Math. Proc. Camb. Phil. Soc. (1999), **127**, 383
Printed in the United Kingdom © 1999 *Cambridge Philosophical Society*

Computing all S-integral points on elliptic curves

BY ATTILA PETHŐ†
Institut of Mathematics and Informatics, Lajos Kossuth University, H-4010 Debrecen, P.O. Box 12, Hungary

HORST G. ZIMMER, JOSEF GEBEL AND EMANUEL HERRMANN‡
Fachbereich 9 Mathematik, Universität des Saarlandes, Postfach 151150, D-66041 Saarbrücken, Germany

(*Received* 1 *December* 1997; *revised* 23 *September* 1998)

1. *Introduction*

Let the elliptic curve E be defined by the equation

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

with $a_1, \dots, a_6 \in \mathbb{Z}$. Define a finite set of places $S = \{q_1, \dots, q_{s-1}, q_s = \infty\}$ of $\mathbb{Q}$ and put $Q = \max\{q_1, \dots, q_{s-1}\}$. Let $E(\mathbb{Q})$ denote the set of $(x, y) \in \mathbb{Q}^2$ satisfying (1) and the infinite point $\mathcal{O}$.

The multiplicative height of a rational point $P = (x, y) \in E(\mathbb{Q})$ is defined as the following product over all places q of $\mathbb{Q}$ (including $q = \infty$):

$$H(P) = \prod_q \max\{1, |x|_q\},$$

where the $|x|_q$s are the normalized multiplicative absolute values of $\mathbb{Q}$ corresponding to the places q.

Let $E(\mathbb{Z}_S)$ denote the set of S-integral points of $E(\mathbb{Q})$, i.e.

$$E(\mathbb{Z}_S) = \{P = (x, y) \in E(\mathbb{Q}) | H_S(P) \leqslant 1\},$$

where

$$H_S(P) = \prod_{q \notin S} \max\{1, |x|_q\}.$$

Siegel [**21**] proved in 1929 that the number of integral points on an elliptic curve E over an algebraic number field $\mathbb{K}$ is finite and Mahler [**17**] generalized this result in 1934 to S-integral points where S is a set of places defined over $\mathbb{K}$. Moreover, beginning with the pioneering work of Baker [**1**], several authors derived bounds for the size of the coordinates of integer points on elliptic curves E over $\mathbb{K}$. Coates [**4**] proved that $E(\mathbb{Z}_S)$ contains only finitely many elements and that these can be effectively computed. The proofs used algebraic-number theoretical methods; equation (1) was transformed into finitely many S-unit equations.

† Research partially supported by the Hungarian National Foundation for Scientific Research, Grant nos. T25157 and T16975.
‡ Research partially supported by Siemens AG.

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

A completely different method for proving the finiteness of $E(\mathbb{Z}_S)$ was proposed by Lang [**15**] and Zagier [**30**]. Here one makes use of the group structure of $E(\mathbb{Q})$ and invokes properties of ordinary and q-adic elliptic logarithms. After David [**6**] established an explicit lower bound for linear forms in ordinary elliptic logarithms, Lang's idea could be transformed into an algorithm for computing all integer points on elliptic curves. This was done by Gebel, Pethő and Zimmer [**9**] and independently by Stroeker and Tzanakis [**26**]. The algorithm of Gebel, Pethő and Zimmer was implemented by Gebel in the computer algebra package SIMATH and is available free of charge.

Smart [**24**] generalized the above method to an algorithm for finding all S-integral points on elliptic curves over $\mathbb{Q}$. Unfortunately, his approach, which seems to work well in practice, depends on an unproved lower bound for linear forms in q-adic elliptic logarithms. If the rank of $E(\mathbb{Q})$ is at most 2, then such a bound was obtained by Rémond and Urfels [**20**] and applied by Gebel, Pethő and Zimmer [**10**, **11**] to find all S-integral points on Mordell's curves $y^2 = x^3 + k$, with $|k| \leqslant 10^4$ and such that the rank of the curve is strictly less than 3. In this note we combine the advantages of the methods of Siegel–Baker–Coates and of Lang–Zagier to overcome the absence of an explicit lower bound for linear forms in q-adic elliptic logarithms. This was made possible by a recent, completely explicit upper bound for the S-integral solutions of (1) established by Hajdu and Herendi [**14**].

In Section 2 we state our theoretical result and in the subsequent section we prove it. In Section 4 we are dealing with the computational aspects of the main result. Finally we show in Section 7, through an example, how our method works in practice.

2. *Notations and the theorem*

To state our result we require several definitions. Let us start out from an elliptic curve $E(\mathbb{Q})$ in long Weierstraß form (1). Tate's quantities are

$$\begin{aligned} &b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6,\\ &b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\ &c_4 = b_2^2 - 24b_4,\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

E has discriminant

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = -16\Delta_0$$

and absolute invariant

$$j = \frac{c_4^3}{\Delta} = \frac{j_1}{j_2} \quad (j_1, j_2 \in \mathbb{Z},\ \gcd(j_1, j_2) = 1).$$

We remark that equation (1) defines an elliptic curve if and only if $\Delta \neq 0$, which we assume throughout this paper.

The invariant differential of E is

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.$$

Let $P = (x, y) \in E(\mathbb{Q})$. The mapping

$$\varphi(P) = (X, Y) = (36x + 3b_2, 108y + 54a_1x + 54a_3)$$

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

with inverse

$$\varphi^{-1}((X,Y)) = \left(\frac{X-3b_2}{36}, \frac{Y-3a_1X+9a_1b_2-108a_3}{108}\right)$$

is an isomorphism between E and the curve E_1 defined by the equation

$$Y^2 = X^3 - 27c_4X - 54c_6$$

(see e.g. [**22**]). The discriminant Δ_1 of E_1 satisfies

$$\Delta_1 = -2^2 \times 3^9(c_4^3 - c_6^2) = -2^{12} \times 3^{12}\Delta_0.$$

Let $P_1, \ldots, P_r$ denote a basis of the Mordell–Weil group of $E(\mathbb{Q})$ and let g be the order of the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ of $E(\mathbb{Q})$. We have $g \leqslant 12$ by a famous result of Mazur [**19**]. Let $\hat{h}$ denote the Néron–Tate height as well as the associated symmetric bilinear form on $E(\mathbb{Q})$. Designate by λ the smallest eigenvalue of the positive definite regulator matrix $(\hat{h}(P_i, P_j))_{1 \leqslant i,j \leqslant r}$.

Let $\wp(u)$ be the Weierstraß $\wp$-function corresponding to the curve $E_1(\mathbb{C})$. Let $\mathbf{\Omega} = \langle \omega_1, \omega_2 \rangle$ be its fundamental lattice and ω_1 its real period. There exists, for any $P = (x,y) \in E(\mathbb{C})$, an element $u \in \mathbb{C}/\mathbf{\Omega}$ such that $\varphi(P) = (X,Y) = (\wp(u), \frac{1}{2}\wp'(u))$. This u is called the (*complex*) *elliptic logarithm* of P. In the sequel $u_{i,\infty}$ denotes the elliptic logarithm of P_i for $i = 1, \ldots, r$. We put $u'_{i,\infty} = gu_{i,\infty}/\omega_1$.

For a prime q of $\mathbb{Q}$ let $E_0(\mathbb{Q}_q)$ denote the points of $E(\mathbb{Q}_q)$ with non-singular reduction modulo q. If equation (1) is minimal at q, then the index $[E(\mathbb{Q}_q)\colon E_0(\mathbb{Q}_q)]$ is finite and equal to the Tamagawa number c_q. Let further $\tilde{E}$ denote the reduced curve E modulo q. Let $\mathscr{N}_q = \#\tilde{E}(\mathbb{F}_q)$ be the number of rational points on $\tilde{E}/\mathbb{F}_q$. With the order g of the torsion group, we define the number[1]

$$m = m_q = \operatorname{lcm}(g, c_q \cdot \mathscr{N}_q).$$

Finally, for the finite places $q \in S$, let $u'_{i,q}$ denote the q-adic elliptic logarithm of mP_i for $i = 1, \ldots, r$. Now we are in the position to state our main result.

