Publ. Math. Debrecen
51 / 3-4 (1997), 331–342

On a diophantine equation concerning the number of integer points in special domains II

By L. HAJDU (Debrecen)

Abstract. In an earlier paper we considered a family of polynomial diophantine equations which are closely related to the number of integer points in special domains, and we solved some of these equations. In this paper we investigate a more general family of equations. We give some properties of the polynomials involved, and we solve all those equations, which turn to be elliptic ones.

1. Introduction

In an earlier paper (cf. [5]) we dealt with the diophantine equation

$$\begin{aligned} &\#\{(x_1,x_2)\in\mathbb{Z}^2 : |x_1|+|x_2|\le r\}\\ &=\#\{(y_1,\dots,y_n)\in\mathbb{Z}^n : \sum_{i=1}^{n}|y_i|\le R\}. \end{aligned} \tag{1}$$

As we remarked in [5], this equation has some geometrical and combinatorical aspects. For $n=3$ and $n=4$, equation (1) was completely solved. Further, we made the conjecture that for every $n>2$, equation (1) has only finitely many solutions. In the first part of this paper we will prove this conjecture for $n=6$. In fact we will solve (1) in this case completely.

Mathematics Subject Classification: Primary 11P21, 11D41, 11D25; Secondary 11B83.
Key words and phrases: integer points, polynomial recurrence, polynomial diophantine equations, elliptic equations.
Research supported in part by the Hungarian Academy of Sciences, by Grants 014245 and T 016 975 from the Hungarian National Foundation for Scientific Research and by the Universitas Foundation of Kereskedelmi Bank RT.

Moreover, one can consider the following, more general equation:

$$\begin{aligned}&\#\{(x_1,\dots,x_k)\in\mathbb{Z}^k:\sum_{i=1}^{k}|x_i|\le r\}\\ &=\#\{(y_1,\dots,y_n)\in\mathbb{Z}^n:\sum_{i=1}^{n}|y_i|\le R\}.\end{aligned}\tag{2}$$

Subsequently we will completely solve equation (2) in the cases $(k,n)=(3,4)$ and $(4,6)$.

All three above equations turn out (after certain substitutions) to be elliptic equations. As we mentioned also in [5], the recent bounds concerning the solutions of elliptic equations are still too large, in general, to use them for solving a concrete equation. (For the best known explicit bounds concerning the solutions cf. [6].) Thus, just as in [5], we will use the elliptic equation package of the computational numbertheoretical program package SIMATH (cf. [9]) to solve our equations. We mention here that the elliptic curve package of SIMATH is based on an algorithm developed by J. Gebel, A. Pethő and H. G. Zimmer [3], and independently R. J. Stroeker and N. Tzanakis [10].

2. Notation

First we introduce our notation. Let, as in [5],

$$f_n(r)=\#\{(x_1,\dots,x_n)\in\mathbb{Z}^n:\ |x_1|+\dots+|x_n|\le r\}\text{ for }n=1,2,\dots$$

and

$$f_n(r)=1\text{ for }n=0.$$

For $n\le 6$ we have

$$f_0(r)=1,\ f_1(r)=2r+1,\ f_2(r)=2r^2+2r+1,$$
$$f_3(r)=\frac{4}{3}r^3+2r^2+\frac{8}{3}r+1,$$
$$f_4(r)=\frac{2}{3}r^4+\frac{4}{3}r^3+\frac{10}{3}r^2+\frac{8}{3}r+1,$$
$$f_5(r)=\frac{4}{15}r^5+\frac{2}{3}r^4+\frac{8}{3}r^3+\frac{10}{3}r^2+\frac{46}{15}r+1,$$

and

$$f_6(r)=\frac{4}{45}r^6+\frac{4}{15}r^5+\frac{14}{9}r^4+\frac{8}{3}r^3+\frac{196}{45}r^2+\frac{46}{15}r+1.$$

One can verify easily that the degree of f_n is n, and for $n \geq 1$ the polynomials satisfy the following recursion:

$$f_n(r) = 2\sum_{k=0}^{r-1} f_{n-1}(k) \;+\; f_{n-1}(r).$$

3. Results

In this section we formulate our results.[1] First we give some trivial properties of the polynomials f_n.

Theorem 1.

1. *If n is odd (resp. even) then the polynomial $f_n(r)$ is odd (resp. even) with respect to $-\frac{1}{2}$, that is for every $r \in \mathbb{R}$ we have $f_n(-\frac{1}{2}+r) = -f_n(-\frac{1}{2}-r)$ (resp. $f_n(-\frac{1}{2}+r) = f_n(-\frac{1}{2}-r)$).*
2. *For nonnegative integers n and k we have $f_n(k) = f_k(n)$.*

The above statements can be proved simply e.g. by induction, and we omit the details.

