COLLOQUIUM MATHEMATICUM

VOL. 121 2010 NO. 2

ON SYSTEMS OF DIOPHANTINE EQUATIONS WITH A LARGE NUMBER OF SOLUTIONS

BY

JERZY BROWKIN (Warszawa)

Abstract. We consider systems of equations of the form $x_i + x_j = x_k$ and $x_i \cdot x_j = x_k$, which have finitely many integer solutions, proposed by A. Tyszka. For such a system we construct a slightly larger one with much more solutions than the given one.

1. Introduction. In the present paper we construct some systems of diophantine equations of the form considered by A. Tyszka (see [T]) with a large number of solutions.

Let

$$E_n := \{x_1 = 1,\ x_i + x_j = x_k,\ x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\}\}.$$

We consider systems S of equations contained in E_n, and their integer solutions. For simplicity we assume that the equation $x_1 = 1$ does not belong to S, but it is not an essential restriction.

We assume that the system $S \subseteq E_n$ has a finite number N_S of solutions. Obviously $0 := (0, \ldots, 0)$ is a solution, so $N_S \geq 1$. For a solution $a := (a_1, \ldots, a_n)$ of S we denote (1) $m(a) := \max_{1 \leq j \leq n} a_j$. Let

$$M_S := \max_a m(a),$$

where a runs over all solutions of S.

In an earlier preprint Tyszka conjectured that $N_S \leq 2^n$, under the above assumptions and notation. Later he found counterexamples with $n \geq 14$ (2).

In the present paper we construct for $n \geq 16$ an example of a system S with N_S much larger than 2^n. Next we show that every system $S \subseteq E_n$ with a finite number of solutions, which has a solution a with a sufficiently large $m(a)$, can be extended to a system T with slightly more variables than in S, which has a finite but large number of solutions. A precise statement is given in Theorem 1.

2010 *Mathematics Subject Classification*: 11D45, 11D72, 11E25.

Key words and phrases: systems of equations, number of solutions.

(1) It is not a mistake: We define $m(a)$ to be $\max a_j$, and not $\max |a_j|$.

(2) See also the note at the end of the paper.

DOI: 10.4064/cm121-2-3

2. An example. Let us consider the system

$$x_1 + x_1 = x_2, \qquad x_1 \cdot x_1 = x_2. \tag{1}$$

Obviously it has only two solutions $(x_1, x_2) = (0,0)$ and $(2,4)$.

Then we extend it adding the equations

$$x_2 \cdot x_2 = x_3, \quad x_3 \cdot x_3 = x_4, \ \ldots, \ x_{m-1} \cdot x_{m-1} = x_m. \tag{2}$$

Obviously the system (1)–(2) has only two solutions $(x_1, \ldots, x_m) = (0, \ldots, 0)$ and $(2, 4, 16, \ldots, 2^{2^{m-1}})$.

Now we consider the equations

$$\begin{aligned} y_1 \cdot y_1 &= y_5, & y_2 \cdot y_2 &= y_6, & y_3 \cdot y_3 &= y_7, \\ y_4 \cdot y_4 &= y_8, & y_5 + y_6 &= y_9, & y_7 + y_8 &= y_{10}. \end{aligned} \tag{3}$$

From (3) it follows that $y_9 = y_1^2 + y_2^2$ and $y_{10} = y_3^2 + y_4^2$.

Finally we consider the equations

$$x_1 + x_m = x_{m+1}, \qquad y_9 + y_{10} = x_{m+1}. \tag{4}$$

Denote by S the system (1)–(4). It depends on $n := m + 11$ variables. Obviously, the zero solution of the system (1)–(2) extends, by (4) and (3), only to the zero solution of the system S. The nonzero solution of (1)–(2) leads, by (3) and (4), to the system

$$x_{m+1} = 2^{2^{m-1}} + 2, \qquad x_{m+1} = y_1^2 + y_2^2 + y_3^2 + y_4^2.$$

Hence the number of nonzero solutions of the system S equals the number of solutions of the equation

$$2^{2^{m-1}} + 2 = y_1^2 + y_2^2 + y_3^2 + y_4^2. \tag{5}$$

The theorem of Jacobi (see [K]) says that for a positive integer k not divisible by 4 the number of representations of k as the sum of four squares of integers equals $8\sigma(k)$, where $\sigma(k)$ is the sum of positive divisors of k.