THEOREM. *Let the elliptic curve $E(\mathbb{Q})$ be defined by equation* (1)*, which is minimal at every finite prime $q \in S$. Assume that the S-integral point $P = (x,y) \in E(\mathbb{Z}_S)$ has the representation*

$$P = \sum_{i=1}^{r} n_i P_i + T \tag{2}$$

with $n_i \in \mathbb{Z}$, $i = 1, \ldots, r$ and T a torsion point of $E(\mathbb{Q})$. For $N = \max |n_i| 1 \leqslant i \leqslant r$, we have

$$N \leqslant N_0 = \sqrt{(k_1/2 + k_2)/\lambda}, \tag{3}$$

with

$$k_2 = \log \max\{|b_2|, |b_4|^{\frac{1}{2}}, |b_6|^{\frac{1}{3}}, |b_8|^{\frac{1}{4}}\},$$

$$k_1 = 7 \times 10^{38s+49} s^{20s+15} Q^{24} (\log^* Q)^{4s-2} k_3 (\log k_3)^2 \times ((20s-19)k_3 + \log(ek_4)) + 2\log(2|b_2| + 6),$$

[1] We thank an anonymous referee for pointing out an error in the definition of m in an earlier version of this paper.

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

where $a = \max\{|a_1|, |a_2|\}, \log^* Q = \max\{\log Q, 1\}$ *for* $Q = \max\{q_1, \dots, q_{s-1}\}$,

$$k_3 = \tfrac{32}{3}\sqrt{|\Delta_1|}\left(8 + \tfrac{1}{2}\log|\Delta_1|\right)^4,$$

$$k_4 = 20^4 \max\{3^6 c_4^2, 16\sqrt{|\Delta_1|}^3\}.$$

Moreover, there exists a place $q \in S$ *such that*

$$\left|\sum_{i=1}^{r} n_i u'_{i,q} + n_{r+1}\right|_q \leqslant k_5 \exp\{-(\lambda/s)N^2 + k_2/s\}, \tag{4}$$

with $n_{r+1} \in \mathbb{Z}$ *if* $q = \infty$ *and* $n_{r+1} = 0$ *otherwise, and with* $k_5 = 2g/(3\omega_1)$ *if* $q = \infty$ *and* $k_5 = 1$ *otherwise.*

Remarks

(1) If $r \leqslant 2$, then we can use the estimate of Rémond and Urfels [**20**] for linear forms in q-adic elliptic logarithms to derive an upper bound for N (see [**10**]). The example shown in Section 6 reveals that this bound can be much smaller than our bound N_0.

(2) The proof of the Theorem will show that k_1 can be replaced by any upper bound for the height of S-integer points in $E(\mathbb{Q})$. For example, in the important special case, when $E(\mathbb{Q})$ is defined by the short Weierstraß equation

$$y^2 = x^3 + Ax + B,$$

which is minimal at every finite place $q \in S,\ q \neq 2, 3$ one can take

$$k_3 = k_3^{sh} = \tfrac{32}{3}\sqrt{|\Delta_0|}\left(8 + \tfrac{1}{2}\log|\Delta_0|\right)^4,$$

$$k_4 = k_4^{sh} = 10^4 \max\{16A^2, 256\sqrt{|\Delta_0|}^3\}$$

with $\Delta_0 = 4A^3 + 27B^2$ and k_3^{sh} and k_4^{sh} denote the values for k_3, k_4 on the short Weierstraß equation.

Further, in the case of $s = 1$, one can take the smaller constant

$$k_1' = 5 \times 10^{64} k_3^{sh} \log(k_3^{sh}(k_3^{sh} + \log k_4^{sh}))$$

instead of specializing to $s = 1$ in the formula for k_1 (see [**14**, theorem 1]). Then we obtain

$$N \leqslant N_0' = \sqrt{(k_1'/2 + k_2)/\lambda}$$

instead of (3).

In the case when $s = 1$ and E is given in short Weierstraß form, Gebel, Pethő and Zimmer [**9**][2] as well as Stroeker and Tzanakis [**26**] established another bound for N, namely

$$N \leqslant N_1 = 2^{r+3}\sqrt{k_6 k_7}\log^{(r+3)/2}(k_7(r+3)^{r+3})$$

[2] The constants given here differ from those in [**9**] because in [**9**, pp. 179–180] two corrections are necessary. First r must be replaced by $r + 1$ and second, C requires an adjustment to the new version of the theorem in [**6**].

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

with

$$k_6 = \max\left\{\frac{\log(2\sqrt{2}\sqrt[3]{4}g/\omega_1)}{\lambda}, 1\right\},$$

$$k_7 = \max\left\{\frac{C}{\lambda}, 10^9\right\}\left(\frac{h}{2}\right)^{r+2}\prod_{i=0}^{r}\log V_i,$$

$$C = 2.9\times 10^{6(r+2)}4^{2(r+1)^2}(r+2)^{2r^2+13r+23.3},$$

$$h = \log\max\{4|Aj_2|, 4|Bj_2|, |j_1|\} \quad \text{for } j = \frac{j_1}{j_2},$$
$$j_1, j_2 \in \mathbb{Z},\ \gcd(j_1, j_2) = 1$$

and

$$\log V_i \geqslant \max\left\{\hat{h}(P_i), h, \frac{3\pi|u_{i,\infty}|_\infty^2}{\omega_1^2\ \mathrm{Im}\,\tau}\right\}, \quad i = 1, \ldots, r,$$

$$\log V_0 \geqslant \max\left\{h, \frac{3\pi}{\mathrm{Im}\,\tau}\right\}$$

and

$$\tau = \pm\frac{\omega_1}{\omega_2},$$

where ω_2 is the complex period and the signum is chosen such that $\mathrm{Im}\,\tau > 0$. It seems hard to compare the size of N_0' and N_1 because they depend on different parameters of the curve. The numerical examples of Section 6 suggest that $N_1 \leqslant N_0'$ if $r \leqslant 2$, but $N_1 > N_0'$ if $r > 2$. Therefore, it makes sense to compute both bounds N_0' and N_1 before starting the reduction procedure, which is based on inequality (4) and does not depend on the way by which an upper bound for N was obtained.

3. *Proof of the theorem*

The proof of the theorem is divided into three parts. First we obtain an explicit upper bound for the ordinary additive height $h(P)$ of the S-integral points P in $E(\mathbb{Q})$. In the second part we prove a relation between $h(P)$ and N and derive (3). Finally, we prove (4) by using properties of ordinary and q-adic elliptic logarithms.

3·1. *Estimation of $h(P)$*

Proposition. *Let S be the finite set of rational places (containing the infinite place ∞) defined above. Then all S-integral solutions*

$$(x, y) = \left(\frac{\xi}{\zeta^2}, \frac{\eta}{\zeta^3}\right), \quad \xi, \eta, \zeta \in \mathbb{Z}, \quad \gcd(\xi, \zeta) = 1 = \gcd(\eta, \zeta),$$

of the elliptic diophantine equation

$$Y^2 = X^3 + AX + B, \quad A, B \in \mathbb{Z}, \tag{5}$$

satisfy

$$\log\max\{|\xi|, |\eta|, |\zeta|^3\} \leqslant K_1 = K_1(A, B),$$

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

with

$$K_1 = 7 \times 10^{38s+49} s^{20s+15} Q^{24} (\log^* Q)^{4s-2} k_3^{sh} (\log k_3^{sh})^2 ((20s-19)k_3^{sh} + \log(ek_4^{sh})),$$

where the constants k_3^{sh} *and* k_4^{sh} *are defined in Remark* (2), *after the theorem.*

Proof [**14**, theorem 2].

