MATEMATYKA
DYSKRETNA
www.ii.uj.edu.pl/preMD/

Apoloniusz TYSZKA

Some conjectures on integer arithmetic

Preprint Nr MD 046
(otrzymany dnia 4 I 2010)

Kraków
2010

Some conjectures on integer arithmetic

Apoloniusz Tyszka

Abstract. We conjecture: if integers $x_1, \ldots, x_n$ satisfy $x_1^2 > 2^{2^n} \vee \ldots \vee x_n^2 > 2^{2^n}$, then

$$(\forall i,j,k \in \{1,\ldots,n\}\ (x_i + x_j = x_k \Rightarrow y_i + y_j = y_k)) \wedge$$
$$(\forall i,j,k \in \{1,\ldots,n\}\ (x_i \cdot x_j = x_k \Rightarrow y_i \cdot y_j = y_k))$$

for some integers $y_1, \ldots, y_n$ satisfying $y_1^2 + \ldots + y_n^2 > n \cdot (x_1^2 + \ldots + x_n^2)$. By the conjecture, for Diophantine equations with finitely many integer solutions, the modulus of solutions are bounded by a computable function of the degree and the coefficients of the equation. If the set $\{(u, 2^u) : u \in \{1,2,3,\ldots\}\} \subseteq \mathbb{Z}^2$ has a finite-fold Diophantine representation, then the conjecture fails for sufficiently large values of n.

It is unknown whether there is a computing algorithm which will tell of a given Diophantine equation whether or not it has a solution in integers, if we know that its set of integer solutions is finite. For any such equation, the following Conjecture 1 implies that all integer solutions are determinable by a brute-force search.

Conjecture 1 ([3, p. 4, Conjecture 2b]). If integers $x_1, \ldots, x_n$ satisfy $x_1^2 > 2^{2^n} \vee \ldots \vee x_n^2 > 2^{2^n}$, then

$$(*) \qquad (\forall i \in \{1,\ldots,n\}\ (x_i = 1 \Rightarrow y_i = 1)) \wedge$$
$$(\forall i,j,k \in \{1,\ldots,n\}\ (x_i + x_j = x_k \Rightarrow y_i + y_j = y_k)) \wedge$$
$$(\forall i,j,k \in \{1,\ldots,n\}\ (x_i \cdot x_j = x_k \Rightarrow y_i \cdot y_j = y_k))$$

for some integers $y_1, \ldots, y_n$ satisfying $y_1^2 + \ldots + y_n^2 > n \cdot (x_1^2 + \ldots + x_n^2)$.

The bound 2^{2^n} cannot be decreased, because the conclusion does not hold for $(x_1, \ldots, x_n) = (2, 4, 16, 256, \ldots, 2^{2^{n-2}}, 2^{2^{n-1}})$.

Lemma 1. If $x_1^2 > 2^{2^n} \vee \ldots \vee x_n^2 > 2^{2^n}$ and $y_1^2 + \ldots + y_n^2 > n \cdot (x_1^2 + \ldots + x_n^2)$, then $y_1^2 > 2^{2^n} \vee \ldots \vee y_n^2 > 2^{2^n}$.

Proof. By the assumptions, it follows that $y_1^2 + \ldots + y_n^2 > n \cdot 2^{2^n}$. Hence, $y_1^2 > 2^{2^n} \vee \ldots \vee y_n^2 > 2^{2^n}$.

□

2000 Mathematics Subject Classification: 03B25, 03B30, 11D99, 11U05, 15A06.
Key words and phrases: Diophantine equation with a finite number of integer solutions, upper bound for the solutions of a Diophantine equation, Davis-Putnam-Robinson-Matiyasevich theorem, finite-fold Diophantine representation, Presburger arithmetic.

By Lemma 1, Conjecture 1 is equivalent to saying that infinitely many integer n-tuples $(y_1, \dots, y_n)$ satisfy the condition $(*)$, if integers $x_1, \dots, x_n$ satisfy $\max(|x_1|, \dots, |x_n|) > 2^{2^{n-1}}$. This formulation is simpler, but lies outside the language of arithmetic. Let

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

Another equivalent formulation of Conjecture 1 is thus: if a system $S \subseteq E_n$ has only finitely many integer solutions, then each such solution $(x_1, \dots, x_n)$ satisfies $|x_1|, \dots, |x_n| \leq 2^{2^{n-1}}$.