Now we turn to the equations

$$f_2(r) = f_6(R) \text{ in } \; r, R \in \mathbb{Z}, \; r, R \geq 0, \tag{3}$$

$$f_3(r) = f_4(R) \text{ in } \; r, R \in \mathbb{Z}, \; r, R \geq 0, \tag{4}$$

and

$$f_4(r) = f_6(R) \text{ in } \; r, R \in \mathbb{Z}, \; r, R \geq 0. \tag{5}$$

Here we would like to mention that for all the remaining pairs (n,k) (that is for $(n,k) \notin \{(2,3),(2,6),(3,4),(4,6)\}$) the equation

$$f_n(r) = f_k(R) \text{ in } \; r, R \in \mathbb{Z}, \; r, R \geq 0$$

does not seem to be an elliptic equation. Hence to solve this equation for the remaining pairs (n,k), some other method should be used. (In fact in [5] to solve equation (1) for $(n,k) = (2,4)$ we used the arguments of Á. Pintér [8] and B. M. M. de Weger [13].)

We also remark that very recently B. Brindza and Á. Pintér (cf. [1]) obtained finiteness results concerning the solutions of equations of the type $f(x) = g(y)$, where f and g are polynomials with integer coefficients. However, in [1] f and g are of some special kind, and unfortunately the method

[1] *Added in proof.* After this paper was accepted for publication, Professor J. Vaaler informed me that Theorem 1 was independently proved in a joint paper (to appear) of D. Bump, K. K. S. Choi, P. Kurlberg and J. Vaaler.

of B. Brindza and Á. Pintér does not seem to be applicable for our equations.

First we will prove that the only solutions of (3) are $(r,R)=(0,0)$, $(2,1)$ and $(6,2)$. In fact we will prove more, we show that the only solutions of (3) in *integers* are $(r,R)=(-7,2)$, $(-7,-3)$, $(-3,1)$, $(-3,-2)$, $(-1,0)$, $(-1,-1)$, $(0,0)$, $(0,-1)$, $(2,1)$, $(2,-2)$, $(6,2)$ and $(6,-3)$.

This statement will follow from Theorem 2. Put $x=90R^2+90R+435$ and $y=4050r+2025$. Then from equation (3) we get the elliptic equation

$$x^3-288225x+47165625=y^2 \quad \text{in integers } x,y. \tag{6}$$

We have the following

Theorem 2. *The only integer solutions of equation* (6) *are* $(x,\pm y)=$ $(40,5975)$, $(-375,10125)$, $(165,2025)$, $(2271,105381)$, $(435,2025)$, $(-600,2025)$, $(3891,240489)$, $(129,3483)$, $(23115,3513375)$,$(85,4825)$, $(975,26325)$, $(-240,10125)$, $(475,4175)$, $(-456,9153)$, $(615,10125)$, $(-51,7857)$ *and* $(57475,13778425)$.

As a simple consequence of Theorem 2 we obtain our statement concerning the solutions of (3).

We will also prove that the only nonnegative integer solutions of (4) are $(r,R)=(0,0)$ and $(4,3)$. We shall prove more, namely that the only solutions of (4) in *integers* are $(r,R)=(0,0)$, $(0,-1)$, $(4,3)$ and $(4,-4)$. This statement will follow from Theorem 3. Put $x=2r+1$ and $y=2R^2+2R+4$. Then from equation (4) we get the equation

$$x^3+5x+10=y^2 \quad \text{in integers } x,y. \tag{7}$$

We have the following

Theorem 3. *The only integer solutions of equation* (7) *are* $(x,\pm y)=$ $(1,4)$, $(-1,2)$, $(9,28)$ *and* $(6,16)$.

Our statement concerning the solutions of (4) now follows as a simple consequence.

