Journal de Théorie des Nombres
de Bordeaux **13** (2001), 443–451

S-integral points on elliptic curves - Notes on a paper of B. M. M. de Weger

par Emanuel HERRMANN * et Attila PETHŐ **

Résumé. Nous donnons une nouvelle preuve beaucoup plus courte d'un résultat de B. M. M de Weger. Cette preuve est basée sur la théorie des formes linéaires de logarithmes complexes, p-adiques et elliptiques, pour lesquelles nous obtenons une majoration en confrontant les résultats de Hajdu et Herendi à ceux de Rémond et Urfels.

Abstract. In this paper we give a much shorter proof for a result of B.M.M de Weger. For this purpose we use the theory of linear forms in complex and p-adic elliptic logarithms. To obtain an upper bound for these linear forms we compare the results of Hajdu and Herendi and Rémond and Urfels.

1. Introduction

In a recent paper [12] B.M.M. de Weger solved the Diophantine equation

$$y^2 = x^3 - 228x + 848 \tag{1}$$

completely in rational numbers x, y such that their denominator in the lowest form is a power of 2. With other words, he solved (1) in S-integers where $S = \{2, \infty\}$. De Weger uses in the proof algebraic number theoretical considerations and lower estimates for linear forms in complex and q-adic logarithms of algebraic numbers.

In the present paper we will give a much shorter proof of a generalization of Theorem 1 of [12]. Here we use the theory of elliptic curves and linear forms in elliptic logarithms. More precisely, we are using a theorem of Rémond and Urfels [6], which can be applied for curves of rank at most 2. An alternative method which avoids lower bounds for linear forms in q-adic elliptic logarithms is given in [5]. However the bounds coming from [5] are

Manuscrit reçu le 3 août 1999.

* This paper was partly written while the author was a Visiting Scholar at the School of Mathematics and Statistics at the University of Sydney. His research was supported in part by grants from the Australian Research Council and the Defense Science and Technology Organization.

** Research partially supported by Hungarian National Foundation for Scientific Research, Grant No. T25157 and T16975.

in the actual case much larger as working directly with the Theorem of Rémond and Urfels (cf. Section 3).

We now state our result.

Theorem 1. *Let* $S = \{2, 3, 5, 7, \infty\}$. *Then the equation*

$$y^2 = x^3 - 228x + 848$$

has only 65 *S-integer solutions* $(x, \pm y)$ *listed in Table 2 at the end of this paper.*

2. Notations and Auxiliary Results

Let the elliptic curve be defined by the equation

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}. \tag{2}$$

Let $S = \{q_1, \ldots, q_{s-1}, q_s = \infty\}$ be a set of primes including the infinite prime. To simplify the presentation we assume that the equation (2) is minimal for every finite prime $q \in S$. For the general case we refer to the paper [5].

Let $P_1, \ldots, P_r$ denote a basis of the Mordell-Weil group $E(\mathbb{Q})$ and let g be the order of the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ of $E(\mathbb{Q})$. Let $\hat{h}$ denote the Néron-Tate height on $E(\mathbb{Q})$. Designate by λ the smallest eigenvalue of the positive definite regulator matrix $(\hat{h}(P_i, P_j))_{1 \le i,j \le r}$.

Let $\wp(u)$ be the Weierstrass $\wp$-function corresponding to the curve $E(\mathbb{C})$. Let $\Omega = \langle \omega_1, \omega_2 \rangle$ be its fundamental lattice and ω_1 its real period. There exists, for any $P = (x, y) \in E(\mathbb{C})$, an element $u \in \mathbb{C}/\Omega$ such that $(x, y) = (\wp(u), \frac{1}{2}\wp'(u))$. This 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 $u'_{i,\infty} = g\frac{u_{i,\infty}}{\omega_1}$.