To each system $S \subseteq E_n$ we assign the system $\widetilde{S}$ defined by

$$(S \setminus \{x_i = 1 :\ i \in \{1, \dots, n\}\}) \cup$$
$$\{x_i \cdot x_j = x_j :\ i, j \in \{1, \dots, n\} \text{ and the equation } x_i = 1 \text{ belongs to } S\}$$

In other words, in order to obtain $\widetilde{S}$ we remove from S each equation $x_i = 1$ and replace it by the following n equations:

$$\begin{array}{rcl} x_i \cdot x_1 & = & x_1 \\ & \dots & \\ x_i \cdot x_n & = & x_n \end{array}$$

Lemma 2. For each system $S \subseteq E_n$

$$\{(x_1, \dots, x_n) \in \mathbb{Z}^n :\ (x_1, \dots, x_n) \text{ solves } \widetilde{S}\} \ =$$
$$\{(x_1, \dots, x_n) \in \mathbb{Z}^n :\ (x_1, \dots, x_n) \text{ solves } S\} \cup \{(\underbrace{0, \dots, 0}_{n-\text{times}})\}$$

By Lemma 2, Conjecture 1 restricted to n variables has the following three equivalent formulations:

(I) If a system $S \subseteq \{x_i + x_j = x_k,\ x_i \cdot x_j = x_k :\ i, j, k \in \{1, \dots, n\}\}$ has only finitely many integer solutions, then each such solution $(x_1, \dots, x_n)$ satisfies $|x_1|, \dots, |x_n| \leq 2^{2^{n-1}}$.

(II) If integers $x_1, \dots, x_n$ satisfy $x_1^2 > 2^{2^n} \vee \dots \vee x_n^2 > 2^{2^n}$, then

$$(\bullet) \qquad \begin{array}{l} (\forall i, j, k \in \{1, \dots, n\}\ (x_i + x_j = x_k \Rightarrow y_i + y_j = y_k)) \wedge \\ \quad (\forall i, j, k \in \{1, \dots, n\}\ (x_i \cdot x_j = x_k \Rightarrow y_i \cdot y_j = y_k)) \end{array}$$

for some integers $y_1, \dots, y_n$ satisfying $y_1^2 + \dots + y_n^2 > n \cdot (x_1^2 + \dots + x_n^2)$.

(III) Infinitely many integer n-tuples $(y_1, \dots, y_n)$ satisfy the condition $(\bullet)$, if integers $x_1, \dots, x_n$ satisfy $\max(|x_1|, \dots, |x_n|) > 2^{2^{n-1}}$.

Let $\texttt{CoLex}$ denote the colexicographic order on $\mathbb{Z}^n$. We define a linear order $\mathcal{C}o\mathcal{L}$ on $\mathbb{Z}^n$ by saying $(s_1, \ldots, s_n)\mathcal{C}o\mathcal{L}(t_1, \ldots, t_n)$ if and only if

$$\max(|s_1|, \ldots, |s_n|) < \max(|t_1|, \ldots, |t_n|)$$

or

$$\max(|s_1|, \ldots, |s_n|) = \max(|t_1|, \ldots, |t_n|) \wedge (s_1, \ldots, s_n)\texttt{CoLex}(t_1, \ldots, t_n)$$

The ordered set $(\mathbb{Z}^n, \mathcal{C}o\mathcal{L})$ is isomorphic to $(\mathbb{N}, \leq)$ and the order $\mathcal{C}o\mathcal{L}$ is computable. Let

$$\begin{gathered} B_n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : \ \exists y_1 \in \mathbb{Z} \ldots \exists y_n \in \mathbb{Z} \\ (\forall i, j, k \in \{1, \ldots, n\} \ (x_i + x_j = x_k \Rightarrow y_i + y_j = y_k)) \wedge \\ (\forall i, j, k \in \{1, \ldots, n\} \ (x_i \cdot x_j = x_k \Rightarrow y_i \cdot y_j = y_k)) \wedge \\ y_1^2 + \ldots + y_n^2 > n \cdot (x_1^2 + \ldots + x_n^2)\} \end{gathered}$$

Theorem 1. The set B_n is listable.

Proof. For a positive integer m, let $(y_{(m,1)}, \ldots, y_{(m,n)})$ be the m-th element of $\mathbb{Z}^n$ in the order $\mathcal{C}o\mathcal{L}$. All integer n-tuples $(x_1, \ldots, x_n)$ satisfying

$$\begin{gathered} (\forall i, j, k \in \{1, \ldots, n\} \ (x_i + x_j = x_k \Rightarrow y_{(m,i)} + y_{(m,j)} = y_{(m,k)})) \wedge \\ (\forall i, j, k \in \{1, \ldots, n\} \ (x_i \cdot x_j = x_k \Rightarrow y_{(m,i)} \cdot y_{(m,j)} = y_{(m,k)})) \wedge \\ y_{(m,1)}^2 + \ldots + y_{(m,n)}^2 > n \cdot (x_1^2 + \ldots + x_n^2) \end{gathered}$$

have Euclidean norm less than $\sqrt{\dfrac{y_{(m,1)}^2 + \ldots + y_{(m,n)}^2}{n}}$. Therefore, these n-tuples form a finite set and they can be effectively found. We list them in the order $\mathcal{C}o\mathcal{L}$. The needed listing of B_n is the concatenation of the listings for $m = 1, 2, 3, \ldots$

$\square$

Conjecture 2. The set B_n is not computable for sufficiently large values of n.