Applying the Jacobi theorem we find that the number N_S of solutions of the system S equals

$$N_S = 1 + 8\sigma(2^{2^{m-1}} + 2) > 8 \cdot 2^{2^{m-1}} = 2^{2^{m-1}+3} = 2^{2^{n-12}+3}.$$

Consequently, $N_S > 2^n$ if $2^{n-12} + 3 > n$, which holds for $n \geq 16$.

3. Extending of a system S. Let $S \subseteq E_n$ be a system with a finite number of solutions, which has a solution a with $m(a)$ sufficiently large. Before extending it to a larger system T we prove a lemma.

LEMMA 1. *If a system $S \subseteq E_n$ has a finite number of solutions and has a nonzero solution $a = (a_1, \ldots, a_n)$, then*

(i) $m(a) \geq 0$,
(ii) *if* $m(a) = 0$, *then* $-a$ *is also a solution of* S, *and* $m(-a) > 0$.

Thus $M_S > 0$.

Proof. If the system S is linear, then it has infinitely many solutions $r \cdot a$, for $r \in \mathbb{Z}$, and we get a contradiction. Therefore S is not linear, hence some equation of the form $x_i \cdot x_j = x_k$ belongs to S.

Suppose that $m(a) < 0$, i.e. $a_t < 0$ for $1 \leq t \leq n$. Consequently, $a_i a_j > 0$ and $a_i a_j = a_k < 0$, which gives a contradiction. This proves (i).

If $m(a) = 0$, then $a_i \leq 0, a_j \leq 0, a_k \leq 0$. Hence $a_k = a_i a_j \geq 0$, which implies that $a_k = 0$, $a_i a_j = 0$. Consequently, $(-a_i)(-a_j) = 0 = -a_k$.

Therefore every nonlinear equation in S satisfied by a is also satisfied by $-a$. Obviously the same holds for linear equations. Consequently, $-a$ is a solution of S.

Since $m(a) = \max_j a_j = 0$ and $a \neq 0$, we have $\min_j a_j < 0$. Consequently, $m(-a) = \max_j(-a_j) = -\min_j a_j > 0$, which proves (ii). ■

We shall prove some relations between the numbers M_S and N_T, where T is a system containing S, defined below. Roughly speaking, we prove that if a system S has a solution a with a large value of $m(a)$, then extending slightly this system we get a system T with a finite number N_T of solutions, and this number is large. More precisely, a solution a of a system S with a large $m(a)$ extends to a large number of solutions of a slightly larger system T.

Theorem 1. *Assume that a system* $S \subseteq E_n$ *has a finite number of solutions, and it has a nonzero solution. Then there is a system* $T \subseteq E_m$, *where* $m = n + 23$, *with a finite number* N_T *of solutions, containing* S, *and satisfying*

$$N_T \geq M_S^2.$$

Proof. Let $a = (a_1, , \ldots, a_n)$ be a solution of S such that $M_S = m(a) = a_j$ for some j, $1 \leq j \leq n$. From Lemma 1 it follows that $M_S > 0$, thus $a_j > 0$.

We define a system $T \subseteq E_m$, where $m = n + 23$, and the variables in T are denoted by $x_1, \ldots, x_n, y_1, \ldots, y_{11}, y'_1, \ldots, y'_{11}, z$. Namely

$$T = S \cup U \cup U' \cup W,$$

where

$$U = \{y_1 \cdot y_1 = y_5,\ y_2 \cdot y_2 = y_6,\ y_3 \cdot y_3 = y_7,\ y_4 \cdot y_4 = y_8,$$
$$y_5 + y_6 = y_9,\ y_7 + y_8 = y_{10},\ y_9 + y_{10} = y_{11}\}.$$

The system U' is obtained from U by replacing y_j by y'_j for $j = 1, \ldots, 11$.

Finally

$$W = \{y_{11} + z = x_j,\ z + x_j = y'_{11}\},$$

where the index j is defined at the beginning of the proof.

From the definition of the system U we get $y_{11} = y_1^2 + y_2^2 + y_3^2 + y_4^2$, and similarly for y'_{11}. Consequently, y_{11} and y'_{11} take only nonnegative values for every solution of U, respectively U'. Then from the system W it follows that

$$x_j - z = y_{11} \geq 0, \qquad x_j + z = y'_{11} \geq 0.$$

Consequently,

$$-x_j \leq z \leq x_j, \quad \text{i.e.} \quad |z| \leq x_j. \tag{6}$$

We shall prove that the system T has a finite number of solutions. Let $e = (b_1, \ldots, b_n, c_1, \ldots, c_{11}, c'_1, \ldots, c'_{11}, d)$ be a solution of T. Then $b = (b_1, \ldots, b_n)$ is a solution of S, so there are only finitely many possibilities for the n-tuples b, by assumption.