For a finite prime $q \in S$ let $E_0(\mathbb{Q}_q)$ denote the points of $E(\mathbb{Q}_q)$ with non-singular reduction modulo q. Then the index $[E(\mathbb{Q}_q) : E_0(\mathbb{Q}_q)]$ is finite, and equal to the Tamagawa number c_q because by our assumption equation (2) is minimal at q. Let further $\tilde{E}$ denote the reduced curve E modulo q. Let $\mathcal{N}_q = \#\tilde{E}(\mathbb{F}_q)$ be the number of rational points of $\tilde{E}/\mathbb{F}_q$. With the order g of the torsion group, we define the number

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

Finally for the finite places $q \in S$, let $u'_{i,q}$ denote the q-adic elliptic logarithm of mP_i for $i = 1, \ldots, r$. For the definition and basic properties of q-adic elliptic logarithms we refer to Silverman [7] and to [5]. Now we state the main result of [5] in the special case considered, i.e. for curves given in short Weierstrass form.

Theorem A. *Let the elliptic curve* $E(\mathbb{Q})$ *be defined by equation (2), which is minimal for every finite prime* $q \in S$. *Assume that the S-integral point*

$P = (x,y) \in E(\mathbb{Z}_S)$ has the representation

$$P = \sum_{i=1}^{r} n_i P_i + T \tag{3}$$

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

$$N(P) \le N_0 = \sqrt{\tfrac{1}{\lambda}(\tfrac{k_1}{2} + k_2)} \tag{4}$$

with $k_2 = \log\max\{|2A|^{1/2}, |4B|^{1/3}\}$,

$$\begin{aligned} k_1' &= 7 \cdot 10^{38s+49} s^{20s+15} Q^{24} (\log^* Q)^{4s-2} k_3 (\log k_3)^2 ((20s-19)k_3 + \log(ek_4)), \\ k_1 &= k_1' + 2\log 6, \end{aligned}$$

where $\log^* Q = \max\{\log Q, 1\}$ for $Q = \max\{q_1, \ldots, q_{s-1}\}$, $s=\#S$,

$$\begin{aligned} k_3 &= \tfrac{32}{3}\sqrt{|\Delta_0|}\left(8 + \tfrac{1}{2}\log|\Delta_0|\right)^4, \\ k_4 &= 10^4 \max\{16A^2, 256\sqrt{|\Delta_0|}^3\} \end{aligned}$$

with $\Delta_0 = 4A^3 + 27B^2$. Moreover, there exists a place $q \in S$ such that

$$\left| \sum_{i=1}^{r} n_i u'_{i,q} + n_{r+1} \right|_q \le k_5 \exp\{-\tfrac{\lambda}{s} N(P)^2 + \tfrac{k_2}{s}\} \tag{5}$$

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

Theorem A together with numerical Diophantine approximation techniques is sufficient to prove our Theorem 1. However it was pointed out already in [5] that combining the method of Smart [8] with results of David [2] and of Rémond and Urfels [6] one can obtain a much better estimate for $N(P)$ as by the one implied by Theorem A. In the sequel we assume $r \le 2$. To formulate the next theorem we have to introduce further notations. Let

$j = \frac{j_1}{j_2}$ with $j_1, j_2 \in \mathbb{Z}$ and $\gcd(j_1, j_2) = 1$ be the j−invariant of $E(\mathbb{Q})$. Put

$$\begin{aligned}
h &= \log\max\{4|Aj_2|, 4|Bj_2|, |j_1|\},\\
\log V_i &= \max\left\{\hat{h}(P_i), h, \frac{3\pi|u'_{i,\infty}|_\infty^2}{\mathrm{Im}\tau}\right\}, \quad i = 1, 2,\\
\log V_0 &= \max\left\{h, \frac{3\pi}{\mathrm{Im}\tau}\right\},\\
k_{6,\infty} &= \frac{k_2 + s\log k_5}{\lambda},\\
k_{7,\infty} &= \frac{2\cdot 10^{68}\cdot s\cdot h^5}{\lambda}\prod_{i=0}^{2}\log V_i.
\end{aligned}$$