Corollary. There exists a Diophantine equation that is logically undecidable.

Proof. We describe a procedure which to an integer n-tuple $(a_1, \ldots, a_n)$ assigns some finite system of Diophantine equations. We start its construction from the equation

$$n \cdot (a_1^2 + \ldots + a_n^2) + 1 + s^2 + t^2 + u^2 + v^2 = y_1^2 + \ldots + y_n^2$$

where $n \cdot (a_1^2 + \ldots + a_n^2) + 1$ stands for a concrete integer. Next, we apply the following rules:

if $i, j, k \in \{1, \ldots, n\}$ and $a_i + a_j = a_k$, then we incorporate the equation $y_i + y_j = y_k$,

if $i, j, k \in \{1, \ldots, n\}$ and $a_i \cdot a_j = a_k$, then we incorporate the equation $y_i \cdot y_j = y_k$.

The obtained system of equations we replace by a single Diophantine equation $D_{(a_1,\ldots,a_n)}(s,t,u,v,y_1,\ldots,y_n)=0$ with the same set of integer solutions. We prove that if n is sufficiently large, then there exist integers $a_1,\ldots,a_n$ for which the Diophantine equation $D_{(a_1,\ldots,a_n)}(s,t,u,v,y_1,\ldots,y_n)=0$ is logically undecidable. Suppose, on the contrary, that for each integers $a_1,\ldots,a_n$ the solvability of the equation $D_{(a_1,\ldots,a_n)}(s,t,u,v,y_1,\ldots,y_n)=0$ can be either proved or disproved. This would yield the following algorithm for deciding whether an integer n-tuple $(a_1,\ldots,a_n)$ belongs to B_n: examine all proofs (in order of length) until for the equation $D_{(a_1,\ldots,a_n)}(s,t,u,v,y_1,\ldots,y_n)=0$ a proof that resolves the solvability question one way or the other is found.

□

For integers $x_1,\ldots,x_n$, the following code in *MuPAD* finds the first integer n-tuple $(y_1,\ldots,y_n)$ that lies after $(x_1,\ldots,x_n)$ in the order $\mathcal{C}o\mathcal{L}$ and satisfies

$$\max(|x_1|,\ldots,|x_n|)<\max(|y_1|,\ldots,|y_n|)\ \wedge$$
$$(\forall i,j,k\in\{1,\ldots,n\}\ (x_i+x_j=x_k \Rightarrow y_i+y_j=y_k))\ \wedge$$
$$(\forall i,j,k\in\{1,\ldots,n\}\ (x_i\cdot x_j=x_k \Rightarrow y_i\cdot y_j=y_k))$$

If an appropriate $(y_1,\ldots,y_n)$ does not exist, then the algorithm does not end and the output is empty. The names `x1,...,xn` should be replaced by concrete integers.

```
X:=[x1,...,xn]:
a:=max(abs(X[t]) $t=1..nops(X)):
B:=[]:
for t from 1 to nops(X) do
B:=append(B,-a-1):
end_for:
repeat
m:=0:
S:=[1,1,1]:
repeat
if (X[S[1]]+X[S[2]]=X[S[3]] and B[S[1]]+B[S[2]]<>B[S[3]]) then m:=1
end_if:
if (X[S[1]]*X[S[2]]=X[S[3]] and B[S[1]]*B[S[2]]<>B[S[3]]) then m:=1
end_if:
i:=1:
while (i<=3 and S[i]=nops(X)) do
```

```
i:=i+1:
end_while:
if i=1 then S[1]:=S[1]+1 end_if:
if i=2 then
S[1]:=S[2]+1:
S[2]:=S[2]+1:
end_if:
if i=3 then
S[1]:=1:
S[2]:=1:
S[3]:=S[3]+1:
end_if:
until (S=[nops(X),nops(X),nops(X)] or m=1) end_repeat:
Y:=B:
b:=max(abs(B[t]) $t=1..nops(X)):
if nops(X)>1 then w:=max(abs(B[t]) $t=2..nops(X)) end_if:
q:=1:
while (q<=nops(X) and B[q]=b) do
q:=q+1:
end_while:
if (nops(X)=1 and q=1) then B[1]=b end_if:
if (nops(X)>1 and q=1 and w<b) then B[1]:=b end_if:
if (nops(X)>1 and q=1 and w=b) then B[1]:=B[1]+1 end_if:
if (q>1 and q<=nops(X)) then
for u from 1 to q-1 do
B[u]:=-b:
end_for:
B[q]:=B[q]+1:
end_if:
if q=nops(X)+1 then
B:=[]:
for t from 1 to nops(X) do
B:=append(B,-b-1):
end_for:
end_if:
until m=0 end_repeat:
print(Y):
```

