $-213(U+7573V)^2 + 27337\cdot 118V(U+12822V) \equiv 0 \bmod 27337^2$, giving $U+7573V \equiv 0 \equiv V(U+12822V) \bmod 27337$, contradicting $(U,V)=1$. So the above gcd is $\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_3'$ (α *odd*), $\mathfrak{q}_2'\mathfrak{q}_3\mathfrak{q}_3'$ (α *even*).

At (19), let the ideal $(83U+(10+\theta)V) = \mathfrak{p}_{83}'\mathfrak{a}$, so that we obtain as ideals:

$$\mathrm{Norm}_{\mathbb{K}/\mathbb{L}}(3\alpha+\beta\varphi) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'(h)^{-1}\mathfrak{a}^2. \tag{20}$$

Now, from (17), $(h) \in \mathcal{S} \cup \mathfrak{p}_2\mathfrak{p}_2'\mathcal{S}$ where $\mathcal{S}$ is the set $\{(1), \mathfrak{p}_{23}^2, \mathfrak{p}_{2377}^2, \mathfrak{p}_{23}^2\mathfrak{p}_{2377}^2\}$; and thus (20) implies an ideal equation

$$\mathrm{Norm}_{\mathbb{K}/\mathbb{L}}(3\alpha+\beta\varphi) = \begin{cases} \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'\mathfrak{b}^2 \\ \mathfrak{p}_2'\mathfrak{p}_3\mathfrak{p}_3'\mathfrak{b}^2 \end{cases} \quad \text{for an integral ideal } \mathfrak{b} \text{ of } \mathfrak{O}_{\mathbb{L}}. \tag{21}$$

From the above remarks on greatest common divisor, (21) implies an ideal equation in $\mathbb{K}$ of type

$$(3\alpha+\beta\varphi) = \begin{cases} \mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_3'\mathfrak{B}^2 \\ \mathfrak{q}_2'\mathfrak{q}_3\mathfrak{q}_3'\mathfrak{B}^2 \end{cases} \quad \text{for an integral ideal } \mathfrak{B} \text{ of } \mathfrak{O}_{\mathbb{K}}.$$

But this gives a contradiction in the class-group of $\mathbb{K}$. For in the group $\mathbb{Z}_{504}\times\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$,

$$\mathfrak{q}_2 \sim [466,0,1,0,0], \quad \mathfrak{q}_2' \sim [38,2,1,0,0], \quad \mathfrak{q}_3 \sim [30,0,0,1,0], \quad \mathfrak{q}_3' \sim [222,2,0,0,0]$$

so that $\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_3' \sim [214,2,1,1,0]$, $\mathfrak{q}_2'\mathfrak{q}_3\mathfrak{q}_3' \sim [290,0,1,1,0]$.

If $\mathfrak{B} \sim [\varepsilon_0,\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4]$, then $\mathfrak{B}^2 \sim [2\varepsilon_0, 2\varepsilon_1, 0,0,0]$, implying $(3\alpha+\beta\varphi) \sim [*,*,1,1,0]$ is in the principal class, a contradiction.

Consequently there are no global solutions for $\delta = 2$, and $|E_{68}(\mathbb{Q})/\hat{\phi}(E_{68}'(\mathbb{Q}))| = 2^2$.

It should be noted here that the ideal classes are given relative to a certain (unspecified) ordered basis. This basis will generally change with each interactive session, resulting in

different representations for the ideal classes.
Also, the algorithms used in PARI for constructing the class-group are correct under GRH. However, in most cases it should be comparativelyeasy to verify the results PARI produces.

Next we consider the isogenous curve (12). In a completely analogous way it can be seen that, starting with

$$\Delta A^4 - 4860 A^2 B^2 - \frac{1968156}{\Delta} B^4 = C^2, \qquad \Delta \mid 2 \cdot 3 \cdot 23 \cdot 2377,$$

it suffices to show that there are no global solutions for $\Delta = -2$. Now, the class-group of the relevant quartic number field generated by a zero of $x^4 + 2430x^2 - 492039$ is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$. An argument similar to that used before applies and ultimately we find $|E'_{68}(\mathbb{Q})/\phi(E_{68}(\mathbb{Q}))| = 2^2$, thus proving that $r_{68} = 2$.

2.3 Constructing generators

The next step towards the construction of Mordell-Weil bases is to find on each curve the maximal number of linearly independent points. APECS was used extensively but failed to find the right number of points in six instances. It was necessary to perform the extra descent described above and search the resulting quartics for global solutions, which, when found, could be pulled back to the corresponding points of (4). This descent finds the points of large height in Table 1; and it is clear why the APECS search failed to find them.

Further we remark that any determination of generators of a Mordell-Weil group will depend on estimation of height functions on the curve, in particular the relation between the logarithmic height $h(P)$ and the canonical height $\hat{h}(P)$ of a point P on the curve. Silverman [11] gives general estimates for the difference $h(P) - 2\hat{h}(P)$, but it turns out that these are not precise enough for our purposes, and it was necessary to tailor his arguments specifically to the curve (4).

Lemma 2. (i) *For $P \in E_1(\mathbb{Q})$,*

$$-\log 6 - 4.076 \leq h(P) - 2\hat{h}(P) \leq \log 6 + 4.504$$

(ii) *For $k \geq 2$ and $P \in E_k(\mathbb{Q})$,*

$$-\frac{2}{3}\log\left(3 - \frac{1}{(2k-1)^2}\right) \leq h(P) - 2\hat{h}(P) \leq \log 12 + \frac{1}{2}\log C_k$$

where $C_k = (6k^2 - 6k + 1)\prod_p p^{e_p/2}$, the product running over all primes p for which p^{e_p} exactly divides $12k^2 - 12k - 1$ and $e_p \geq 2$.

Proof. (i) Example 2.2 of Silverman [11].

(ii) This is a careful book-keeping exercise using the methods and formulae of Silverman [11], [12]. Brief details of the proof are given below.

Theorem 4.1 of Silverman [11] gives

$$-\frac{1}{24}\log^+|j|_p \leq \lambda_p(P) - \frac{1}{2}\log^+|x(P)|_p \leq -\frac{1}{12}\log|\Delta|_p \tag{22}$$

for all finite primes p (where λ_p is the local component of the height); and that for primes p dividing the denominator of j to the first power, (22) may be replaced by

$$\frac{1}{12}\log^+|j|_p \leq \lambda_p(P) - \frac{1}{2}\log^+|x(P)|_p \leq -\frac{1}{12}\log|\Delta|_p. \tag{23}$$

Summing over the finite primes results in

$$F(k) \leq \hat{h}(P) - \lambda_\infty(P) - \frac{1}{2}\ln(\mathrm{den}(x(P))) \leq \frac{1}{12}\log|\Delta|, \tag{24}$$

where

$$F(k) = -\frac{1}{24}\ln(|\mathrm{den}(j)|) + \frac{1}{8}\ln(\text{squarefree part of } |1+12k-12k^2|). \tag{25}$$

To compute the component $\lambda_\infty(P)$ of the height of P at infinity, refer to Silverman [12], noting it is the height there termed λ' that is used in the inequalities (22), (23). See also [12, Remark, p. 341].

The cubic in x, $x^3-36x-864k(k-1)(2k-1)$, has precisely one real zero at $x=12k-6$; so for $P(x,y)\in E(\mathbb{R})$ then necessarily $x\geq 12k-6$, and $h(P)=\ln(\mathrm{num}(x))=\ln(x)+\ln(\mathrm{den}(x))$.

Define a sequence of reals $\{x_n\}$ by

$$x_0 = x, \quad x_{n+1} = \frac{x_n^4+72x_n^2+6912k(k-1)(2k-1)x_n+1296}{4(x_n^3-36x_n-864k(k-1)(2k-1))}$$

and a sequence $\{z_n\}$ by $z_n = Z(x_n)$, where

$$Z(x) = \frac{x^4+72x^2+6912k(k-1)(2k-1)x+1296}{x^4}.$$

Then $\lambda_\infty(P) = -\frac{1}{12}\ln|\Delta| + \frac{1}{8}\ln(Z(x)x^4) + \frac{1}{8}\sum_{n=1}^{\infty}4^{-n}\ln|z_n|$ so that (24) implies

$$F(k) - \frac{1}{12}\ln|\Delta| \leq \hat{h}(P) - \frac{1}{2}h(P) - \frac{1}{8}\ln Z(x) - \frac{1}{8}\sum_{n=1}^{\infty}4^{-n}\ln|z_n| \leq 0. \tag{26}$$

Now using $x \geq 6(2k-1)$,

$$Z(x) \leq 1 + \frac{2}{(2k-1)^2} + \frac{32k(k-1)}{(2k-1)^2} + \frac{1}{(2k-1)^4} = \left(3 - \frac{1}{(2k-1)^2}\right)^2.$$

Similarly,

$$0 \leq \ln|z_n| \leq 2\ln\left(3 - \frac{1}{(2k-1)^2}\right)$$

so that

$$0 \leq \sum_{n=1}^{\infty} 4^{-n}\ln|z_n| \leq \frac{2}{3}\ln\left(3 - \frac{1}{(2k-1)^2}\right).$$

Substituting into (26) results in

$$F(k) - \frac{1}{12}\ln|\Delta| \leq \hat{h}(P) - \frac{1}{2}h(P) \leq \frac{1}{3}\ln\left(3 - \frac{1}{(2k-1)^2}\right),$$

where the left-hand side is

$$F(k) - \frac{1}{12}\ln(2^{12}3^6) - \frac{1}{12}\ln(\mathrm{den}(j)) = -\frac{1}{2}\ln(12) - \frac{1}{4}\ln C_k,$$

by (25). This completes the proof of Lemma 2 (ii). □

At the final step, determination of bases for the Mordell-Weil groups, we choose to consider four cases, according to rank.

Rank 1 (31 instances)

Suppose the known point P is *not* a generator. It is easy to verify in each case that neither P nor $P+T_k$ lies in $2E_k(\mathbb{Q})$, so there exists $m \in \mathbb{Z}$, $Q \in E_k(\mathbb{Q})$ with $P = mQ$, $m \geq 3$, and where, without loss of generality, we may suppose m prime. By looking at $E_k(\mathbb{F}_p)$ for a suitable prime p, it can be shown in each of the cases that $m \neq 3$. So $m \geq 5$, and $\hat{h}(Q) = \frac{1}{m^2}\hat{h}(mQ) = \frac{1}{m^2}\hat{h}(P) \leq \frac{1}{25}\hat{h}(P)$. Using the bounds of Lemma 2, a simple search shows no such Q can exist in any of the cases.