For a finite place $q \in S$ let

$$\begin{aligned}
\alpha_q &= \begin{cases} 3, & \text{if } q = 2\\ \frac{1}{q-1}, & \text{otherwise}\end{cases}\\
\sigma_q &= (q^{\alpha_q}\max\{|u'_{1,q}|_q, |u'_{2,q}|_q\})^{-1},\\
d_q &= \max\{1, 1/\log\sigma_q\},\\
a_i &= \max\{1, \hat{h}(P_i)\}, \quad i = 1, 2,\\
\beta &= \max\{\log N(P), \log|A|_\infty, \log|B|_\infty, a_1, a_2, d_q\},\\
\gamma &= \max\{\log|A|_\infty, \log|B|_\infty, \log\beta\},\\
k_{6,q} &= \frac{k_2}{\lambda},\\
k_{7,q} &\geq (3.6\cdot 10^{25}s\cdot a_1a_2d_q^6\log\sigma_q)/\lambda.
\end{aligned}$$

Theorem B. *Assuming that $r \leq 2$ and using the notations introduced in Theorem A and above we have*

$$N(P) \leq N_1 := \max\{N_q \ : \ q \in S\},$$

where

$$N_q = \begin{cases} 2^5\sqrt{k_{6,\infty}k_{7,\infty}}(\log 5^5 k_{7,\infty})^{5/2}, & \text{if } q = \infty,\\ 2^4\sqrt{k_{6,q}k_{7,q}}(\log 4^4 k_{7,q})^2, & \text{if } q \in S\setminus\{\infty\}.\end{cases}$$

Proof. Combining inequality (5) with the lower bounds for linear forms in elliptic logarithms due to David [2] and for linear forms in at most two q−adic elliptic logarithms due to Rémond and Urfels [6] one obtains the upper bound for $N(P)$ analogously as described for example in Gebel, Pethő and Zimmer [3, 4]. Therefore we omit the details. □

3. Proof of Theorem 1

3.1. Basic data of the elliptic curve. In the sequel we denote by E the elliptic curve over $\mathbb{Q}$ defined by equation (1). Let $S = \{2, 3, 5, 7, \infty\}$. It is easy to check, that (1) is minimal for every finite prime $q \in S$. Actually, it is a global minimal model of E. The discriminant of E is $\Delta = -16\Delta_0$ with $\Delta_0 = -27993600$. We have

$$E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^2,$$

where the only non-trivial torsion point is $(4, 0)$ and a basis of the infinite part of the Mordell-Weil group is $P_1 = (-2, 36), P_2 = (-11, 45)$. (See Tzanakis [10], or one of of the programs apecs [13], Magma[1] [1], mwrank [14] or Simath [15].)

Now we can compute the fundamental parallelogram of the associated Weierstrass $\wp$-function and get

$$\omega_1 = 0.767848, \quad \omega_2 = -0.631356 \cdot i \quad \text{and} \quad \tau = \tfrac{\omega_1}{\omega_2} = 1.216188 \cdot i.$$

The regulator matrix of E is

$$R = \begin{pmatrix} 0.423441 & -0.158771 \\ -0.158771 & 0.906408 \end{pmatrix},$$

hence its smallest eigenvalue is given by $\lambda = 0.375922$.

Using Tate's algorithm [9] we compute the Tamagawa numbers

$$c_2 = 4, \quad c_3 = 4, \quad c_5 = 2 \quad \text{and} \quad c_7 = 1.$$

The curve E has additive reduction at the primes 2 and 3, multiplicative reduction at 5 and good reduction at 7. Hence,

$$\mathcal{N}_2 = 2, \quad \mathcal{N}_3 = 3, \quad \mathcal{N}_5 = 6 \quad \text{and} \quad \mathcal{N}_7 = 12.$$