Let a Diophantine equation $D(x_1, \ldots, x_p) = 0$ has only finitely many integer solutions. Let M denote the maximum of the absolute values of the coefficients of $D(x_1, \ldots, x_p)$, d_i denote the degree of $D(x_1, \ldots, x_p)$ with respect to the variable x_i. As the author proved ([3, p. 9, Corollary 2]), Conjecture 1 restricted to $n = (2M+1)^{(d_1+1) \cdot \ldots \cdot (d_p+1)}$ implies that $|x_1|, \ldots, |x_p| \leq 2^{2^{n-1}}$ for each integers $x_1, \ldots, x_p$ satisfying $D(x_1, \ldots, x_p) = 0$. Therefore, the equation $D(x_1, \ldots, x_p) = 0$ can be fully solved by exhaustive search.

Davis-Putnam-Robinson-Matiyasevich theorem states that every listable set $\mathcal{M} \subseteq \mathbb{Z}^n$ has a Diophantine representation, that is

$$(a_1, \ldots, a_n) \in \mathcal{M} \Longleftrightarrow \exists x_1 \in \mathbb{Z} \ldots \exists x_m \in \mathbb{Z} \; D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$$

for some polynomial D with integer coefficients. Such a representation is said to be finite-fold if for any integers $a_1, \ldots, a_n$ the equation $D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ has at most finitely many integer solutions $(x_1, \ldots, x_m)$.

It is an open problem whether each listable set $\mathcal{M} \subseteq \mathbb{Z}^n$ has a finite-fold Diophantine representation, see [1, p. 42].

Lemma 3. Each Diophantine equation $D(x_1, \ldots, x_p) = 0$ can be equivalently written as a system $S \subseteq E_n$, where $n \geq p$ and both n and S are algorithmically determinable. If the equation $D(x_1, \ldots, x_p) = 0$ has only finitely many integer solutions, then the system S has only finitely many integer solutions.

A much more general and detailed formulation of Lemma 3 is given in [3, p. 9, Lemma 2].

Let the sequence $\{a_n\}$ be defined inductively by $a_1 = 2$, $a_{n+1} = 2^{a_n}$.

Theorem 2. If the set $\{(u, 2^u) : \; u \in \{1, 2, 3, \ldots\}\} \subseteq \mathbb{Z}^2$ has a finite-fold Diophantine representation, then Conjecture 1 fails for sufficiently large values of n.

Proof. By the assumption and Lemma 3, there exists a positive integer m such that in integer domain the formula $x_1 \geq 1 \; \wedge \; x_2 = 2^{x_1}$ is equivalent to $\exists x_3 \ldots \exists x_{m+2} \;\; \Phi(x_1, x_2, x_3, \ldots, x_{m+2})$, where $\Phi(x_1, x_2, x_3, \ldots, x_{m+2})$ is a conjunction of formulae of the form $x_i = 1$, $x_i + x_j = x_k$, $x_i \cdot x_j = x_k$, and for each integers x_1, x_2 at most finitely many integer m-tuples $(x_3, \ldots, x_{m+2})$ satisfy $\Phi(x_1, x_2, x_3, \ldots, x_{m+2})$. Therefore, for each integer $n \geq 2$, the following quantifier-free formula

$$x_1 = 1 \wedge \Phi(x_1, x_2, y_{(2,1)}, \dots, y_{(2,m)}) \ \wedge \ \Phi(x_2, x_3, y_{(3,1)}, \dots, y_{(3,m)}) \ \wedge \ \dots \ \wedge$$
$$\Phi(x_{n-2}, x_{n-1}, y_{(n-1,1)}, \dots, y_{(n-1,m)}) \ \wedge \ \Phi(x_{n-1}, x_n, y_{(n,1)}, \dots, y_{(n,m)})$$

has $n + m \cdot (n-1)$ variables and its corresponding system of equations has at most finitely many integer solutions. In integer domain, this system implies that $x_i = a_i$ for each $i \in \{1, \dots, n\}$. Each sufficiently large integer n satisfies $a_n > 2^{2^{n+m\cdot(n-1)-1}}$. Hence, for each such n, Conjecture 1 fails.

