Math. Proc. Camb. Phil. Soc. (1994), **116**, 391
Printed in Great Britain

S-integral points on elliptic curves

By N. P. SMART
Department of Computing Mathematics, University of Wales College of Cardiff, Cardiff CF2 4YN, Wales.

(*Received* 23 *July* 1993; *revised* 17 *January* 1994)

In this paper I give an algorithm to find all 'small' S-integral points on an elliptic curve. I would like to thank N. Stephens for suggesting I consider such equations and the Wingate Foundation for supporting me whilst carrying out the research. As is usual $c_1, c_2, \ldots$, will denote positive real constants which are effectively computable.

In [**1**], conditions were given on finding S-integral points on an elliptic curve of the form

$$Y^2 = X^3 - AX - B,$$

where S is the set of primes dividing $\Delta = 16(4A^3 - 27B^2)$. All points were found when the curve had rank one and either no torsion or one torsion point of order two.

In [**12**], various methods were given to find explicitly large integral points on elliptic curves. For curves of rank one it was shown that the continued fraction algorithm could be used to find large integral points. It was also noted that if the rank was greater than one then the L^3 algorithm [**5**] could be used for the same problem. Also it was pointed out that using estimates for linear forms in logarithms all integral points could be found in principle.

This method was adopted in [**7**], where all integral points on two particular elliptic curves were found. These elliptic curves had rank 2 and 3. All integral points were found because of the lower bounds on elliptic logarithms given in [**3**]. As we shall note below there are no known explicit lower bounds on p-adic elliptic logarithms. Thus the following method for finding S-integral points of small height will not guarantee that all such points have been found.

1. *Inequalities between the coordinates of a point and its height*

Let E be the elliptic curve defined over $\mathbb{Q}$, with the model

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \tag{1}$$

where $a_i \in \mathbb{Z}$. We shall consider points $P = (x, y) \in \mathbb{Q}^2$. It will be necessary for our method to assume that we can calculate the Mordell–Weil group

$$E(\mathbb{Q}) = \langle P_1 \rangle \times \cdots \times \langle P_r \rangle \times Tors_{\mathbb{Q}}(E).$$

Let S be a finite set of primes of $\mathbb{Q}$, including ∞. We wish to find all points P on (1) with coordinates in $\mathbb{Z}_S$ where $\mathbb{Z}_S = \{z \in \mathbb{Z} : |z|_v \leqslant 1 \quad \forall v \notin S\}$. Let P be such a point and write $P = q_1 P_1 + \cdots + q_r P_r + T$, where $T \in Tors_{\mathbb{Q}}(E)$. Let $K = \max |q_i|$. We shall assume that we have an upper bound on K, say $K \leqslant K_0$. This assumption would not be necessary if we had an estimate in the p-adic case for linear forms in elliptic

https://doi.org/10.1017/S0305004100072698 Published online by Cambridge University Press

logarithms. Explicit estimates have been given in the real case by David [3], but I do not know of any explicit estimates in the p-adic case. To see how an upper bound on K could be derived from such explicit estimates see [4], chapter VI, section 8.

The following method should reduce the given upper bound K_0 to a new upper bound of size $\sqrt{[(r+1)\ln K_0]}$. This assumes that real (respectively p-adic) elliptic logarithms behave as random real (respectively p-adic) numbers. There is therefore no guarantee that the above reduction will occur. However, we expect, and experience shows, that such a reduction does occur.

Let $H(x(P))$ or $H(P)$ denote the naive height, i.e.

$$H(P) = \prod_v \max(1, |x(P)|_v),$$

where v ranges over the finite and infinite primes of $\mathbb{Q}$. Let $h(P) = \ln H(P)$ and let $\hat{h}(P)$ denote the Néron–Tate height,

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

We also set $b_2 = a_1^2 + 4a_2$. We shall require the following lemma which gives a bound on K in terms of the naive height of the point.

LEMMA 1. *We have* $h(P) \geqslant c_2 K^2 - c_1$.

Proof. By [2, p. 60] we have $h(P) \geqslant \hat{h}(P) - c_1$. Let $R = A^t A$ be the Cholesky decomposition of R, where R is the matrix $R = (\langle P_i, P_j\rangle)$ for

$$\langle P_i, P_j\rangle = \tfrac{1}{2}(\hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j)).$$

By a standard argument for quadratic forms we have $h(P) \geqslant c_2 K^2 - c_1$, where $c_2 = 1/\|A^{-1}\|_2^2$. ∎

Note that in the above lemma we used the normalization of the regulator matrix, R, which is compatible with the Birch and Swinnerton-Dyer conjecture, see [2, p. 55].