3·2. *Height estimates and the proof of* (3)

We begin by estimating heights. In the introduction we defined the multiplicative height of a rational point $P = (x, y) \in E(\mathbb{Q})$. The *ordinary additive height* is then

$$h(P) \coloneqq \tfrac{1}{2} \log H(P)$$

and the *Néron–Tate* or *canonical additive height* is

$$\hat{h}(P) \coloneqq \lim_{n\to\infty} \frac{h(2^n P)}{2^{2n}}.$$

From theorem 5 in [**33**] (cf. also [**23**, **31**, **32**]), one readily derives the inequality

$$h(P) \geqslant \hat{h}(P) - k_2 \quad \text{for } P \in E(\mathbb{Q}) \tag{6}$$

with the constant k_2 defined in the theorem.

Let, as before, $P_1, \dots, P_r$ be a basis of the free part of the Mordell–Weil group $E(\mathbb{Q})$. Then $P \in E(\mathbb{Q})$ has the (unique) representation (2) with $n_i \in \mathbb{Z}, i = 1, \dots r$, and T a torsion point. Put $N = \max\{|n_i|, i = 1, \dots, r\}$. The canonical height $\hat{h}$ can be extended to the r-dimensional real vector space $E(\mathbb{Q})/E_{\text{tors}} \otimes_{\mathbb{Z}} \mathbb{R}$ and the extension of $\hat{h}$ is a positive definite quadratic form on this space.

As explained in [**9**], this leads to the lower estimate on non-torsion points

$$\hat{h}(P) \geqslant \lambda N^2$$

involving the smallest eigenvalue λ of the regulator matrix associated with the basis points $P_1, \dots, P_r \in E(\mathbb{Q})$ via the canonical height $\hat{h}$. This, together with (6), implies

$$h(P) \geqslant \lambda N^2 - k_2 \quad \text{for } P \in E(\mathbb{Q}) \setminus E(\mathbb{Q})_{\text{tors}}. \tag{7}$$

Now let $P = (x, y) = (\xi/\zeta^2, \eta/\zeta^3) \in E(\mathbb{Z}_S)$. Then, $\varphi(P) = (X, Y) = (\Xi/\Psi^2, \Sigma/\Psi^3) \in E_1(\mathbb{Z}_S)$ because $a_1, a_3, b_2 \in \mathbb{Z}$. We have

$$\max\{|\Xi|, |\Sigma|, |\Psi|^3\} \leqslant K_1(27c_4, 54c_6)$$

by applying the proposition with $A = -27c_4$ and $B = -54c_6$. As

$$x = \frac{\xi}{\zeta^2} = \frac{\Xi - 3b_2\Psi^2}{36\Psi^2},$$

we obtain

$$\begin{aligned} |\log \max\{|\xi|, |\zeta|^2\} - \log \max\{|\Xi|, |\Psi|^2\}| &\leqslant \log \max\{36, 1 + 3|b_2|\} \\ &\leqslant 2 \log(2|b_2| + 6). \end{aligned}$$

This implies

$$2h(P) = \log \max\{|\xi|, |\zeta|^2\} \leqslant K_1(27c_4, 54c_6) + 2\log(2|b_2| + 6) = k_1.$$

On combining the lower and upper estimates for $h(P)$, we obtain

$$\lambda N^2 - k_2 \leqslant k_1/2.$$

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

This implies the asserted inequality (3):

$$N \leqslant \sqrt{\left(\frac{k_1/2 + k_2}{\lambda}\right)}.$$

3·3. *Elliptic logarithms and the proof of inequality* (4)

Now let $P = (x, y) \in E(\mathbb{Q})$ be an S-integral point and choose $q \in S$ such that

$$|x|_q = \max\{|x|_{q_1}, \ldots, |x|_{q_{s-1}}, |x|_\infty\}. \tag{8}$$

In the sequel we keep this q fixed. First we conclude that

$$H(P) \leqslant |x|_q^s \quad \text{for } s := \sharp S$$

and hence that

$$h(P) \leqslant \frac{s}{2} \log |x|_q. \tag{9}$$

Combining (7) and (9) yields (cf. [**7**])

$$\frac{1}{|x|_q^{\frac{1}{2}}} \leqslant k_8 \exp(-k_9 N^2) \tag{10}$$

with

$$k_8 := \exp\left(\frac{k_2}{s}\right), \quad k_9 := \frac{\lambda}{s}.$$

To transform the upper bound for $|x|_q^{-\frac{1}{2}}$ into the upper bound for the left-hand side of the inequality (4), we must study the properties of elliptic logarithms. Two cases are to be distinguished, the classical case of $q = \infty$ and the q-adic case.

Case 1. $q = \infty \in S$

Let $\wp(u)$ be the Weierstraß function associated to the curve E_1. Let $\mathbf{\Omega} = \langle \omega_1, \omega_2 \rangle$ be the period lattice of $\wp(u)$, generated by the two fundamental periods ω_1 and ω_2, where ω_1 is real and ω_2 is complex. Let $P = (x, y) \in E(\mathbb{Q})$ and denote by $u = u(P)$ its elliptic logarithm, i.e. that residue class $u \in \mathbb{C} \bmod \mathbf{\Omega}$ for which $\varphi(P) = (X, Y) = (\wp(u), \frac{1}{2}\wp'(u))$.

Then we have

$$u \equiv \int_X^\infty \frac{dt}{\sqrt{t^3 - 27c_4 t - 54c_6}} \pmod{\mathbf{\Omega}},$$

or equivalently

$$u \equiv \int_{36x+3b_2}^\infty \frac{dt}{\sqrt{t^3 - 27c_4 - 54c_6}} \pmod{\mathbf{\Omega}}$$

(see [**30**]).

Let

$$t^3 - 27c_4 t - 54c_6 = (t - \alpha)(t - \beta)(t - \gamma)$$

be the decomposition of the cubic polynomial into linear factors with roots

$$\alpha < \beta < \gamma \quad \text{if } \alpha, \beta, \gamma \in \mathbb{R}$$

and

$$\alpha = \bar{\beta} \in \mathbb{C}, \quad \gamma \in \mathbb{R} \text{ otherwise.}$$

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

Define

$$M = \begin{cases} 0, & \text{if } \gamma \geqslant 0 \\ \dfrac{\max\{3|3c_4|^{\frac{1}{2}}, 3|2c_6|^{\frac{1}{3}}\}}{2^{\frac{1}{3}} - 1}, & \text{if } \gamma < 0 \end{cases}$$

and put

$$x_0 = \max\{\alpha + \beta, 2\gamma\} + M.$$

With this notation, we have

LEMMA. *Let $X \in \mathbb{R}$ such that $X > \max\{0, x_0\}$. Then*

$$\int_X^\infty \frac{dt}{\sqrt{t^3 - 27c_4t - 54c_6}} \leqslant \frac{\sqrt{8}}{\sqrt{X}}.$$

Proof [**9**, pp. 176, 181–183]. Note that in [**9**], the number X is assumed to be the first coordinate of an integer point of $E(\mathbb{Q})$, but in the proof this assumption was not needed.

Let now $P = (x, y)$ be an S-integral point on $E(\mathbb{Q})$ with first coordinate of absolute value

$$|x|_\infty \geqslant x_1 := \frac{\max\{0, x_0\} + 6|b_2|}{36} \tag{11}$$

Denote by u its elliptic logarithm. Assume furthermore that (8) holds with $q = \infty$. Then, by the Lemma and by (10), we obtain, on normalizing u to $0 < |u|_\infty \leqslant \omega_1/2$,

$$|u|_\infty \leqslant \frac{2}{3|x|_\infty^{\frac{1}{2}}} \leqslant 2\ k_8\ \exp(-k_9N^2)/3. \tag{12}$$

Let $u_{i,\infty} = u(P_i), i = 1, \ldots, r$, denote the elliptic logarithms of $P_1, \ldots, P_r$. Then

$$u(gP) = u\left(\sum_{i=1}^r n_i(gP_i)\right) = \sum_{i=1}^r n_i(gu_{i,\infty}),$$

where g is the order of the torsion subgroup of $E(\mathbb{Q})$. Moreover, there exists an integer $n_{r+1} \in \mathbb{Z}$ such that

$$|n_1(gu_{1,\infty}) + \cdots + n_r(gu_{r,\infty}) + n_{r+1}\omega_1|_\infty \leqslant 2\ g\ k_8\ \exp(-k_9N^2)/3.$$

Dividing by ω_1 we obtain (4) in the case of $q = \infty$.