□

Let $W_n = \{x_i = 1, \ x_i + x_j = x_k : \ i, j, k \in \{1, \dots, n\}\}$.

Conjecture 3. If a system $S \subseteq W_n$ has only finitely many integer solutions, then each such solution $(x_1, \dots, x_n)$ satisfies $|x_1|, \dots, |x_n| \le 2^{n-1}$.

The bound 2^{n-1} cannot be decreased, because the system

$$\begin{cases} x_1 &= 1 \\ x_1 + x_1 &= x_2 \\ x_2 + x_2 &= x_3 \\ x_3 + x_3 &= x_4 \\ & \dots \\ x_{n-1} + x_{n-1} &= x_n \end{cases}$$

has a unique integer solution, namely $(1, 2, 4, 8, \dots, 2^{n-2}, 2^{n-1})$.

A simple reasoning by contradiction proves the following Lemma 4.

Lemma 4. If a system $S \subseteq W_n$ has only finitely many integer solutions, then S has at most one integer solution.

By Lemma 4, Conjecture 3 is equivalent to the following statement: if integers $x_1, \dots, x_n$ satisfy

$$\Big(x_1 + \underbrace{1 + \ldots + 1}_{2^{n-1}-\text{times}} < 0\Big) \vee \Big(\underbrace{1 + \ldots + 1}_{2^{n-1}-\text{times}} < x_1\Big) \vee \ \dots \ \vee$$
$$\Big(x_n + \underbrace{1 + \ldots + 1}_{2^{n-1}-\text{times}} < 0\Big) \vee \Big(\underbrace{1 + \ldots + 1}_{2^{n-1}-\text{times}} < x_n\Big)$$

then

$$(\forall i \in \{1, \dots, n\} \ (x_i = 1 \Rightarrow y_i = 1)) \wedge$$
$$(\forall i, j, k \in \{1, \dots, n\} \ (x_i + x_j = x_k \Rightarrow y_i + y_j = y_k))$$

for some integers $y_1, \dots, y_n$ satisfying $x_1 \neq y_1 \vee \dots \vee x_n \neq y_n$.

The above statement is decidable for each fixed n, because the first-order theory of $\langle \mathbb{Z}; =, <; +; 0, 1 \rangle$ (Presburger arithmetic) is decidable.

Conjecture 4 ([2]). If a system $S \subseteq W_n$ is consistent over $\mathbb{Z}$, then S has an integer solution $(x_1, \ldots, x_n)$ in which $|x_j| \leq 2^{n-1}$ for each j.

By Lemma 4, Conjecture 4 implies Conjecture 3. Conjecture 4 is equivalent to the following statement: for each integers $x_1, \ldots, x_n$ there exist integers $y_1, \ldots, y_n$ such that

$$(\forall i \in \{1, \ldots, n\}\ (x_i = 1 \Rightarrow y_i = 1)) \wedge$$
$$(\forall i, j, k \in \{1, \ldots, n\}\ (x_i + x_j = x_k \Rightarrow y_i + y_j = y_k)) \wedge$$
$$\forall i \in \{1, \ldots, n\}\ \Bigl(\Bigl(0 \leq \underbrace{1 + \ldots + 1}_{2^{n-1}-\text{times}} + y_i\Bigr) \wedge \Bigl(y_i \leq \underbrace{1 + \ldots + 1}_{2^{n-1}-\text{times}}\Bigr)\Bigr)$$

The above statement is decidable for each fixed n, because the first-order theory of $\langle \mathbb{Z}; =, <; +; 0, 1\rangle$ (Presburger arithmetic) is decidable.

References

[1] Yu. Matiyasevich, *Hilbert's tenth problem: what was done and what is to be done*. Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), 1–47, Contemp. Math. 270, Amer. Math. Soc., Providence, RI, 2000.

[2] A. Tyszka, *Bounds of some real (complex) solution of a finite system of polynomial equations with rational coefficients*, http://arxiv.org/abs/math/0702558, a shortened and revised version will appear in Mathematical Logic Quarterly 56 (2010), no. 2, under the title *"Two conjectures on the arithmetic in $\mathbb{R}$ and $\mathbb{C}$"*.

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

Apoloniusz Tyszka
University of Agriculture
Faculty of Production and Power Engineering
Balicka 116B, 30-149 Kraków, Poland
E-mail: *rttyszka@cyf-kr.edu.pl*