Ranks 3, 4 (14, 3 instances, respectively)

In each case the known independent points do not have particularly large height, and the following idea of Silverman is applicable.

Let $P_1, \ldots, P_r$ be a maximal set of independent points in $E_k(\mathbb{Q})$ corresponding to a set of generators for $E_k(\mathbb{Q})/E_k(\mathbb{Q})_{\mathrm{tors}}$. Select a complete set S of 2^r representatives for $E_k(\mathbb{Q})/2E_k(\mathbb{Q})$ from the set

$$\left\{ \sum_{i=1}^{r} \varepsilon_i P_i \,\middle|\, \varepsilon_i \in \{0, \pm 1\} \right\}$$

and set $B = \max_{P \in S} \hat{h}(P)$. Then $E_k(\mathbb{Q})$ is generated by all points X of $E_k(\mathbb{Q})$ satisfying $\hat{h}(X) \leq B$.

The most intransigent of these cases occurred at $k = 74$ with $B = 13.1286$, leading to $h(P) \leq 20.8066$ and a run-time of several hours on a SUN workstation.

Rank 2 (52 instances)

The above method of Silverman works in many instances, but cannot deal with the cases where one of the two known independent points has large height, for example $k = 75$, where the known points have heights 2.6069 and 28.3739. We need to introduce a further idea. Suppose the known points P_1, P_2 generate a subgroup of index m in $E_k(\mathbb{Q})/E_k(\mathbb{Q})_{\text{tors}}$. It is straightforward to verify in all the cases that m is odd, by showing that if $\varepsilon_1 P_1 + \varepsilon_2 P_2 + \varepsilon_3 T_k \in 2E_k(\mathbb{Q})$ for $\varepsilon_i \in \{0, 1\}$, then $\varepsilon_i = 0$ for $i = 1, 2, 3$.

Suppose now $m > 1$, and let q be a prime dividing m. Then *either* $P_2 \in qE_k(\mathbb{Q})$ *or* at least one of the points $P_1 \pm rP_2$ with $r \in \{0, 1, \ldots, \frac{q-1}{2}\}$ lies in $qE_k(\mathbb{Q})$. In the latter case, let $P_1 + rP_2 = qQ$, $|r| \leq \frac{q-1}{2}$. Then

$$\begin{aligned}\hat{h}(P_1 + rP_2) + \hat{h}(P_1 - rP_2) = 2\hat{h}(P_1) + 2\hat{h}(rP_2) &= 2\hat{h}(P_1) + 2r^2\hat{h}(P_2) \\ &\leq 2\hat{h}(P_1) + \tfrac{1}{2}(q-1)^2\hat{h}(P_2),\end{aligned}$$

so that

$$q^2\hat{h}(Q) = \hat{h}(qQ) = \hat{h}(P_1 + rP_2) \leq 2\hat{h}(P_1) + \tfrac{1}{2}(q-1)^2\hat{h}(P_2),$$

from which

$$\hat{h}(Q) \leq \frac{2}{q^2}\hat{h}(P_1) + \frac{1}{2}\left(1 - \frac{1}{q}\right)^2\hat{h}(P_2) \leq \frac{2}{q^2}\hat{h}(P_1) + \tfrac{1}{2}\hat{h}(P_2). \tag{27}$$

Thus *either* there exists $Q \in E_k(\mathbb{Q})$ satisfying $\hat{h}(Q) = \frac{1}{q^2}\hat{h}(P_2)$ *or* there exists $Q \in E_k(\mathbb{Q})$ satisfying the inequality (27).

In each numerical case we eliminate the possibilities $q = 3, 5, 7$ by showing that none of $P_2, P_1 \pm rP_2$ with $r \in \{0, 1, \ldots, \frac{q-1}{2}\}$ lies in $qE_k(\mathbb{Q})$. As an example, when $k = 24$, the structure of the groups $E_{24}(\mathbb{F}_{19})$ and $E_{24}(\mathbb{F}_{137})$ was used to eliminate $q = 7$. It follows that $q \geq 11$, with consequently a point $Q \in E_k(\mathbb{Q})$ satisfying *either* $\hat{h}(Q) \leq \frac{1}{121}\hat{h}(P_2)$ *or* $\hat{h}(Q) \leq \frac{2}{121}\hat{h}(P_1) + \frac{1}{2}\hat{h}(P_2)$. By choosing P_1 to be the point with larger height than P_2, only the second inequality matters. It implies a manageable bound for $h(Q)$, and by search there are no such Q.

It only remains to indicate how in practice the search for points of bounded height was carried out.

We are searching on the curve (4) for points P with $h(P) < B$, for some known bound B. Let $X(P)$ at (7) be given by r/s^2, so that using (6),

$$0 \leq r + 6(2k-1)s^2 \leq e^B,$$

whence

$$0 \le s \le \left(e^B/(6(2k-1))\right)^{1/2}, \qquad 0 \le r \le e^B - 6(2k-1)s^2. \tag{28}$$

In practice, write $r = \delta\rho^2$ where δ is a squarefree divisor of $72(6k^2-6k+1)$. Then for each δ, (28) becomes

$$0 \le s \le \left(e^B/(6(2k-1))\right)^{1/2}, \qquad 0 \le \rho \le \left(\frac{e^B - 6(2k-1)s^2}{\delta}\right)^{1/2}.$$

Of course one can also restrict to those δ known to correspond to everywhere locally solvable curves, but in our cases the time of running was so short that this minor refinement was unnecessary.

Table 1: The Mordell-Weil groups $E_k(\mathbb{Q})$, $k = 1, \dots, 100$

Rank and generators of $E_k(\mathbb{Q})$, $k = 1, \dots, 100$		
k	rank r_k	generators $P_1, \dots, P_{r_k}$ on (4)
1	1	(18, 72)
2	1	(30, 144)
3	2	(42, 216), (54, 360)
4	2	(54, 288), (46, 152)
5	1	(66, 360)
6	1	(78, 432)
7	3	(144, 1584), (90, 504), (124, 1196)
8	2	(102, 576), (286, 4760)
9	2	(114, 648), (390, 7632)
10	2	(126, 720), (189, 2295)
11	2	(138, 792), (132706/25, 48342896/125)
12	2	(150, 864), (864, 25344)
13	2	(162, 936), (300, 4860)
14	2	(174, 1008), (166, 568)
15	2	(252, 3276), (186, 1080)
16	2	(198, 1152), (1342, 49096)
17	2	(474, 9936), (405, 7659)
18	2	(342, 5544), (222, 1296)
19	1	(234, 1368)
20	4	(246, 1440), (258, 2088), (522, 11376), (396, 7020)
21	2	(258, 1512), (1398, 52128)
		continued on next page

continued from previous page (Table 1)

Rank and generators of $E_k(\mathbb{Q})$, $k = 1, \ldots, 100$

k	rank r_k	generators $P_1, \ldots, P_{r_k}$ on (4)
22	3	(540, 11844), (634, 15416), (14076, 1670004)
23	1	(282, 1656)
24	2	(294, 1728), (30952606/101761, 77602986872/32461759)
25	4	(606, 14040), (333, 3393), (306, 1800), (300, 1260)
26	1	(318, 1872)
27	3	(714, 18216), (330, 1944), (406, 5896)
28	3	(342, 2016), (480, 8640), (930, 27720)
29	1	(354, 2088)
30	2	(366, 2160), (1777/4, 52649/8)
31	2	(378, 2232), (127824/289, 30083760/4913)
32	3	(390, 2304), (396, 2844), (3886/9, 138952/27)
33	2	(402, 2376), (5981669022636/908721025, 14628110492415103884/27393395298625)
34	1	(414, 2448)
35	2	(426, 2520), (139164, 51914700)
36	2	(438, 2592), (5278/9, 301112/27)
37	1	(450, 2664)
38	3	(1158, 38232), (582, 10296), (528, 7488)
39	2	(474, 2808), (12726/25, 721224/125)
40	1	(486, 2880)
41	2	(498, 2952), (2398896/3025, 3259927944/166375)
42	1	(510, 3024)
43	1	(522, 3096)
44	4	(534, 3168), (810, 19728), (1122, 35640), (24739884/25, 123054213348/125)
45	2	(546, 3240), (590713/16, 454008653/64)
46	2	(558, 3312), (909, 24255)
47	2	(570, 3384), (108734694/46225, 1126245391128/9938375)
48	3	(582, 3456), (3093, 171477), (5230/9, 89720/27)
49	1	(594, 3528)
50	2	(1317, 45549), (1558, 59768)
51	1	(618, 3672)
52	3	(780, 15444), (630, 3744), (814, 17416)
53	1	(642, 3816)
54	1	(654, 3888)

continued on next page

continued from previous page (Table 1)

Rank and generators of $E_k(\mathbb{Q})$, $k = 1, \ldots, 100$

k	rank r_k	generators $P_1, \ldots, P_{r_k}$ on (4)
55	2	(666, 3960), (42402, 8731296)
56	2	(678, 4032), (13101598/1089, 47418685768/35937)
57	1	(690, 4104)
58	2	(702, 4176), (25590, 4093560)
59	1	(714, 4248)
60	3	(1110, 31680), (813, 13167), (726, 4320)
61	1	(738, 4392)
62	1	(750, 4464)
63	2	(957, 21321), (762, 4536)
64	2	(774, 4608), (1644, 63252)
65	3	(1461, 51525), (786, 4680), (1068, 27468)
66	1	(798, 4752)
67	3	(810, 4824), (1398, 47160), (102198, 32671080)
68	2	(822, 4896), (53374/25, 11989432/125)
69	1	(834, 4968)
70	1	(846, 5040)
71	2	(858, 5112), (1442448, 1732408272)
72	2	(870, 5184), (1584, 57816)
73	3	(2334, 109800), (1246, 35720), (882, 5256)
74	3	(894, 5328), (2469, 119853), (353329/400, 14064983/8000)
75	2	(906, 5400), (31369672308565186839058333/20547499572797428243336, 4966969507247775157308223126323839317/931404796554775170586751810035 84)
76	2	(918, 5472), (1194, 30960)
77	2	(930, 5544), (164364/25, 66545388/125)
78	2	(942, 5616), (5187822/5329, 4230301536/389017)
79	2	(954, 5688), (3355673398086/82283041, 6147051433138245528/746389464911)
80	1	(966, 5760)
81	2	(978, 5832), (6548193/4096, 14792957487/262144)
82	1	(990, 5904)
83	3	(2253, 102303), (2674, 134720), (78768/49, 19353312/343)
84	2	(1014, 6048), (26494/25, 1696472/125)
85	1	(1026, 6120)
86	2	(1038, 6192), (812416/625, 522039464/15625)
87	2	(1050, 6264), (1638, 57240)
88	2	(1062, 6336), (132093/121, 15938217/1331)

continued on next page

continued from previous page (Table 1)