Case 2. $q = q_i \in S$ (for some $i \in \mathbb{N}$ such that $1 \leqslant i \leqslant s - 1$).

Here we use q-adic elliptic logarithms (cf. [**7**, **22**, **24**]).

For the convenience of the reader, we explain in some detail how one proceeds in the q-adic case. Let $\mathbb{Q}_q$ be the q-adic completion of $\mathbb{Q}$ and $\mathbb{Z}_q$ be its ring of q-adic integers. Denote by

$$E_0(\mathbb{Q}_q) := \{P \in E(\mathbb{Q}_q) \mid \tilde{P} \text{ is non-singular}\},$$

as well as by

$$E_1(\mathbb{Q}_q) := \{P \in E(\mathbb{Q}_q) \mid \tilde{P} = \tilde{\mathcal{O}}\}$$

the kernel of the reduction map modulo q, where E is regarded as a curve over $\mathbb{Q}_q$

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

and $\tilde{P}$, $\tilde{\mathcal{O}}$ are the reduced points $P, \mathcal{O}$ modulo q. It is known that if E is minimal at q, then $[E(\mathbb{Q}_q)\colon E_0(\mathbb{Q}_q)]$ is finite and equal to the Tamagawa number c_q.

Designate by $\mathscr{E}(q\mathbb{Z}_q)$ the formal group associated to E (cf. [**22**, **24**]). We consider the isomorphism

$$\begin{aligned}\mathscr{E}(q\mathbb{Z}_q) &\longrightarrow E_1(\mathbb{Q}_q)\\ z &\longmapsto \left\{\begin{array}{ll} 0 & \text{if } z = 0\\ \left(\dfrac{z}{w(z)}, -\dfrac{1}{w(z)}\right) & \text{if } z \neq 0\end{array}\right\},\end{aligned}$$

where

$$z = -\frac{x}{y},\ w(z) = -\frac{1}{y}.$$

The equation for $w = w(z)$ inferred from the long Weierstraß equation for $E(\mathbb{Q})$ becomes

$$w = z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3 = f(z, w).$$

A recursive procedure based on this equation (see [**22**]) leads to the power series

$$\begin{aligned} w &= z^3 + a_1 z^4 + (a_1^2 + a_2)z^5 + (a_1^3 + 2a_1 a_2 + a_3)z^6\\ &\quad +(a_1^4 + 3a_1^2 a_2 + 3a_1 a_3 + a_2^2 + a_4)z^7 + \cdots\\ &\in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[z]].\end{aligned}$$

This is the unique power series in z satisfying the relation

$$w(z) = f(z, w(z)).$$

From it we also get the Laurent series for x and y, namely.

$$\left.\begin{aligned} x(z) = \frac{z}{w(z)} &= \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3)z^2 - \cdots,\\ y(z) = -\frac{1}{w(z)} &= -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3)z + \cdots.\end{aligned}\right\} \tag{13}$$

The invariant differential has the expansion

$$\begin{aligned}\omega(z) = (1 + a_1 z + (a_1^2 + a_2)z^2 + (a_1^3 + 2a_1 a_2 + a_3)z^3\\ +(a_1^4 + 3a_1^2 a_2 + 6a_1 a_3 + a_2^2 + 2a_4)z^4 + \cdots)dz.\end{aligned}$$

Note that in these expansions the coefficients of the powers of z each have the same weight depending on the exponent of z.

The q-adic elliptic logarithm is now the image under the homomorphism to the additive group $\hat{G}_a$ (over the completion $\mathbb{C}_q$ of the algebraic closure of $\mathbb{Q}_q$) defined as follows:

$$\begin{aligned}&\psi_q\colon E_1(\mathbb{Q}_q) \longrightarrow \hat{G}_a\\ &P = (x, y) \longmapsto \psi_q(P) = \int \omega(z) = z + \frac{d_2}{2}z^2 + \frac{d_3}{3}z^3 + \cdots.\end{aligned}$$

In particular, the q-adic logarithm ψ_q has the properties

$$\psi_q(P + Q) = \psi_q(P) + \psi_q(Q)$$

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

and

$$|\psi_q(P)|_q = |z|_q = \left|-\frac{x}{y}\right|_q .$$

As before, let $\tilde{E}$ be the reduced curve E modulo q and denote by $\mathscr{N}_q = \sharp\tilde{E}(\mathbb{F}_q)$ the number of rational points on $\tilde{E}/\mathbb{F}_q$. With the number

$$m = m_q = \operatorname{lcm}(g, c_q \cdot \mathscr{N}_q)$$

defined in Section 2, we have from the Lutz filtration of E (see [**16**]):

$$mP_i =: P_i' \in E_1(\mathbb{Q}_q) \quad (i = 1, \dots, r)$$

for the generating points P_i of $E(\mathbb{Q})$ and

$$mP_{r+1} = \mathcal{O}$$

for the torsion points $P_{r+1} \in E(\mathbb{Q})_{\text{tors}}$.

The representation (2) of an S-integral point $P = (x, y) \in E(\mathbb{Q})$ then gives rise to the representation

$$P' = n_1'P_1 + \cdots + n_r'P_r = n_1P_1' + \cdots n_rP_r' \quad (n_i' \coloneqq mn_i \in \mathbb{Z}) \tag{14}$$

of its m-multiple $P' = (x', y') = mP \in E_1(\mathbb{Q}_q)$. In analogy to (13), we have the Laurent series

$$x' = \frac{z'}{w(z')} = \frac{1}{z'^2} - \frac{a_1}{z'} - a_2 - a_3z' - (a_4 + a_1a_3)z'^2 - \cdots ,$$

and this expansion entails the estimate

$$|x'|_q \leqslant \frac{1}{|z'|_q^2} = \frac{1}{|u_q'|_q^2}, \tag{15}$$

where we use the abbreviating notation $u_q' \coloneqq \psi_q(P')$ for the elliptic logarithm of P'.

On combining the inequalities (10) and (15) and observing that $|x'|_q \geqslant |x|_q$, we end up with the upper estimate for the q-adic elliptic logarithm $u_q' = \psi_q(P')$ of the point $P' = (x', y') = mP = m(x, y)$:

$$|u_q'|_q \leqslant \frac{1}{|x'|_q^{\frac{1}{2}}} \leqslant \frac{1}{|x|_q^{\frac{1}{2}}} \leqslant k_8 \exp(-k_9N^2).$$

From (14), we have the relation

$$u_q' = n_1'u_{1,q} + \cdots + n_r'u_{r,q} = n_1u_{1,q}' + \ldots + n_ru_{r,q}' \quad (n_i' = mn_i \in \mathbb{Z})$$

between the elliptic logarithms $u_q' = \psi_q(P')$ of the m-multiple $P' = mP$ of the given S-integral point P, $u_{i,q} = \psi_q(P_i)$ of the generating points P_i and $u_{i,q}' = \psi_q(P_i')$ of their m-multiples $P_i' = mP_i \in E(\mathbb{Q})$; the inequality (4) is therefore proved in this case too.

4. *Computational aspects of the theorem*

The Theorem, together with some computational techniques for elliptic curves and with diophantine approximation methods, in practice makes it possible to compute all S-integral solutions of (1). To this end, we must carry out the following steps.

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

(i) compute a basis $P_1, \dots, P_r$ of the Mordell–Weil group $E(\mathbb{Q})$. This can be achieved, for example, by employing the algorithm [**8**] (see also [**18**, **32**]). Having obtained the basis, one can easily compute the constants k_1, k_2 and λ and thus the upper bound N_0 for N, defined by the inequality (3).