Assume v is such that

$$|x(P)|_v = \max_{v_i \in S} |x(P)|_{v_i}.$$

Then for $s = \#S$ we have $H(P) \leqslant |x(P)|_v^s$ and therefore $h(P) \leqslant \ln |x(P)|_v^s$, which gives $(c_2 K^2 - c_1)/s \leqslant \ln |x(P)|_v$. Thus

$$\frac{1}{|x(P)|_v} \leqslant e^{c_1/s - c_2 K^2/s} \leqslant c_3 e^{-c_4 K^2}, \tag{2}$$

where $c_3 = e^{c_1/s}$ and $c_4 = c_2/s$.

As we do not know which v satisfies our assumption we need to consider all possibilities. We have two cases to consider $v = \infty$ or $v = p$, a rational prime.

2. *Case 1:* $v = \infty$

For this section we abbreviate $|\cdot|_\infty$ by $|\cdot|$, remembering that v has been chosen to maximize $|x(P)|_v$. Let $\wp(z)$ be the Weierstrass $\wp$-function, i.e. the solution to

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3,$$

https://doi.org/10.1017/S0305004100072698 Published online by Cambridge University Press

where g_2 and g_3 are calculated as usual from our curve E. This is a doubly periodic function with periods $\omega_1, \omega_2 (\omega_1 \in \mathbb{R}, \omega_1 > 0)$. Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be the period lattice, then we have the map

$$\mathbb{C}/\Lambda \xrightarrow{\phi} E$$

$$z \mapsto \begin{cases} (\wp(z) - b_2/12, (\wp'(z) - a_1 x - a_3)/2)) & z \notin \Lambda \\ \infty & z \in \Lambda \end{cases}.$$

The 'inverse' of this map, after choosing a fundamental region, we shall call the elliptic logarithm, ψ. It is given, see [**6**, Chapter VI], by

$$z_P = \psi(P) = \int_{\infty}^{x+b_2/12} \frac{dt}{\sqrt{(4t^3 - g_2 t - g_3)}} \pmod{\Lambda}.$$

As a fundamental region we take

$$\mathfrak{I} = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{R}, 0 \leqslant a, b < 1\}.$$

From now on ψ will always take its principal value, i.e. $\psi(P) \in \mathfrak{I}$.

Following Zagier[**12**] and Stroeker and Tzanakis[**7**], we shall only use real valued elliptic logarithms by considering the identity component $E^0(\mathbb{R})$. However, one should note that [**7**] a different parametrization was used. We shall use the parametrization given above because one can then use the widely available package GP/PARI to compute the elliptic logarithms. If $P \in E^0(\mathbb{R})$ then $\psi(P) \in \mathbb{R}$, and if a point P is not in $E^0(\mathbb{R})$ then $2P$ is in $E^0(\mathbb{R})$.

For the r generators of $E(\mathbb{Q})$ put

$$Q_i = \begin{cases} P_i & \text{if} \quad P_i \in E^0(\mathbb{R}) \\ 2P_i & \text{otherwise.} \end{cases}$$

Then we can write our S-integral point as

$$P = s_1 Q_1 + \ldots + s_r Q_r + T + U,$$

where U comes from a finite set of points and $|s_i| \leqslant |q_i|$.

Now put $f(t) = 4t^3 - g_2 t - g_3$ and denote its roots by $\gamma_1, \gamma_2, \gamma_3$. Set $c_5 = 2\max(|\gamma_i|)$ and $c_6 = c_5 + b_2/12$. Now if $K \geqslant \sqrt{[\ln(c_3 c_6)/c_4]}$ then, by equation (2), we have $|x(P)| \geqslant c_6$ and therefore $\wp(z_P) \geqslant c_5$. Hence P lies on the identity component, $E^0(\mathbb{R})$. Then $T + U \in E^0(\mathbb{R})$ and we have a linear form in real valued elliptic logarithms given by

$$\psi(P) = \sum_{i=1}^{r} s_i \psi(Q_i) + \psi(U+T) + m\omega_1,$$

where $|m| \leqslant rK + 1 + r$.

