ELLIPTIC BINOMIAL DIOPHANTINE EQUATIONS

ROELOF J. STROEKER AND BENJAMIN M. M. DE WEGER

ABSTRACT. The complete sets of solutions of the equation $\binom{n}{k} = \binom{m}{\ell}$ are determined for the cases $(k, \ell) = (2, 3), (2, 4), (2, 6), (2, 8), (3, 4), (3, 6), (4, 6), (4, 8)$. In each of these cases the equation is reduced to an elliptic equation, which is solved by using linear forms in elliptic logarithms. In all but one case this is more or less routine, but in the remaining case $((k, \ell) = (3, 6))$ we had to devise a new variant of the method.

1. INTRODUCTION

In Pascal's Triangle, composed of the binomial coefficients $\binom{n}{k}$ for $n = 0, 1, 2, \ldots, 0 \leq k \leq n$, all natural numbers, with the exception of 2, occur at least twice, and many three times or more. Not counting multiple occurrences of trivial type, coming from $\binom{n}{0} = 1$, $\binom{n}{1} = n$ and $\binom{n}{k} = \binom{n}{n-k}$, one could formulate the following problem.

Main Problem. *To determine all natural numbers that occur at least twice in Pascal's Triangle as binomial coefficient $\binom{n}{k}$ with $2 \leq k \leq \frac{1}{2}n$.*

As yet this problem is unsolved in its full generality. The only nontrivial solutions known at this time are the following:

(1)
$$\binom{16}{2} = \binom{10}{3} = 120, \quad \binom{21}{2} = \binom{10}{4} = 210, \quad \binom{56}{2} = \binom{22}{3} = 1540,$$
$$\binom{120}{2} = \binom{36}{3} = 7140, \quad \binom{153}{2} = \binom{19}{5} = 11628, \quad \binom{221}{2} = \binom{17}{8} = 24310,$$
$$\binom{78}{2} = \binom{15}{5} = \binom{14}{6} = 3003,$$
$$\text{and} \quad \binom{F_{2i+2}F_{2i+3}}{F_{2i}F_{2i+3}} = \binom{F_{2i+2}F_{2i+3} - 1}{F_{2i}F_{2i+3} + 1} \quad \text{for} \quad i = 1, 2, \ldots,$$

where F_n is the nth Fibonacci number, defined by $F_0 = 0, F_1 = 1$, and $F_{n+1} = F_n + F_{n-1}$ for $n = 1, 2, \ldots$. This infinite family of solutions is due to D.A. Lind [L] and D.A. Singmaster [Sin]. It is conjectured that there are no other nontrivial solutions, and it is known that there are none with $\binom{n}{k} \leq 10^{30}$ or $n \leq 1000$, cf. [dW2].

For fixed k, ℓ (with $2 \leq k < \ell$) the equation $\binom{n}{k} = \binom{m}{\ell}$ has been completely solved in three cases only, namely for $(k, \ell) = (2, 3)$ by È.T. Avanesov [A], for $(k, \ell) = (2, 4)$ by one of us [dW1] and independently by A. Pintér [P], and for $(k, \ell) = (3, 4)$ by a remark of one of us, noting that the equation in this case reduces at once to an equation solved by L.J. Mordell [M1], see [dW2].

For a few choices of (k, ℓ) the equation $\binom{n}{k} = \binom{m}{\ell}$ represents an elliptic curve, or can be transformed into another equation representing an elliptic curve. Note that $\binom{n}{k}$ is, for fixed k, a polynomial in n of degree k with rational coefficients. For even k, using the obvious symmetry about $n - \frac{k-1}{2}$, it is also a polynomial in $(n - \frac{k-1}{2})^2$ of degree $\frac{1}{2}k$ with rational coefficients. In particular,

$$\binom{n}{2} \text{ is quadratic in } n, \qquad \binom{n}{3} \text{ is cubic in } n,$$

$$\binom{n}{4} \text{ is quartic in } n, \text{ and also quadratic in } (n - \tfrac{3}{2})^2,$$

$$\binom{n}{6} \text{ is cubic in } (n - \tfrac{5}{2})^2, \qquad \binom{n}{8} \text{ is quartic in } (n - \tfrac{7}{2})^2.$$

Now, let $f_q, g_q \in \mathbb{Z}[x]$ be polynomials of degree q. Then the equations

$$y^2 = f_3(x), \qquad y^2 = f_4(x), \qquad f_3(y) = g_3(x)$$

generically represent elliptic curves. Equations of the first two types $y^2 = f_q(x)$ for $q = 3, 4$ can be reduced to a number of Thue equations, cf. L.J. Mordell [M1], and for Thue equations general solution methods exist, based on estimations for linear forms in logarithms of algebraic numbers, cf. N. Tzanakis and B.M.M. de Weger [TW]. Such methods were used in [dW1] and [P] cited above, for solving $\binom{n}{2} = \binom{m}{4}$. An alternative, though often less practical approach is provided by Yu. Bilu and G. Hanrot [BH]. For the case $f_3(y) = g_3(x)$ however we do not know of any practical method that works in general. Only some very special types can be solved, such as superelliptic equations (where $f_3(y) = y^3$, see [BH]). In theory an upper bound for the absolute values of the coordinates of an integral point on any model $g(x, y) = 0$ for an elliptic curve is explicitly known (cf. [BC]), but the known upper bounds are so large as to render the corresponding search range completely unworkable.

Only recently techniques have been developed involving estimations of linear forms in elliptic logarithms for the solution of elliptic diophantine equations. We felt that most likely this method should also work quite efficiently for the binomial equations at hand. Success should be almost guaranteed for any reasonable equation of type $y^2 = f_q(x)$ for $q = 3, 4$, as the elliptic logarithm method, developed independently by R.J. Stroeker and N. Tzanakis [ST1], by J. Gebel, A. Pethő and H.G. Zimmer [GPZ], and by N.P. Smart [Sm] for $q = 3$, and by N. Tzanakis [T] for $q = 4$, is quite generally applicable.

For the case $f_3(y) = g_3(x)$, which also represents an elliptic curve, a similar method should be applicable, but such a method is not to be found yet in the literature. As it turned out, the main ideas of [ST1] and [T] carried through to this case too, without significant changes. This points at the probable existence of an efficient method for solving any reasonable equation of type $f_3(y) = g_3(x)$, and even of the more general type $f_3(x, y) = 0$, where $f \in \mathbb{Z}(x, y)$ has degree 3 and is not

necessarily homogeneous. We study this general type of equation in a forthcoming paper [SW]; in the present paper we merely concentrate on the particular equation coming from $\binom{n}{3} = \binom{m}{6}$.

All this enabled us to prove the following results. Three of them are already known, but for these we present different proofs. From now on we do not maintain the restriction $m, n > 0$ anymore, but we will allow $m, n \in \mathbb{Z}$, based on the definition

$$\binom{n}{k} = \frac{1}{k!} \prod_{i=0}^{k-1} (n-i) \quad \text{for } k \geq 0.$$

Theorem A23 (Avanesov). *The only solutions of $\binom{n}{2} = \binom{m}{3}$ are those listed in Table T23.*

Theorem A24 (de Weger, Pintér). *The only solutions of $\binom{n}{2} = \binom{m}{4}$ are those listed in Table T24.*

Theorem A26. *The only solutions of $\binom{n}{2} = \binom{m}{6}$ are those listed in Table T26.*

Theorem A28. *The only solutions of $\binom{n}{2} = \binom{m}{8}$ are those listed in Table T28.*

Theorem A34 (Mordell, de Weger). *The only solutions of $\binom{n}{3} = \binom{m}{4}$ are those listed in Table T34.*

Theorem A36. *The only solutions of $\binom{n}{3} = \binom{m}{6}$ are those listed in Table T36.*

Theorem A46. *The only solutions of $\binom{n}{4} = \binom{m}{6}$ are those listed in Table T46.*

Theorem A48. *The only solutions of $\binom{n}{4} = \binom{m}{8}$ are those listed in Table T48.*

One might wonder what can be said about other combinations of values for k and ℓ in $\binom{n}{k} = \binom{m}{\ell}$ than those considered here. If $k = 2$ or $k = 4$ then we encounter an equation of type $y^2 = f_\ell(x)$, which represents a hyperelliptic curve of genus $\lfloor \frac{\ell-1}{2} \rfloor \geq 2$ when $\ell \geq 5$. For such equations there are approaches that should work as a rule, like those by Thue equations, or by Bilu's method [BH], but in any practical sense these techniques seem too complex by far, even for the case of $\binom{n}{2} = \binom{m}{5}$. For other values of (k, ℓ) no methods are known, and all we can say is that in many of these cases the binomial equation $\binom{n}{k} = \binom{m}{\ell}$ possibly represents an algebraic curve of genus > 1, and therefore at most finitely many rational solutions exist, by celebrated results of G. Faltings [F].

Very recently we have been able to completely solve the equations $\binom{n}{k} = \binom{n-1}{k+2}$ (which has no nontrivial solutions) and $\binom{n}{k} = \binom{n-2}{k+1}$ (which has no nontrivial solutions other than $\binom{6}{1} = \binom{4}{2}$). We did this by the same variant of the elliptic logarithms method that we use in the present paper for solving $\binom{n}{3} = \binom{m}{6}$. We intend to give details in our forthcoming paper [SW].

TABLE 1. Transformations from binomial equations to elliptic equations

(k, ℓ)	transformation	
$(2,3)$	$X = 3m - 3$	$Y = 9n - 5$
$(2,4)$	$U = m - 2$	$V = 6n - 3$
$(2,6)$	$X = \frac{5}{2}m^2 - \frac{25}{2}m + 8$	$Y = 75n - 38$
$(2,8)$	$U = \frac{1}{2}m^2 - \frac{7}{2}m + 6$	$V = 210n - 105$
$(3,4)$	$X = n - 1$	$Y = \frac{1}{2}m^2 - \frac{3}{2}m$
$(3,6)$	$U = n - 1$	$V = \frac{1}{2}m^2 - \frac{5}{2}m + 3$
$(4,6)$	$X = \frac{15}{2}m^2 - \frac{75}{2}m + 25$	$Y = \frac{225}{2}n^2 - \frac{675}{2}n + 112$
$(4,8)$	$U = \frac{1}{2}m^2 - \frac{7}{2}m + 3$	$V = 105n^2 - 315n + 105$

We now turn to the above mentioned eight cases, which we shall call *elliptic binomial equations.* Inspired by the above remarks, we introduce changes of variables as given in Table 1. Notice that the new variables $(X, Y$ or $U, V)$ are integral valued.

