ACTA ARITHMETICA
113.1 (2004)

Note on J. H. E. Cohn's paper "The Diophantine equation $x^n = Dy^2 + 1$"

by

E. Herrmann (Saarbrücken), I. Járási (Debrecen)
and A. Pethő (Debrecen)

1. Introduction. A classical problem of the theory of diophantine equations is to find the solutions of

$$x^n = Dy^2 + 1 \tag{1}$$

in integers x, y. Using elementary and algebraic number theoretical tools J. H. E. Cohn [2] proved necessary conditions for the unsolvability of (1). Moreover, he solved (1) completely for $D \le 100$ up to the six pairs

$$(n, D) = (3, 31), (5, 31), (3, 38), (3, 61), (5, 71) \text{ and } (7, 71)$$

and parity conditions on x. We summarize our results in the following theorem.

Theorem. *Apart from* $(x, y) = (1, 0)$ *equation* (1) *has the solutions*

$$\begin{aligned}
&(x, y) = (5, \pm 12) && \text{if } (n, D) = (3, 31),\\
&(x, y) = (2, \pm 1) && \text{if } (n, D) = (5, 31),\\
&(x, y) = (7, \pm 3) && \text{if } (n, D) = (3, 38),\\
&(x, y) = (13, \pm 6) && \text{if } (n, D) = (3, 61),\\
&\textit{none} && \text{if } (n, D) = (5, 71),\\
&\textit{none} && \text{if } (n, D) = (7, 71).
\end{aligned}$$

This confirms the conjecture of Cohn [2].

To prove the Theorem, recently developed techniques of numerical diophantine analysis are used. Notice that if $n = 3$ then (1) is an elliptic curve in canonical form over $\mathbb{Q}$ and if $n = 5$ then we can transform it by using a straightforward argument to some curve of genus one. In the case $n = 3$ one

2000 *Mathematics Subject Classification*: Primary 11D25, 11D41.

The research of the second and third authors was supported by the Hungarian National Foundation for Scientific Research Grants No. T037367 and No. T042985 and 38225 as well as by the OTKA-NWO project NWO N34001.

can use directly the method developed by J. Gebel, A. Pethő, H. G. Zimmer [4] and R. J. Stroeker and N. Tzanakis [7].

The equation

$$(D^2y)^2 = (Dx)^3 - D^3$$

was solved in Gebel, Pethő and Zimmer [5] for $D = 31$ and $D = 38$ assuming the Birch and Swinnerton-Dyer conjecture. This is equivalent to (1) for $(n, D) = (3, 31)$ and $(3, 38)$. To avoid the Birch and Swinnerton-Dyer conjecture in the above cases and to handle $(n, D) = (3, 61)$ we used J. Cremona's program *mwrank* combined with the method of [5].

If $n = 5$, then (1) can be easily transformed to some equations of the form

$$v^2 = Q(u),$$

where Q is a quartic polynomial with integer coefficients. We solve the resulting equations partly by referring to results of Cohn's paper and partly by using the method of N. Tzanakis [8], which was implemented by the first author in the computer algebra system Magma [1].

When $n = 7$ we use the arguments of M. Mignotte and B. M. M. de Weger [6] and we reduce our equation to several Thue equations.

We are grateful to Gary Walsh for calling our attention to the paper of Cohn.

2. The case $n = 3$. Cohn was not able to solve completely the equations

$$\mathcal{E}'_D\colon \quad x^3 = Dy^2 + 1, \quad \text{with } D = 31, 38, 61 \text{ and } x \text{ odd}. \tag{2}$$

Multiplying both sides of (2) by D^3 we obtain

$$(Dx)^3 = (D^2y)^2 + D^3,$$

which with the notation $Dx = u$, $D^2y = v$ has the shape

$$\mathcal{E}_D\colon \quad v^2 = u^3 - D^3. \tag{3}$$

Equation (3) represents a Mordell's equation $v^2 - u^3 = k$ and the integer points of this kind of equation were computed by Gebel, Pethő and Zimmer [5] for $|k| \le 10^5$ provided that the Birch and Swinnerton-Dyer conjecture is true. For the values 31 and 38 the inequality $D^3 < 10^5$ holds, hence $|u| \le 3.791 \cdot 10^9$ by [5, Table 8]. Using J. Cremona's *mwrank* [10] we checked the computation of [5] and observed that the results coincide, but now without the assumption of the Birch and Swinnerton-Dyer conjecture.