We will prove as well that the only nonnegative integer solutions of (5) are $(r,R)=(0,0)$ and $(6,4)$. We will prove more again, namely that the only solutions of (5) in *integers* are $(r,R)=(-7,4)$, $(-7,-5)$, $(-1,0)$, $(-1,-1)$, $(0,0)$, $(0,-1)$, $(6,4)$ and $(6,-5)$. This statement will follow from

Theorem 4. Put $x = 30R^2 + 30R + 145$ and $y = 450r^2 + 450r + 900$. Then from equation (5) we get the equation

$$x^3 - 32025x + 2405000 = y^2 \quad \text{in integers } x,\ y. \tag{8}$$

We have the following

Theorem 4. *The only integer solutions of equation* (8) *are* $(x, \pm y) =$ $(200, 2000)$, $(55, 900)$, $(145, 900)$, $(-200, 900)$, $(655, 16200)$, $(745, 19800)$, $(100, 450)$, $(-55, 2000)$, $(-145, 2000)$ *and* $(158600, 63161800)$.

Our statement concerning the solutions of (5) now follows immediately.

4. Proofs of the Theorems

As was previously remarked, we omit the easy proof of Theorem 1.

To the proof of our Theorems 2, 3 and 4, we need a Lemma and some new notation. In fact we will use the usual notations concerning elliptic curves, but for the convenience of the reader we give them here as well. For a more detailed study of elliptic curves we refer to [3] and [4].

Let E be an elliptic curve over $\mathbb{Q}$ defined by

$$E: \quad y^2 = x^3 + ax + b \quad (a, b \in \mathbb{Z})$$

with nonzero discriminant. Let r denote the rank, g the number of torsion points and j the j-invariant (or modular invariant) of E. For any point P of E denote by $\hat{h}(P)$ the canonical height (or Néron-Tate height) of P. $\hat{h}$ is a positive definite quadratic form; denote by λ_1 its smallest eigenvalue.

Choose a basis $P_1, \ldots, P_r$ of the Mordell-Weyl group of E. Now every point P of E has a unique representation of the form

$$P = \sum_{i=1}^{r} n_i P_i + P_{r+1} \ (n_i \in \mathbb{Z}),$$

where P_{r+1} is some torsion point. Let

$$N = \max_{1 \le i \le r} |n_i|.$$

Denote by μ_∞ the height of E, i.e.

$$\mu_\infty = \log \max\{|a|^{1/2}, |b|^{1/3}\}.$$

Denote by $\wp$ Weierstrass' $\wp$ function corresponding to E, and let P be any point of E. Then we have

$$P = (\wp(u), \wp'(u))$$

for some complex number u with $|u| \leq \frac{1}{2}$. Here u is called the elliptic logarithm of P. Denote by ω_1 and ω_2 the real and the complex period of E, respectively, and let $\tau = \pm\omega_2/\omega_1$, such that $\mathrm{Im}(\tau) > 0$. Let $j = \frac{j_1}{j_2}$ with $j_1, j_2 \in \mathbb{Z}$, $(j_1, j_2) = 1$ and put $h = \log\max\{4|aj_2|, 4|bj_2|, |j_1|, |j_2|\}$. Choose real numbers $V_1, \ldots, V_r$ with

$$\log V_i \geq \max\left\{\hat{h}(P_i), h, \frac{3\pi|u_i|^2}{\omega_1^2\,\mathrm{Im}(\tau)}\right\} \quad \text{for } i = 1, \ldots, r,$$

where u_i is the elliptic logarithm of P_i, $i = 1, \ldots, r$.

It is well-known that already from a result of L. J. Mordell [7], by a famous theorem of A. Thue [11], it follows that the number of integer points on E is finite.

Using the following Lemma (due to J. Gebel, A. Pethő and H. G. Zimmer [3]), one can find, at least in principle, all the integer points on a given elliptic curve. We remark that we used this Lemma in [5] as well.

Lemma. *Preserving the above notations, let* $P = \sum_{i=1}^{r} n_i P_i + P_{r+1}$ *be an integral point on the elliptic curve* E*, where* $P_1, \ldots, P_r$ *is a basis of the Mordell-Weyl group of* E*, and* P_{r+1} *is a torsion point. Then the maximum*

$$N = \max_{1 \leq i \leq r}\{|n_i|\}$$

satisfies the inequality

$$N \leq \max\left\{2^{r+2}\sqrt{c_1c_2}\left(\log(c_2(r+2)^{r+2})\right)^{(r+2)/2}, \frac{2\max\limits_{1\leq i\leq r}\{V_i\}}{r+1}\right\},$$

where

$$c_1 = \max\left\{\frac{\log(g{c_1}')}{\lambda_1}, 1\right\} \text{ and } c_2 = \max\left\{\frac{C}{\lambda_1}, 10^9\right\}\left(\frac{h}{2}\right)^{r+1}\prod_{i=1}^{r}\log V_i$$

with

$${c_1}' = \frac{2^{\frac{13}{6}}}{\omega_1} \text{ and } C = 2.9 \cdot 10^{6r+6} \cdot 4^{2r^2} \cdot (r+1)^{2r^2+9r+12.3}.$$

Proof. This statement is proved in [3] (see the Theorem in [3] on page 180) using a lower bound for linear forms in elliptic logarithms, due to S. David [2].