These transformations are chosen such that the resulting equations have a convenient form. For the cases of type $f_2(Y) = g_3(X)$ this means that a global minimal Weierstrass equation over $\mathbb{Z}$ is obtained; for the cases of type $f_2(V) = g_4(U)$ this means that $f_2(V) = V^2$, the constant term in $g_4(U)$ is a square, and the coefficients are integers as small as possible; and for the case $f_3(U) = g_3(V)$ the coefficients of both polynomials are again integers, as small as possible.

It now will be clear that Theorems A23 to A48 are consequences of the following results.

Theorem B23. *The complete set of solutions in rational integers X, Y of the equation*

(W23) $$Y^2 + Y = X^3 - 9X + 20$$

is given in Table T23.

TABLE T23. The solutions to (W23) and to $\binom{n}{2} = \binom{m}{3}$

X	Y	n	m	m_1	m_2		X	Y	n	m	m_1	m_2
-3	-5	0	0	1	1		6	13	2	3	1	-1
-3	4	1	0	-1	-1		10	-31			-2	-2
-2	-6			0	-2		10	30			2	2
-2	5			0	2		12	-41	-4	5	2	1
0	-5	0	1	-1	0		12	40	5	5	-2	-1
0	4	1	1	1	0		27	-140	-15	10	1	-2
1	-4			2	0		27	139	16	10	-1	2
1	3			-2	0		63	-500	-55	22	-3	0
3	-5	0	2	0	-1		63	499	56	22	3	0
3	4	1	2	0	1		105	-1076	-119	36	1	3
6	-14	-1	3	-1	1		105	1075	120	36	-1	-3

Theorem B24. *The complete set of solutions in rational integers U, V of the equation*

(Q24) $$V^2 = 3U^4 + 6U^3 - 3U^2 - 6U + 9$$

is given in Table T24.

TABLE T24. The solutions to (Q24) and to $\binom{n}{2} = \binom{m}{4}$

U	V	n	m	m_1	m_2	m_T
-9	-123	-20	-7	0	2	1
-9	123	21	-7	-1	-1	0
-5	-33	-5	-3	1	0	1
-5	33	6	-3	-2	1	0
-3	-9	-1	-1	-2	0	1
-3	9	2	-1	1	1	0
-2	-3	0	0	0	1	1
-2	3	1	0	-1	0	0
-1	-3	0	1	0	0	1
-1	3	1	1	-1	1	0

U	V	n	m	m_1	m_2	m_T
0	-3	0	2	-1	1	1
0	3	1	2	0	0	0
1	-3	0	3	-1	0	1
1	3	1	3	0	1	0
2	-9	-1	4	1	1	1
2	9	2	4	-2	0	0
4	-33	-5	6	-2	1	1
4	33	6	6	1	0	0
8	-123	-20	10	-1	-1	1
8	123	21	10	0	2	0

Theorem B26. *The complete set of solutions in rational integers* X, Y *of the equation*

(W26) $$Y^2 + Y = X^3 + X^2 - 58X + 1294$$

is given in Table T26.

TABLE T26. The solutions to (W26) and to $\binom{n}{2} = \binom{m}{6}$

X	Y	n	m	m_1	m_2
-13	-5			0	-2
-13	4			0	2
-7	-38	0	$2,3$	-1	0
-7	37	1	$2,3$	1	0
-2	-38	0	$1,4$	1	1
-2	37	1	$1,4$	-1	-1
2	-35			-2	2
2	34			2	-2
8	-38	0	$0,5$	0	-1
8	37	1	$0,5$	0	1
14	-59			2	0
14	58			-2	0

X	Y	n	m	m_1	m_2
23	-113	-1	$-1,6$	-1	1
23	112	2	$-1,6$	1	-1
68	-563	-7	$-3,8$	1	-2
68	562	8	$-3,8$	-1	2
133	-1538	-20	$-5,10$	-2	3
133	1537	21	$-5,10$	2	-3
233	-3563			-2	-1
233	3562			2	1
323	-5813	-77	$-9,14$	3	-1
323	5812	78	$-9,14$	-3	1
2234	-105614			0	4
2234	105613			0	-4

Theorem B28. *The complete set of solutions in rational integers* U, V *of the equation*

(Q28) $$V^2 = 35U^4 - 350U^3 + 945U^2 - 630U + 11025$$

is given in Table T28.

Theorem B34 (Mordell). *The complete set of solutions in rational integers* X, Y *of the equation*

(W34) $$Y^2 + Y = X^3 - X$$

is given in Table T34.

TABLE T28. The solutions to (Q28) and to $\binom{n}{2} = \binom{m}{8}$

U	V	n	m	m_1	m_2	m_3	m_4	m_5
-147	-132195			1	0	-1	0	-1
-147	132195			0	0	0	-1	1
-25	-4445			1	0	-2	0	0
-25	4445			0	0	1	-1	0
-15	-1785			1	-1	0	-1	0
-15	1785			0	1	-1	0	0
-4	-245			0	1	0	0	0
-4	245			1	-1	-1	-1	0
0	-105	0	3, 4	1	0	-1	-1	0
0	105	1	3, 4	0	0	0	0	0
1	-105	0	2, 5	0	0	-1	0	0
1	105	1	2, 5	1	0	0	-1	0
3	-105	0	1, 6	1	0	0	0	0
3	105	1	1, 6	0	0	-1	-1	0
6	-105	0	0, 7	0	0	0	-1	0
6	105	1	0, 7	1	0	-1	0	0
8	-175			1	1	-1	0	0
8	175			0	-1	0	-1	0
10	-315	-1	$-1, 8$	1	0	0	-1	1
10	315	2	$-1, 8$	0	0	-1	0.	-1
21	-1995	-9	$-3, 10$	0	-1	-1	-1	0
21	1995	10	$-3, 10$	1	1	0	0	0
55	-16275	-77	$-7, 14$	1	1	0	1	0
55	16275	78	$-7, 14$	0	-1	-1	-2	0
91	-46305	-220	$-10, 17$	0	1	-1	-1	0
91	46305	221	$-10, 17$	1	-1	0	0	0

TABLE T34. The solutions to (W34) and to $\binom{n}{3} = \binom{m}{4}$

X	Y	n	m	m_1
-1	-1	0	1, 2	3
-1	0	0	0, 3	-3
0	-1	1	1, 2	-1
0	0	1	0, 3	1
1	-1	2	1, 2	-2

X	Y	n	m	m_1
1	0	2	0, 3	2
2	-3	3		4
2	2	3	$-1, 4$	-4
6	-15	7		-6
6	14	7	$-4, 7$	6

TABLE T36. The solutions to (C36) and to $\binom{n}{3} = \binom{m}{6}$

U	V	n	m	m_1	m_2	m_3	m_4
-1	0	0	2, 3	0	1	1	0
-1	1	0	1, 4	0	0	0	-1
-1	3	0	0, 5	-1	0	0	0
0	0	1	2, 3	0	0	0	0
0	1	1	1, 4	-1	1	0	0
0	3	1	0, 5	0	0	1	-1

U	V	n	m	m_1	m_2	m_3	m_4
1	0	2	2, 3	-1	0	0	-1
1	1	2	1, 4	0	0	1	0
1	3	2	0, 5	0	1	0	0
2	6	3	$-1, 6$	-1	0	1	-1
8	21	9	$-4, 9$	1	0	0	0

Theorem B36. *The complete set of solutions in rational integers U, V of the equation*

(C36) $$15U^3 - 15U = V^3 - 4V^2 + 3V$$

is given in Table T36.

TABLE T46. The solutions to (W46) and to $\binom{n}{4} = \binom{m}{6}$

X	Y	n	m	m_1	m_2	m_3
-29	-32			1	1	-1
-29	31			-1	-1	1
-25	-88			0	1	1
-25	87			0	-1	-1
-20	-113	$1,2$	$2,3$	0	-1	0
-20	112	$0,3$	$2,3$	0	1	0
-14	-122			-2	0	0
-14	121			2	0	0
-5	-113	$1,2$	$1,4$	1	1	0
-5	112	$0,3$	$1,4$	-1	-1	0
5	-88			-1	0	-1
5	87			1	0	1
14	-75			-2	-2	0
14	74			2	2	0
16	-77			1	1	1
16	76			-1	-1	-1
20	-88			1	-1	0
20	87			-1	1	0
25	-113	$1,2$	$0,5$	-1	0	0
25	112	$0,3$	$0,5$	1	0	0
49	-320			0	2	0
49	319			0	-2	0
70	-563			0	0	-1
70	562	$-1,4$	$-1,6$	0	0	1
79	-680			1	-1	1
79	679			-1	1	-1
130	-1463			-1	0	1
130	1462			1	0	-1
250	-3938			-1	-2	0
250	3937			1	2	0
305	-5313			1	2	-1
305	5312			-1	-2	1
400	-7988			2	1	1
400	7987	$-7,10$	$-5,10$	-2	-1	-1
695	-18313			-3	-1	0
695	18312			3	1	0
1555	-61313			2	-1	0
1555	61312			-2	1	0
1645	-66713			0	2	1
1645	66712			0	-2	-1
18895	-2597288			-1	1	-2
18895	2597287			1	-1	2

Theorem B46. *The complete set of solutions in rational integers X, Y of the equation*

(W46) $$Y^2 + Y = X^3 - 525X + 10156$$

is given in Table T46.