Now as $\wp(z_P) \geqslant c_5$, by the proof of Inequality 2 of [**7**] we obtain

$$|z_P| \leqslant \left| \int_{\infty}^{x+b_2/12} \frac{dt}{\sqrt{f(t)}} \right| \leqslant 2\sqrt{2}\,|x + b_2/12|^{-\frac{1}{2}}.$$

As $P \in E^0(\mathbb{R})$ we also have $|z_P| \leqslant |\omega_1|$ and so

$$|z_P|^2 \leqslant \frac{8 + |\omega_1^2 b_2|/12}{|x(P)|} = \frac{c_7}{|x(P)|}.$$

https://doi.org/10.1017/S0305004100072698 Published online by Cambridge University Press

Hence

$$|\psi(P)| \leqslant \sqrt{(c_3 c_7)}\, e^{-c_4 K^2/2} = c_8\, e^{-c_9 K^2}.$$

Suppose we are given a large upper bound, K_0, on K. We shall want to reduce this to a more manageable bound so we can directly enumerate all the possibilities. For this purpose we use the L^3 algorithm [**5**]. The use of this algorithm for the purposes of diophantine approximation has become quite standard and we refer the reader to [**11**] for a general discussion of the philosophy behind the method.

We have, from above, the linear form with real coefficients

$$|s_1 \psi(Q_1) + \cdots + s_r \psi(Q_r) + \psi(T+U) + m\omega_1| \leqslant c_8\, e^{-c_9 K^2},$$

where $|m| \leqslant rK+1+r$. Choose a constant C such that $C \approx K_0^{r+1}$. Define $[x]$, for $x \in \mathbb{R}$, by $|x-[x]| \leqslant \frac{1}{2}$, $[x] \in \mathbb{Z}$. For the points where $[x]$ is non-unique by the above definition, i.e. $n/2$ for n odd, we take the value that is closest to zero. Then set

$$\mathscr{A} = \begin{pmatrix} 1 & & & \\ & \ddots & & \bigcirc \\ \bigcirc & & 1 & \\ [C\psi(Q_1)] & \cdots & [C\psi(Q_r)] & [C\omega_1] \end{pmatrix} \in \mathbb{Z}^{(r+1)^2}.$$

Also for each possible $T+U$ such that $T+U \in E^0(\mathbb{R})$,

$$\underline{y} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -[C\psi(T+U)] \end{pmatrix} \in \mathbb{Z}^{r+1}.$$

Let Γ be the lattice generated by the columns of $\mathscr{A}$. The idea behind the reduction process is that a vector close to $\underline{y}$ in our lattice will correspond to a small value for our linear form. This in turn will correspond to large values for the s_i. Since we wish to show there are no such large values of s_i, we need to show that there is no vector which is close to $\underline{y}$. From [**11**] we can find a lower bound on the shortest distance between a lattice point and $\underline{y}$ using the L^3 reduction algorithm.

We shall assume we have applied the L^3 algorithm [**5**], to $\mathscr{A}$ to obtain a lower bound K_1 on $l(\Gamma, \underline{y})$. Here $l(\Gamma, \underline{y})$ denotes the length of the smallest non-zero vector in the lattice if $\underline{y} = \underline{0}$. Otherwise $l(\Gamma, \underline{y})$ denotes the shortest distance from a lattice point to $\underline{y}$. Since our matrix has integral entries one should use the integral L^3 algorithm given in [**10**].

The following lemma should reduce our large upper bound K_0 to one of size $\sqrt{[(r+1)\ln K_0]}$. If this should fail then a larger constant C should be chosen and the L^3 reduction attempted again.

LEMMA 2. *Let* $c_{10} = (2rK_0+2+r)/2$. *If* $K_1^2 \geqslant c_{10}^2 + rK_0^2$ *then set* $c_{11} = \sqrt{(K_1^2 - rK_0^2)} - c_{10}$ *and if* $Cc_8 \geqslant c_{11}$ *then*

$$K \leqslant \left(\frac{\ln(Cc_8) - \ln(c_{11})}{c_9}\right)^{\frac{1}{2}}.$$

Proof. Consider the lattice point $\underline{x} = \mathscr{A} \begin{pmatrix} q_1 \\ \vdots \\ q_r \\ m_1 \end{pmatrix}$. Then $\underline{x} - \underline{y} = \begin{pmatrix} q_1 \\ \vdots \\ q_r \\ \phi \end{pmatrix}$, where

https://doi.org/10.1017/S0305004100072698 Published online by Cambridge University Press