Now we will prove Theorems 2, 3 and 4. As the proofs are similar, we will give them simultaneously.

Proof of the Theorems. We will follow the discussion in [4] and [5], and we preserve the above notations. Let

$$E_1 = \{(x,y) \mid (x,y) \in \mathbb{Q}^2,\ x^3 - 288225x + 47165625 = y^2\} \cup \{\mathcal{O}\},$$

$$E_2 = \{(x,y) \mid (x,y) \in \mathbb{Q}^2,\ x^3 + 5x + 10 = y^2\} \cup \{\mathcal{O}\},$$

and

$$E_3 = \{(x,y) \mid (x,y) \in \mathbb{Q}^2,\ x^3 - 32025x + 2405000 = y^2\} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ denotes the point at infinity. In the sequel we determine some parameters of E_1, E_2 and E_3 using SIMATH. Writing E_i we will always suppose that $i \in \{1,2,3\}$, and $p(E_i)$ will denote the corresponding parameter p of E_i. The modular invariant of E_i is

	E_1	E_2	E_3
$j(E_i) = j_1(E_i)/j_2(E_i) =$	$\frac{19930747648}{4300641}$	$\frac{270}{1}$	$\frac{-4982686912}{544071}$

and the height of E_i is

	E_1	E_2	E_3
$\mu_\infty(E_i) =$	6.28574835...	0.80471895...	5.18713606...

To use our Lemma, one has to know a basis as well as the torsion group of E_i. Using SIMATH, it turns out that the only torsion point of E_i is $\mathcal{O}$, hence $g(E_i) = 1$. The rank of E_i is

	E_1	E_2	E_3
$r(E_i) =$	3	1	3

We can determine a basis $B(E_i)$ of the Mordell-Weyl group of E_i. We obtain $B(E_1) = \{P_1 = (165, 2025),\ P_2 = (435, 2025),\ P_3 = (975, 26325)\}$, $B(E_2) = \{P_4 = (1, 4)\}$ and $B(E_3) = \{P_5 = (55, 900),\ P_6 = (145, 900),\ P_7 = (100, 450)\}$ with

$$\hat{h}(P_1) = 1.09722796\ldots,\ \hat{h}(P_2) = 1.22682755\ldots,\ \hat{h}(P_3) = 1.98354011\ldots,$$

$$\hat{h}(P_4) = 0.12837506\ldots,$$

and

$$\hat{h}(P_5) = 1.67154020\ldots, \ \hat{h}(P_6) = 1.71887124\ldots,$$
$$\hat{h}(P_7) = 1.84960414\ldots.$$

Hence we get

	E_1	E_2	E_3
$\lambda_1(E_i) =$	0.79418680...	0.12837506...	1.51120454...

The real and the complex periods of E_i are

	E_1	E_2	E_3
$\omega_1(E_i) =$	0.41216398...	2.52921076...	0.51927608...

and

	E_1	E_2	E_3
$\omega_2(E_i)$=	$i \cdot 0.31380448\ldots$	$1.26460538\ldots+$ $i \cdot 0.90405376\ldots$	$0.25963804\ldots+$ $i \cdot 0.08867484\ldots$

respectively, whence

	E_1	E_2	E_3
$\mathrm{Im}(\tau(E_i)) =$	0.76135834...	0.35744500...	0.17076627...

We have

	E_1	E_2	E_3
${c_1}'(E_i) <$	10.89335407	1.77519733	8.64636044

and

	E_1	E_2	E_3
$c_1(E_i) <$	3.00704175	4.47058465	1.42742985

Moreover, we obtain

	E_1	E_2	E_3
$h(E_i) <$	34.32974491	5.59842196	29.28618986

Therefore we may choose

$$V_i = e^{h(E_1)} = 811369682662500 \text{ for } i = 1, 2, 3,$$
$$V_i = e^{h(E_2)} = 270 \text{ for } i = 4,$$

and

$$V_i = 1.67 \cdot 10^{22} \text{ for } i = 5, 6, 7.$$

For the constant $C(E_i)$ we obtain

	E_1	E_2	E_3
$C(E_i) <$	$6.28 \cdot 10^{69}$	$4.80 \cdot 10^{20}$	$6.28 \cdot 10^{69}$

whence

	E_1	E_2	E_3
$c_2(E_i) <$	$2.78 \cdot 10^{79}$	$1.64 \cdot 10^{23}$	$2.56 \cdot 10^{79}$

Using the above parameters, our Lemma yields the estimates

	E_1	E_2	E_3
$N(E_i) <$	$1.48 \cdot 10^{47}$	$2.93 \cdot 10^{15}$	$9.74 \cdot 10^{46}$

Now using B. M. M. de Weger's method (see [12]), these initial bounds can be reduced, and using SIMATH again, we obtain all the integral points on E_i. In the following tables we give these integral points as well as their coordinates in the above calculated basis of E_i.