Theorem B48. *The complete set of solutions in rational integers U, V of the equation*

(Q48) $$V^2 = 105U^4 + 210U^3 - 945U^2 - 1890U + 11025$$

TABLE T48. The solutions to (Q48) and to $\binom{n}{4} = \binom{m}{8}$

U	V	n	m	m_1	m_2	m_3	U	V	n	m	m_1	m_2	m_3
-3	-105	$1,2$	$3,4$	0	1	0	3	-105	$1,2$	$0,7$	-1	0	0
-3	105	$0,3$	$3,4$	-1	0	-1	3	105	$0,3$	$0,7$	0	1	-1
-2	-105	$1,2$	$2,5$	0	0	-1	7	-525			1	1	-1
-2	105	$0,3$	$2,5$	-1	1	0	7	525	$-1,4$	$-1,8$	-2	0	0
0	-105	$1,2$	$1,6$	-1	1	-1	33	-11445			-2	0	-1
0	105	$0,3$	$1,6$	0	0	0	33	11445	$-9,12$	$-5,12$	1	1	0

is given in Table T48.

Remarks. Theorem B23 is a bit more general than the result of Avanesov [A], and our proof is rather different.

Theorem B24 is merely a restatement of the main result of [dW1] and [P]. Again the proof we give below is of a different nature.

Theorem B34 is the main result of [M1]. See also J.H. Silverman [Sil1, Exercise 9.13, p. 275] for a different proof, and see [dW2]. The proof we give below is new.

The meaning of the parameters $m_1, \ldots, m_r, m_T$, given in the Tables T23 to T48, will be made clear in the next sections.

2. THE CASES "QUADRATIC = CUBIC"

In this section we shall prove the Theorems B23, B26, B34 and B46, and thus also Theorems A23, A26, A34 and A46. We start by giving in Table 2 some data on the elliptic curves defined by (W23), (W26), (W34) and (W46), namely the minimal discriminant Δ, the j-invariant j, and the torsion group. These data are easy to compute, e.g. with Apecs.

Further we need the rank r, and a basis $P_1, \ldots, P_r$ for the free part of the Mordell-Weil group. This is more difficult, but can be done. We have the following result.

Proposition 1. *The elliptic curves* (W23), (W26), (W34) *and* (W46) *have ranks* r *and bases* $P_1, \ldots, P_r$ *for the free parts of their Mordell-Weil groups as in Table* 3.

Proof of Proposition 1. We used J.E. Cremona's program mwrank (dated 21 February 1997, see [Cr]) on a Sun Sparcstation 4 to compute (unconditionally) the ranks and the Mordell-Weil groups of the four curves. During execution no unusual events occurred.

Briefly, what the program does is this. First a 2-descent is carried out in order to determine a basis for the quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$. What might go wrong – but it didn't in these four cases – is that one of the relevant homogeneous spaces to

TABLE 2. Data of elliptic curves

curve	Δ	j	torsion
(W23)	$-130491 = -3^6 \cdot 179$	$-110592/179 = -2^{12} \cdot 3^3 \cdot 179^{-1}$	trivial
(W26)	$-732796875 = -3^5 \cdot 5^6 \cdot 193$	$-1404928/46899 = -2^{12} \cdot 3^{-5} \cdot 7^3 \cdot 193^{-1}$	trivial
(W34)	37	$110592/37 = 2^{12} \cdot 3^3 \cdot 37^{-1}$	trivial
(W46)	$-35299546875 = -3^7 \cdot 5^6 \cdot 1033$	$-1404928/3099 = -2^{12} \cdot 3^{-1} \cdot 7^3 \cdot 1033^{-1}$	trivial

TABLE 3. Ranks and bases of Mordell-Weil groups

curve	r	P_1	P_2	P_3
(W23)	2	$(0, 4)$	$(3, 4)$	
(W26)	2	$(-7, 37)$	$(8, 37)$	
(W34)	1	$(0, 0)$		
(W46)	3	$(25, 112)$	$(-20, 112)$	$(70, 562)$

TABLE 4. Relevant constants on heights of basis points

curve	(W23)	(W26)	(W34)	(W46)
B	0.3027	0.6939	0.0256	1.561
H	6.530	9.152	4.832	11.30
runtime	3s	14s	2s	7m 26s

be searched for rational points happens to be locally solvable at all primes, without any actual rational point being detected. A successful 2-descent should determine the rank of the curve. Next, an infinite descent has to be done. The purpose of this is to obtain a basis for $E(\mathbb{Q})$, given a basis for $E(\mathbb{Q})/mE(\mathbb{Q})$ for some $m \geq 2$. Here always $m = 2$. To this end usually Zagier's theorem [Sik, Theorem 1.1] is used: if the set

$$S(B) := \{P \in E(\mathbb{Q}) \mid \hat{h}(P) \leq B\}$$

contains a complete set of coset representatives for $mE(\mathbb{Q})$ in $E(\mathbb{Q})$, then $S(B)$ generates $E(\mathbb{Q})$. Here $\hat{h}$ is the Néron-Tate height function. For the successful application of Zagier's theorem it is important that B is not too large. The relevant B-values for our curves are rather small, see Table 4.

Finally, the inequality

$$\frac{1}{2}h(P) - \hat{h}(P) \leq \text{Hdif} \qquad \text{for all } P \in E(\mathbb{Q}),$$

where Hdif is Siksek's [Sik] or Silverman's [Sil2] bound, whichever proves to be smaller, gives an upper bound

$$h(P) \leq 2B + 2\text{Hdif} =: H$$

for the naive height $h(P)$ for all $P \in S(B)$. These bounds, given in Table 4, are not too large, so that a direct search does not cause any problems. We also give runtimes on a Sun Sparcstation 4 in Table 4.   □

Note that Cremona and Siksek use a canonical height function $\hat{h}$ which is twice the height function used in [ST1]. Also Apecs uses the latter. Here we shall adopt the convention of [ST1].

Further we remark that by a unimodular transformation we arranged the bases such that the least eigenvalue of the Néron-Tate height pairing matrix, called c_1 below, is as large as possible, see [ST2]. This is of importance for an optimal result of the reduction procedure described below.

To prove Theorems B23, B26, B34 and B46, we use the method of linear forms in elliptic logarithms. We closely follow Stroeker and Tzanakis [ST1], from which paper we also adopt the notation. The proofs are very much a routine matter, taking only a few seconds of runtime on a personal computer.

TABLE 5. Relevant constants from [ST1]

curve	(W23)	(W26)	(W34)	(W46)
$(a_1, a_2, a_3, a_4, a_6)$	$(0,0,1,-9,20)$	$(0,1,1,-58,1294)$	$(0,0,1,-1,0)$	$(0,0,1,-525,10156)$
(u,v,w,z)	$(1,0,0,-\frac{1}{2})$	$(1,-\frac{1}{3},0,-\frac{1}{2})$	$(1,0,0,-\frac{1}{2})$	$(1,0,0,-\frac{1}{2})$
(a,b)	$(-9,\frac{81}{4})$	$(-\frac{175}{3},\frac{141875}{108})$	$(-1,\frac{1}{4})$	$(-525,\frac{40625}{4})$
γ	$-3.78765\ldots$	$-12.7143\ldots$	$0.837565\ldots$	$-29.4862\ldots$
$\hat{h}(P_1)$	$0.170261\ldots$	$0.224280\ldots$	$0.0255557\ldots$	$0.321316\ldots$
$\hat{h}(P_2)$	$0.202708\ldots$	$0.213613\ldots$		$0.374043\ldots$
$\hat{h}(P_3)$				$0.703410\ldots$
c_1	$0.147776\ldots$	$0.122596\ldots$	$0.0255557\ldots$	$0.210864\ldots$
c_2	$7.57530\ldots$	$25.4286\ldots$	$2.21431\ldots$	$58.9725\ldots$
X_0	8	26	3	59
c_3	$0.902545\ldots$	$2.21110\ldots$	$1.97333\ldots$	$2.63185\ldots$
ω	$5.89947\ldots$	$2.67273\ldots$	$5.98691\ldots$	$2.06023\ldots$
$\Im\tau$	$0.739959\ldots$	$0.820738\ldots$	$1.22112\ldots$	$0.751930\ldots$
$\phi(P_1)$	$0.347573\ldots$	$0.401475\ldots$	$0.189458\ldots$	$0.202441\ldots$
$\phi(P_2)$	$0.206446\ldots$	$0.246042\ldots$		$0.429501\ldots$
$\phi(P_3)$				$0.117061\ldots$
u_1	$2.05050\ldots$	$1.073036\ldots$	$1.13427\ldots$	$0.417077\ldots$
u_2	$1.21792\ldots$	$0.657605\ldots$		$0.884874\ldots$
u_3				$0.241173\ldots$
h_E	$11.6136\ldots$	$14.1554\ldots$	$11.6136\ldots$	$14.1554\ldots$
A_0	$42.6087\ldots$	$36.0874\ldots$	$11.6136\ldots$	$41.5942\ldots$
A_1	$11.6136\ldots$	$14.1554\ldots$	$11.6136\ldots$	$14.1554\ldots$
A_2	$11.6136\ldots$	$14.1554\ldots$		$14.1554\ldots$
A_3				$14.1554\ldots$
c_4	$3.60535\ldots \times 10^{73}$	$4.53651\ldots \times 10^{73}$	$4.81455\ldots \times 10^{43}$	$8.46092\ldots \times 10^{110}$
$\mathcal{E}$	e	e	e	e
c_5	1	1	1	1
c_6	$12.6136\ldots$	$15.1554\ldots$	$12.6136\ldots$	$15.1554\ldots$
c_7	$1.724397\ldots$	$1.724397\ldots$	1.0625	$2.11944\ldots$
c_8	$12.8748\ldots$	$15.4167\ldots$	$12.6361\ldots$	$15.5592\ldots$
M_0	4.62556×10^{40}	7.50381×10^{40}	2.28469×10^{25}	1.42762×10^{60}

For an integral point we write $P = m_1 P_1 + \ldots + m_r P_r$, where $P_1, \ldots, P_r$ is the basis from Table 3. We write $M = \max\limits_{1 \leq i \leq r} |m_i|$. We omit most of the details of the method, as we do not want to repeat the material of the paper [ST1]. Let us just say that the linear form in elliptic logarithms has the shape

$$L(P) = m_0\omega + m_1 u_1 + \ldots + m_r u_r,$$

where $u_i = \omega\phi(P_i)$ are the elliptic logarithms. Here $m_0 \in \mathbb{Z}$ is taken such that all ϕ-values are in $[0,1)$. It follows that $\max\{M, |m_0|\} \leq rM$.