For $D = 61$ the value of D^3 is larger than 10^5, hence we computed the solution of (3) in this case by using the computer algebra system Magma. We note that for $D \in \{31, 38, 61\}$ the torsion subgroup $\mathcal{E}_D^{\mathrm{tors}}(\mathbb{Q})$ has order two and is generated by the point $(D, 0)$. The results of our computation are listed in Table 1.

Table 1

D	$\mathcal{E}_D(\mathbb{Q})/\mathcal{E}_D^{\mathrm{tors}}(\mathbb{Q})$	$\mathcal{E}_D(\mathbb{Z})$	$\mathcal{E}'_D(\mathbb{Z})$
31	$\langle(155, 1922)\rangle$	$(31, 0), (155, \pm 1922)$	$(1, 0), (5, \pm 2)$
38	$\langle(57, 361)\rangle \times \langle(522, 11924)\rangle$	$(522, \pm 11924), (38, 0)$ $(57, \pm 361), (266, \pm 4332)$	$(1, 0), (7, \pm 3)$
61	$\left\langle\left(\frac{610}{8}, \frac{3721}{8}\right)\right\rangle \times \left\langle\left(\frac{4230480540}{3796416}, \frac{1412088887617}{3796416}\right)\right\rangle$	$(793, \pm 22326), (61, 0)$	$(1, 0), (13, \pm 6)$

3. The case $n = 5$. In Cohn's paper two equations remain unsolved:

$$x^5 = 31y^2 + 1, \tag{4}$$

$$x^5 = 71y^2 + 1. \tag{5}$$

In both cases he did not determine the solutions with even x. Equations (4) and (5) have the common shape

$$x^5 - 1 = py^2.$$

By computing the factorization of the left hand side of this equation we obtain

$$(x - 1)(x^4 + x^3 + x^2 + x + 1) = py^2.$$

For integers x the greatest common divisor of $x - 1$ and $x^4 + x^3 + x^2 + x + 1$ is 1 or 5. Hence, it remains to consider the following systems of diophantine equations:

$$\text{(I)} \quad \begin{cases} y_1^2 = x - 1, \\ py_2^2 = x^4 + x^3 + x^2 + x + 1; \end{cases}$$

$$\text{(II)} \quad \begin{cases} py_1^2 = x - 1, \\ y_2^2 = x^4 + x^3 + x^2 + x + 1; \end{cases}$$

$$\text{(III)} \quad \begin{cases} 5y_1^2 = x - 1, \\ 5py_2^2 = x^4 + x^3 + x^2 + x + 1; \end{cases}$$

$$\text{(IV)} \quad \begin{cases} 5py_1^2 = x - 1, \\ 5y_2^2 = x^4 + x^3 + x^2 + x + 1. \end{cases}$$

The second equation of (II) is not solvable for even x by [2, Lemma 2.3]. For the second equation of (IV) we can apply Corollary 3 of [2] and conclude that its only solution is $(y_1, y_2) = (0, 1)$.