Rank and generators of $E_k(\mathbb{Q})$, $k = 1, \dots, 100$		
k	rank r_k	generators $P_1, \dots, P_{r_k}$ on (4)
89	2	(1074, 6408), (68688707715787803174/26984922344516161, 548220350317108568623851392352/4432836967250255286207841)
90	1	(1086, 6480)
91	2	(1098, 6552), (1968, 79632)
92	1	(1110, 6624)
93	1	(1122, 6696)
94	2	(1134, 6768), (38713/4, 7611085/8)
95	2	(1146, 6840), (174025341/25, 2295719061111/125)
96	2	(1158, 6912), (967461/529, 826267725/12167)
97	2	(1170, 6984), (57772/9, 13845140/27)
98	2	(1182, 7056), (1677, 55809)
99	1	(1194, 7128)
100	2	(1206, 7200), (184812, 79450236)

2.4 A rank 1 conjecture

From Table 1 it can be seen that for all 31 curves of rank 1 the point

$$Q_k = (12k + 6, 72k)$$

on (4) serves as a generator for $E_k(\mathbb{Q})/E_k(\mathbb{Q})_{\mathrm{tors}}$. Can this be a coincidence? We think not, but we have no more hard evidence than these 31 examples. Nevertheless, we wish to formulate the

Conjecture. *If the curve given by* (4) *has rank* 1*, then*

$$E_k(\mathbb{Q})/E_k(\mathbb{Q})_{\mathrm{tors}} \simeq \langle Q_k \rangle.$$

Support of a heuristic nature may be found in the following remark which contains ideas due to Samir Siksek. We are grateful to him for allowing us to use them.

Remark. The Szpiro ratio of an elliptic curve E over $\mathbb{Q}$ is the ratio

$$\sigma_E = \log(\text{discriminant } E)/\log(\text{conductor } E),$$

and is conjectured to be bounded. Hindry and Silverman [6] show that all non-torsion points $P \in E(\mathbb{Q})$ satisfy $\hat{h}(P) \geq (20\sigma_E)^{-8}10^{-1.1-4\sigma_E}\log(\text{discriminant } E)$, so that applied to the curves E_k, we obtain an estimate $\hat{h}(P) > c\log(k)$ where c is an absolute and effective constant, provided σ_E is bounded. On the other hand, our estimates indicate that $\hat{h}(Q_k)$ is asymptotic to $\frac{1}{2}\log(k\sqrt{6})$. So if Q_k generates a subgroup of index m in $E_k(\mathbb{Q})$, then $Q_k = mQ'_k + T$, for some $Q'_k \in E(\mathbb{Q})$ and torsion point T, and $m^2 c\log(k) < m^2\hat{h}(Q'_k) = \hat{h}(Q_k) \sim \frac{1}{2}\log(k\sqrt{6})$ implying a uniform bound on the index m for sufficiently large k.

It now seems plausible that for a rank 1 curve, there can only be finitely many k where the index m exceeds 1. For otherwise, there exists $m_0 \in \mathbb{N}$ such that $Q_k = m_0(x, y)$ as an equation in $E_k(\mathbb{Q})$ is solvable for $x, y \in \mathbb{Q}$ for infinitely many k. Equating first components, there results an equation $F(x, k) = 0$ of degree m_0^2 in x, which is known to have infinitely many rational solutions x, k. Further, $Q_k = m_0(x, y)$ forces x to be an integer, so $F(x, k) = 0$ has infinitely many integer solutions x, k. Consequently, $F(x, k)$ must represent a curve of genus 0, which seems unlikely in general.

3 Determination of integral points

Now that the rank r_k and a complete set of generators for $E_k(\mathbb{Q})$ are known, set

$$E_k(\mathbb{Q})/E_k(\mathbb{Q})_{\mathrm{tors}} = \langle P_1, \ldots, P_{r_k}\rangle.$$

For $P \in E_k(\mathbb{Q})$, there exist integers $m_1, \ldots, m_{r_k}$ such that

$$P = m_1 P_1 + \cdots + m_{r_k} P_{r_k} + P_0, \tag{29}$$

where P_0 is a torsion point, satisfying (from Lemma 1) $2P_0 = \mathbf{0}$ in $E_k(\mathbb{Q})$. For integral $P = (x(P), y(P))$ we intend to estimate the integral vector $\mathbf{m} = (m_1, \ldots, m_{r_k})$. Once (small) upper bounds for its coordinates m_i are known, an attempt can be made to recover all integral points by direct search.

3.1 Elliptic logarithms

Considering $\mathbf{m}$ as a column vector, then $\hat{h}(P) = \mathbf{m}^T\mathcal{H}_k\mathbf{m}$ where $\mathcal{H}_k$ is the $r_k \times r_k$ height-pairing matrix

$$\mathcal{H}_k = \left(\frac{1}{2}\langle P_i, P_j\rangle\right)$$

with $\langle R, S\rangle = \hat{h}(R+S) - \hat{h}(R) - \hat{h}(S)$ the Néron-Tate pairing. The matrix $\mathcal{H}_k$ is positive definite and hence

$$\hat{h}(P) \geq \lambda_k M_k^2 \tag{30}$$

where λ_k is the smallest eigenvalue of $\mathcal{H}_k$ and $M_k = \max_{1\leq i\leq r_k} |m_i|$.

Suppose now P is an integral point of (7) with $X(P) > 0$, that is, $x(P) > 6(2k-1)$. Then P is a point on the component of $E_k(\mathbb{R})$ containing the identity $\mathbf{0}$ of $E_k(\mathbb{Q})$. The known boundedness of $x(P)$ can be expressed by saying that P cannot be too close to $\mathbf{0}$. In order to measure the distance between P and $\mathbf{0}$, we use the group isomorphism

$$\phi : E'_k(\mathbb{R}) \to \mathbb{R}/\mathbb{Z} \text{ (circle group)}$$

where $E'_k = E_k$ for $k \geq 2$ and $E'_1(\mathbb{R})$ is the noncompact component of $E_1(\mathbb{R})$, with ϕ given by

$$\phi(P) \equiv \begin{cases} 0 \bmod 1 & \text{if } P = 0, \\ \dfrac{1}{\omega}\displaystyle\int_{x(P)}^{\infty} \frac{dt}{\sqrt{t^3 - 36t + b_k}} \bmod 1 & \text{if } y(P) \geq 0, \\ -\phi(-P) \bmod 1 & \text{if } y(P) < 0. \end{cases}$$

(see Zagier [14, p. 429]). Here $b_k = -864k(k-1)(2k-1)$, and $\omega = 2\int_{6(2k-1)}^{\infty} \frac{dt}{\sqrt{t^3-36t+b_k}}$ is the fundamental real period of the Weierstraß $\wp$-function associated with (4). There is no loss of generality in assuming that $\phi(P) \in [0,1)$, so that $\phi(P) \in [0, \frac{1}{2}]$ when $y(P) \geq 0$, which henceforth we shall assume. The quantities $u_i = \omega\phi(P_i)$ are known as the elliptic logarithms associated with the basis $\{P_1, \ldots, P_{r_k}\}$. Applying ϕ to (29) yields

$$\phi(P) \equiv m_1\phi(P_1) + \cdots + m_{r_k}\phi(P_{r_k}) + \tfrac{1}{2}\varepsilon \bmod 1,$$

where $\varepsilon = 0, 1$, according to whether $P_0 = \mathbf{0}$, $P_0 \neq \mathbf{0}$, respectively. Hence there exists $m_0 \in \mathbb{Z}$ such that

$$\phi(P) = m_0 + \frac{1}{2}\varepsilon + m_1\phi(P_1) + \cdots + m_{r_k}\phi(P_{r_k}). \tag{31}$$

Clearly, $|m_0| \leq 1 + |m_1| + \cdots + |m_{r_k}| \leq 1 + r_k M_k$. Multiplying by $u_0 = \omega$ and setting $L(P) = \omega\phi(P)$ yields

$$L(P) = \left(m_0 + \frac{1}{2}\varepsilon\right)u_0 + m_1 u_1 + \cdots + m_{r_k} u_{r_k}. \tag{32}$$

It is now straightforward to obtain an upper bound for $|L(P)|$ in terms of k and M_k.

Lemma 3. *Let $P = (x(P), y(P)) \in E_k(\mathbb{Q})$ be an integral point of (4) with $x(P) > 12k$, $y(P) > 0$. Suppose that P satisfies (29), and let $L(P)$ be as in (32). Then*

$$|L(P)| \leq d_k\sqrt{k}\exp(-\lambda_k M_k^2),$$

where

$$d_1 = 53.2 \text{ and } d_k = 4.08 \text{ for } k \geq 2.$$

Proof. From the definition of ϕ and by (32), it follows that

$$\begin{aligned}|L(P)| &= \int_{X(P)}^{\infty} \frac{dt}{\sqrt{t^3+18(2k-1)t^2+72(6k^2-6k+1)t}}\\ &\le \int_{X(P)}^{\infty} t^{-3/2}dt \le 2X(P)^{-1/2}.\end{aligned}$$

Using the estimates of Lemma 2 applied to (30), together with $x(P) > 12k$, we deduce for $k \ge 2$,

$$\begin{aligned}\log X(P) = \log(x(P)-6(2k-1)) &= \log x(P) + \log\left(1-\frac{6(2k-1)}{x(P)}\right)\\ &= h(P) + \log\left(1-\frac{6(2k-1)}{x(P)}\right)\\ &\ge 2\lambda_k M_k^2 - \frac{2}{3}\log\left(3-\frac{1}{(2k-1)^2}\right) + \log\left(\frac{1}{2k}\right)\\ &\ge 2\lambda_k M_k^2 - \log k - \frac{1}{3}\log 72,\end{aligned}$$

and the result follows. For $k=1$ the reasoning is similar. □

The upper bound for $|L(P)|$ of Lemma 3, combined with Sinnou David's lower bound (Lemma 4) produces an upper bound for M_k. We shall state this lower bound for $|L(P)|$ as it applies to the curves (4), referring the reader to Stroeker & Tzanakis [14] for further details.