All integer points on E_1:

$(x, \pm y)$	coeff. of P_1	coeff. of P_2	coeff. of P_3
$(40, 5975)$	1	-2	0
$(-375, 10125)$	-1	1	0
$(165, 2025)$	1	0	0
$(2271, 105381)$	2	0	0
$(435, 2025)$	0	1	0
$(-600, 2025)$	-1	-1	0
$(3891, 240489)$	0	-2	0
$(129, 3483)$	-1	1	-1
$(23115, 3513375)$	-2	1	-1
$(85, 4825)$	-1	0	1
$(975, 26325)$	0	0	1
$(-240, 10125)$	1	0	1
$(475, 4175)$	2	0	1
$(-456, 9153)$	1	-1	-1
$(615, 10125)$	0	-1	-1
$(-51, 7857)$	-1	-1	-1
$(57475, 13778425)$	2	-2	-1

All integer points on E_2:

$(x, \pm y)$	coeff. of P_4
$(1, 4)$	1
$(-1, 2)$	-2
$(9, 28)$	-3
$(6, 16)$	4

All integer points on E_3:

$(x, \pm y)$	coeff. of P_5	coeff. of P_6	coeff. of P_7
$(200, 2000)$	1	-1	0
$(55, 900)$	1	0	0
$(145, 900)$	0	1	0
$(-200, 900)$	-1	-1	0
$(655, 16200)$	0	-1	1
$(745, 19800)$	1	0	-1
$(100, 450)$	0	0	1
$(-55, 2000)$	-1	0	-1
$(-145, 2000)$	0	1	1
$(158600, 63161800)$	-1	-1	2

$\square$

Acknowledgements. I would like to thank Professors K. Győry and A. Pethő for their valuable and useful advices and Professor Á. Pintér for his generous help.

References

[1] B. Brindza and Á. Pintér, On the irreducibility of some polynomials in two variables (*to appear*).

[2] S. David, Minorations de formes linéaires de logarithmes elliptiques, *Mémoires de la Société Mathématique de France, Nouvelle série, Supplément ou Bulletin de la Société Mathématique de France* **No 62** (1995), t. 123.

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

[4] J. Gebel, A. Pethő and H. G. Zimmer, On Mordell's equation *Compositio Math.*, (*to appear*).

[5] L. Hajdu, On a diophantine equation concerning the number of integer points in special domains *Acta. Math. Hung.*, (*to appear*).

[6] L. Hajdu and T. Herendi, Explicit bounds for the solutions of elliptic equations (*in preparation*).

[7] L. J. Mordell, Indeterminate equations of the third and fourth degrees, *Quart. J. Pure and Appl. Math.* **45** (1914), 170–186.

[8] Á. Pintér, A note on the Diophantine equation $\binom{x}{4} = \binom{y}{2}$, *Publ. Math. Debrecen* **47**/3–4 (1995), 411–415.

[9] SIMATH Manual, *Universität des Saarlandes, Saarbrücken*, *Germany*, 1993.
[10] R. J. Stroeker and N. Tzanakis, Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms, *Acta Arith.* **67** (1994), 177–196.
[11] A. Thue, Über Annäherungswerte algebraischer Zahlen, *J. Reine Angew. Math.* **135** (1909), 284–305.
[12] B. M. M. de Weger, Algorithms for diophantine equations, CWI Tract 65, *Stichting Mathematisch Centrum*, *Amsterdam*, 1989.
[13] B. M. M. de Weger, A binomial diophantine equation, *Quart. J. Math. Oxford* (2) **47** (1996), 221–231.

LAJOS HAJDU
INSTITUTE OF MATHEMATICS AND INFORMATICS
LAJOS KOSSUTH UNIVERSITY
H–4010 DEBRECEN, P.O.BOX 12
HUNGARY
E-MAIL: hajdul@math.klte.hu

(Received February 10, 1997)