On the one hand we have an upper bound for this linear form:

$$(2) \qquad\qquad |L(P)| < 4\sqrt{2}e^{c_3 - c_1 M^2},$$

where the constants are defined in [ST1]; their values and other particulars of our equations are given in Table 5. For the calculation of c_3 the Siksek bound [Sik] was used.

On the other hand the main result by David [D] on linear forms in elliptic logarithms plays an essential rôle, as it provides a lower bound for the linear form:

$$|L(P)| > \exp\left(-c_4(\log(M) + c_7)(\log\log(M) + c_8)^{r+2}\right).$$

Together with (2) this yields an absolute upper bound M_0 for M.

The calculations for Table 5 were performed with Apecs 4.2, and required negligible runtime.

TABLE 6. Data of the reduction steps

curve	M_0	C	$d >$	M_1	C	$d >$	M_2	C	$d >$	M_3
(W23)	4.62556×10^{40}	10^{123}	1.62319×10^{41}	36	10^6	121.136	9	10^4	31.8904	7
(W26)	7.50381×10^{40}	10^{124}	2.22699×10^{41}	39	10^6	138.701	10	10^5	52.9622	9
(W34)	2.28469×10^{25}	10^{51}	7.58375×10^{25}	49	10^4	110.788	18	10^3	61.4003	16
(W46)	1.42762×10^{60}	10^{243}	5.88376×10^{60}	44	10^9	164.322	10	10^7	36.9323	9

To reduce the large upper bound M_0, we apply lattice base reduction to the lattice spanned by the columns of the matrix

$$\mathcal{A} = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ [Cu_1] & [Cu_2] & \ldots & [Cu_r] & [C\omega] \end{pmatrix},$$

where C is a large constant, of the size of M_0^{r+1}, and where $[\cdot]$ denotes rounding to the nearest integer. For a possible solution of our elliptic equation we look at the lattice point

$$\mathcal{A}(m_1, \ldots, m_r, m_0)^\top = (m_1, \ldots, m_r, \lambda)^\top,$$

where λ thus is a good approximation to $CL(P)$, viz.

$$|\lambda - CL(P)| \leq \frac{1}{2}(rM_0 + |m_0|) \leq rM_0.$$

We applied Zagier's algorithm for computing the values of $\phi(P_i)$ to the desired precision (of somewhat more than $(r+1)\log_{10} M_0$ decimal digits). For each of the four lattices we computed a reduced basis by the LLL-algorithm. These computations were done by Pari 1.39.

From the reduced basis we find a lower bound d for the length of the shortest nonzero lattice vector. We may assume that d is large enough. If it isn't, then we have to try a larger value of C. We find that either $m_1 = \ldots = m_r = 0$, or

$$|\lambda| \geq \sqrt{d^2 - m_1^2 - \ldots - m_r^2} \geq \sqrt{d^2 - rM_0^2},$$

and thus

$$|L(P)| \geq \frac{1}{C}\left(\sqrt{d^2 - rM_0^2} - rM_0\right).$$

Together with inequality (2) this yields a reduced upper bound M_1 for M, namely

$$M_1 = \left\lfloor \sqrt{\frac{1}{c_1}\left(\log\left(4\sqrt{2}C\right) + c_3 - \log\left(\sqrt{d^2 - rM_0^2} - rM_0\right)\right)} \right\rfloor.$$

Iterating the procedure, we reduced M_1 further to M_2 and finally to M_3. In Table 6 we list the values for C that we chose, the values for d that follow from the application of the LLL-algorithm, and the reduced upper bounds M_1, M_2, M_3 for M.

We checked all points P corresponding to r-tuples $(m_1, \ldots, m_r)$ with $M \leq M_3$ for being solutions to inequality (2). The solutions thus found we checked for integrality of the coordinates X, Y of P. These computations we again did in

TABLE 7. Runtimes

curve	comput. of $\phi(P_i)$	reduction	small solut.
(W23)	3s	< 1s	6s
(W26)	3s	< 1s	10s
(W34)	< 1s	< 1s	1s
(W46)	25s	8s	4m 28s

Apecs. This produced the results mentioned above, and thus completes our proof. Finally we give in Table 7 the runtimes on a Pentium 75Mhz personal computer.

3. The cases "quadratic = quartic"

In this section we prove Theorems B24, B28 and B48, and thus also Theorems A24, A28 and A48. We use the method of linear forms in elliptic logarithms. We follow Tzanakis [T], but at certain points use slight variations in the arguments. The proofs are to some extent a routine matter, but now things are essentially more complicated than in the previous section. We start by giving some information on the elliptic curves represented by the equations (Q24), (Q28) and (Q48).

The birational transformations

$$\begin{cases} U = \frac{6X_1 - 18}{X_1 + Y_1 - 17}, \\ V = \frac{-27X_1^2 + 3Y_1^2 + 882X_1 + 84Y_1 - 4167}{(X_1 + Y_1 - 17)^2}, \end{cases} \qquad \begin{cases} X_1 = \frac{-U^2 - 6U + 6V + 18}{U^2}, \\ Y_1 = \frac{18U^3 - 18U^2 - 6UV - 54U + 36V + 108}{U^3} \end{cases}$$

relate equation (Q24) and the minimal model

$$(W24) \qquad\qquad\qquad Y_1^2 = X_1^3 - 147X_1 + 610.$$

The birational transformations

$$\begin{cases} U = \frac{210X_1 + 130410}{3X_1 + Y_1 + 35805}, \\ V = \frac{195615X_1^2 + 105Y_1^2 + 340341750X_1 - 7127820Y_1 - 226983637125}{(3X_1 + Y_1 + 35805)^2}, \end{cases}$$

$$\begin{cases} X_1 = \frac{315U^2 - 630U + 210V + 22050}{U^2}, \\ Y_1 = \frac{-36750U^3 + 198450U^2 - 630UV - 198450U + 44100V + 4630500}{U^3} \end{cases}$$

relate equation (Q28) and the minimal model

$$(W28) \qquad\qquad Y_1^2 = X_1^3 - 1620675X_1 + 385103250.$$

TABLE 8. Data of elliptic curves

curve	Δ	j	torsion
(W24)	$42550272 =$ $2^{10} \cdot 3^7 \cdot 19$	$470596/57 =$ $2^2 \cdot 3^{-1} \cdot 7^6 \cdot 19^{-1}$	$\mathbb{Z}/2\mathbb{Z} = \langle T \rangle,$ $T = (5, 0)$
(W28)	$208370506291920000000 =$ $2^{10} \cdot 3^7 \cdot 5^7 \cdot 7^6 \cdot 53 \cdot 191$	$114354828/50615 =$ $2^2 \cdot 3^5 \cdot 5^{-1} \cdot 7^6 \cdot 53^{-1} \cdot 191^{-1}$	trivial
(W48)	$999362923039687500 =$ $2^2 \cdot 3^9 \cdot 5^7 \cdot 7^6 \cdot 1381$	$112678587/27620 =$ $2^{-2} \cdot 3^3 \cdot 5^{-1} \cdot 7^3 \cdot 23^3 \cdot 1381^{-1}$	trivial

TABLE 9. Ranks and bases of Mordell-Weil groups

curve	r	P_1	P_2	P_3	P_4	P_5
(W24)	2	$(11, 18)$	$(29, 144)$			
(W28)	5	$(105, 14700)$	$(-1365, 7350)$	$(-315, -29400)$	$(210, 7350)$	$\left(-\frac{4235}{9}, -\frac{872200}{27}\right)$
(W48)	3	$(-236, 11143)$	$(79, 5473)$	$\left(\frac{631}{4}, -\frac{22681}{8}\right)$		

The birational transformations

$$\begin{cases} U = \frac{105X_1 - 18690}{5X_1 + Y_1 - 2403}, \\ V = \frac{-55965X_1^2 + 105X_1Y_1 + 105Y_1^2 + 70087815X_1 + 336420Y_1 - 11480080185}{(5X_1 + Y_1 - 2403)^2}, \end{cases}$$

$$\begin{cases} X_1 = \frac{-157U^2 - 945U + 105V + 11025}{2U^2}, \\ Y_1 = \frac{5591U^3 - 49140U^2 - 525UV - 154350U + 11025V + 1157625}{2U^3} \end{cases}$$

relate equation (Q48) and the minimal model

(W48) $Y_1^2 + X_1Y_1 = X_1^3 - X_1^2 - 332817X_1 + 56191841.$

In Table 8 some data on these elliptic curves are given, namely the minimal discriminant Δ, the j-invariant j, and the torsion group. In the case of nontrivial torsion generators of the torsion group are given.

Further we need the rank r, and a basis $P_1, \dots, P_r$ for the free part of the Mordell-Weil group. We have the following result. In the sequel coordinates of points on the elliptic curves are given for the minimal models (W24), (W28) and (W48), unless explicitly stated otherwise.

Proposition 2. *The elliptic curves* (W24), (W28) *and* (W48) *have ranks r and bases $P_1, \dots, P_r$ for the free parts of their Mordell-Weil groups as in Table 9.*

Proof of Proposition 2. Again we use Cremona's mwrank. No difficulties were encountered with (W24). But with (W28) and (W48) mwrank ran into trouble, as the upper bounds H the program computed for these curves turned out to be too large. Table 10 gives the relevant values found by mwrank, where the runtimes on a Sun Sparcstation 4 for (W28) and (W48) reflect the time it took mrank (without 'w') to compute a set of representatives for $E(\mathbb{Q})/2E(\mathbb{Q})$.