(ii) N_0 is usually very large (see the examples), but we also have the estimate (4) at one of the places $q \in S$. Some observations on the computation of rational approximations of the elliptic logarithms with the necessary very high precision will be made in the next Section. The solutions of the system of inequalities (3) and (4) are then found by the reduction method of de Weger [**28**]. Since this method is well-described in [**24**], we omit the details here. Of course, one must perform de Weger's reduction for all places $q \in S$. Let $\mathscr{M}_q$ denote the bound for N after the reduction with respect to a prime $q \in S$, assuming that (8) holds for some $q \in S$. Then we change the value of N_0 to $\max\{\mathscr{M}_q; q \in S\}$. If possible we iterate the reduction.

(iii) Experience shows that the last value of N_0 obtained after several reductions is sufficiently small in order to enable one to test the points $\sum_{i=1}^{r} n_i P_i + T$ within the range $N = \max\{|n_i|, i = 1, \dots, r\} \leqslant N_0$ and with $T \in E_{\text{tors}}(\mathbb{Q})$ for S-integrality. However, this can be a lengthy procedure. Therefore, we describe here some ideas as to how to proceed in a more economical way. If the r-tuple $\underline{n} = (n_1, \dots, n_r)$ of integer vectors is such that $N = \max\{|n_i|, i = 1, \dots, r\} \leqslant N_0$, then we first test for $q \in S$ by floating point approximation (if $q = \infty$) or by q-adic approximation (if q is a finite place) of $u'_{i,q}$, whether or not (4) is true. If, for an $\underline{n}$, inequality (4) does not hold for some $q \in S$, then there is no S-integral point on the curve given by the vector $\underline{n}$ in the representation (2). Otherwise we must test all linear combinations $\sum_{i=1}^{r} n_i P_i + T$ with varying torsion points T for S-integrality.

(iv) There is one extra search to be carried out eventually. This is due to the fact that, if (8) holds for $q = \infty$, then (12) and (4) hold only for those S-integral points $P = (x, y)$, whose first coordinate satisfies the inequality (11). We must also determine the S-integral points for which (11) is violated. Then, by (8), we have

$$|x|_{q_i} \leqslant x_1, \quad i = 1, \dots, s-1.$$

Write

$$x = \frac{\xi}{q_1^{\alpha_1} \cdots q_{s-1}^{\alpha_{s-1}}} \quad \text{with } \gcd(\xi, q_i) = 1, \quad i = 1, \dots, s-1. \tag{16}$$

This yields

$$|x|_{q_i} = q_i^{\alpha_i},$$

so that

$$\alpha_i \leqslant \log x_1 / \log q_i, \quad i = 1, \dots, s-1. \tag{17}$$

Hence the exponents α_i are bounded. We note that the exponents α_i are even. The negation of inequality (11), together with the boundedness relations (17) for the coordinates (16), shows that there are only finitely many S-integral points, which are to be tested in this case.

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

5. *Computation of the q-adic elliptic logarithms*

The complex elliptic logarithms can be computed either by applying the arithmetic-geometric mean method (see [**5**]) or by employing a method of Zagier [**30**].

In contrast to the case of complex elliptic logarithms, there exists, for the computation of q-adic elliptic logarithms, a quadratically convergent procedure only for Tate curves (see [**13**]).[3] That is why we must apply a different q-adic procedure here. In fact, we simply use the formulae of Section 3. However, we must overcome some technical difficulties if we need to calculate the q-adic elliptic logarithms to a precision of up to 1000 or more digits. Of course, we can compute the formal Laurent series expansion of $w(T)$ by Newton iteration. However, unfortunately the coefficients in this expansion soon become very large. We circumvent this problem by invoking the Lutz filtration of E over $\mathbb{Q}_q$ and calculating q-adic approximations to a sufficient high precision as follows.

Suppose that, for some given positive integer t, we have computed an approximation

$$\tilde{\psi}(T) \coloneqq \sum_{i=1}^{t} \frac{d_i}{i} T^i \equiv \psi(T) \pmod{T^{t+1}}$$

of the formal elliptic integral $\psi(T) = \int w(T)\, dT$, where $d_1 = 1$. We want to compute an approximation $\widehat{\psi_q(P)}$ of the q-adic elliptic logarithm $\psi_q(P)$ of $P \in E_1(\mathbb{Q}_q)$ such that

$$|\psi_q(P) - \widehat{\psi_q(P)}|_q \leqslant q^{-n}$$

for some positive integer n. (In practice, t is fixed and n depends on q and is much larger than t.) Put $V = [n/t]$ and define $P_V = q^V P$. Then we have $P_V \in E_{V+1}(\mathbb{Q}_q)$ by the Lutz filtration theorem [**16**]. Now we can compute a suitable q-adic approximation $\tilde{P}_V$ of the point P_V since E is considered as a curve over $\mathbb{Q}_q$ as in Section 3·3. Here a suitable approximation means that, for the point $P_V = (x_{P_V}, y_{P_V}) \in E(\mathbb{Q}_q)$, we choose $\tilde{P}_V = (\tilde{x}_{P_V}/q^{2(V+1)}, \tilde{y}_{P_V}/q^{3(V+1)})$ with $\tilde{x}_{P_V}, \tilde{y}_{P_V} \in \mathbb{Z}$ such that

$$\left| \frac{x_{P_V}}{y_{P_V}} - \frac{\tilde{x}_{P_V}}{\tilde{y}_{P_V}} q^{V+1} \right|_q \leqslant q^{-n'},$$

with $n' = n + V$. To this end we take $\tilde{z}_{P_V} \in \mathbb{Z}$ such that

$$|\tilde{z}_{P_V}|_q = \left| -\frac{\tilde{x}_{P_V}}{\tilde{y}_{P_V}} q^{V+1} \right|_q \quad \text{and} \quad \left| \tilde{z}_{P_V} + \frac{\tilde{x}_{P_V}}{\tilde{y}_{P_V}} q^{V+1} \right|_q \leqslant q^{-n'}.$$

Then we have

$$\left| \tilde{z}_{P_V} + \frac{x_{P_V}}{y_{P_V}} \right|_q \leqslant q^{-n'},$$

which implies

$$\begin{aligned} \left| \tilde{\psi}(\tilde{z}_{P_V}) - \tilde{\psi}\left(-\frac{x_{P_V}}{y_{P_V}} \right) \right|_q &= \left| \sum_{i=1}^{t} \frac{d_i}{i} \left(\tilde{z}_{P_V}^i - \left(-\frac{x_{P_V}}{y_{P_V}} \right)^i \right) \right|_q \\ &\leqslant \left| \tilde{z}_{P_V} + \frac{x_{P_V}}{y_{P_V}} \right|_q \leqslant q^{-n'}. \end{aligned}$$

[3] We wish to thank J. H. Silverman for calling our attention to the paper [**13**].

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

On the other hand, we have

$$\left|\psi\left(-\frac{x_{P_V}}{y_{P_V}}\right)-\tilde{\psi}\left(-\frac{x_{P_V}}{y_{P_V}}\right)\right|_q=\left|\sum_{i=t+1}^{\infty}\frac{d_i}{i}\left(-\frac{x_{P_V}}{y_{P_V}}\right)^i\right|_q$$

$$\leqslant\left|\frac{d_{t+1}}{t+1}\left(-\frac{x_{P_V}}{y_{P_V}}\right)^{t+1}\right|_q\leqslant\frac{q^{-(t+1)(V+1)}}{|t+1|_q}\leqslant q^{-n'}$$

by the choice of V. Thus

$$\left|\psi\left(-\frac{x_{P_V}}{y_{P_V}}\right)-\tilde{\psi}(\tilde{z}_{P_V})\right|_q\leqslant q^{-n'}.$$

We have

$$\psi\left(-\frac{x_{P_V}}{y_{P_V}}\right)=\psi_q(P_V)=q^V\psi_q(P),$$

hence

$$|\psi_q(P)-\tilde{\psi}(\tilde{z}_{P_V})/q^V|_q\leqslant q^{-n'+V}=q^{-n},$$

i.e. $\tilde{\psi}(\tilde{z}_{P_V})/q^V$ is the required approximation of $\psi_q(P)$, the q-adic elliptic logarithm of P.