Lemma 4. (David) *Let $P \in E_k(\mathbb{Q})$ be as in* Lemma 3. *Put*

$$h_k = \begin{cases}\log 1728, & \text{if } k=1,\\ \log\left((12k^2-12k-1)(6k^2-6k+1)^2\right), & \text{if } k\ge 2,\end{cases} \tag{33}$$

and for $j = 0,\ldots,r_k$, let A_j be a positive number satisfying

$$A_j \ge \max\{\hat{h}(P_j), h_k\}$$

(where $P_0 = \mathbf{0}$ by definition). If

$$B_k \ge \max\{\exp(A_0),\ldots,\exp(A_{r_k}), 2|m_0|+1, |m_1|,\ldots,|m_{r_k}|, 16\}, \tag{34}$$

then a lower bound for $|L(P)|$ is given by

$$|L(P)| \ge \exp\left(-c_k(\log B_k+1)(\log\log B_k+1+h_k)^{r_k+2}\right),$$

where

$$c_k = 2\cdot 10^{7r_k+15}\left(\frac{2}{e}\right)^{2(r_k+1)^2}(r_k+2)^{4r_k^2+18r_k+14}\prod_{j=0}^{r_k} A_j.$$

This is a special case of David [3, Théorème 2.1]). □

Remark. Following closely Stroeker & Tzanakis [14, Appendix], we have, for $k \geq 2$, taken the following fundamental periods for E_k:

$$\omega_1 = \Omega_1 + \Omega_2, \quad \omega_2 = 2\Omega_1 \quad \text{and} \quad \tau = \omega_1/\omega_2,$$

where

$$\Omega_1 = \frac{\pi}{M\left(\sqrt{6}\sqrt[4]{3(2k-1)^2-1}, \frac{1}{2}\sqrt{18(2k-1)+12\sqrt{3(2k-1)^2-1}}\right)},$$

$$\Omega_2 = \frac{\pi i}{M\left(\sqrt{6}\sqrt[4]{3(2k-1)^2-1}, \frac{1}{2}\sqrt{-18(2k-1)+12\sqrt{3(2k-1)^2-1}}\right)}.$$

Here $M(u, v)$ denotes the AGM (Arithmetic-Geometric Mean) of u and v. Also note that $\Omega_1 = \frac{1}{2}\omega$ is the real period of the Weierstraß $\wp$ function associated with (4). Then τ satisfies the requirements $\Re\tau = \frac{1}{2}$, $\Im\tau > 0$, $|\tau| \geq 1$, and for $j = 0, \ldots, r_k$ we have

$$\frac{3\pi u_j^2}{|\omega_1|^2 \Im\tau} < \frac{3}{2}\pi < \min_k(h_k).$$

For $k = 1$, we have chosen

$$\omega_1 = \frac{2\pi}{M(\sqrt{12}, \sqrt{6})}, \quad \omega_2 = \omega_1 i, \quad \text{and} \quad \tau = \omega_2/\omega_1 = i.$$

Then $\omega = \omega_1$ and

$$\frac{3\pi u_j^2}{|\omega_1|^2 \Im\tau} < \frac{3}{4}\pi < \min_k(h_k).$$

Moreover, the number $\mathcal{E}$ of [14, Appendix] has been chosen equal to e.

Corollary 5. *If B_k satisfies the inequality* (34) *then*

$$\lambda_k M_k^2 < c_k(\log B_k + 1)(\log\log B_k + 1 + h_k)^{r_k+2} + \log(d_k\sqrt{k}). \tag{35}$$

Proof. Combine Lemmas 3 and 4. □

Remark. If we take $B_k = 2r_kM_k + 3$ then $B_k \geq \max\{2|m_0| + 1, |m_1|, \ldots, |m_{r_k}|\}$. Furthermore, if M_k is taken sufficiently large to meet the remaining conditions of (34), then (35) says that M_k cannot be *too* large.

It is clear from (35) that r_k is the dominant factor in the calculation of the upper bound for M_k. For this reason we shall put the curves E_k into classes, depending on their rank. Only the first curve ($k = 1$) will be treated separately. Second to the rank, λ_k is the major contributor to the size of the upper bound for M_k; the values of h_k, d_k and the A_j have only a minor influence. Therefore it is not necessary to distinguish between the curves where these quantities are concerned. Since from (33)

$$\max_{2\le k\le 100} h_k \le \max_{2\le k\le 100} \log\left(\frac{27}{4}(2k-1)^6\right) < 33.67,$$

we replace h_k in (35) by 33.67. Furthermore,

$$\max_{2\le k\le 100}\ \max_{1\le j\le r_k} \hat{h}(P_j) = 28.3739\ldots,$$

and hence A_j may be chosen as 28.4 for all $2 \le k \le 100$, $1 \le j \le r_k$.
Finally,

$$\max_{1\le k\le 100} \log(d_k\sqrt{k}) < \log 40.8 = 3.708\ldots,$$

which makes it possible to replace $\log(d_k\sqrt{k})$ by 3.71 in (35) for all $2 \le k \le 100$.
For $k = 1$ we have $\hat{h}(P_1) = 0.4443\ldots$ and $h_1 = 7.454\ldots$, so that we may choose $A_0 = A_1 = 7.46$.

The following table gives particulars about the calculations of the upper bound for M_k, broken into cases for $k = 1$ and for each of the rank-classes.

Upper bound K for M_k by (35) in the range $1 \le k \le 100$			
r_k	k	λ_k	K
1	1	0.444	5.80×10^{22}
r_k	$\#\ k$	$\min \lambda_k$	K
1	30	0.800	8.90×10^{23}
2	52	0.607	5.73×10^{39}
3	14	0.740	2.40×10^{60}
4	3	0.705	2.07×10^{86}

3.2 LLL-reduction

Clearly the resulting upper bounds K are far too large to be of practical use, and it is necessary now to apply the LLL-reduction process described in detail in Stroeker & Tzanakis [14, Sec. 5] in order to reduce the magnitude of the bounds. See also de Weger [16, Chap. 3]. A brief description of the procedure should suffice here.

From Lemma 3,

$$|\phi(P)| < K_1 \exp(-K_2 M_k^2) \quad \text{and} \quad M_k < K, \tag{36}$$

where $K_1 = d_k\sqrt{k}/\omega$, and $K_2 = \min \lambda_k$. But we can bound $|\phi(P)|$ from below, as follows. Let $\mathcal{L}$ be the $(r_k+1)-$dimensional lattice, generated by the columns of the integral matrix

$$\mathcal{A}_{\mathcal{L}} = \begin{pmatrix} 1 & \dots & 0 & 0 \\ 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \\ [K_0\phi(P_1)] & \dots & [K_0\phi(P_r)] & K_0 \end{pmatrix},$$

(here $[\alpha]$ means rounding α towards 0, that is, $[\alpha] = \lceil \alpha \rceil$ if $\alpha \le 0$, and $[\alpha] = \lfloor \alpha \rfloor$ if $\alpha > 0$) where K_0 will be a large integer that will be conveniently chosen later. If the vector $(m_1, \dots, m_{r_k}, m_0) \in \mathbb{Z}^{r_k+1}$ satisfies $|m_j| < K$ for $j = 1, \dots, r_k$, put

$$\ell_k = \mathcal{A}_{\mathcal{L}} \begin{pmatrix} 2m_1 \\ \vdots \\ 2m_{r_k} \\ 2m_0 + \varepsilon \end{pmatrix} = \begin{pmatrix} 2m_1 \\ \vdots \\ 2m_{r_k} \\ t_k \end{pmatrix},$$

with

$$t_k = \sum_{j=1}^{r_k} 2m_i[K_0\phi(P_j)] + (2m_0 + \varepsilon)K_0.$$

Then using (31),

$$t_k = 2\sum_{j=1}^{r_k} m_i\Big([K_0\phi(P_j)] - K_0\phi(P_j)\Big) + 2K_0\phi(P)$$

so that

$$|t_k| \le 2r_k K + 2K_0\phi(P)$$

and

$$\|\ell_k\|^2 = 4\sum_{i=1}^{r_k} m_i^2 + t_k^2 \le 4r_k K^2 + 4(r_k K + K_0|\phi(P)|)^2. \tag{37}$$

On the other hand, if $\{\mathbf{b}_1, \dots, \mathbf{b}_{r_k+1}\}$ is an LLL-reduced basis of $\mathcal{L}$, then

$$\|\mathbf{b}_1\|^2 \le 2^{r_k}\|\ell_k\|^2. \tag{38}$$

Combining (37) with (38) yields

$$K_0|\phi(P)| \geq \sqrt{2^{-r_k-2}\|\mathbf{b}_1\|^2 - r_k K^2} - r_k K. \tag{39}$$

From (36), (39), we have a new upper bound for M_k, given implicitly by the inequality

$$M_k^2 \leq K_2^{-1}\left(\log(K_0K_1) - \log(\sqrt{2^{-r_k-2}\|\mathbf{b}_1\|^2 - r_k K^2} - r_k K)\right), \tag{40}$$

provided that the right-hand side of (39) is positive, that is, provided

$$\|\mathbf{b}_1\| > 2^{1+r_k/2} K \sqrt{r_k^2 + r_k}. \tag{41}$$

It is reasonable to expect that $\|\mathbf{b}_1\| \approx (\det \mathcal{A}_{\mathcal{L}})^{1/(r_k+1)} = K_0^{1/(r_k+1)}$. Therefore, if we choose K_0 such that $K_0^{1/(r_k+1)}$ is slightly larger than the right-hand side of (41), then it is likely (41) will be satisfied. In that case, (40) produces a new upper bound which is of the size of $\sqrt{\log K}$, a considerable improvement. There is nothing to prohibit using this reduction process as many times as possible; we found in practice that at most three reduction steps were needed to bring the upper bound for M_k down to a manageable size (between 3 and 6). In order to execute the reduction process, it is necessary to know the values of $\phi(P_j)$ to a great number of decimal places (600 in the case of rank 4). Zagier [17] describes a very efficient algorithm to compute these values to the precision needed, and this was programmed in the very fast UBASIC language. The LLL-reduction step was carried out using the integral LLL algorithm of PARI/GP. Below we list the outcome of each reduction process.