Starting from here, we calculated by hand improved sets of representatives resulting in much better values for B. The bounds H on the logarithmic height so obtained appear to be small enough for Cremona's findinf to run successfully. This is true for (W48), but in the case of (W28) findinf produces erroneous results like points not on the curve, or it overlooks existing relations between points. John

TABLE 10. Relevant constants on heights of basis points

curve	(W24)	(W28)	(W48)
B	0.8105	5.117	2.734
H	9.063	22.79	17.93
runtime	13s	6h 54m	75h 9m

TABLE 11. Relevant constants on heights of basis points

curve	(W28)	(W48)
B	3.199	1.711
H	16.265	12.634
runtime (findinf)	$\approx$ 2 weeks	2h

Cremona told us that these errors are most likely due to roundoff. We give the improved values for B and H in Table 11. Here the runtime given in the case of (W28) is the expected total runtime for a hypothetically completely succesful run of the program findinf, estimated from the amount of work it had completed when it ran into serious trouble.

In the case of (W28) we use the sieving technique described in [Sik, section 4.1]. As a result of the 2-descent, we know that the points P_i ($i = 1, \ldots, 5$) of Table 9 generate a subgroup of odd index m in $E(\mathbb{Q})$.

First we have to find an upper bound for m. This we do by [Sik, Theorem 3.1]. To compute λ such that $\hat{h}(Q) \leq \lambda$ has no solutions $Q \in E(\mathbb{Q})$ other than the point at infinity, we try to show that there are no such points with $\hat{h}(Q) < \hat{h}(P_3) = 0.794302\ldots$. Because Siksek's upper bound for $\frac{1}{2}h(Q) - \hat{h}(Q)$ is Hdif $= 4.93332\ldots$, we search, using Cremona's findinf, for the points with $h(Q) < 2(\hat{h}(P_3) + \text{Hdif}) < 11.4553$. This search took 13 minutes and 40 seconds on a Sun Sparcstation 4, and revealed that there are no points Q with $\hat{h}(Q) \leq \lambda = 0.794302$.

The regulator of $P_1, \ldots, P_5$ is $R = 28.3648\ldots$. Now [Sik, Theorem 3.1] tells us that

$$m \leq \left(\frac{8R}{(2\lambda)^5} \right)^{1/2} = 4.73582\ldots,$$

so that $m \leq 3$. Note that Siksek uses twice our height.

Now we start the sieving, to show that $m \neq 3$. Let

$$V_3 = \{(a_1, \ldots, a_5) \mid a_i \in \{-1, 0, 1\}, a_1 P_1 + \ldots + a_5 P_5 \in 3E(\mathbb{Q})\}.$$

As $m = 3$ implies the existence of a nonzero element of V_3, we intend to show that $V_3 = \{(0, 0, 0, 0, 0)\}$.

Let v be a prime of good reduction, such that $\#E(\mathbb{F}_v)$ is divisible by 3, but not by 9. Put $\ell = \frac{1}{3}\#E(\mathbb{F}_v)$. Then the group $\ell E(\mathbb{F}_v)$ has order 3. Compute a generator G of this group, and compute $m_1, \ldots, m_5 \in \{-1, 0, 1\}$ such that $\ell P_i \equiv m_i G \pmod{v}$. Now, if $(a_1, \ldots, a_5) \in V_3$, then $\ell(a_1 P_1 + \ldots + a_5 P_5) \in 3\ell E(\mathbb{Q})$, so that

$$(m_1 a_1 + \ldots + m_5 a_5)G \equiv a_1 \ell P_1 + \ldots + a_5 \ell P_5 \equiv 0 \pmod{v}.$$

TABLE 12. Relations found in Siksek sieving

v	ℓ	G	m_1	m_2	m_3	m_4	m_5
11	5	$5P_1$	1	0	1	1	1
17	7	$7P_1$	1	0	1	-1	-1
23	10	$10P_1$	1	-1	-1	1	-1
31	11	$11P_1$	1	1	0	-1	1
43	16	$16P_2$	0	1	-1	1	-1
47	20	$20P_2$	0	1	-1	-1	0
59	20	$20P_1$	1	1	1	0	1

As G generates a group of order 3 in $E(\mathbb{F}_v)$, we find that

$$m_1a_1 + \ldots + m_5a_5 \equiv 0 \pmod{3},$$

which constitutes a relation on the a_i.

We do the above computation for a number of primes v, to find as many independent relations as needed or as possible. It turned out that seven primes, starting from the smallest, is a sufficient number in our situation to find 5 independent relations, thus proving that $V_3 = \{(0,0,0,0,0)\}$. In Table 12 we give the primes v, and for each prime the number ℓ, the generator G, and the relation $m_1, \ldots, m_5$. Note that the 7×5 matrix of the m_i, defined (mod 3), has rank 5 indeed. $\qquad\square$

Again note that each Mordell-Weil basis given is optimal for the least eigenvalue of the Néron-Tate height pairing matrix.

We note that there is some symmetry, namely the irrelevance of the sign of V, that we now describe. We take the point Q as follows:

$$
\begin{array}{llll}
\text{(W24):} & Q = -P_1 + P_2 + T & = & (3, -14) \\
\text{(W28):} & Q = P_1 - P_3 - P_4 & = & (-621, 33942) \\
\text{(W48):} & Q = -P_1 + P_2 - P_3 & = & (178, -1691)
\end{array}
$$

If a point P on the curve has coordinates $U(P), V(P)$ on the quartic model, then we have

$$
\begin{cases}
U(-P + Q) & = & U(P), \\
V(-P + Q) & = & -V(P).
\end{cases}
$$

As $\Delta > 0$, the Weierstrass curve $E(\mathbb{R})$ has a compact component and an infinite component. We denote the infinite component by $E_0(\mathbb{R})$. Since Q is on the compact component, it follows that of the two points $P, -P + Q$ always one is on $E_0(\mathbb{R})$. Thus from now on we may assume without loss of generality that our point P is on the infinite component. In the case of (W24) this implies that P is in the free part of the Mordell-Weil group, i.e. that we can forget about the torsion point.

In the case of equation (W24) there is yet another symmetry:

$$
\begin{cases}
U(P + T) & = & -U(P) - 1, \\
V(P + T) & = & -V(P),
\end{cases}
\qquad
\begin{cases}
U(-P + Q + T) & = & -U(P) - 1, \\
V(-P + Q + T) & = & V(P)
\end{cases}
$$

(note that $Q + T$ is in the free part of the Mordell-Weil group). It follows that in this case we may as well assume without loss of generality that $U \geq 0$.

In Table 14 (later) we give the relevant constants from [T].

For all three of our elliptic curves we have that $x_0 > e_1$, so that $U > U_0$ implies that the point P is on $E_0(\mathbb{R})$. The group $E_0(\mathbb{Q})$ of rational points on this infinite

TABLE 13. Bases of relevant subgroups of Mordell-Weil groups

curve	R_1	R_2	R_3	R_4	R_5
(W24)	$P_1 = (11, 18)$	$P_2 = (29, 144)$			
(W28)	$P_1 + P_4 =$ $(4585, 298900)$	$P_2 + P_4 =$ $(1155, -7350)$	$P_3 + P_4 =$ $(5005, -343000)$	$P_1 + P_2 + P_3 + P_4 =$ $\left(\frac{10990}{9}, \frac{406700}{27}\right)$	$-P_4 + P_5 =$ $(1605, -43800)$
(W48)	$P_1 - P_2 =$ $(2914, 152893)$	$P_1 + P_2 =$ $(464, 993)$	$P_2 - P_3 =$ $(989, 25843)$		

component is a subgroup of $E(\mathbb{Q})$ of index 2. Clearly all that we need is a basis $R_1, \dots, R_r$ for this smaller group only. It's easy to show that we can take this basis as in Table 13. Note that we took these bases such that an optimal least eigenvalue of the Néron-Tate height pairing matrix is obtained.

For the rational point P we now put

$$P = m_1 P_1 + \dots + m_r P_r = m_1' R_1 + \dots + m_r' R_r.$$

For the solutions we give in Tables T24, T28 and T48 the corresponding values of $m_1, \dots m_r$, also for the points not on the infinite component $E_0(\mathbb{R})$. In the case of (Q24) we have $P = m_T T + m_1 P_1 + m_2 P_2$, with $m_T = 0$ if P is on $E_0(\mathbb{R})$, and $m_T = 1$ if P is in the compact component. But as argued above we may assume that P is on $E_0(\mathbb{R})$, i.e. $m_T = 0$. Note that

$$\begin{aligned}
\text{for (Q24):} \quad & m_1' = m_1, m_2' = m_2, \\
\text{for (Q28):} \quad & m_1' = \tfrac{1}{2}(m_1 - m_2 - m_3 + m_4 + m_5), \\
& m_2' = \tfrac{1}{2}(-m_1 + m_2 - m_3 + m_4 + m_5), \\
& m_3' = \tfrac{1}{2}(-m_1 - m_2 + m_3 + m_4 + m_5), \\
& m_4' = \tfrac{1}{2}(m_1 + m_2 + m_3 - m_4 - m_5), m_5' = m_5, \\
\text{for (Q48):} \quad & m_1' = \tfrac{1}{2}(m_1 - m_2 - m_3), \\
& m_2' = \tfrac{1}{2}(m_1 + m_2 + m_3), m_3' = -m_3.
\end{aligned}$$

In any case we put

$$M = \max\{|m_1'|, \dots, |m_r'|\},$$

and we have

$$\phi(P) = m_0' + m_1' \phi(R_1) + \dots + m_r' \phi(R_r),$$

where we take $m_0' \in \mathbb{Z}$ such that $0 \le \phi(P) < 1$. It follows that $|m_0'| \le rM$. An interesting point to notice about (Q24) is that P_0 is not independent of R_1 and R_2. Indeed, we have $2P_0 = -R_1 + R_2$. In terms of ϕ we have

$$2\phi(P_0) = -\phi(R_1) + \phi(R_2) + 1.$$

It follows that we do not have to count with P_0 anymore, when we multiply the linear form by 2 and adapt m_i'. Equally interesting is the fact that in both cases (Q28) and (Q48) a similar relation (over $\mathbb{Q}$) does not exist, or so it seems, at least not with very small coefficients.