6. *Comparison of the theorem with earlier estimates*

We first consider the $S=\{3,5,\infty\}$-integer points of the curve

$$E_{\mathrm{Sm}}(\mathbb{Q})\colon y^2+y=x^3+x^2-2x,$$

treated by Smart [**24**]. He proved that $P_1=(0,0), P_2=(1,0)$ form a basis of the Mordell–Weil group of E_{Sm} over $\mathbb{Q}$ and that E_{Sm} has no non-trivial torsion points. Moreover, he showed that if

$$P=n_1P_1+n_2P_2$$

is an S-integral point on E_{Sm} with $\max\{|n_1|,|n_2|\}\leqslant 10^{40}$, then $\pm(n_1,n_2)=(0,1)$, $(0,2)$, $(0,3)$, $(1,0)$, $(1,1)$, $(1,-1)$, $(1,-4)$, $(2,0)$, $(2,-1)$, $(2,2)$, $(2,-2)$, $(2,-3)$, $(3,0)$, $(3,1)$, $(3,-2)$, $(4,-1)$, $(1,2)$.

As the discriminant of the equation for E_{Sm} is 389, it is minimal at every finite prime q. Thus we may apply the theorem, which implies that

$$N=\max\{|n_1|,|n_2|\}\leqslant N_0=6\times 10^{121},$$

as follows by a simple computation. This bound is much larger then the bound used by Smart. However, by performing one de Weger reduction with this *unconditional* bound, we obtain

$$\max\{|n_1|,|n_2|\}\leqslant 106.$$

This shows that Smart indeed found all S-integral points on E_{Sm}.

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

Table 1

k	r_k	N_1	N_0'
108	1	$2{\cdot}8 \times 10^{26}$	$1{\cdot}8 \times 10^{41}$
225	2	$1{\cdot}3 \times 10^{41}$	$4{\cdot}5 \times 10^{41}$
1 025	3	$5{\cdot}5 \times 10^{60}$	$3{\cdot}1 \times 10^{42}$
2 089	4	$1{\cdot}1 \times 10^{84}$	$7{\cdot}7 \times 10^{42}$
−28 279	5	$2{\cdot}1 \times 10^{112}$	$2{\cdot}0 \times 10^{42}$

Table 2

k	r_k	N_1	N_0'
1	1	$8{\cdot}9 \times 10^{23}$	$1{\cdot}3 \times 10^{41}$
3	2	$5{\cdot}8 \times 10^{39}$	$1{\cdot}8 \times 10^{44}$
7	3	$2{\cdot}4 \times 10^{60}$	$5{\cdot}9 \times 10^{45}$
20	4	$2{\cdot}1 \times 10^{86}$	$2{\cdot}9 \times 10^{47}$

As the rank of E_{Sm} is 2, one can also apply the theorem of Rémond and Urfels [**20**] to estimate N in the way described in [**10**]. Using that method one easily verifies that

$$N \leqslant 4{\cdot}7 \times 10^{41}.$$

Here the worst case appears when $\max\{|u|_3, |u|_5, |u|_\infty\} = |u|_\infty$. This is a much smaller bound for N than the one which follows from the Theorem and hence we obtain another proof that Smart found all S-integral points on E_{Sm}, this time without any further computation.

In Section 2, Remark (2) and thereafter, we gave two different bounds N_0' and N_1 for N in the case of $s = 1$. Now we are going to compare them for some curves, for which all integer points were found by the elliptic logarithm method.

The first set of examples is taken from [**12**], where the classical Mordell equations

$$y^2 = x^3 + k$$

were solved[4] for $|k| \leqslant 10^5$. In Table 1 we list, for some ks, the rank r_k of the curve $y^2 = x^3 + k$ and the values of N_1 and N_0'.

Next, in Table 2, we take some examples from [**2**], where the family of elliptic curves

$$y^2 = x^3 - 36x - 864k(k-1)(2k-1)$$

was considered.

Finally, we consider four curves from [**7**, **9**, **27**] of the form

$$y^2 = x^3 + Ax + B.$$

[4] The rank one cases left open in [**12**] have been settled by Wildanger in his PhD thesis 'Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganzen Punkte einer Mordellschen Kurve' (Berlin 1997). In those cases, the Mordell curves have no integral points – as conjectured by the authors.

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

Table 3

A	B	r	N_1	N_0'
−203 472	18 487 440	5	$2{\cdot}3 \times 10^{111}$	$7{\cdot}9 \times 10^{47}$
−1 642 032	628 747 920	6	$1{\cdot}1 \times 10^{144}$	$2{\cdot}1 \times 10^{49}$
−147 952	21 183 760	7	$2{\cdot}7 \times 10^{187}$	$1{\cdot}1 \times 10^{47}$
−5 818 216 808 130	5 401 285 759 982 786 436	8	$8{\cdot}67 \times 10^{224}$	$2{\cdot}33 \times 10^{58}$

Table 4

i	1	2	3	4
P_i	$(12, 13)$	$(-14, 13)$	$(-1, 26)$	$(38, 221)$
$\psi_3(7P_i)$	$(1, 2, 1, \ldots, 0, 2, 2)$	$(2, 0, 1, \ldots, 2, 1, 2)$	$(1, 1, 0, \ldots, 2, 2, 2)$	$(0, 2, 2, \ldots, 0, 1, 1)$
$\psi_5(10P_i)$	$(3, 0, 4, \ldots, 3, 3, 4)$	$(4, 4, 0, \ldots, 0, 3, 1)$	$(2, 2, 3, \ldots, 3, 3, 0)$	$(4, 3, 4, \ldots, 0, 1, 1)$
$\psi_7(12P_i)$	$(0, 6, 0, \ldots, 2, 3, 4)$	$(5, 2, 5, \ldots, 0, 2, 4)$	$(2, 1, 1, \ldots, 5, 6, 2)$	$(1, 4, 4, \ldots, 1, 2, 1)$

In Table 3 we exhibit, for certain coefficients A, B, the rank r of these curves and the corresponding values of N_1 and N_0'.

The examples indicate that $N_1 < N_0'$, if $r \leqslant 2$, but $N_1 > N_0'$, if $r > 2$. Of course, for rank 0 curves it is quite easy to find all integer points by examining the algebra of the curve. Our comparison shows that N_1 is significantly smaller than N_0' if $r = 1$. For $r = 2$, N_1 and N_0' are of a similar size, but N_1 appears to be slightly smaller than N_0'. For $r \geqslant 3$, the constant N_0' becomes much smaller than N_1 and with growing rank r, the difference becomes rather significant. This can be very well observed in the above rank 7 and 8 examples. The reason for this phenomenon probably lies in the fact that in David's [**6**] lower bound, which enters into the bound N_1, the constant

$$C = 2{\cdot}9 \times 10^{6(r+2)} 4^{2(r+1)^2} (r+2)^{2r^2+13r+23.3}$$

shows up, and this constant depends exponentially on r^2. On the other hand, the constant term of N_0' does not depend on r.

Our examples make it plausible that, in order to find all integer points on elliptic curves, it makes sense to first compute both bounds N_1 and N_0' and then start the reduction procedure with the smaller one.

7. *An example*

To illustrate our method, we choose the rank-four curve

$$E: y^2 = x^3 - 172x + 505 \tag{18}$$

from the paper by Wiman [**29**] (see also Bremner and Tzanakis [**3**]). Wiman showed that there are at least 58 integer points on E. Here we prove that there are exactly 58 integer points and, moreover, 144 S-integer points on E, where $S = \{3, 5, 7, \infty\}$. More precisely, we prove the following theorem.