Using these data we can compute the numbers m_q and obtain

$$m_2 = 8, \quad m_3 = 12, \quad m_5 = 12 \quad \text{and} \quad m_7 = 12.$$

3.2. Upper Bounds for $N(P)$.
(i) The first way to obtain an upper bound for $N(P)$ is to calculate N_0 of Theorem A. We have actually $Q = 7, s = 5$,

$$\begin{aligned} k_2 &= \log \max\{456^{1/2}, 3392^{1/3}\} = 3.061246, \\ k_3 &= \tfrac{32}{3}\sqrt{|\Delta_0|}\left(8 + \tfrac{1}{2}\log|\Delta_0|\right)^4 = 4.258342 \cdot 10^9, \\ k_4 &= 10^4 \max\{16 \cdot 228^2, 256 \cdot |\Delta_0|^{3/2}\} = 3.791649 \cdot 10^{17} \end{aligned} \tag{6}$$

and $k_1 = 3.730724 \cdot 10^{369}$, hence $N(P) \leq N_0 = 7.044216 \cdot 10^{184}$.
(ii) Another, a bit more complicated, way to find an upper bound for $N(P)$ is to compute $N_1 = \max\{N_q \ : \ q \in S\}$ as defined in Theorem B.

[1]Magma version 2.6 will have an implementation of the algorithm described in [5].

Consider first the case $q=\infty$. Then we have

$$\begin{aligned}
h &= \log\max\{4\cdot 228\cdot 75, 4\cdot 848\cdot 75, 2^5\cdot 19^3\} = 12.446663,\\
\log V_0 &= \max\{h, \tfrac{3\pi}{\mathrm{Im}\tau}\} = 12.446663,\\
\log V_1 &= \max\{\hat{h}(P_1), h, \tfrac{3\pi g^2|u_{1,\infty}|_\infty^2}{\omega_1^2\mathrm{Im}\tau}\} = 21.645104,\\
\log V_2 &= \max\{\hat{h}(P_2), h, \tfrac{3\pi g^2|u_{2,\infty}|_\infty^2}{\omega_1^2\mathrm{Im}\tau}\} = 28.279603,\\
k_{5,\infty} &= \tfrac{4}{3\omega_1} = 1.736455,\\
k_{6,\infty} &= 15.483196,\\
k_{7,\infty} &= 6.054145\cdot 10^{78}.
\end{aligned}$$

Thus we obtain $N_\infty \le 1.530526\cdot 10^{47}$ after a simple computation.

Next we have to consider the cases $q=2,3,5$ and 7. In Table 1 below you find the actual values of α_q, σ_q and d_q.

Table 1

q	2	3	5	7
α_q	3	1/2	1/4	1/6
σ_q	2	$3^{1/2}$	$5^{3/4}$	$7^{5/6}$
d_q	$1/\log 2$	$2/\log 3$	1	1
$k_{7,q}$	$2.992592\cdot 10^{27}$	$9.5742\cdot 10^{27}$	$5.779766\cdot 10^{26}$	$7.76455\cdot 10^{26}$

The following values are independent of $q\in\{2,3,5,7\}$

$$\begin{aligned}
a_1 &= \max\{1, \hat{h}((-2,36))\} = \max\{1, 0.423441\} = 1,\\
a_2 &= \max\{1, \hat{h}((-11,45))\} = \max\{1, 0.906408\} = 1,\\
k_{6,q} &= k_2/\lambda = 8.143301.
\end{aligned}$$

Choosing the worst cases from Table 1 we see that we can take

$$k_{7,q} = k_{7,3} = 9.5742\cdot 10^{27}, \quad q=2,3,5,7,$$

thus

$$N_q = N_3 = 2.187487\cdot 10^{19}, \quad q=2,3,5,7.$$

These inequalities imply

$$N(P) \le N_1 = \max\{N_q : q\in S\} = 1.530526\cdot 10^{47}$$

by Theorem B. Since N_1 is much smaller than N_0 we use this value in the sequel.