Therefore we have to deal in what follows only with the equations (I) and (III) for $p = 31$ and 71. To obtain the integral solutions of the occurring quartic elliptic equations we follow closely the arguments from the article of N. Tzanakis [8]. Since for each curve the calculation is similar we explain the method only for the equation

$$355y^2 = x^4 + x^3 + x^2 + x + 1 \tag{6}$$

which, by putting $Y = 355y$, is also given in the more suitable form

$$Y^2 = 355(x^4 + x^3 + x^2 + x + 1).$$

To apply the algorithm from [8] we have to find a non-trivial rational point on this curve. By a direct search the point $(-26/9, 11005/81)$ was found. We put

$$u = 9x \quad \text{and} \quad v = 81Y = 28755y.$$

This results in the quartic elliptic equation

$$\mathcal{Q}: \quad v^2 = 355u^4 - 33725u^3 + 1219425u^2 - 19714925u + 121110025 =: Q(u) \tag{7}$$

for which we can apply the algorithm of Tzanakis. Note that $(0, 11005)$ is a rational point on this curve.

Using the birational map

$$x' = \frac{22010\sqrt{Q(u)} - 19714925u + 22010}{u^2} + 406475 =: f^*(u),$$

$$y' = -\frac{484440100\sqrt{Q(u)} + 5331263300500}{u^3} + \frac{-433925499250u + \frac{569183383625}{62u^2}}{u^3} + \frac{55535}{62}\,x' + \frac{437315625}{62}$$

we obtain the elliptic curve

$$\mathcal{E}: \quad y'^2 = x'^3 - 2756166750x' - 22014881915625 =: g(x')$$

which is in canonical form. Applying Cremona's *mwrank* program [10] we find that $\mathcal{E}$ has rank one over the rational numbers and that a generator of the infinite part of the Mordell–Weil group is given by

$$P_1 = (890919999/14161, -12337932682818/1685159).$$

The torsion subgroup has order two and is generated by $T = (-47925, 0)$.

The main idea of [8] is to express the elliptic integral related to the quartic elliptic equation by real values of elliptic logarithms u_i of points of $\mathcal{E}(\mathbb{R})$. Denote by ω the fundamental real period of the Weierstraß $\wp$-function associated to $\mathcal{E}$ and by e_1 the largest real root of the equation $g(t) = 0$. Then by [9] we can define for every point $P = (x_P, y_P) \in \mathcal{E}(\mathbb{R})$ with $x_P \geq e_1$ the elliptic logarithm of P by

$$\psi(P) \equiv \pm\frac{1}{\omega} \int_{x_P}^{\infty} \frac{dt}{\sqrt{g(t)}} \pmod 1.$$

We need some further notation: Denote by $(U, V) \in \mathcal{Q}(\mathbb{Z})$ an integral solution of equation (7) and by $P \in \mathcal{E}(\mathbb{R})$ the corresponding point on $\mathcal{E}$. Further let P_0 be the point $(x_0, y_0) = (22010\sqrt{355} + 406475, 19714925\sqrt{355} +$

$371143625) \in \mathcal{E}(\mathbb{R})$. We assume in what follows that U is a positive integer. Then, by a simple but tedious calculation we obtain

$$\int_U^\infty \frac{du}{\sqrt{Q(u)}} = -\int_{x_0}^{f^*(U)} \frac{dt}{\sqrt{g(t)}}$$

if $U > 55$. Checking the criteria from [8] we see that relation (13) in [8] holds. Moreover, either P or $P+T$ may be written as $m_1 P_1$ for a suitable integer $m_1 \in \mathbb{Z}$. It follows that

$$-\int_U^\infty \frac{du}{\sqrt{Q(u)}} = \psi(P_0) + m_1\psi(P_1) + m_0\omega.$$

Since P_0 and P_1 are linearly independent over the rational numbers the last equation defines already a linear form in elliptic logarithms. The values of these logarithms are given by

$$\omega = 0.09850931\ldots, \quad \psi(P_0) = 0.00993580\ldots \quad \text{and} \quad \psi(P) = 0.05808409\ldots$$