Reduction process for $1 \leq k \leq 100$
(d stands for the number of digits precision)

	step 1			step 2			step 3		
k	K_0	d	K	K_0	d	K	K_0	d	K
1	10^{50}	100	11	10^5	20	5	10^4	20	4

	step 1			step 2			step 3		
r_k	K_0	d	K	K_0	d	K	K_0	d	K
1	10^{50}	100	9	10^6	20	4	$10^3, 10^4$	20	3
2	10^{125}	200	18	10^{10}	30	6	$10^7, 10^8$	20	5^*
3	10^{250}	400	24	10^{12}	30	6	5×10^9	20	5
4	10^{440}	600	34	10^{16}	40	7	6.6×10^{12}	30	6

The * in the final column indicates one exception at $k = 79$, in which case the process stopped at step 2 with K value of 6.

3.3 All integral points for $1 \leq k \leq 100$

When completing the final search for integral points with the K values from the above table, the worst instances occur for rank 4 curves. Corresponding to $m_1 > 0$; $m_1 = 0$, $m_2 > 0$; $m_1 = m_2 = 0$, $m_3 > 0$; $m_1 = m_2 = m_3 = 0$, $m_4 > 0$ in (29), there are respectively $2 \cdot 6 \cdot 13^3$, $2 \cdot 6 \cdot 13^2$, $2 \cdot 6 \cdot 13$, $2 \cdot 6$ cases to consider, a total of $13^4 - 1 = 28560$ points to check for integrability. For each k-value, this search took about three hours using Apecs on a 486 desktop with 16 Mbytes of extended memory. For the other ranks, this final search was significantly shorter. A list of all the integral points found is given in Table 2. In fact the coefficients m_j corresponding to integral points rarely exceed unity; there are only five instances where this is not true (for $k = 1, 2, 7, 9$ and 20), and then the largest (absolute) coefficient is 2.

Table 2: Integer points on (7), $k = 1, \ldots, 100$

All integer points (X, Y) with $Y \geq 0$ for the curves (7), $k = 1, \ldots, 100$, omitting in each case the point $(0, 0)$	
k	(X, Y)
1	(-12,0), (-6,0), (-9, 9), (-8, 8), (6, 36), (12, 72), (288, 5040)
2	(12, 144), (78, 936)
3	(12, 216), (18, 288), (24, 360), (111, 1665), (148, 2368), (222, 3996), (2178, 103752), (6936, 581400), (11532, 1243224)
4	(4, 152), (12, 288), (147, 2583), (438, 10512), (1314, 49932), (2883, 158193)
5	(12, 360), (726, 21780)
6	(12, 432), (1086, 39096)
7	(12, 504), (46, 1196), (66, 1584), (88, 2024), (207, 4761), (276, 6624), (396, 10296), (600, 17640), (882, 29736), (1518, 63756), (2208, 109296), (18975, 2629935), (26508, 4334904)
8	(12, 576), (196, 4760), (363, 9603), (2022, 97056)
9	(12, 648), (288, 7632), (294, 7812), (2598, 140292), (6624588, 17050940568)
10	(12, 720), (75, 2295), (196, 5320), (3246, 194760)
11	(12, 792), (3966, 261756), (274776, 144134136)
12	(12, 864), (726, 25344), (4758, 342576)
13	(12, 936), (150, 4860), (1152, 46944), (5622, 438516)
14	(4, 568), (12, 1008), (2523, 139113), (6558, 550872), (19674, 2793708), (38307, 7545123)
15	(12, 1080), (78, 3276), (1164, 48888), (3744, 245232), (7566, 680940)

continued on next page

continued from previous page (Table 2)

All integer points (X, Y) with $Y \geq 0$ for the curves (7), $k = 1, \ldots, 100$, omitting in each case the point $(0, 0)$

k	(X, Y)
16	(12, 1152), (1156, 49096), (8646, 830016)
17	(12, 1224), (207, 7659), (276, 9936), (426, 15336), (568, 21016), (9798, 999396), (63948, 16246296)
18	(12, 1296), (132, 5544), (1002, 42084), (2475, 139095), (11022, 1190376)
19	(12, 1368), (12318, 1404252)
20	(12, 1440), (24, 2088), (162, 7020), (288, 11376), (294, 11592), (1587, 77625), (2178, 118404), (3468, 225216), (6843, 595341), (13686, 1642320), (18723, 2610081), (20164, 2913272), (85698, 25190244), (14652300, 56087890560)
21	(12, 1512), (1152, 52128), (15126, 1905876)
22	(12, 1584), (282, 11844), (376, 15416), (531, 21771), (708, 29736), (13818, 1670004), (16638, 2196216), (82668, 23880096), (1848411, 2513556999)
23	(12, 1656), (18222, 2514636)
24	(12, 1728), (19878, 2862432)
25	(6, 1260), (12, 1800), (39, 3393), (288, 13104), (312, 14040), (588, 25704), (831, 37395), (1300, 63440), (1734, 91188), (2548, 151424), (6648, 578376), (7200, 648720), (18954, 2670408), (21606, 3240900), (43212, 9074520), (259200, 132187680), (1277679, 1444716117), (4926999, 10937361897)
26	(12, 1872), (23406, 3651336)
27	(12, 1944), (88, 5896), (162, 8856), (396, 18216), (766, 35236), (1650, 87120), (3447, 230949), (4056, 289224), (25278, 4095036)
28	(12, 2016), (150, 8640), (600, 27720), (1152, 56736), (20667, 3042531), (27222, 4573296)
29	(12, 2088), (29238, 5087412)
30	(12, 2160), (2028, 116064), (31326, 5638680)
31	(12, 2232), (33486, 6228396)
32	(12, 2304), (18, 2844), (6936, 625464), (23812, 3762296), (30603, 5453091), (35718, 6857856), (48672, 10863216), (735000, 630617400), (1785900, 2387391120)
33	(12, 2376), (38022, 7528356)
34	(12, 2448), (40398, 8241192)
35	(12, 2520), (42846, 8997660), (138750, 51914700)

continued on next page

continued from previous page (Table 2)

All integer points (X, Y) with $Y \geq 0$ for the curves (7), $k = 1, \ldots, 100$, omitting in each case the point $(0, 0)$

k	(X, Y)
36	(12, 2592), (1875, 110025), (45366, 9799056)
37	(12, 2664), (47958, 10646676)
38	(12, 2736), (78, 7488), (132, 10296), (531, 29205), (708, 38232), (858, 46332), (1144, 62920), (2475, 157905), (3744, 271440), (4602, 358956), (7788, 747648), (50622, 11541816), (142572, 54088416)
39	(12, 2808), (53358, 12485772), (58482, 14310648)
40	(12, 2880), (56166, 13479840)
41	(12, 2952), (59046, 14525316)
42	(12, 3024), (61998, 15623496)
43	(12, 3096), (65022, 16775676)
44	(12, 3168), (147, 12537), (288, 19728), (600, 35640), (1734, 106488), (2178, 139788), (42483, 8918217), (68118, 17983152)
45	(12, 3240), (460374, 312911388), (71286, 19247220)
46	(12, 3312), (363, 24255), (74526, 20569176)
47	(12, 3384), (77838, 21950316)
48	(12, 3456), (2523, 171477), (20667, 3094821), (81222, 23391936), (58159227, 443541563451)
49	(12, 3528), (84678, 24895332)
50	(12, 3600), (723, 45549), (964, 59768), (1098, 68076), (1464, 92232), (88206, 26461800), (187500, 81576000)
51	(12, 3672), (91806, 28092636)
52	(12, 3744), (162, 15444), (196, 17416), (1152, 72864), (4056, 319176), (11163, 1278621), (95478, 29789136)
53	(12, 3816), (99222, 31552596)
54	(12, 3888), (103038, 33384312)
55	(12, 3960), (41748, 8731296), (106926, 35285580)
56	(12, 4032), (110886, 37257696)
57	(12, 4104), (114918, 39301956)
58	(12, 4176), (24900, 4093560), (119022, 41419656)
59	(12, 4248), (123198, 43612092)
60	(12, 4320), (99, 13167), (396, 31680), (3862, 308960), (15448, 2054584), (20164, 3016648), (38148, 7661016), (127446, 45880560)
61	(12, 4392), (131766, 48226356)
62	(12, 4464), (136158, 50650776)
63	(12, 4536), (207, 21321), (8152, 839656), (140622, 53155116)

continued on next page

continued from previous page (Table 2)

All integer points (X, Y) with $Y \geq 0$ for the curves (7), $k = 1, \ldots, 100$, omitting in each case the point $(0, 0)$

k	(X, Y)
64	(12, 4608), (882, 63252), (2904, 220968), (145158, 55740672)
65	(12, 4680), (294, 27468), (687, 51525), (2616, 196200), (10368, 1175904), (16023, 2176839), (37098, 7370136), (149766, 58408740)
66	(12, 4752), (154446, 61160616)
67	(12, 4824), (600, 47160), (2178, 160776), (30772, 5609296), (101400, 32671080), (159198, 63997596)
68	(12, 4896), (164022, 66920976)
69	(12, 4968), (168918, 69932052)
70	(12, 5040), (173886, 73032120)
71	(12, 5112), (178926, 76222476), (1441602, 1732408272)
72	(12, 5184), (726, 57816), (184038, 79504416)
73	(12, 5256), (376, 35720), (1098, 83448), (1464, 109800), (1551, 116325), (2068, 157168), (6039, 573705), (7942, 826804), (189222, 82879236), (273612, 143803944)
74	(12, 5328), (1587, 119853), (194478, 86348232), (437772, 290524752)
75	(12, 5400), (199806, 89912700)
76	(12, 5472), (288, 30960), (14406, 1894536), (205206, 93573936)
77	(12, 5544), (210678, 97333236)
78	(12, 5616), (216222, 101191896)
79	(12, 5688), (221838, 105151212)
80	(12, 5760), (227526, 109212480)
81	(12, 5832), (233286, 113376996)
82	(12, 5904), (239118, 117646056)
83	(12, 5976), (1263, 102303), (1684, 134720), (1746, 139680), (2328, 188568), (245022, 122020956), (311052, 174308904)
84	(12, 6048), (250998, 126502992)
85	(12, 6120), (257046, 131093460)
86	(12, 6192), (263166, 135793656)
87	(12, 6264), (600, 57240), (7938, 849744), (269358, 140604876)
88	(12, 6336), (275622, 145528416)
89	(12, 6408), (281958, 150565572)
90	(12, 6480), (288366, 155717640)
91	(12, 6552), (882, 79632), (2904, 249480), (294846, 160985916)
92	(12, 6624), (301398, 166371696)

continued on next page

continued from previous page (Table 2)	
All integer points (X, Y) with $Y \geq 0$ for the curves (7), $k = 1, \ldots, 100$, omitting in each case the point $(0, 0)$	
k	(X, Y)
93	(12, 6696), (308022, 171876276)
94	(12, 6768), (314718, 177500952)
95	(12, 6840), (321486, 183247020), (522786, 379225440)
96	(12, 6912), (328326, 189115776)
97	(12, 6984), (335238, 195108516)
98	(12, 7056), (507, 55809), (12100, 1528120), (342222, 201226536)
99	(12, 7128), (349278, 207471132)
100	(12, 7200), (183618, 79450236), (356406, 213843600)

From Table 2, it is immediate to deduce a full list of integer solutions (n, t) to equation (2) in the range $1 \leq k \leq 100$. These are listed in Table 3, in the form of triples $(k, k + n - 1, t)$.