We put $u_i = \omega\phi(R_i)$ for $i = 1, \dots, r$, and $u_0 = \omega\phi(P_0)$. Our linear form in elliptic logarithms then is

$$L(P) = m_0'\omega + m_1' u_1 + \dots + m_r' u_r + u_0,$$

for which we have the inequality

$$(3) \qquad\qquad |L(P)| < c_9 e^{\frac{1}{2}c_{10} + c_{11} - c_1 M^2}.$$

On the other hand, in the cases of (Q28) and (Q48), David [D] gives

$$|L(P)| > \exp\left(-c_4 (\log(rM) + c_5)(\log\log(rM) + c_6)^{r+3}\right).$$

But in the case of (Q24) we use

$$2L(P) = (2m_0' + 1) + (2m_1' - 1)u_1 + (2m_2' + 1)u_2$$

instead of $L(P)$ itself, as it has one term less. Then, based on $r = 2$ and the inequality $\max\{|2m_0' + 1|, |2m_1' - 1|, |2m_2' + 1|\} \le 4M + 1$, David [D] gives

$$|2L(P)| > \exp\left(-c_4(\log(4M + 1) + c_5)(\log\log(4M + 1) + c_6)^4\right).$$

Whatever the case may be, together with (3) this yields an absolute upper bound M_0 for M.

In Table 14 we take A_0 corresponding to ω, and A_0' corresponding to u_0. To compute A_0' we had to estimate the Néron-Tate height of the non-rational point P_0. We used $\hat{h}(P) \le c_{11} + \frac{1}{2}h(X_1(P))$, where $h(X)$ is the absolute logarithmic Weil height for the algebraic number X. For computing c_{11} we always used the minimal model. Note that $D \le 2$, since the coordinates of P_0 are quadratic.

The reduction in the case of (Q24) goes just as in the previous section, based on inequality (3), but working with $2L(P)$. We take

$$\mathcal{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ [Cu_1] & [Cu_2] & [C\omega] \end{pmatrix},$$

and we look at the lattice point

$$\mathcal{A}(2m_1' - 1, 2m_2' + 1, 2m_0' + 1)^\top = (2m_1' - 1, 2m_2' + 1, \lambda)^\top,$$

where λ thus is a good approximation to $2CL(P)$, viz.

$$|\lambda - 2CL(P)| \le \frac{1}{2}(2(2M_0 + 1) + 2|m_0'| + 1) \le 4M_0 + \frac{3}{2},$$

because $|m_0| \le 2M_0$. As in the previous section we obtain by (3) a reduced upper bound M_1 for M, namely

$$M_1 = \left\lfloor \sqrt{\frac{1}{c_1}\left(\log(2c_9 C) + \frac{1}{2}c_{10} + c_{11} - \log\left(\sqrt{d^2 - 2(2M_0 + 1)^2} - (4M_0 + \frac{3}{2})\right)\right)} \right\rfloor.$$

In Table 15 we give the data for this reduction.

In the cases (Q28) and (Q48) the reduction procedure is slightly different, because now the linear forms in elliptic logarithms are inhomogeneous. We take the lattice as usual, spanned by the columns of

$$\mathcal{A} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ [Cu_1] & [Cu_2] & \dots & [Cu_r] & [C\omega] \end{pmatrix},$$

and look at the point

$$\mathbf{y} = (0, 0, \dots, 0, -[Cu_0])^\top,$$

TABLE 14. Relevant constants from [T]

curve	(Q24)	(Q28)	(Q48)
$(a, b, c,$ $d, e)$	$(3, 6, -3,$ $-6, 3)$	$(35, -350, 945,$ $-630, 105)$	$(105, 210, -945,$ $-1890, 105)$
$(a_1, a_2, a_3,$ $a_4,$ $a_6)$	$(-2, -4, 36,$ $-108,$ $432)$	$(-6, 936, -73500,$ $-1543500,$ $-1444716000)$	$(-18, -1026, 44100,$ $-4630500,$ $4750893000)$
(A, B)	$(-147, 610)$	$(-1620675,$ $385103250)$	$(-5325075,$ $3590952750)$
(X_1, Y_1)	(x, y)	(x, y)	$(\frac{1}{4}(x+1),$ $\frac{1}{8}(-x+y-1))$
σ	1	-1	1
x_0	$-1 + 6\sqrt{3}$	$315 + 210\sqrt{35}$	$-315 + 210\sqrt{105}$
u_0	0	9.38860	0
e_1	$8.82475\ldots$	$1131.51\ldots$	$1835.35\ldots$
e_2	5	$246.906\ldots$	$755.246\ldots$
e_3	$-13.8247\ldots$	$-1378.42\ldots$	$-2590.60\ldots$
ω	$1.96209\ldots$	$0.160046\ldots$	$0.130311\ldots$
$\Im\tau$	$1.41977\ldots$	$1.14814\ldots$	$1.28813\ldots$
U_0	0	9.38860	0
P_0	$(-1 + 6\sqrt{3},$ $18 - 6\sqrt{3})$	$(315 + 210\sqrt{35},$ $36750 + 630\sqrt{35})$	$(\frac{-157+105\sqrt{105}}{2},$ $\frac{5591-525\sqrt{105}}{2})$
$\hat{h}(R_1)$	$0.202321\ldots$	$1.76131\ldots$	$1.12812\ldots$
$\hat{h}(R_2)$	$0.506291\ldots$	$1.17118\ldots$	$1.00476\ldots$
$\hat{h}(R_3)$		$2.00293\ldots$	$1.52711\ldots$
$\hat{h}(R_4)$		$2.80407\ldots$	
$\hat{h}(R_5)$		$2.10666\ldots$	
c_1	$0.194012\ldots$	$0.612991\ldots$	$0.613916\ldots$
$\phi(R_1)$	$0.352986\ldots$	$0.185963\ldots$	$0.142707\ldots$
$\phi(R_2)$	$0.192459\ldots$	$0.540398\ldots$	$0.469004\ldots$
$\phi(R_3)$		$0.822229\ldots$	$0.252395\ldots$
$\phi(R_4)$		$0.422353\ldots$	
$\phi(R_5)$		$0.664566\ldots$	
$\phi(P_0)$		$0.342498\ldots$	$0.491395\ldots$
c_9	$\frac{1}{3}\sqrt{3} = 0.577350\ldots$	$0.234326\ldots$	0.104791
c_{10}	$\log(10) = 2.30258\ldots$	7.73976	7.71756
c_{11}	$3.28540\ldots$	$5.61238\ldots$	$4.87006\ldots$
$\hat{h}(P_0) \leq$		9.15817	8.00858
u_1	$0.692592\ldots$	$0.0297628\ldots$	$0.0185963\ldots$
u_2	$0.377623\ldots$	$0.0864891\ldots$	$0.0611166\ldots$
u_3		$0.131595\ldots$	$0.0328899\ldots$
u_4		$0.0675963\ldots$	
u_5		$0.106361\ldots$	
u_0		$0.0548158\ldots$	$0.0640343\ldots$
h_E	$13.0617\ldots$	$19.0758\ldots$	$21.3085\ldots$
D	1	2	2
A_0	$13.3810\ldots$	$19.0758\ldots$	$21.3085\ldots$
A_1	$13.0617\ldots$	$19.0758\ldots$	$21.3085\ldots$
A_2	$13.0617\ldots$	$19.0758\ldots$	$21.3085\ldots$
A_3		$19.0758\ldots$	$21.3085\ldots$
A_4		$19.0758\ldots$	
A_5		$19.0758\ldots$	
A_0'		$19.0758\ldots$	$21.3085\ldots$
c_4	1.43221×10^{73}	5.61880×10^{277}	2.07088×10^{160}
c_5	1	$1.69314\ldots$	$1.69314\ldots$
c_6	$14.0617\ldots$	$20.7690\ldots$	$23.0016\ldots$
M_0	2.90912×10^{40}	8.81788×10^{145}	5.88682×10^{85}

which most likely will not be a lattice point. Here the relevant distance d is that between $\mathbf{y}$ and the nearest lattice point, since now λ defined by $\mathcal{A}(m_1', \ldots, m_r', m_0')^\top - \mathbf{y} = (m_1', \ldots, m_r', \lambda)^\top$ is approximately $CL(P)$. To be precise, we have

$$|\lambda - CL(P)| \leq \frac{1}{2}(rM_0 + |m_0'| + 1) \leq rM_0 + \frac{1}{2}.$$

TABLE 15. Data of the reduction steps

curve	M_0	C	$d >$	M_1	C	$d >$	M_2	C	$d >$	M_3
(Q24)	2.90912×10^{40}	10^{125}	2.42146×10^{41}	31	10^7	231.400	9	10^6	83.0301	8
(Q28)	8.81788×10^{145}	10^{883}	9.12503×10^{146}	52	10^{17}	340.506	8	10^{12}	52.0672	7
(Q48)	5.88682×10^{85}	10^{347}	2.66374×10^{86}	31	10^{10}	123.292	6			

TABLE 16. Runtimes

curve	comput. of $\phi(P_i)$	reduction	small solut.
(Q24)	3s	< 1s	5s
(Q28)	20m 8s	16m 56s	2h 20m
(Q48)	1m 2s	21s	3m 43s

With this taken into account, noting that the LLL-algorithm also provides a lower bound for this type of d, and using inequality (3), we get a reduced upper bound M_1 for M, namely

$$M_1 = \left\lfloor \sqrt{\frac{1}{c_1}\left(\log\left(c_9 C\right) + \frac{1}{2}c_{10} + c_{11} - \log\left(\sqrt{d^2 - rM_0^2} - (rM_0 + \frac{1}{2})\right)\right)} \right\rfloor.$$

We have reduction data as in Table 15.