$\phi = \sum_{i=1}^{r} s_i[C\psi(Q_i)] + [C\psi(T+U)] + m[C\omega_1]$. We can bound $|\phi|$ in terms of K by $|\phi| \leqslant |\phi - C\psi(P)| + |C\psi(P)| \leqslant c_{10} + Cc_8 e^{-c_9 K^2}$. Thus we obtain

$$K_1^2 \leqslant l(\Gamma, \underline{y})^2 \leqslant \sum_{i=1}^{r} q_i^2 + \phi^2 \leqslant rK_0^2 + |\phi|^2$$
$$\leqslant rK_0^2 + (c_{10} + Cc_8 e^{-c_9 K^2})^2.$$

Then, as $Cc_8 \geqslant c_{11}$, we have

$$K^2 \leqslant \frac{1}{c_9}(\ln(Cc_8) - \ln(c_{11})).$$

Hence our new bound follows. ∎

If required, after a reduced bound has been found one can repeat the method with a smaller constant, C, using the reduced bound possibly to find an even smaller bound. This can be repeated until the reduced bound is of a sufficiently small size to enable direct enumeration of all possible points.

3. *Case 2: $v = p$*

For brevity we denote in this section $|\cdot|_p$ by $|\cdot|$, once again remembering that v has been chosen to maximize $|x(P)|_v$. Denote reduction of a point P on the curve modulo p by $\tilde{P}$, and define

$$E_1(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \tilde{P} = \tilde{0}\},$$
$$\hat{E}(p\mathbb{Z}_p) = \text{Formal group associated to } E.$$

We have the isomorphism, [**6**, p. 175],

$$\hat{E}(p\mathbb{Z}_p) \to E_1(\mathbb{Q}_p)$$
$$z \mapsto \begin{cases} 0 & z = 0 \\ \left(\dfrac{z}{w(z)}, -\dfrac{1}{w(z)}\right) & z \neq 0 \quad \text{i.e. } z = -x/y. \end{cases}$$

We need to calculate $w(z)$, as a power series in z, to a high accuracy very quickly. This is done by using a Newton/Hensel type algorithm. From the power series for $w(z)$ we also calculate Laurent series for x and ω, in terms of z, see [**6**, p. 113], namely

$$x(z) = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 - \ldots,$$

$$\omega(z) = (1 + a_1 z + (a_1^2 + a_2) z^2 + (a_1^3 + 2a_1 a_2 + a_3) z^3 + \ldots)\, dz$$
$$= (1 + d_1 z + d_2 z^2 + d_3 z^3 + \ldots)\, dz.$$

Here $\omega(z)$ is the invariant differential. We are now able to define the p-adic elliptic logarithm,

$$\psi_p : E_1(\mathbb{Q}_p) \to \hat{\mathbb{G}}_a$$
$$P = (x, y) \mapsto \int \omega(z_p) = z_p + \frac{d_1 z_p^2}{2} + \frac{d_2 z_p^3}{3} + \ldots.$$

https://doi.org/10.1017/S0305004100072698 Published online by Cambridge University Press

This satisfies $\psi_p(P+Q) = \psi_p(P)+\psi_p(Q)$ and $|z_p| = |\psi_p(P)|$. We can find an integer m such that $mP_i = Q_i \in E_1(\mathbb{Q}_p)$ and $mT = 0$. We can take m as the least common multiple of the orders of $Tors_{\mathbb{Q}}(E)$ and $E(\mathbb{F}_p)$. So $mP = \sum_{i=1}^{r} q_i Q_i \in E_1(\mathbb{Q}_p)$. Now we have

$$|x(mP)| = \left| \frac{1}{z_{mp}^2} - \frac{a_1}{z_{mp}} - a_2 - a_3 z_{mp} + \dots \right|$$

$$\leqslant \frac{1}{|z_{mp}|^2} = \frac{1}{|\psi_p(mP)|^2}.$$

Now since $|x(mP)| \geqslant |x(P)|$ we have, by equation (2), $|\psi_p(mP)|^2 \leqslant \dfrac{1}{|x(P)|} \leqslant c_3 e^{-c_4 K^2}$, that is

$$|\psi_p(mP)| < c_{12} e^{-c_9 K^2} \quad c_{12} = \sqrt{c_3}.$$

Suppose we are given a large upper bound K_0 on K. It is desirable to reduce this to a more manageable bound so we can directly enumerate all the possibilities. This is done in a way similar to the previous case by showing that no small vectors occur in a certain lattice. This is a standard technique, see [11], but for completeness we repeat it here.