From (6) we get $|d| \leq b_j$, so the number of values of d is finite. Moreover, from W we get $c_{11} + d = b_j$, $c'_{11} = d + b_j$. Hence c_{11} and c'_{11} are bounded. Finally, from U and U' we get $|c_k| \leq c_{11}$ and $|c'_k| \leq c'_{11}$ for $k = 1, \ldots, 10$.

We conclude that the number N_T of solutions of T is finite.

Now we estimate from below the number of solutions e of T which are of the form

$$e = (a_1, \ldots, a_n, c_1, \ldots, c_{11}, c'_1, \ldots, c'_{11}, d),$$

where $(a_1, \ldots, a_n)$ is the solution of the system S fixed at the beginning of the proof.

We choose arbitrarily the quadruple (c_1, c_2, c_3, c_4) of integers satisfying $|c_k| \leq \sqrt{a_j/2}$, $k = 1, 2, 3, 4$, and extend it (uniquely!) to a solution $(c_1, \ldots, c_{11})$ of the system U. Then

$$0 \leq c_1^2 + c_2^2 + c_3^2 + c_4^2 \leq 2a_j.$$

Define $d := a_j - c_{11}$; then $d + a_j = 2a_j - c_{11} \geq 0$. Consequently, $d + a_j$ is the sum of the squares of four integers: $d + a_j = {c'_1}^2 + {c'_2}^2 + {c'_3}^2 + {c'_4}^2$. Finally, we extend (uniquely!) the quadruple (c'_1, c'_2, c'_3, c'_4) to a solution $(c'_1, \ldots, c'_{11})$ of the system U'.

Thus we get a solution e of T. The number of solutions obtained in this way is equal to the number of quadruples (c_1, c_2, c_3, c_4) satisfying $|c_k| \leq \sqrt{a_j/2}$. This number is equal to $(2\lfloor\sqrt{a_j/2}\rfloor + 1)^4$. One can easily verify that $2\lfloor\sqrt{t/2}\rfloor + 1 \geq \sqrt{t}$ for every positive integer t.

Consequently,

$$N_T \geq (2\lfloor\sqrt{a_j/2}\rfloor + 1)^4 \geq \sqrt{a_j}^{\,4} = a_j^2 = M_S^2. \ \blacksquare$$

Remark 1. In the proof of Theorem 1 we did not use essentially the assumption that $M_S = a_j$. In fact, we have proved that for a fixed index j, $1 \leq j \leq n$, and every solution a of S with $a_j > 0$ there are at least a_j^2

solutions of T extending a. Therefore

$$N_T \geq \sum_a a_j^2,$$

where a runs over all solutions of S with $a_j > 0$, where j is fixed.

4. An asymptotic result. Improving slightly the argument in the proof of Theorem 1 we can get a better asymptotic result.

THEOREM 2. *Consider a family of systems $S \subseteq E_n$, where n depends on S, with finite numbers of solutions. Assume that the values of M_S are not bounded. For each S let T be the extended system defined in the proof of Theorem* 1. *Then*

$$N_T \geq 2\pi^2 M_S^2 + O(M_S \log M_S) \quad \text{as } M_S \to \infty.$$

Proof. As in the proof of Theorem 1, we shall describe the solutions of the system T which have the form

$$e = (a_1, \ldots, a_n, c_1, \ldots, c_{11}, c'_1, \ldots, c'_{11}, d),$$

where $a = (a_1, \ldots, a_n)$ is a solution of S with $a_j = M_S > 0$ for some fixed j. We look for all quadruples of integers (c_1, c_2, c_3, c_4) such that

$$0 \leq c_1^2 + c_2^2 + c_3^2 + c_4^2 \leq 2a_j = 2M_S.$$

Their number equals

$$\sum_{k=0}^{2M_S} r_4(k),$$

where $r_4(k)$ is the number of representations of a nonnegative integer k as the sum of four squares of integers.

Then we extend (uniquely!) the quadruple (c_1, c_2, c_3, c_4) to a solution of the system U. Next we define $d := a_j - c_{11}$, hence $-a_j \leq d \leq a_j$. Since $d + a_j \geq 0$, there are integers c'_1, c'_2, c'_3, c'_4 (not unique, in general) satisfying $d + a_j = {c'_1}^2 + {c'_2}^2 + {c'_3}^2 + {c'_4}^2$. We extend (uniquely!) the quadruple (c'_1, c'_2, c'_3, c'_4) to a solution of the system U'.