3.3. Reduction of the large upper bound for $N(P)$. By Theorem 1, and by the last section we have to solve the Diophantine approximation problem

$$\begin{aligned} |n_1 u'_{1,q} + n_2 u'_{1,q} + n_3|_q &\leq k_5 \exp\{0.075184 \cdot N(P)^2 + 0.6122492\}, \\ N(P) &\leq N_1 = 1.530526 \cdot 10^{47} \end{aligned}$$

for each $q \in S$.

To solve these systems we use the well known reduction procedure of de Weger [11]. (See also Smart [8].) For details about the high precision computation of q-adic elliptic logarithms we refer to Pethő et al. [5]. We shall also use the notations introduced there.

We first take $q = \infty$ and perform a de Weger reduction with $C = 10^{142}$. We obtain the new upper bound $N(P) \leq \mathcal{M}_\infty = 67$ in the case $q = \infty$. Comparing this bound with $N_q, q = 2, 3, 5, 7$ we obtain

$$N(P) \leq N_3 = 2.187487 \cdot 10^{19},$$

i.e. we may perform the $q-$adic reduction steps with this value.

To do this we compute for each $q \in S \setminus \{\infty\}$, the q-adic elliptic logarithms of $m_q P_i, i = 1, 2$, with precision at least

$$n_2 = 129, \quad n_3 = 82, \quad n_5 = 56, \quad n_7 = 46.$$

This precision is necessary to carry out the q-adic de Weger reduction. For this purpose we use the method of [5].

$$\begin{aligned}
u'_{1,2} &= 134584334573222732131510464853384888320 + O(2^{128}) \\
u'_{2,2} &= 224603122385055121905025779589746548856 + O(2^{128}) \\
u'_{1,3} &= 35130898366670225251067310603381664587 + O(3^{81}) \\
u'_{2,3} &= 32674326287561878726624624078558984866 + O(3^{81}) \\
u'_{1,5} &= 118414103305724592543524002578287458095 + O(5^{55}) \\
u'_{2,5} &= 193714651202697832194263283063279750580 + O(5^{55}) \\
u'_{1,7} &= 49086609441793589144883973076015987885 + O(7^{46}) \\
u'_{2,7} &= 723939447229120403790851561285560713079 + O(7^{46})
\end{aligned}$$

Now we perform the q-adic de Weger reduction with the values $C_2 = 2^{128}$, $C_3 = 3^{81}$, $C_5 = 5^{55}$ and $C_7 = 7^{46}$ and obtain the new bound

$$N(P) \leq \max\{\mathcal{M}_\infty = 67, \mathcal{M}_2 = 12, \mathcal{M}_3 = 13, \mathcal{M}_5 = 13, \mathcal{M}_7 = 13\}.$$

This new upper bound for $N(P)$ can be further reduced. On repeating this reduction process 3-times, we eventually get $N(P) \leq 13$, which cannot be reduced any further.

Table 2

S-integral points $P=(x,y)=\left(\frac{\xi}{\zeta^2},\ \frac{\eta}{\zeta^3}\right)=\sum_{i=1}^{2} n_i P_i + T_j,\quad j=0,1$
on $E:\ y^2=x^3-228x+848$ for $S=\{2,\ 3,\ 5,\ 7,\ \infty\}$