We have,

$$|q_1 \psi_p(Q_1) + \dots + q_r \psi_p(Q_r)| < c_{12} e^{-c_9 K^2}.$$

Let $\alpha_i = \psi_p(Q_i)$ and renumber the α_i such that

$$ord_p(\alpha_r) = \min_i ord_p(\alpha_i).$$

Set $\beta_i = -\alpha_i/\alpha_r$. Choose a constant c such that $p^c \approx K_0^r$. Now for $\alpha \in \mathbb{Z}_p$ let $\alpha^{(c)}$ denote the unique rational integer $0 \leqslant \alpha^{(c)} < p^c - 1$ such that $\alpha^{(c)} \equiv \alpha (p^c)$. Set

$$\mathscr{A} = \begin{pmatrix} 1 & & \mathrm{O} \\ & \ddots & \\ \mathrm{O} & & 1 \\ \beta_1^{(c)} & \dots & \beta_{r-1}^{(c)} \quad p^c \end{pmatrix} \in \mathbb{Z}^{r^2}.$$

Let Γ be the lattice generated by the columns of $\mathscr{A}$. Again we shall assume we have applied the L^3 algorithm to obtain a lower bound, K_1, on $l(\Gamma, \underline{0})$. Note in this case we use the integral L^3 algorithm as well.

LEMMA 3. *If* $K_1^2 > rK_0^2$ *then*

$$K < \left(\frac{\ln p}{c_9} \left(c + ord_p(\alpha_r) + \frac{\ln(c_{12})}{\ln p} \right) \right)^{\frac{1}{2}}.$$

Proof. Let $\Lambda = \sum_{i=1}^{r} q_i \psi_p(Q_i)$ so that $p^{-ord_p(\Lambda)} < c_{12} e^{-c_9 K^2}$. Thus

$$\mathrm{ord}_p(\Lambda) > \frac{-\ln(c_{12}) + c_9 K^2}{\ln p}.$$

Hence $ord_p(\Lambda/\alpha_r) > (c_9 K^2 - \ln c_{12})/\ln p - ord_p(\alpha_r)$. If we assume that K is larger than our proposed new bound then we have $ord_p(\Lambda/\alpha_r) > c$ and

$$ord_p\left(-\sum_{i=1}^{r-1} q_i \beta_i + q_r \right) > c.$$

https://doi.org/10.1017/S0305004100072698 Published online by Cambridge University Press

So if $\lambda = (\sum_{i=1}^{r-1} -q_i\beta_i^{(c)} + q_r)/p^c$ then $\lambda \in \mathbb{Z}$ and

$$\mathscr{A}\begin{pmatrix} q_1 \\ \vdots \\ q_{r-1} \\ \lambda \end{pmatrix} = \begin{pmatrix} q_1 \\ \vdots \\ q_{r-1} \\ q_r \end{pmatrix} \in \Gamma.$$

Hence we obtain $K_1^2 \leqslant rK_0^2$ a contradiction. ∎

We expect to reduce the bound to one of the order of $\sqrt{(r \ln K_0)}$. However, if we do not succeed at the first attempt, then the constant c should be increased and the method tried again. As before, after a reduced upper bound has been found the method can be repeated again.

4. *Example*

As an example we take

$$E: y^2 + y = x^3 + x^2 - 2x, \quad K_0 = 10^{40}.$$

$E(\mathbb{Q})$ has rank 2 and conductor 389. It is the curve of smallest conductor with rank 2 over $\mathbb{Q}$ as described in the tables of [**2**]. The Mordell–Weil group is given by $E(\mathbb{Q}) = \langle P_1 \rangle \times \langle P_2 \rangle$ where $P_1 = (0,0)$ and $P_2 = (1,0)$ are independent points of infinite order. For our set S we take $S = \{\infty, 3, 5\}$. Let our S-integral point be given by

$$P = nP_1 + mP_2.$$

We wish to find all such points where $K = \max(|n|, |m|) \leqslant K_0 = 10^{40}$. If we choose $v \in S$ to maximize $|x(P)|_v$ then, by equation (2), we have the inequality

$$|x(P)|_v^{-1} \leqslant c_3 e^{-c_4 K^2},$$

where $c_3 = 7{\cdot}8784$ and $c_4 = 0{\cdot}10228$. We have three cases to consider depending on the choice of v. We shall again abbreviate $|\cdot| = |\cdot|_v$.