In this way we get some solutions of T extending the solution a of S. Thus the number of these solutions of T can be estimated from below by $\sum_{k=0}^{2M_S} r_4(k)$.

There are known exact and asymptotic formulas for this sum. By a theorem of Jacobi (see [K]) we have

$$\sum_{k \leq x} r_4(k) = 8 \sum_{k \leq x} \sigma(k) - 32 \sum_{k \leq x/4} \sigma(k).$$

By the well known asymptotic formula

$$\sum_{k\le x}\sigma(k)=\frac{\pi^2}{12}x^2+O(x\,\log x)\qquad \text{as } x\to\infty,$$

we get

$$\sum_{k\le x}r_4(k)=\frac{\pi^2}{2}x^2+O(x\,\log x)\qquad \text{as } x\to\infty.$$

Therefore

$$\begin{aligned}N_T\ge\sum_{k=0}^{2M_S}r_4(k)&=\frac{\pi^2}{2}(2M_S)^2+O(M_S\,\log M_S)\\&=2\pi^2M_S^2+O(M_S\,\log M_S)\end{aligned}$$

as $M_S\to\infty$. ∎

5. Another example. We apply Theorems 1 and 2 to the system $S\subseteq E_m$ considered in [T],

$$\begin{aligned}S=\{&x_1+x_1=x_2,\ x_1\cdot x_1=x_2,\\&x_2\cdot x_2=x_3,\ x_3\cdot x_3=x_4,\ \ldots,\ x_{m-1}\cdot x_{m-1}=x_m\}.\end{aligned}$$

It has a unique nonzero solution $a=(a_1,\ldots,a_m)=(2,4,16,\ldots,2^{2^{m-1}})$ with $m(a)=a_m=2^{2^{m-1}}=M_S$. The extension T of S, defined in the proof of Theorem 1, has $n=m+23$ variables. Then, by Theorem 1, we get

$$N_T\ge M_S^2=2^{2^m}=2^{2^{n-23}}.$$

Consequently, $N_T>2^n$ if $2^{n-23}>n$, which holds for $n\ge 28$.

By the asymptotic result in Theorem 2 we get

$$N_T\ge 2\pi^2M_S^2+O(M_S\log M_S)=2\pi^2 2^{2^{n-23}}+O(2^{n-2+2^{n-24}})$$

as $n\to\infty$.

Note added in proof (October 2010). Recently we have obtained counterexamples with $n\ge 10$. Namely, let us consider the system

$$\begin{aligned}&x_1=1,\quad x_1+x_1=x_2,\\&x_2\cdot x_2=x_3,\quad x_3\cdot x_3=x_4,\ \ldots,\ x_{k-1}\cdot x_{k-1}=x_k.\end{aligned}\tag{7}$$

It has the unique solution $x_j=2^{2^{j-2}}$ for $2\le j\le k$. Then we extend it by adding the equations

$$y_1\cdot y_2=x_k,\quad y_3\cdot y_4=x_k,\ \ldots,\ y_{2m-1}\cdot y_{2m}=x_k.\tag{8}$$

Every y_{2i-1}, $1\le i\le m$, is an arbitrary divisor of $x_k=2^{2^{k-2}}$, hence $y_{2i-1}=\pm 2^{r_i}$, $0\le r_i\le 2^{k-2}$. It follows that y_{2i-1} can take $2(2^{k-2}+1)=2^{k-1}+2$ values. Then the corresponding value of y_{2i} is determined uniquely.

Therefore the number N_S of solutions of the system S given by (7) and (8) equals $(2^{k-1}+2)^m$. The number of variables in S is $n=k+2m$.

We have $N_S > 2^{m(k-1)}$, hence $N_S > 2^n$ holds if $m(k-1) \geq k+2m$, equivalently, if $k(1-1/m) \geq 3$. This inequality is valid for every pair (k,m) with $m \geq 2,\ k \geq 6$, hence for every $n=k+2m \geq 10$.

REFERENCES

[K] E. Krätzel, *Zahlentheorie*, Deutscher Verlag Wiss., Berlin, 1981.

[T] A. Tyszka, *A hypothetical upper bound for the solutions of a Diophantine equation with a finite number of solutions*, preprint, 2009; http://arxiv.org/abs/0901.2093.

Jerzy Browkin
Institute of Mathematics
Polish Academy of Sciences
Śniadeckich 8
00-956 Warszawa, Poland
E-mail: browkin@impan.pl

Received 29 November 2009 (5303)