Again it is straightforward to find all solutions below the reduced bounds (although in the rank 5 case this takes some runtime). This completes the proof.

Finally we give in Table 16 the runtimes on a Pentium 75Mhz personal computer.

4. THE CASE "CUBIC = CUBIC"

In this section we prove Theorem B36, and thus also Theorem A36. In order to do this we develop a variant of the elliptic logarithms method. See also [SW], where we hope to describe the method for solving any equation of type

$$s_1 U^3 + s_2 U^2 V + s_3 UV^2 + s_4 V^3 + s_5 U^2 + s_6 UV + s_7 V^2 + s_8 U + s_9 V + s_{10} = 0$$

that represents an elliptic curve. However, here we concentrate on the equation (C36) only, as a first example to gain experience with the method.

The birational transformations

(4) $$\begin{cases} U = \frac{237X+15Y-3375}{5X^2+45X-21Y+4860}, \\ V = \frac{315X-75Y+17415}{5X^2+45X-21Y+4860}, \end{cases} \qquad \begin{cases} X = \frac{45U-75V+300}{5U+V}, \\ Y = \frac{6750U^2+1410V^2+6300U-4740V}{(5U+V)^2} \end{cases}$$

relate equation (C36) and the minimal model

(W36) $$Y^2 = X^3 - 1575X + 52650.$$

See [N] and [Co, Section 1.4] for an algorithm to compute these transformations.

In Table 17 some data on this elliptic curves are given, namely the minimal discriminant Δ, the j-invariant j, and the torsion group.

Further we need the rank r, and a basis $P_1, \dots, P_r$ for the free part of the Mordell-Weil group. We have the following result.

TABLE 17. Data of elliptic curve

curve	Δ	j	torsion
(W36)	$-947466720000 = -2^8 \cdot 3^6 \cdot 5^4 \cdot 8123$	$3704400/8123 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 8123^{-1}$	trivial

TABLE 18. Rank and basis of Mordell-Weil group

curve	r	P_1	P_2	P_3	P_4
(W36)	4	$(-15, 270)$	$(15, 180)$	$(45, 270)$	$(-45, 180)$

TABLE 19. Relevant constants on heights of basis points

curve	(W36)
B	3.927
H	12.73
runtime	1h 27m

Proposition 3. *The elliptic curve* (W36) *has rank* r *and basis* $P_1, \dots, P_r$ *for the free part of its Mordell-Weil group as in Table* 18.

Proof of Proposition 3. Again we use Cremona's mwrank. No difficulties were encountered. We give the constants B and H as well as the runtimes on a Sun Sparcstation 4 in Table 19.   □

Again note that the basis given is optimal for the least eigenvalue of the Néron-Tate height pairing matrix.

We consider a point

$$P = m_1 P_1 + m_2 P_2 + m_3 P_3 + m_4 P_4$$

on the curve, with integral coordinates U, V on (C36). We put

$$M = \max_{1 \le i \le 4} |m_i|.$$

As $\dfrac{dV}{3U^2 - 1}$ and $\dfrac{dX}{Y}$ are two differential forms on the same elliptic curve, there should be a rational relationship. Indeed, a bit of calculation (see the birational transformations (4)) shows that

$$(5) \qquad\qquad \frac{dV}{3U^2 - 1} = -\frac{15}{2} \frac{dX}{Y}.$$

For $(U, V) \in \mathbb{R}^2$ on (C36) with $V \ge 4$, we see that U is a strictly increasing function of V, and likewise for $V \le -1$. See Figure 1.

For each point $(U, V) \in \mathbb{R}^2$ on (C36) with $V \le -1$ or $V \ge 4$ there is a unique point $(X, Y) \in \mathbb{R}^2$ on (W36) with $Y \ge 0$, given by (4). For a point P on the curve we use $(U, V) = (U(P), V(P))$ and $(X, Y) = (X(P); Y(P))$ to denote coordinates on both models. Let $F : (-\infty, -1] \cup [4, \infty) \longrightarrow \mathbb{R}$ be given by

$$F(v) = 15 \frac{3u(v) - 5v + 20}{5u(v) + v},$$

where $u(v)$ is the unique solution to $15u(v)^3 - 15u(v) = v^3 - 4v^2 + 3v$ for the given v. Then $X = F(V)$.
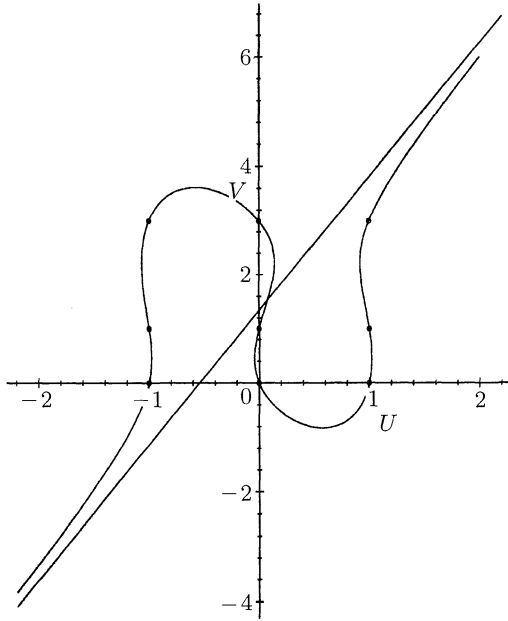
FIGURE 1. The elliptic curve (C36)

For $V \geq 4$ we have by (5) that

$$(6) \qquad \int_V^\infty \frac{dV}{3U^2 - 1} = \frac{15}{2} \int_{X_0}^X \frac{dX}{Y},$$

where

$$X_0 = \lim_{v \to \infty} F(v) = 15 \frac{3 - 5\alpha}{5 + \alpha} = -15\alpha + 3\alpha^2,$$

for $\alpha = \sqrt[3]{15}$. Let $Q_0 = (-15\alpha + 3\alpha^2, -90 + 60\alpha^2)$. Then $Q_0 \in E(\mathbb{K})$, where $\mathbb{K} = \mathbb{Q}(\alpha)$, a cubic field, and $X_0 = X(Q_0)$.

Likewise, for $V \leq -1$ we have by (5) that

$$(7) \qquad \int_{-\infty}^V \frac{dV}{3U^2 - 1} = \frac{15}{2} \int_X^{X_0} \frac{dX}{Y},$$

with X_0 as above. Note that $\alpha U - V + \frac{4}{3} = 0$ is the asymptote of the curve (C36); see Figure 1.

For $\alpha U + \frac{4}{3} > V \geq 4$ or $\alpha U + \frac{4}{3} < V \leq -1$ we have $3U^2 - 1 \geq \left(\frac{4}{45}\alpha - \frac{1}{16} \right) V^2$, so that in the case $V \geq 4$ we have

$$(8) \qquad \int_V^\infty \frac{dV}{3U^2 - 1} \leq c \int_V^\infty \frac{dV}{V^2} = \frac{c}{V},$$

and in the case $V \leq -1$ we have

$$(9) \qquad \int_{-\infty}^V \frac{dV}{3U^2 - 1} \leq c \int_{-\infty}^V \frac{dV}{V^2} = \frac{c}{-V},$$

where $c = \frac{45 \cdot 16}{64\alpha - 45} = 6.38085 \ldots$.

Now consider equation (W36). We have

$$
\begin{aligned}
\int_{X_0}^{X} \frac{dX}{Y} &= \int_{X_0}^{X} \frac{dX}{\sqrt{X^3 - 1575X + 52650}} \\
&= \int_{X_0}^{\infty} \frac{dX}{\sqrt{X^3 - 1575X + 52650}} - \int_{X}^{\infty} \frac{dX}{\sqrt{X^3 - 1575X + 52650}},
\end{aligned}
$$

and note that $X \in \mathbb{Q}$. Further,

$$
\begin{aligned}
\phi(P) &= \phi(m_1 P_1 + m_2 P_2 + m_3 P_3 + m_4 P_4) \\
&= m_1 \phi(P_1) + m_2 \phi(P_2) + m_3 \phi(P_3) + m_4 \phi(P_4) + m_0,
\end{aligned}
$$

with $m_0 \in \mathbb{Z}$ such that all ϕ-values are in $[0,1)$. By (6) it follows in the case $V \geq 4$ that

$$
(10) \quad
\begin{aligned}
\int_{V}^{\infty} \frac{dV}{3U^2 - 1} &= \frac{15}{2} \int_{X_0}^{X} \frac{dX}{Y} = \frac{15}{2} \left(\omega\phi(Q_0) - \omega\phi(P) \right) \\
&= \frac{15}{2} \left(\omega\phi(Q_0) - m_1 \omega\phi(P_1) - \ldots - m_4 \omega\phi(P_4) - m_0\omega \right),
\end{aligned}
$$

where ω is the fundamental real period. Similarly, in the case $V \leq -1$ by (7) we have

$$
(11) \quad
\begin{aligned}
\int_{-\infty}^{V} \frac{dV}{3U^2 - 1} &= -\frac{15}{2} \int_{X_0}^{X} \frac{dX}{Y} \\
&= \frac{15}{2} \left(-\omega\phi(Q_0) + m_1 \omega\phi(P_1) + \ldots + m_4 \omega\phi(P_4) + m_0\omega \right).
\end{aligned}
$$

Put $u_0 = \omega\phi(Q_0)$ and $u_i = \omega\phi(P_i)$ for $i = 1, 2, 3, 4$, and let

$$
L(P) = u_0 - m_1 u_1 - \ldots - m_4 u_4 - m_0 \omega.
$$

Then (8), (9), (10) and (11) imply

$$
(12) \quad |L(P)| = \frac{2}{15} \int_{I} \frac{dV}{3U^2 - 1} \leq \frac{2}{15} \frac{c}{|V|},
$$

with as integration interval $I = [V, \infty)$ if $V \geq 4$, and $I = (-\infty, V]$ if $V \leq -1$.