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

Table 5

S-integral points $P = (x, y) = \left(\frac{\xi}{\zeta^2}, \frac{\eta}{\zeta^3}\right) = \sum_{i=1}^{4} n_i P_i$ on
$E: y^2 = x^3 - 172x + 505$ for $S = \{3, 5, 7, \infty\}$

	Rank . . .	4
	Basis . . .	$P_1 = (12, 13),\ P_2 = (-14, 13),\ P_3 = (-1, 26),\ P_4 = (38, 221)$
	Torsion . . .	trivial

No.	ξ	η	ζ	F	(n_1, n_2, n_3, n_4)
1	−14	13	1		(0, 1, 0, 0)
2	−12	29	1		(0, 0, 1, 1)
3	−10	35	1		(−1, 0, −1, 0)
4	−8	37	1		(0, −1, 0, −1)
5	−2	29	1		(1, 0, −1, 0)
6	−1	26	1		(0, 0, 1, 0)
7	2	13	1		(−1, −1, 0, 0)
8	3	4	1		(−1, 1, 0, 0)
9	12	13	1		(1, 0, 0, 0)
10	14	29	1		(−1, 0, 0, −1)
11	16	43	1		(0, −1, −1, 0)
12	19	64	1		(1, 1, 1, 1)
13	24	101	1		(0, 1, −1, 0)
14	31	158	1		(1, 0, 0, −1)
15	38	221	1		(0, 0, 0, 1)
16	76	653	1		(−2, 0, 0, 0)
17	90	845	1		(0, −1, −1, −1)
18	131	1 492	1		(−1, −1, 1, −1)
19	168	2 171	1		(1, 1, 1, 0)
20	284	4 781	1		(0, −2, 0, 0)
21	415	8 450	1		(2, 0, 0, 1)
22	467	10 088	1		(0, 1, −1, −1)
23	1 046	33 827	1		(1, 0, 2, 1)
24	1 266	45 043	1		(−1, 1, 1, −1)
25	1 314	47 629	1		(−1, 1, −1, 1)
26	3 028	166 621	1		(1, 0, −2, 0)
27	9 502	926 237	1		(−2, −2, 0, −1)
28	11 283	1 198 496	1		(−2, 1, 1, 1)
29	1 402 464	1 660 877 429	1		(0, −3, −1, −2)
30	−128	233	3	3	(−2, −1, 0, 1−)
31	4	559	3	3	(−1, 0, −1, −1)
32	28	1	3	3	(0, 0, 1, −1)
33	106	287	3	3	(−1, 1, 1, 1)
34	160	1 495	3	3	(−1, −1, 1, 0)
35	823	23 374	3	3	(0, 2, 0, 1)
36	11 134	1 174 769	3	3	(−1, −2, −2, −1)
37	33 524 044	194 104 052 639	3	3	(0, 0, 2, −2)
38	−1085	14 680	9	3^2	(−1, 1, 2, 0)
39	−926	22 789	9	3^2	(2, −1, 0, 0)
40	−536	26 819	9	3^2	(−1, −1, 0, 1)
41	4 612	305 227	9	3^2	(−1, 0, −2, 0)
42	2 182	811 433	27	3^3	(−1, −2, −1, −2)
43	14 119	13 113 463	27	3^3	(−1, 2, 0, −1)
44	1 709 021	62 200 333	81	3^4	(2, 0, 2, 1)
45	−181	4 628	5	5	(2, 1, 0, 0)
46	7 824	691 457	5	5	(−2, −1, −1, −2)
47	1 064	33 137	5	5	(2, −1, −1, 0)
48	294	1 303	5	5	(−1, −2, 0, −1)
49	3 314	189 863	5	5	(−1, −1, −1, 1)

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

Table 5 (*cont.*)

No.	ξ	η	ζ	F	(n_1, n_2, n_3, n_4)
50	−324	2 951	5	5	$(1, 0, -1, 1)$
51	1 191	39 614	5	5	$(-1, 0, 2, 1)$
52	346	3 481	5	5	$(1, -1, 1, 1)$
53	−64	3 809	5	5	$(-1, 1, 0, 1)$
54	−7 034	497 861	25	5^2	$(0, 0, -1, -2)$
55	1 754	104 117	25	5^2	$(0, 1, -2, 0)$
56	7 405 599	15 552 621 382	625	5^4	$(1, -2, -2, 1)$
57	334	53 677	15	3×5	$(0, 2, 1, 0)$
58	441 046	292 380 031	45	$3^2 \times 5$	$(3, 0, 0, -1)$
59	−26	12 571	7	7	$(-2, 0, 1, 0)$
60	−657	6 866	7	7	$(-1, -2, -1, 0)$
61	16	7 267	7	7	$(1, -1, 0, 1)$
62	128	2 941	7	7	$(0, 1, 2, 1)$
63	554	811	7	7	$(1, 1, -1, -1)$
64	562	2 197	7	7	$(0, 1, -1, 1)$
65	1 082	29 653	7	7	$(2, -1, -1, -1)$
66	140 260	52 528 645	7	7	$(1, 0, 0, -2)$
67	−33 666	1 488 019	49	7^2	$(0, -2, -1, -2)$
68	−24 097	4 109 846	49	7^2	$(-1, 0, 1, -2)$
69	399 988	252 199 571	49	7^2	$(1, -2, -2, 0)$
70	−2 498	333 593	21	3×7	$(-1, 2, -1, 0)$
71	28 596	4 114 769	35	5×7	$(2, 0, 2, 0)$
72	430 259	157 313 848	175	$5^2 \times 7$	$(-1, 3, 1, 1)$

THEOREM ′. *Let* $S = \{3, 5, 7, \infty\}$. *Then all S-integer points* $P = (x, \pm y)$ *with* $x = \xi/\zeta^2, y = \eta/\zeta^3; \xi, \eta, \zeta \in \mathbb{Z}, \gcd(\xi, \zeta) = \gcd(\eta, \zeta) = 1$ *on* E *over* $\mathbb{Q}$ *are those displayed in Table* 5.

Proof. First we observe that equation (18) is minimal at every finite prime $q \neq 2, 3$. Next we compute the quantities k_1, k_2, k_3 and k_4 of the Theorem in Section 2 to obtain N_0 in dependence on λ only. For this purpose, we do not need any geometrical information about the elliptic curve E. We have $A = -172$ and $B = 505$, hence

$$\Delta_0 = 2\,198\,992, \quad k_2 = 1{\cdot}81, \quad k_3 = 8{\cdot}7 \times 10^8 \quad \text{and} \quad k_4 = 8{\cdot}35 \times 10^{15}.$$

Taking $s = 4$ and $Q = 7$, we obtain

$$k_1 = 4{\cdot}564 \times 10^{305},$$

and this yields

$$N_0 = 4{\cdot}777 \times 10^{152}/\sqrt{\lambda}.$$

Now we consider E as an elliptic curve over $\mathbb{Q}$. Inserting the coefficients of E into SIMATH we obtain, after some minutes of computation, that E has trivial torsion, its rank is 4, and a basis of its Mordell–Weil group is given by the points:

$$P_1 = (12, 13), P_2 = (-14, 13), P_3 = (-1, 26) \quad \text{and} \quad P_4 = (38, 221).$$

The regulator of the curve is $R = 2{\cdot}79\,532$, the real period is $\omega_1 = 0{\cdot}808\,974$ and the least eigenvalue corresponding to the chosen basis is $\lambda = 0{\cdot}7\,467\,531$.

We have $g = 1$, hence $m_q = \mathcal{N}_q$ and the actual values of m_q are $m_3 = 7, m_5 = 10$

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

and $m_7 = 12$. By the Theorem, for each $q \in S$, we have to solve the following diophantine approximation problems

$$\left|\sum_{i=1}^{4} n_i u'_{i,q} + n_{r+1}\right|_q \leqslant \exp\{-0{\cdot}149 \times N^2 + k_{10}\},$$
$$N = \max\{|n_1|, \ldots, |n_4|\} \leqslant N_0 = 5{\cdot}53 \times 10^{152}$$

for each $q \in S$, where $k_{10} = 1{\cdot}62$, if $q = \infty$ and $k_{10} = 0{\cdot}362$ otherwise.