Following the arguments in [8], we can derive an upper bound for the absolute value of the occurring linear form. A combination of this upper bound and the lower bound for linear forms in elliptic logarithms due to S. David [3] results in the upper bound $M \le 10^{26}$ for the size of the absolute value $|m_1|$. From the normalization of the elliptic logarithm it is immediate that $|m_0|$ is bounded by $M+1$. Applying two times standard reduction techniques in combination with Proposition 4 of [8] we are able to reduce the initial bound on M to 3. We compute all linear combinations m_1P_1 and m_1P_1+T for $|m_1| \le 3$, map these points back to the quartic elliptic equation and check if we found an integral solution or not. Finally, we have to make sure that we found all "small solutions". This can be done by checking if $Q(u)$ is a square for integer values $0 \le u \le 55$. The calculation showed that the only integral solutions of equation (7) are given by $(0, \pm 11005)$.

Remark. In the last computations we assumed $U > 0$. For negative values of U we have to do the same calculations for the quartic equation $v^2 = Q(-u)$. The computations for this curve have been done too and did not yield any new solutions. It follows that equation (6) has no integral points.

The three remaining quartic elliptic equations were solved analogously. It turned out that all curves correspond to elliptic curves in canonical form with rank one over the rational numbers. Finally, we were able to show that only the elliptic curve $31y^2 = x^4 + x^3 + x^2 + x + 1$ has integral solutions. These solutions are given by $(2, \pm 1)$.

4. The case $n = 7$. Finally, we consider the diophantine equation

$$x^7 = 71y^2 + 1.$$

By putting $X = 71x$ and $Y = 71^4 y$ we obtain the equation

$$X^7 = Y^2 + 71^6 \cdot 71. \tag{8}$$

The computation of all integer solutions of (8) can be reduced to the analysis of several Thue equations. This approach was used by M. Mignotte and B. M. M. de Weger to solve two similar equations of degree five [6]. Below we follow the arguments from [6].

We denote by $\mathbb{K}$ the imaginary quadratic number field $\mathbb{Q}(\sqrt{-71})$. The class number of $\mathbb{K}$ is seven and an integral basis of $\mathbb{K}$ is given by the two generators $w_0 = 1$ and $w_1 = (1+\sqrt{-71})/2$. To find the set of Thue equations corresponding to equation (8) we consider this equation as an equation in ideals in $\mathbb{K}$. Then we have

$$\langle Y + 71^3 \cdot \sqrt{-71} \rangle = \mathfrak{a}^7$$

for some integral ideal $\mathfrak{a}$ in $\mathbb{K}$. We observe that the prime 3 splits, say

$$\langle 3 \rangle = \mathfrak{p}\overline{\mathfrak{p}},$$

where $\mathfrak{p} = \langle 3, 1 + 2w_1 \rangle$. It follows that the ideal class of $\mathfrak{p}$ has order 7 in the classgroup and that there is an integer k with $|k| \le 3$ such that $\mathfrak{p}^{-k}\mathfrak{a}$ is a principal ideal. Moreover there exist $u', v' \in N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p})^{-\max\{0,k\}} \cdot \mathbb{Z}$ with

$$\mathfrak{p}^{-k}\mathfrak{a} = \langle u' + v'w_1 \rangle.$$

It follows that

$$Y + 71^3 \cdot \sqrt{-71} = \gamma^k (u' + v'w_1)^7, \tag{9}$$

where γ is a generator of the principal ideal $\mathfrak{p}^7$. A value for γ may be computed by solving a norm equation in the number field $\mathbb{K}$. Our computation showed that we can take $\gamma = -45 - 2w_1$. Comparing the imaginary parts in equation (9) and multiplying by a common denominator leads to the desired Thue equations. By taking a closer look at these equations it follows by symmetry reasons that it suffices to restrict further considerations to the cases with $k \ge 0$.