Table 3: Integer solutions of (1), $k = 1, \ldots, 100$

All integer solutions $(k + n - 1, t)$ with $t > k$ of (1) No entry for k indicates no solution exists	
k	$(k + n - 1, t)$
1	(24, 70)
3	(4, 5), (580, 8075), (963, 17267)
7	(29, 92), (39, 143), (56, 245), (190, 1518), (2215, 60207)
9	(32, 106), (552057, 236818619)
11	(22908, 2001863)
13	(108, 652)
15	(111, 679), (326, 3406)
17	(39, 138), (5345, 225643)
18	(28, 77)
20	(21, 29), (43, 158), (308, 3128), (1221044, 778998480)
21	(116, 724)
22	(80, 413), (6910, 331668)
25	(48, 182), (50, 195), (73, 357), (578, 8033), (624, 9010), (3625, 126035), (21624, 1835940)
27	(59, 253), (364, 4017)
	continued on next page

continued from previous page (Table 3)	
All integer solutions $(k+n-1,t)$ with $t>k$ of (1) No entry for k indicates no solution exists	
k	$(k+n-1,t)$
28	(77, 385), (123, 788)
30	(198, 1612)
32	(609, 8687), (4087, 150878), (61281, 8758575), (148856, 33158210)
38	(48, 143), (96, 531), (349, 3770), (686, 10384), (11918, 751228)
44	(67, 274), (93, 495)
50	(171, 1281), (15674, 1133000)
52	(147, 1012), (389, 4433)
55	(3533, 121268)
58	(2132, 56855)
60	(92, 440), (3238, 106403)
64	(305, 3069)
65	(282, 2725), (928, 16332)
67	(116, 655), (8516, 453765)
73	(194, 1525), (22873, 1997277)
74	(36554, 4035066)
76	(99, 430)
83	(276, 2619), (26003, 2420957)
87	(136, 795)
91	(332, 3465)

3.4 The rank 1 case

Now we restrict attention to the case where the rank of $E_k(\mathbb{Q})$ equals 1. The point $Q_k=(1,k)$ at (2), respectively, $Q_k=(12k+6,72k)$ on (4), is a point of infinite order. We show here that for any integer k, then neither mQ_k $(m>1)$ nor mQ_k+T_k $(m\geq 1)$ can be an integer point of (2). By virtue of the previous determination of $E_k(\mathbb{Z})$ for $1\leq k\leq 100$, we could assume $k>100$, but in fact we shall assume only $k\geq 2$, implying that the torsion point T_k is $(0,0)$ on (2) or as at (5) on (4). A consequence of this result is that if Q_k is indeed a generator for the group $E_k(\mathbb{Q})/E_k(\mathbb{Q})_{\mathrm{tors}}$, then the only integer solution of (2) is $(n,t)=(1,k)$.

The approach of this section is much in the spirit of Ayad [1] and it is from that paper that it has been inspired. The idea is in essence quite simple. When expressing the x-coordinate of mQ_k as the quotient of two polynomials in $\mathbb{Z}[k]$, it turns out that the resultant of these two polynomials is an integer divisible by only 2 and 3; so any common factor of the polynomials upon specialization to any integer k is also divisible by only 2 and 3. But the numerator polynomial lies in $1+12\mathbb{Z}[k]$; so numerator and denominator are coprime for any integer k. Provided the denominator is not 1, the result follows. In practice, it proved rather slippery converting these ideas into a formal proof, and several intricate induction arguments are necessary.

For any point $P=(x,y)$ on (4), define the associated division polynomials $\psi_m(P)$ as follows (see, for example, Silverman [10, Ch. III, Exercise 3.7]):

$$\begin{aligned}
&\psi_0(P)=0, \qquad \psi_1(P)=1, \qquad \psi_2(P)=2y,\\
&\psi_3(P)=3x^4-216x^2-10368k(k-1)(2k-1)x-1296,\\
&\psi_4(P)=4y(x^6-180x^4-17280k(k-1)(2k-1)x^3-6480x^2-124416k(k-1)(2k-1)x\\
&\qquad -46656(8k^2-8k+1)(64k^4-128k^3+72k^2-8k-1),
\end{aligned}$$

with, for $m\geq 2$,

$$\psi_{2m+1}=\psi_{m+2}\psi_m^3-\psi_{m-1}\psi_{m+1}^3, \qquad 2y\psi_{2m}=\psi_m(\psi_{m+2}\psi_{m-1}^2-\psi_{m-2}\psi_{m+1}^2). \tag{42}$$

Then

$$mP=(x(mP),y(mP))=\left(x-\frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2},\frac{\psi_{2m}}{2\psi_m^4}\right). \tag{43}$$

For the specific point Q_k we have

$$\begin{aligned}
\psi_2(Q_k)&=2^4\cdot 3^2k,\\
\psi_3(Q_k)&=2^6\cdot 3^4(-1-12k+24k^2+72k^3-36k^4),\\
\psi_4(Q_k)&=2^{14}3^8k(1+6k-6k^2)(-1-12k+12k^2+36k^4).
\end{aligned} \tag{44}$$

Henceforth we shall simply write ψ_m instead of $\psi_m(Q_k)$, but shall always write explicitly $\psi_m(P)$ for any point $P\neq Q_k$. The only primes p such that Q_k is singular on $E_{k,p}(\mathbb{F}_p)$ are $p=2,3$. Let $\mathcal{S}=\{2,3\}$; then from Ayad [1], we have the following lemma.

Lemma 6. (i) *For any positive integer m, the point mQ_k on E_k is $\mathcal{S}$-integral if and only if the only prime divisors of ψ_m are 2 and 3,*

(ii) *For any positive integer m, the point mQ_k+T_k on E_k is $\mathcal{S}$-integral if and only if the only prime divisors of $12\psi_m^2-\psi_{m+1}\psi_{m-1}$ are 2 and 3.*

Proof. For a proof we refer to [1]. □

We introduce the following relatively standard notation. Let p be prime, and $f(k)\in\mathbb{Q}(k)$. Write $\nu_p(f)=e\in\mathbb{Z}$ to denote that

$$f(k)=p^e\frac{g(k)}{h(k)},$$

where $g, h \in \mathbb{Z}[k]$, and in both g and h at least one coefficient is not divisible by p. It is easy to see that $\nu_p(FG) = \nu_p(F) + \nu_p(G)$ and $\nu_p(F+G) \geq \min\{\nu_p(F), \nu_p(G)\}$ with equality if $\nu_p(F) \neq \nu_p(G)$.

Lemma 7. (i) *For any integer $m \geq 1$ we have*

$$\begin{aligned} \nu_2(\psi_{2m-1}) &= 3m(m-1), & \nu_3(\psi_{2m-1}) &= 2m(m-1), \\ \nu_2(\psi_{2m}) &\geq 3m^2+1, & \nu_3(\psi_{2m}) &\geq 2m^2. \end{aligned}$$

(ii) *Defining $\bar{\psi}_j$ to be the part of ψ_j prime to 6, or more precisely*

$$(-1)^{[(j-1)/2]}\psi_j = 2^{\nu_2(\psi_j)}\, 3^{\nu_3(\psi_j)}\, \bar{\psi}_j,$$

then for $m \geq 1$,

$$\bar{\psi}_{2m-1} \in 1 + 12k\mathbb{Z}[k], \quad \bar{\psi}_{2m} \in k\mathbb{Z}[k]. \tag{45}$$

Proof. Use induction on m. Both parts are certainly true for $m = 1, 2$; cf. (44).

Consider now $m \geq 3$, and suppose the lemma is valid for all indices less than m. First, for m odd, $m = 2r+1$, $r \geq 1$, then (42) gives

$$\psi_{2m-1} = \psi_{2r+2}\psi_{2r}^3 - \psi_{2r-1}\psi_{2r+1}^3 \tag{46}$$

and by the induction hypothesis,

$$\begin{aligned} \nu_2(\psi_{2r+2}\psi_{2r}^3) &\geq 3(r+1)^2 + 1 + 3(3r^2+1) = 12r^2 + 6r + 7, \\ \nu_2(\psi_{2r-1}\psi_{2r+1}^3) &= 3r(r-1) + 3 \cdot 3(r+1)r = 12r^2 + 6r, \end{aligned}$$

so that

$$\nu_2(\psi_{2m-1}) = 12r^2 + 6r = 3m(m-1)$$

as claimed. Also from (42),

$$144k \cdot \psi_{2m} = \psi_{2r+1}(\psi_{2r+3}\psi_{2r}^2 - \psi_{2r-1}\psi_{2r+2}^2) \tag{47}$$

and, by the induction hypothesis,

$$\begin{aligned} \nu_2(\psi_{2r+1}\psi_{2r+3}\psi_{2r}^2) &\geq 12r^2 + 12r + 8, \\ \nu_2(\psi_{2r+1}\psi_{2r-1}\psi_{2r+2}^2) &\geq 12r^2 + 12r + 8, \end{aligned}$$

so that

$$4 + \nu_2(\psi_{2m}) \geq 12r^2 + 12r + 8,$$

whence, as claimed,

$$\nu_2(\psi_{2m}) \geq 12r^2 + 12r + 4 = 3m^2 + 1.$$

The induction for ν_3 is similar, and details are safely left to the reader.

To show part (ii) of the Lemma (still under hypothesis $m = 2r+1$), observe that (46) and the ensuing valuations imply

$$\bar{\psi}_{2m-1} \in \bar{\psi}_{2r-1}\bar{\psi}_{2r+1}^3 + 2^7 \cdot 3^2 k^4 \mathbb{Z}[k].$$

By the induction hypothesis, $\bar{\psi}_{2r-1}$ and $\bar{\psi}_{2r+1}$ lie in $1 + 12k\mathbb{Z}[k]$, and hence so does $\bar{\psi}_{2m-1}$, as claimed.