$v = \infty$

We find that $P_1 \notin E^0(\mathbb{R})$ and $P_2 \in E^0(\mathbb{R})$. If $K \geqslant 5$ then, by choice of v, $P \in E^0(\mathbb{R})$. Therefore we have

$$P = \left(\frac{n}{2}\right) 2P_1 + mP_2 \quad \text{and} \quad |\psi(P)| \leqslant c_8 e^{-c_9 K^2},$$

where $c_8 = 8{\cdot}9057$ and $c_9 = c_4/2 = 0{\cdot}05114$.

We calculated the elliptic logarithms of $2P_1$ and P_2 to an accuracy of about 150 decimal digits using GP/PARI 1·38 and found

$$\psi(2P_1) \approx 1{\cdot}931\,12, \quad \psi(P_2) \approx 1{\cdot}4449.$$

We also found $\omega_1 \approx 2{\cdot}490\,21$. Then applying Lemma 2 with $C = 10^{130}$ we found $K \leqslant 63{\cdot}03$.

$v = 3$

We have $N_3 = |E(\mathbb{F}_3)| = 6$ and so $6P_1$, $6P_2 \in E_1(\mathbb{Q}_3)$. Setting $Q_i = 6P_i$ and $z_i = -x(Q_i)/y(Q_i)$ we find

$$z_1 = 3 + 3^2 + 3^3 + 2{\cdot}3^4 + O(3^5), \quad z_2 = 3 + 3^4 + O(3^5).$$

https://doi.org/10.1017/S0305004100072698 Published online by Cambridge University Press

Using these values we calculate the 3-adic elliptic logarithms to an accuracy of about 3^{200} to find,

$$\psi_3(Q_1) = 3+2\cdot 3^2+3^3+2\cdot 3^4+O(3^5), \quad \psi_3(Q_2) = 3+3^2+O(3^5).$$

Then

$$|\psi_3(6P)| = |n\psi_3(Q_1)+m\psi_3(Q_2)| \leqslant c_{12}\, e^{-c_9 K^2},$$

where $c_{12} = 2{\cdot}8068$. We apply Lemma 3 with $c = 182$ to find $K \leqslant 62{\cdot}85$.

$v = 5$

In this case we have $N_5 = 9$ and so we set $Q_i = 9P_i$ and $z_i = -x(Q_i)/y(Q_i)$. We find

$$z_1 = 4\cdot 5+4\cdot 5^2+O(5^5), \quad z_2 = 2\cdot 5+3\cdot 5^2+4\cdot 5^3+4\cdot 5^4+O(5^5).$$

We then calculate the 5-adic logarithms to an accuracy of about 5^{150} to find,

$$\psi_5(Q_1) = 4\cdot 5+4\cdot 5^2+3\cdot 5^3+2\cdot 5^4+O(5^5), \quad \psi_5(Q_2) = 2\cdot 5+3\cdot 5^2+5^4+O(5^5).$$

Then $|\psi_5(9P)| \leqslant c_{12}\, e^{-c_9 K^2}$. Applying Lemma 3 again with $c = 124$ we find a new bound of $K \leqslant 62{\cdot}88$.

So in all three cases we find $K \leqslant 63$, the total CPU-time to reduce the bound to 63 was 4 minutes on a SUN 4/670 MP, this includes all the time needed to calculate the real and p-adic logarithms.

Thus we have shown that all S-integral points on E of the form

$$P = n.(0,0)+m.(1,0) \quad n, m \in \mathbb{Z},$$

with $|n|, |m| \leqslant 10^{40}$ are given by $|n|, |m| \leqslant 63$. At first sight it seems very surprising that one application of L^3 in each case should give such small bounds. But on reflection one notices that, as the height function is a quadratic form, the inequality we are using is of the form

$$|L(\underline{x})| \leqslant a_1\, e^{-a_2 K^2}.$$

Therefore when reducing the bound we expect the new bound to be of the size of the square root of the logarithm of the original bound. Compare this with the reduction expected when solving a Thue equation, see [**8**]. This is usually of the order of the logarithm of the original bound.