Let $k \ge 0$ and denote by $u, v \in \mathbb{Z}$ integers such that $u' = 3^{-k}u$ and $v' = 3^{-k}v$. We distinguish four cases:

In the case $k = 0$ we have

$$-3977u^7 + 6307u^6v + 5691u^5v^2 - 1225u^4v^3 - 595u^3v^4 + 21u^2v^5 + 7uv^6 = 715822,$$

which can be solved quite easily. One can check that the only solution (u, v) in integers is given by $(1, -2)$. This solution corresponds to the trivial solution $(x, y) = (1, 0)$ of the original equation.

If $k = 1$ we have to find the integral solutions of the Thue equation

$$219355u^7 - 228137u^6v - 293937u^5v^2 + 36155u^4v^3 + 29225u^3v^4 - 231u^2v^5 - 329uv^6 - 2v^7 = 1565502714.$$

It is not possible to solve this equation modulo 43, hence it has no solution in rational integers.

In the case $k = 2$ we have to consider the equation

$$184u^7 + 14959u^6v - 24675u^5v^2 - 1387435u^4v^3 - 647185u^3v^4 + 14595987u^2v^5 + 7195195uv^6 - 11482961v^7 = 3423754435518.$$

One can observe that in this case we have $9 \mid (u + v)$. This allows us to simplify the equation by putting $\frac{1}{9}(u + v) = U$ and $v = V$, which leads to the equation

$$184U^7 + 1519U^6V - 1365U^5V^2 - 1435U^4V^3 + 665U^3V^4 + 147U^2V^5 - 35V^6U - V^7 = 2 \cdot 71^3.$$

We solved this equation by applying the **ThueSolve** function in Magma, and no solution was found.

Finally, we consider the case $k = 3$. This time we have to find the integral solutions (u, v) of

$$-12554u^7 - 656705u^6v + 2775297u^5v^2 + 63728945u^4v^3 - 19529965u^3v^4 - 699990585u^2v^5 - 163022321uv^6 + 576703027v^7 = 7487750950477866.$$

One can observe that in this case we have $81 \mid (u + 10v)$. As in the previous case a simplification is possible. This time we substitute $\frac{1}{81}(u + 10v) = U$ and $v = V$, which leads to

$$-12554U^7 + 8225U^6V + 21693U^5V^2 - 31535U^4V^3 + 16835U^3V^4 - 4305U^2V^5 + 511UV^6 - 21V^7 = 2 \cdot 71^3.$$

We solved this equation by Magma, and no solution was found. This completes our argument and the Theorem follows.

References

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. 24 (1997), 235–265. See also the Magma home page at http://www.maths.usyd.edu.au:8000/u/magma/.

[2] J. H. E. Cohn, *The Diophantine equation* $x^n = Dy^2 + 1$, Acta Arith. 106 (2003), 73–83.

[3] S. David, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. Fr. (N.S.) 62 (1995), iv+143 pp.

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

[5] —, —, —, *On Mordell's equation*, Compositio Math. 110 (1998), 335–367.

[6] M. Mignotte and B. M. M. de Weger, *On the diophantine equations* $x^2 + 74 = y^5$ *and* $x^2 + 86 = y^5$, Glasgow Math. J. 38 (1996), 77–85.
[7] R. J. Stroeker and N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. 67 (1994), 177–196.
[8] N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations*, ibid. 75 (1996), 165–190.
[9] D. Zagier, *Large integral points on elliptic curves*, Math. Comp. 48 (1987), 425–436.
[10] mwrank, *A package to compute ranks of elliptic curves*. See J. Cremona's home page at http://www.maths.ott.ac.uk/personal/jec/ftp/progs.

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

Institute of Mathematics
University of Debrecen
P.O. Box 12
H-4010 Debrecen, Hungary
E-mail: ijarasi@math.klte.hu

Institute of Informatics
University of Debrecen
P.O. Box 12
H-4010 Debrecen, Hungary
E-mail: pethoe@inf.unideb.hu

Received on 4.3.2003
and in revised form on 14.8.2003 (4480)