Further, (47) implies a relation of type

$$k\bar{\psi}_{2m} = -\bar{\psi}_{2r+1}(2^\alpha 3^\beta \bar{\psi}_{2r+3}\bar{\psi}_{2r}^2 - 2^\gamma 3^\delta \bar{\psi}_{2r-1}\bar{\psi}_{2r+2}^2),$$

where $\alpha, \beta, \gamma, \delta$ are nonnegative integers with $\alpha\gamma = 0$ and $\beta\delta = 0$. By the induction hypothesis, $\bar{\psi}_{2r}, \bar{\psi}_{2r+2} \in k\mathbb{Z}[k]$ and it follows that $\psi_{2m} \in k\mathbb{Z}[k]$, as claimed.

In the second case (m even, $m = 2r$), the induction arguments are similar, using the identities

$$\psi_{2m-1} = \psi_{2r+1}\psi_{2r-1}^3 - \psi_{2r-2}\psi_{2r}^3 \quad \text{and} \quad 144k\psi_{2m} = \psi_{2r}(\psi_{2r+2}\psi_{2r-1}^2 - \psi_{2r-2}\psi_{2r+1}^2).$$

This completes the proof of Lemma 7. $\square$

Now let $m > 1$ be an integer such that mQ_k has integral coordinates. We shall use repeatedly the following fact (see Ayad [1]):

$$\textit{If } nP \textit{ is an } S\textit{-integral point, then } P \textit{ is an } S\textit{-integral point.} \tag{48}$$

If m is even, then the above fact implies that $2Q_k$ is integral: but then $x(2Q_k) = (1+12k-24k^3+36k^4)/4k^2$, a contradiction. If $3|m$, then $3Q_k$ is integral, so by Lemma 6, the only primes dividing ψ_3 are 2 and 3. From (44), this forces $1 + 12k - 24k^2 - 72k^3 + 36k^4 = 1$, impossible for $k \neq 0$. Accordingly, if mQ_k is integral then we may assume $(m, 6) = 1$.

Next we develop a "3-adic" estimation of certain $\bar{\psi}_i$.

Lemma 8. *For every even positive integer n, with $3 \nmid n$, and every positive integer N,*

$$\bar{\psi}_{n3^N \pm 1} \in 1 \pm nk(1 + k - k^3)3^{N+1} + 3^{N+2}k\mathbb{Z}[k]. \tag{49}$$

Remark. Since $1 + k - k^3 \not\equiv 0 \bmod 3$ for all k, it will follow from (49) that for $m > 1$ and $(m, 6) = 1$, then $\bar{\psi}_m \neq 1$. But, by Lemma 7, $\bar{\psi}_m \equiv 1 \bmod 6$ and thus $\bar{\psi}_m$ has a prime divisor larger than 3, which is of course also a prime divisor of ψ_m. This will contradict Lemma 6, establishing the fact that mQ_k cannot be integral.

To prove Lemma 8, two subsidiary lemmas are needed.

Lemma 9. *For every positive integer n with $3 \nmid n$, and any positive integer N,*

$$\nu_3(\psi_{2n\cdot 3^N}) \geq 2n^2 \cdot 3^{2N} + N.$$

Proof. First we fix $n = 1$ and prove the assertion by induction on N. For $N = 1$, straightforward computation (Maple V was used) shows that $\nu_3(\psi_6) = 19$, as required. Suppose now $\nu_3(\psi_{2\cdot 3^N}) = e \geq 2\cdot 3^{2N} + N$; we must show that $\nu_3(\psi_{2\cdot 3^{N+1}}) \geq 2\cdot 3^{2N+2} + N + 1$. From Tschöpe and Zimmer [15, Sec. 1] we have

$$\psi_{rs}(Q_k) = \psi_s^{r^2}(Q_k)\psi_r(sQ_k), \tag{50}$$

from which

$$\psi_{2\cdot 3^{N+1}} = \psi_{3(2\cdot 3^N)} = \psi_{2\cdot 3^N}^9 \cdot \psi_3(2\cdot 3^N Q_k). \tag{51}$$

In order to compute $\psi_3(2\cdot 3^N Q_k)$ we need to substitute $x = x(2\cdot 3^N Q_k)$ into the formula $\psi_3(2\cdot 3^N Q_k) = 3x^4 - 216x^2 - 10368k(k-1)(2k-1)x - 1296$. Now from (43)

$$x(2\cdot 3^N Q_k) = 12k + 6 - \frac{\psi_{2\cdot 3^N - 1}\psi_{2\cdot 3^N + 1}}{\psi_{2\cdot 3^N}^2},$$

and, by Lemma 7, we have $\nu_3(\psi_{2\cdot 3^N - 1}\psi_{2\cdot 3^N + 1}/\psi_{2\cdot 3^N}^2) = 4\cdot 3^{2N} - 2e < 0$, which implies $\nu_3(x(2\cdot 3^N Q_k)) = 4\cdot 3^{2N} - 2e$, and $\nu_3(\psi_3(2\cdot 3^N Q_k)) = \nu_3(3x^4) = 4(4\cdot 3^{2N} - 2e) + 1$.

Consequently, from (51),

$$\nu_3(\psi_{2\cdot 3^{N+1}}) = 9e + 4(4\cdot 3^{2N} - 2e) + 1 \geq 2\cdot 3^{2N+2} + N + 1,$$

as required for the induction.

Second, let $n > 1$ with $3 \nmid n$, and let N be any positive integer. From (50),

$$\psi_{2n\cdot 3^N} = \psi_{2\cdot 3^N}^{n^2} \cdot \psi_n(2\cdot 3^N Q_k). \tag{52}$$

Here, $\psi_n(2\cdot 3^N Q_k)$ is a polynomial in $x = x(2\cdot 3^N Q_k)$ with $\nu_3(x) = 4\cdot 3^{2N} - 2e < 0$, so that $\nu_3(\psi_n(2\cdot 3^N Q_k)) = \nu_3$ (leading term of $\psi_n(x)$). It is well-known that the leading term of $\psi_n(x)$ as polynomial in x is $nx^{(n^2-1)/2}$ for n odd, and $\frac{1}{2}n\psi_2(x)x^{(n^2/2)-2}$ for n even, and accordingly,

$$\nu_3(\psi_n(2\cdot 3^N Q_k)) = \begin{cases} \frac{n^2-1}{2}(4\cdot 3^{2N} - 2e), & \text{if } n \text{ odd}, \\ \left(\frac{n^2}{2} - 2\right)(4\cdot 3^{2N} - 2e) + 2, & \text{if } n \text{ even}. \end{cases}$$

In both cases, the right-hand side is at least $\frac{n^2-1}{2}(4\cdot 3^{2N} - 2e)$, so that from (52),

$$\nu_3(\psi_{2n\cdot 3^N}) \geq n^2 e + \frac{n^2-1}{2}(4\cdot 3^{2N} - 2e) \geq 2n^2 3^{2N} + N,$$

as required. $\square$

Lemma 10. *Let r be a positive even integer, $3 \nmid r$ and N any positive integer. Then the relations*

$$\bar{\psi}_{r3^N-1} \in 1 - rk(1+k-k^3)3^{N+1} + 3^{N+2}ku(k) + 3^{N+3}k\mathbb{Z}[k], \tag{53}$$
$$\bar{\psi}_{r3^N+1} \in 1 + rk(1+k-k^3)3^{N+1} + 3^{N+2}ku'(k) + 3^{N+3}k\mathbb{Z}[k], \tag{54}$$

where $u, u' \in \mathbb{Z}[k]$, imply the relations

$$\bar{\psi}_{2r3^N-1} \in 1 - 2rk(1+k-k^3)3^{N+1} + 3^{N+2}ku'(k) + 3^{N+3}k\mathbb{Z}[k], \tag{55}$$
$$\bar{\psi}_{2r3^N+1} \in 1 + 2rk(1+k-k^3)3^{N+1} + 3^{N+2}ku(k) + 3^{N+3}k\mathbb{Z}[k]. \tag{56}$$

Proof. From (42), $\psi_{2r3^N+1} = \psi_{r3^N+2}\psi^3_{r3^N} - \psi_{r3^N-1}\psi^3_{r3^N+1}$ which gives

$$\bar{\psi}_{2r3^N+1} \in \bar{\psi}_{r3^N-1}\bar{\psi}^3_{r3^N+1} + 3^{N+3}k\mathbb{Z}[k], \tag{57}$$

by Lemmas 7 and 9. Now (54) implies

$$\bar{\psi}^3_{r3^N+1} \in 1 + rk(1+k-k^3)3^{N+2} + 3^{N+3}k\mathbb{Z}[k]$$

and multiplying by (53) in (57) gives (56).

The deduction of (55) is entirely analogous. □

Proof of Lemma 8. The result is first proved for $n = 2$ by induction on N. The case $N = 1$ is verified by direct computation. Suppose the claim is true for the integer N, so that

$$\bar{\psi}_{2\cdot3^N-1} \in 1 - 2k(1+k-k^3)3^{N+1} + 3^{N+2}ku(k) + 3^{N+3}k\mathbb{Z}(k), \tag{58}$$
$$\bar{\psi}_{2\cdot3^N+1} \in 1 + 2k(1+k-k^3)3^{N+1} + 3^{N+2}ku'(k) + 3^{N+3}k\mathbb{Z}(k), \tag{59}$$

for some $u(k), u'(k) \in \mathbb{Z}(k)$. Then by Lemma 10,

$$\bar{\psi}_{4\cdot3^N-1} \in 1 - 4k(1+k-k^3)3^{N+1} + 3^{N+2}ku'(k) + 3^{N+3}k\mathbb{Z}(k), \tag{60}$$
$$\bar{\psi}_{4\cdot3^N+1} \in 1 + 4k(1+k-k^3)3^{N+1} + 3^{N+2}ku(k) + 3^{N+3}k\mathbb{Z}(k). \tag{61}$$

We use the following general relation (see Ayad [1]):

$$\psi_{r+s}\psi_{r-s} = \psi_{r+1}\psi_{r-1}\psi_s^2 - \psi_{s+1}\psi_{s-1}\psi_r^2. \tag{62}$$