All that remains to be done is to search for all solutions satisfying $|n|, |m| \leqslant 63$. We note that if P is an S-integral point then $-P$ is also an S-integral point. So we may assume that $n \geqslant 0$.

When solving an S-unit equation a sieve is used to locate all the small solutions, see [**9**]. In such a situation for each prime p used in the sieve, on average we reduce the number of possibilities that need to be considered by a factor of p. In the case of elliptic curves we are not so lucky, as we describe below.

Let p be a prime not in S. Then if P is an S-integral point we have $P \notin E_1(\mathbb{Q}_p)$. The probability that a random point on our elliptic curve reduces to the identity modulo p is $N_p^{-1} = |E(\mathbb{F}_p)|^{-1}$, which is of order p^{-1}. Hence, on average, we can reduce the number of possibilities by a factor of $(p-1)/p$. This is much worse than the S-unit equation analogue.

Rather than working modulo p it is easier to find congruence conditions on n and m. As an example we shall consider the prime 2. We have $N_2 = 5$ and

https://doi.org/10.1017/S0305004100072698 Published online by Cambridge University Press

$\tilde{P}_1 \equiv 2\tilde{P}_2 \pmod 2$; we then have that $E(\mathbb{F}_2)$ is cyclic of order 5 and generated by $\tilde{P}_2$. So if our point P is S-integral we cannot have $2n+m \equiv 0 \pmod 5$. We can hence eliminate 20 per cent. of all possibilities.

We perform such a sieve for the primes 2, 7, 11, 13, 17, 19, 23, which eliminates about 45% of all cases. The other cases are checked by a brute force approach. One could have used more primes. However, as we have noted, the larger the prime the smaller the number of cases that are eliminated. This is the opposite to the S-unit equation case where the larger the prime taken the greater the number of cases that are eliminated.

After 34 minutes of CPU-time we find that all S-integral points on our elliptic curve with $|n|, |m| \leqslant 10^{40}$ are given by

$$(n,m) = \pm(0,1), \pm(0,2), \pm(0,3), \pm(1,0), \pm(1,1), \pm(1,-1), \pm(1,-4),$$
$$\pm(2,0), \pm(2,-1), \pm(2,2), \pm(2,-2), \pm(2,-3), \pm(3,0), \pm(3,1),$$
$$\pm(3,-2), \pm(4,-1), \pm(1,2).$$

Note that if we had explicit lower bounds on $|\psi(P)|$, $|\psi_3(6P)|$ and $|\psi_5(9P)|$, in terms of K, then we could find an upper bound K_0. As noted before, a lower bound on $|\psi(P)|$ in terms of K has been given by David but no explicit lower bound is known in the p-adic case.

REFERENCES

[1] M. Ayad. Points Δ-entiers sur les courbes elliptiques. *J. Number Theory* **38** (1991), 323–337.

[2] J. E. Cremona. *Algorithms For Modular Elliptic Curves* (Cambridge University Press, 1993).

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

[4] S. Lang. *Elliptic Curves: Diophantine Analysis* (Springer-Verlag, 1978).

[5] A. K. Lenstra, H. W. Lenstra and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.* **261** (1982), 515–534.

[6] J. H. Silverman. *The Arithmetic Of Elliptic Curves* (Springer-Verlag, 1986).

[7] R. J. Stroeker and N. Tzanakis. Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms, to appear in *Acta. Arith.*

[8] N. Tzanakis and B. M. M. de Weger. On the practical solution of the Thue equation. *J. Number Theory* **31** (1989), 99–132.

[9] N. Tzanakis and B. M. M. de Weger. How to explicitly solve a Thue–Mahler equation. *Comp. Math.* **84** (1992), 223–288.

[10] B. M. M. de Weger. Solving exponential diophantine equations using lattice basis reduction algorithms. *J. Number Theory* **26** (1987), 325–367.

[11] B. M. M. de Weger. *Algorithms For Diophantine Equations*. CWI-Tract, Centre For Mathematics and Computer Science (Amsterdam, 1989).

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

https://doi.org/10.1017/S0305004100072698 Published online by Cambridge University Press