If $V \geq 6$ then $\alpha U < V < \alpha U + \frac{4}{3}$, and it follows that $X < 0$. Moreover,

$$
15(-3U + 5V - 20) - (5U + V) = 74V - 50U - 300 > \left(74 - \frac{50}{\alpha} \right) V - 300 > 0,
$$

so that the numerator $15(-3U + 5V - 20)$ of $|X|$ is larger than the denominator $5U + V$.

Similarly, if $V \leq -5$ then $\alpha U + \frac{4}{3} < V < \alpha U + \alpha$, and it follows that $X < 0$. Also,

$$
15(3U - 5V + 20) + (5U + V) = -74V + 50U + 300 > \left(\frac{50}{\alpha} - 74 \right) V + 300 > 0,
$$

so that the numerator $15(3U - 5V + 20)$ of $|X|$ is larger than the denominator $-5U - V$.

So if $V \geq 6$ or $V \leq -5$, then for the Weil height of X we find

$$
(13)
$$
$$
\begin{aligned}
h(X) &\leq \log \left(15|3U - 5V + 20| \right) < \log \left(15 \left(\left(5 - \tfrac{3}{\alpha} \right) |V| + \text{sign}(V) \left(\tfrac{4}{\alpha} - 20 \right) \right) \right) \\
&\leq \log \left(135 - \tfrac{57}{\alpha} \right) + \log |V| < 4.71750 + \log |V|.
\end{aligned}
$$

TABLE 20. Relevant constants

curve	(C36)
$\hat{h}(P_1)$	$0.561125\ldots$
$\hat{h}(P_2)$	$0.566020\ldots$
$\hat{h}(P_3)$	$0.578280\ldots$
$\hat{h}(P_4)$	$0.736397\ldots$
$\hat{h}(Q_0) <$	5.66238
c_1	$0.384689\ldots$
$\phi(P_1)$	$0.383460\ldots$
$\phi(P_2)$	$0.298105\ldots$
$\phi(P_3)$	$0.198210\ldots$
$\phi(P_4)$	$0.459223\ldots$

curve	(C36)
$\phi(Q_0)$	$0.392231\ldots$
u_1	$0.600689\ldots$
u_2	$0.466981\ldots$
u_3	$0.310495\ldots$
u_4	$0.719371\ldots$
u_0	$0.614429\ldots$
h_E	$15.1250\ldots$
D	3
A_0	$15.1250\ldots$

curve	(C36)
A_1	$15.1250\ldots$
A_2	$15.1250\ldots$
A_3	$15.1250\ldots$
A_4	$15.1250\ldots$
A_0'	$15.1250\ldots$
c_4	2.79031×10^{216}
c_5	$2.09861\ldots$
c_6	$17.2236\ldots$
M_0	1.75995×10^{114}

It is noteworthy that the above formula is the only point in this proof where we use the fact that U, V are integral.

From Silverman [Sil2] we have

$$(14) \qquad \hat{h}(P) - \frac{1}{2}h(X) < 3.87831,$$

and moreover

$$(15) \qquad \hat{h}(P) \geq c_1 M^2.$$

Putting everything together, we obtain from (12), (13), (14) and (15), under the condition $V \geq 6$ or $V \leq -5$, that

$$(16) \qquad |L(P)| < \frac{2}{15}\frac{c}{|V|} < e^{12.3126 - 2c_1 M^2}$$

Now we apply David's result [D], and obtain

$$|L(P)| > \exp\left(-c_4(\log(4M) + c_5)(\log\log(4M) + c_6)^7\right).$$

Together with (16) this yields an absolute upper bound M_0 for M. We have the data as in Table 20. Note that we used that $|m_0| \leq 4M$.

The reduction procedure runs just as in the previous section for the cases of (Q28) and (Q48), since the linear form also is inhomogeneous in this case. Thus the lattice is spanned by the columns of

$$\mathcal{A} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ [Cu_1] & [Cu_2] & [Cu_3] & [Cu_4] & [C\omega] \end{pmatrix},$$

and d is the distance between the point

$$\mathbf{y} = (0, 0, 0, 0, -[Cu_0])^\top$$

and the nearest lattice point. We have

$$|\lambda - CL(P)| \leq \frac{1}{2}(4M_0 + |m_0'| + 1) \leq 4M_0 + \frac{1}{2},$$

TABLE 21. Data of the reduction steps for (C36)

curve	M_0	C	$d >$	M_1	C	$d >$	M_2
(C36)	1.75995×10^{114}	10^{575}	1.12582×10^{115}	37	10^{13}	265.465	6

TABLE 22. Runtimes

curve	comput. of $\phi(P_i)$	reduction	small solut.
(C36)	4m 38s	2m 44s	9m 19s

and thus, using inequality (16), we reach a reduced upper bound M_1 for M, namely

$$M_1 = \left\lfloor \sqrt{\frac{1}{2c_1}\left(\log C + 12.3126 - \log\left(\sqrt{d^2 - 4M_0^2} - (4M_0 + \frac{1}{2})\right)\right)} \right\rfloor.$$

We have reduction data as in Table 21.

Again it is straightforward to find all solutions below the reduced bound. This completes the proof.

Finally we give in Table 22 the runtimes on a Pentium 75Mhz personal computer.

REFERENCES

[A]   È.T. AVANESOV, "Solution of a problem on figurative numbers" (Russian), *Acta Arithmetica* **12** [1966/67], 409–420. MR **35**:6619

[BC]   A. BAKER AND J. COATES, "Integer points on curves of genus 1", *Proc. Camb. Phil. Soc.* **67** [1970], 595–602. MR **41**:1638

[BH]   YU. F. BILU AND G. HANROT, "Solving superelliptic Diophantine equations by Baker's method", *Compositio Math.* **112** (3) [1998], 223–312.

[Co]   I. CONNELL, *The elliptic curve handbook*, manuscript, 1997. Available from the ftp site of McGill University in the directory math.mcgill.ca/pub/ECH1. From the same site the Apecs package can be downloaded.

[Cr]   J.E. CREMONA, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1992. MR **93m**:11053 The programs mrank, mwrank, findinf may be downloaded from John Cremona's ftp site euclid.ex.ac.uk/pub/cremona.

[D]   S. DAVID, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. France, Vol. 62, 1995. MR **98f**:11078

[F]   G. FALTINGS, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73** [1983], 349–366. MR **85g**:11026a

[GPZ]   J. GEBEL, A. PETHŐ AND H.G. ZIMMER, "Computing integral points on elliptic curves", *Acta Arithmetica* **68** [1994], 171–192. MR **95i**:11020

[L]   D.A. LIND, "The quadratic field $\mathbb{Q}(\sqrt{5})$ and a certain diophantine equation", *Fibonacci Quarterly* **6** [1968], 86–93. MR **38**:112

[M1]   L.J. MORDELL, "On the integer solutions of $y(y+1) = x(x+1)(x+2)$", *Pacific Journal of Mathematics* **13** [1963], 1347–1351. MR **27**:3590

[M2]   L.J. MORDELL, *Diophantine Equations*, Academic Press, London, New York, 1969. MR **40**:2600

[N]   T. NAGELL, "Sur les propriétés arithmétiques des cubiques planes du premier genre", *Acta Mathematica* **52** [1928/9], 93–126.

[P]   Á. PINTÉR, "A note on the diophantine equation $\binom{x}{4} = \binom{y}{2}$", *Publ. Math. Debrecen* **47** [1995], 411–415. MR **96i**:11027

[Sik]   S. SIKSEK, "Infinite descent on elliptic curves", *Rocky Mountain J. Math.* **25** [1995], 1501–1538. MR **97g**:11053

[Sil1] J.H. SILVERMAN *The arithmetic of elliptic curves*, Springer Verlag, Berlin etc., 1986. MR **87g**:11070

[Sil2] J.H. SILVERMAN, "The difference between the Weil height and the canonical height on elliptic curves", *Math. Comput.* **55** [1990], 723–743. MR **91d**:11063

[Sin] D. SINGMASTER, "Repeated binomial coefficients and Fibonacci numbers", *Fibonacci Quarterly* **13** [1975], 295–298. MR **54**:224

[Sm] N.P. SMART, "*S*-integral points on elliptic curves", *Mathematical Proceedings of the Cambridge Philosophical Society* **116** [1994], 391–399. MR **95g**:11050

[ST1] R.J. STROEKER AND N. TZANAKIS, "Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms", *Acta Arithmetica* **67** [1994], 177–196. MR **95m**:11056

[ST2] R.J. STROEKER AND N. TZANAKIS, "On the Elliptic Logarithm Method for Elliptic Diophantine Equations. Reflections and an Improvement", to appear in Experimental Math.

[SW] R.J. STROEKER AND B.M.M. DE WEGER, "Solving Elliptic Diophantine Equations: The General Cubic Case", submitted to Acta Arithmetica.

[T] N. TZANAKIS, "Solving elliptic diophantine equations by estimating linear forms in ellitpic logarithms. The case of quartic equations", *Acta Arithmetica* **75** [1996], 165–190. MR **96m**:11019

[TW] N. TZANAKIS AND B.M.M. DE WEGER, "On the practical solution of the Thue equation", *J. Number Th.* **31** [1989], 99–132. MR **90c**:11018

[dW1] B.M.M. DE WEGER, "A binomial diophantine equation", *Quarterly Journal of Mathematics* **47** [1996], 221–231. MR **97c**:11041

[dW2] B.M.M. DE WEGER, "Equal binomial coefficients: some elementary considerations", *Journal of Number Theory* **63** [1997], 373–386. MR **98b**:11027

ECONOMETRIC INSTITUTE, ERASMUS UNIVERSITY ROTTERDAM, P.O. BOX 1738, 3000 DR ROTTERDAM, THE NETHERLANDS
E-mail address: `stroeker@few.eur.nl`

SPORTSINGEL 30, 2924 XN KRIMPEN AAN DEN IJSSEL, THE NETERLANDS
E-mail address: `deweger@xs4all.nl`