With $r = 4\cdot 3^N$, $s = 2\cdot 3^N + 1$, then Lemmas 7 and 9 imply

$$\bar{\psi}_{2\cdot3^{N+1}+1}\bar{\psi}_{2\cdot3^N-1} = \bar{\psi}_{4\cdot3^N+1}\bar{\psi}_{4\cdot3^N-1}\bar{\psi}^2_{2\cdot3^N+1} - 2^\gamma 3^\delta \bar{\psi}_{2\cdot3^N+2}\bar{\psi}_{2\cdot3^N}\bar{\psi}^2_{4\cdot3^N}$$

for integers $\gamma \geq 0$, $\delta \geq 3N+2$, where the second summand on the right-hand side lies in $k^4\mathbb{Z}[k]$. Thus

$$\bar{\psi}_{2\cdot 3^{N+1}+1}\bar{\psi}_{2\cdot 3^N-1} \in \bar{\psi}_{4\cdot 3^N+1}\bar{\psi}_{4\cdot 3^N-1}\bar{\psi}^2_{2\cdot 3^N+1} + 3^{N+3}k\mathbb{Z}[k]. \tag{63}$$

In view of (59),

$$\bar{\psi}^2_{2\cdot 3^N+1} \in 1 + 4k(1+k-k^3)3^{N+1} + 2ku'(k)3^{N+2} + 3^{N+3}k\mathbb{Z}[k]. \tag{64}$$

Furthermore, viewing (58) as a relation in $\mathbb{Z}[[k]]$, then $\bar{\psi}_{2\cdot 3^N-1}$ is an invertible element with

$$\bar{\psi}^{-1}_{2\cdot 3^N-1} \in 1 + 2k(1+k-k^3)3^{N+1} - ku(k)3^{N+2} + 3^{N+3}k\mathbb{Z}[[k]]. \tag{65}$$

Multiplying together (60), (61), (64) and (65), there results from (63)

$$\bar{\psi}_{2\cdot 3^{N+1}+1} \in 1 + 2k(1+k-k^3)3^{N+2} + 3^{N+3}k\mathbb{Z}[[k]],$$

where clearly $\mathbb{Z}[[k]]$ may be replaced by $\mathbb{Z}[k]$ since we know a priori that $\bar{\psi}_{2\cdot 3^{N+1}+1} \in \mathbb{Z}[k]$. This completes the reduction on N (for $n=2$) in (49) with the upper sign. The induction on N (for $n=2$) with lower sign at (49) is entirely analogous.

It remains to induct on n. We shall assume that n is an even integer at least 4, $3 \nmid n$, and that (49) is true for all even integers $< n$, not divisible by 3, and all $N \geq 1$. We must show

$$\bar{\psi}_{n3^N\pm 1} \in 1 \pm nk(1+k-k^3)3^{N+1} + 3^{N+2}k\mathbb{Z}[k]$$

for all $N \geq 1$. The inductive arguments needed are similar to those used in the previous lines, and in the proofs of Lemmas 9 and 10. In addition to these lemmas, the relations at (42) and (62) are crucial for the completion of the proof. Although delicate, the remaining arguments do not contain any surprising feature, and so to avoid unnecessary repetition, we suppress further details in the proof, safely leaving them to the reader. This induction on n completes the verification of Lemma 8. $\square$

By the remark immediately following the statement of Lemma 8, mQ_k cannot be integral for $m \geq 2$, and it remains to show that $mQ_k + T_k$ on (2) cannot be integral for $m \geq 1$. As the reader by now will have gotten the gist of our inductive argument, we shall cut down the remaining "torsion twisted" case to its most essential parts.

Since the coordinates of the point $Q_k + T_k$ with respect to (2) are not integral, we may assume that $m > 1$.

Suppose henceforth that $m > 1$ with $mQ_k + T_k$ an integral point of E_k at (2). In view of the transformation (3) and its inverse, the coordinates $x(mQ_k+T_k)$, $y(mQ_k+T_k)$ of the point $mQ_k + T_k$ with respect to the model E_k at (4) are also integers with

$$x(mQ_k + T_k) \equiv 2 \bmod 4. \tag{66}$$

Let $\Psi = 12\psi_m^2 - \psi_{m-1}\psi_{m+1}$, then by Lemma 6 (ii),

$$2 \textit{ and } 3 \textit{ are the only prime divisors of } \Psi. \tag{67}$$

From Lemma 7, it is readily checked that for m even

$$\begin{aligned}\nu_2(\psi_{m-1}\psi_{m+1}) &= \frac{3}{2}m^2 < \frac{3}{2}m^2 + 4 \le \nu_2(12\psi_m^2),\\ \nu_3(\psi_{m-1}\psi_{m+1}) &= m^2 < m^2 + 1 \le \nu_3(12\psi_m^2),\end{aligned}$$

and for m odd,

$$\begin{aligned}\nu_2(\psi_{m-1}\psi_{m+1}) &\ge \frac{3m^2+7}{2} > \frac{3m^2+1}{2} = \nu_2(12\psi_m^2),\\ \nu_3(\psi_{m-1}\psi_{m+1}) &\ge m^2 + 1 > m^2 = \nu_3(12\psi_m^2).\end{aligned}$$

These imply in (67),

$$\Psi = 12\psi_m^2 - \psi_{m-1}\psi_{m+1} = \begin{cases} \pm 2^{3m^2/2} 3^{m^2}, & m \text{ even},\\ \pm 2^{(3m^2+1)/2} 3^{m^2}, & m \text{ odd}.\end{cases} \tag{68}$$

Now compute $x(mQ_k + T_k)$ in terms of the ψ's. We have

$$x(mQ_k + T_k) = -x(mQ_k) - x(T_k) + \left(\frac{y(mQ_k) - y(T_k)}{x(mQ_k) - x(T_k)}\right)^2,$$

and, by (43),

$$\begin{aligned}x(mQ_k) \pm x(T_k) &= 12k + 6 - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2} \pm (12k - 6),\\ y(mQ_k) - y(T_k) &= \frac{\psi_{2m}}{2\psi_m^4} = \frac{\psi_{m-1}^2\psi_{m+2} - \psi_{m+1}^2\psi_{m-2}}{288k\psi_m^3}.\end{aligned}$$

It follows that

$$x(mQ_k + T_k) = \frac{-2^{10}3^4k^2\Psi^3 + (\psi_{m-1}^2\psi_{m+2} - \psi_{m+1}^2\psi_{m-2})^2}{2^{10}3^4k^2\psi_m^2\Psi^2} + 12(1-2k). \tag{69}$$

Let e_2 denote the 2-adic valuation on $\mathbb{Q}$. In the case where m is *odd*, then by Lemma 5 and (68),

$$\begin{aligned}e_2(2^{10}3^4k^2\psi_m^2\Psi^2) &= \frac{1}{2}(9m^2 + 19) + 2e_2(k),\\ e_2(2^{10}3^4k^2\Psi^3) &= \frac{1}{2}(9m^2 + 23) + 2e_2(k),\\ e_2(\psi_{m-1}^2\psi_{m+2} - \psi_{m+1}^2\psi_{m-2}) &\ge \frac{1}{4}(9m^2 + 19) + e_2(k),\end{aligned}$$

so that (69) implies $e_2(x(mQ_k + T_k)) \geq 2$, contradicting (66). Thus m is *even*. Writing $m = 2^N q$ with q odd, then $mQ_k + T_k = q(2^N Q_k + T_k)$ and by (48) it follows that $2^N Q_k + T_k$ is integral. It is checked that $2Q_k + T_k$ is non-integral, so we assume that $N \geq 2$. In order to obtain a contradiction to the integrality of $2^N Q_k + T_k$, we need the following facts accumulated in a final lemma.

Lemma 11. (i) *For* $n \geq 1$,

$$\bar{\psi}_{2^n-1}\bar{\psi}_{2^n+1} \in 1 + 2^{2n}(k + k^4) + 2^{2n+1}k\mathbb{Z}[k]. \tag{70}$$

(ii) *If* $2^N Q_k + T_k$ *is integral, then* k *divides* $3 \cdot 2^{2N}$. *Moreover,*

$$\bar{\psi}_{2^N-1}\bar{\psi}_{2^N+1} \in 1 + 2^{2N+1}k\mathbb{Z}[k]. \tag{71}$$

Proof. Both statements can, as before, be proved by inductive arguments. Although lengthy, and not everywhere trivial, we feel that the reader by now must have acquired sufficient insight in the methods of this section to enable him to produce complete proofs unaided. □

To obtain a contradiction to the integrality of $2^N Q_k + T_k$, first note that $k \neq 3$, because $r_3 = 2$. Thus, from Lemma 11, k must be even. But then (70) and (71) are contradictory.

References

[1] M. Ayad, "Points S-entiers des courbes elliptiques", unpublished, 1991.

[2] J. E. Cremona, "Algorithms for modular elliptic curves", Cambridge Un. Press, 1992.

[3] S. David, "Minorations de formes linéaires de logarithmes elliptiques", *Publ. Math. de l'Un. Pierre et Marie Curie* **106**, Problèmes diophantiens 1991-1992, exp. no. 3.

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

[5] R. K. Guy, "Unsolved Problems in Number Theory", 2nd ed., Springer-Verlag, New York, 1994.

[6] M. Hindry and J. H. Silverman, "The canonical height and integral points on elliptic curves", *Inventiones Math.* **93** (1988), 419–450.

[7] M. Kuwata and J. Top, "An elliptic surface related to sums of consecutive squares", *Expositiones Math.*, **12** (1994), 181–192.

[8] S. Platiel and J. Rung, "Natürliche Zahlen als Summen aufeinander folgender Quadratzahlen", *Expositiones Math.* **12** (1994), 353–361.

[9] J. Rung, "Quadratzahlen als Summen aufeinander folgender Quadrate", preprint (Manuscript eines Vortrages am Math. Inst. der Uni. Zürich, 1991).

[10] J. H. Silverman, "The arithmetic of elliptic curves", Springer-Verlag, New York, 1986.

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

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

[13] R. J. Stroeker, "On the sum of consecutive cubes being a perfect square", *Compositio Math.* **97** (1995), to appear.

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

[15] H. M. Tschöpe and H. G. Zimmer, "Computation of the Néron-Tate height on elliptic curves", *Math. Comp.* **48** (1987), 351–370.

[16] B. M. M. de Weger, "Algorithms for Diophantine equations", CWI Tract 65, Stichting Mathematisch Centrum, Amsterdam, 1989.

[17] D. Zagier, "Large integral points on elliptic curves, *Math. Comp.* **48** (1987), 425–436.