rank	2
basis	$P_1=(-2,36),\ P_2=(-11,45)$
torsion	$T_0=\mathcal{O},\ T_1=(4,0)$

#	ξ	η	ζ	F	(n_1,n_2,j)
1	4	0	1		$(0,0,1)$
2	-11	45	1		$(0,1,0)$
3	16	36	1		$(0,1,1)$
4	94	-900	1		$(1,-1,0)$
5	2	-20	1		$(1,-1,1)$
6	-2	36	1		$(1,0,0)$
7	34	180	1		$(1,0,1)$
8	14	-20	1		$(1,1,0)$
9	-14	-36	1		$(1,1,1)$
10	754	-20700	1		$(1,2,1)$
11	196	2736	1		$(2,-1,1)$
12	13	9	1		$(2,0,0)$
13	-16	20	1		$(2,0,1)$
14	52	-360	1		$(2,1,1)$
15	53	371	1		$(2,2,0)$
16	814	23220	1		$(3,1,0)$
17	534256	-390502764	1		$(4,3,1)$
18	97	-783	2	2	$(0,-2,0)$
19	1	-225	2	2	$(2,1,0)$
20	857	-25027	2	2	$(4,0,0)$
21	49	855	4	2^2	$(2,-1,0)$
22	-16439	-631035	32	2^5	$(2,3,0)$
23	-44	-1160	3	3	$(0,-2,1)$
24	34	172	3	3	$(3,1,1)$
25	1534	42020	9	3^2	$(3,-1,0)$
26	94	-828	5	5	$(1,2,0)$
27	629	-13133	5	5	$(2,-2,0)$
28	-194	-5796	5	5	$(3,0,0)$
29	6361	-282141	20	$2^2\times 5$	$(4,2,0)$
30	-818	-468	7	7	$(1,-2,0)$
31	16	9540	7	7	$(2,2,1)$
32	946	-20700	7	7	$(3,0,1)$
33	8516	1163623840	343	7^3	$(4,-2,1)$

References

[1] W. BOSMA, J. CANNON, C. PLAYOUST, *The Magma algebra system I: The user language.* J. Symb. Comp., **24**, 3/4 (1997), 235–265. (See also the Magma home page at http://www.maths.usyd.edu.au:8000/u/magma/)

[2] S. DAVID, *Minorations de formes linéaires de logarithmes elliptiques.* Mém. Soc. Math. France (N.S.) **62** (1995).

[3] J. GEBEL, A. PETHŐ, H. G. ZIMMER, *Computing integral points on elliptic curves.* Acta Arith. **68** (1994), 171–192.

[4] J. GEBEL, A. PETHŐ, H. G. ZIMMER, *Computing S-integral points on elliptic curves.* Algorithmic number theory (Talence, 1996), 157–171, Lecture Notes in Comput. Sci. **1122**, Springer, Berlin, 1996.

[5] A. PETHŐ, H. G. ZIMMER, J. GEBEL, E. HERRMANN, *Computing all S-integral points on elliptic curves.* Math. Proc. Cambr. Phil. Soc. **127** (1999), 383–402.

[6] G. RÉMOND, F. URFELS, *Approximation diophantienne de logarithmes elliptiques p-adiques.* J. Numb. Th. **57** (1996), 133–169.

[7] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.

[8] N. P. SMART, *S-integral Points on elliptic curves.* Math. Proc. Cambr. Phil. Soc. **116** (1994), 391–399.

[9] J. T. TATE, *Algorithm for determining the type of a singular fibre in an elliptic pencil.* Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 33–52, Lecture Notes in Math. **476**, Springer, Berlin, 1975.

[10] N. TZANAKIS, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations.* Acta Arith. **75** (1996), 165–190.

[11] B. M. M. DE WEGER, *Algorithms for Diophantine equations.* PhD Thesis, Centr. for Wiskunde en Informatica, Amsterdam, 1987.

[12] B. M. M. DE WEGER, *S−integral solutions to a Weierstrass equation,* J. Théor. Nombres Bordeaux **9** (1997), 281–301.

[13] Apecs, *Arithmetic of plane elliptic curves,* ftp://ftp.math.mcgill.ca/pub/apecs.

[14] mwrank, *a package to compute ranks of elliptic curves over the rationals.* http://www.maths.nott.ac.uk/personal/jec/ftp/progs.

[15] Simath, *a computer algebra system for algorithmic number theory.* http://simath.math.uni-sb.de.

Emanuel HERRMANN
FR 6.1 Mathematik
Universität des Saarlandes
Postfach 151150
D-66041 Saarbrücken
Germany
E-mail : `herrmann@math.uni-sb.de`

Attila PETHŐ
Institute of Mathematics and Informatics
Kossuth Lajos University
H-4010 Debrecen, P.O.Box 12
Hungary
E-mail : `pethoe@math.klte.hu`