In order to reduce the huge upper bound for N, we first take $q = \infty$ and perform de Weger reduction with $C = 10^{910}$. We obtain the new upper bound $N \leqslant \mathscr{M}_\infty = 69$. Next, for each $q \in S \setminus \{\infty\}$, we compute the q-adic elliptic logarithms of $P_i, i = 1, \ldots, 4$, with precision at least

$$n_3 = 1281, \quad n_5 = 875, \quad n_7 = 723.$$

This precision is necessary in order to carry out the q-adic de Weger reduction. For this purpose, we use the method of Section 5. We have chosen $t = 200$ and, for safety reasons,

$$V_3 = 8, \quad V_5 = 6, \quad V_7 = 5$$

and computed the approximations of $q^{V_q} P_i$ for $q \in \{3, 5, 7\}$ and $i = 1, \ldots, 4$ with

$$n'_3 = 1700, \quad n'_5 = 1300, \quad n'_7 = 1100$$

q-adic digit numbers. In Table 4 we have listed the first and last three significant digits of $\psi_q(m_q P_i)$, i.e., the digits $\delta_2, \delta_3, \delta_4, \delta_{n_{q-2}}, \delta_{n_{q-1}}$ and δ_{n_q} assuming, that

$$\psi_q(m_q P_i) \approx \sum_{i=1}^{n_q} \delta_i q^i.$$

Note that, as $m_q P_i \in E_1(\mathbb{Q})$, we always have $\delta_1 = 0$.

Now we perform the q-adic de Weger reduction with the values $C_3 = 3^{1281}, C_5 = 5^{875}$ and $C_7 = 7^{723}$ and obtain the new bound

$$N_0 = 124 = \max\{\mathscr{M}_\infty, \mathscr{M}_3, \mathscr{M}_5, \mathscr{M}_7\}.$$

This new upper bound for N can be further reduced. On repeating this reduction process 3-times, we eventually get $N \leqslant 17$, which cannot be reduced any further. In order to compute all S-integral solutions of (18) with this last bound, we use the sieving procedure described in [**7**]. Finally, we must also determine the S-integral points for which (11) is violated. In the case under consideration, we have

$$|x|_{q_i} < \max\{0, 22{\cdot}56\}/36 = 0{\cdot}627, \quad i = 1, \ldots, 4, \tag{19}$$

thus $\alpha_2 \leqslant 4$ and $\alpha_3, \alpha_5 \leqslant 2$, where we used the notation of Section 4(iv). A simple computation shows that all the solutions of (18) satisfying the above inequality (19) are among those already found. Theorem′ is proved.

REFERENCES

[**1**] A. BAKER. The diophantine equation $y^2 = ax^3 + bx^2 + cx + d$. *J. London Math. Soc.* **43** (1968), 1–9.

[**2**] A. BREMNER, R. J. STROEKER and N. TZANAKIS. On sums of consecutive squares. *J. Number Theory* **62** (1997), 39–70.

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

[**3**] A. Bremner and N. Tzanakis. Integral points on $y^2 = x^3 - 7x + 10$. *Math. Comp.* **41** (1983), 731–741.

[**4**] J. Coates. An effective p-adic analogue of a theorem of Thue III; the diophantine equation $y^2 = x^3 + k$. *Acta Arith.* **74** (1970), 425–435.

[**5**] H. Cohen. A course in computational algebraic number theory. Graduate Texts in Math., vol. **139** (Springer Verlag, 1993).

[**6**] S. David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France* **62** (N.S.) (1995), 143 pp.

[**7**] J. Gebel. Bestimmung aller ganzen und S-ganzen Punkte auf elliptischen Kurven über den rationalen Zahlen mit Anwendung auf die Mordellschen Kurven. PhD Thesis, Saarbrücken 1996.

[**8**] J. Gebel and H. G. Zimmer. Computing the Mordell–Weil group of an elliptic curve over $\mathbb{Q}$. In *Elliptic curves and related topics* (Eds. H. Kisilevsky and M. Ram Murty). *CRM Proc. and Lect. Notes, Amer. Math. Soc.* (Providence, RI, 1994), pp. 61–83.

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

[**10**] J. Gebel, A. Pethő and H. G. Zimmer. Computing S-integral points on elliptic curves. In Algorithmic Number Theory, Second International Symposium, ANTS-II, Talence, France, May 1996 (Ed. H. Cohen), Lect. Notes in Comp. Sci., vol. **1122** (Springer Verlag, 1996), pp. 157–171.

[**11**] J. Gebel, A. Pethő and H. G. Zimmer. Computing integral points on Mordell's elliptic curves. *Collect. Math.* **48** (1997), 115–136.

[**12**] J. Gebel, A. Pethő and H. G. Zimmer. On Mordell's equation. *Compositio Math.* **110** (3) (1998), 335–367.

[**13**] G. Henniart and J. F. Mestre. Moyenne arithmético-géométrique p-adique. *C. R. Acad. Sci. Paris* (Série I), **308**, (1989), 391–395.

[**14**] L. Hajdu and T. Herendi. Explicit bounds for the solutions of elliptic equations with rational coefficients. *J. Symbolic Comp.* **25** (1998), 361–366.

[**15**] S. Lang. Elliptic curves: diophantine analysis. *Grundl. Math. Wiss.* **231** (Springer-Verlag, 1978).

[**16**] E. Lutz. Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adiques. *J. reine angew. Math.* **177** (1937), 238–244.

[**17**] K. Mahler. Über die rationalen Punkte auf Kurven vom Geschlecht Eins. *J. reine angew. Math.* **170** (1934), 168–178.

[**18**] Yu. I. Manin. Cyclotomic fields and modular curves. *Russian Math. Surveys* **26** (1971), 7–78.

[**19**] B. Mazur. Rational isogenies of prime degree. *Invent. Math.* **44** (1978), 129–162.

[**20**] G. Rémond and F. Urfels. Approximation diophantienne de logarithmes elliptiques p-adiques. *J. Number Theory* **57** (1996), 133–169.

[**21**] C. L. Siegel. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuss. Akad. Wiss.* (1929), 1–41.

[**22**] J. H. Silverman. The arithmetic of elliptic curves. Graduate Texts in Math., vol. **106** (Springer Verlag, 1986).

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

[**24**] N. Smart. S-integral points on elliptic curves. *Math. Proc. Camb. Phil. Soc.* **116** (1994), 391–399.

[**25**] H. M. Stark. Effective estimates of solutions of some Diophantine equations. *Acta Arith.* **24** (1973), 251–259.

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

[**27**] R. J. Stroeker and N. Tzanakis. On the elliptic logarithms method for elliptic diophantine equations. Reflections and an improvement, preprint, 1997.

[**28**] B. M. M. de Weger. Algorithms for diophantine equations. PhD Thesis, Centr. for Wiskunde en Informatica, Amsterdam 1987.

[**29**] A. Wiman. Über die Punkte mit ganzzahligen Koordinaten auf gewissen Kurven dritter Ordnung. 12te Skand. Matematikerkongressen, Lund 1953, pp. 317–323 (1954).

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

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press

[**31**] H. G. ZIMMER. On the difference of the Weil height and the Néron–Tate height. *Math. Z.* **147** (1976), 35–51.

[**32**] H. G. ZIMMER. Generalization of Manin's conditional algorithm. SYMSAC '76. Proc. 1976 ACM Sympos. on Symb. Alg. Comp. (Ed. R. D. Jenks), pp. 285–299. (Yorktown Heights, N.Y., 1976).

[**33**] H. G. ZIMMER. A limit formula for the canonical height of an elliptic curve and its application to height computations. In *Number theory* (Ed. R. A. Mollin), pp. 641–659 (W. de Gruyter, 1990).

https://doi.org/10.1017/S0305004199003916 Published online by Cambridge University Press