MLQ

MATHEMATICAL LOGIC QUARTERLY

A Journal for Mathematical Logic, Foundations of Mathematics, and Logical Aspects of Theoretical Computer Science

www.mlq-journal.org

WILEY

Math. Log. Quart. **56**, No. 2, 175 – 184 (2010) / **DOI** 10.1002/malq.200910004

Two conjectures on the arithmetic in $\mathbb{R}$ and $\mathbb{C}$*

Apoloniusz Tyszka**

University of Agriculture, Faculty of Production and Power Engineering, Balicka 116B, 30-149 Kraków, Poland

Received 3 January 2009, revised 2 June 2009, accepted 3 June 2009
Published online 18 March 2010

Key words System of polynomial equations, system of linear equations, solution with minimal l_∞ norm.
MSC (2000) 03B30, 12D99, 14P05, 15A06

Let $\boldsymbol{G}$ be an additive subgroup of $\mathbb{C}$, let $W_n = \{x_i = 1,\ x_i + x_j = x_k\ :\ i, j, k \in \{1, \dots, n\}\}$, and define $E_n = \{x_i = 1,\ x_i + x_j = x_k,\ x_i \cdot x_j = x_k :\ i, j, k \in \{1, \dots, n\}\}$. We discuss two conjectures. (1) If a system $S \subseteq E_n$ is consistent over $\mathbb{R}$ ($\mathbb{C}$), then S has a real (complex) solution which consists of numbers whose absolute values belong to $[0, 2^{2^{n-2}}]$. (2) If a system $S \subseteq W_n$ is consistent over $\boldsymbol{G}$, then S has a solution $(x_1, \dots, x_n) \in (\boldsymbol{G} \cap \mathbb{Q})^n$ in which $|x_j| \le 2^{n-1}$ for each j.

1 Systems of equations over $\mathbb{R}$ and $\mathbb{C}$

For a positive integer n we define the set of equations E_n by

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

Conjecture 1.1 ([20]). *Let a system $S \subseteq E_n$ be consistent over $\mathbb{R}$ ($\mathbb{C}$). Then S has a real (complex) solution which consists of numbers whose absolute values belong to $[0, 2^{2^{n-2}}]$.*

Concerning the bound $2^{2^{n-2}}$ in Conjecture 1.1, Vorobjov's theorem ([23]) allows us to compute a weaker estimation by a computable function of n. We present his result here. Let $V \subseteq \mathbb{R}^n$ be a real algebraic variety given by the system of equations $f_1 = \ldots = f_m = 0$, where $f_i \in \mathbb{Q}[x_1, \dots, x_n]$ $(i = 1, \dots, m)$. We denote by L the maximum of the bit-sizes of the coefficients of the system and set $d = \sum_{i=1}^m \deg(f_i)$, $r = \binom{n+2d}{n}$. We recall ([1, p. 285]) that the bit-size of a non-zero integer is the number of bits in its binary representation. More precisely, the bit-size of k is τ if and only if $2^{\tau-1} \le |k| < 2^\tau$. The bit-size of a rational number is the sum of the bit-sizes of its numerator and denominator in reduced form. N. N. Vorobjov, Jr. proved that there exists $(x_1, \dots, x_n) \in V$ such that $|x_i| < 2^{H(r,L)}$ $(i = 1, \dots, n)$, where H is some polynomial not depending on the initial system. For a simplified proof of Vorobjov's theorem, see [8, Lemma 9, p. 56]. For a more general theorem, see [1, Theorem 13.15, p. 516].

It is algorithmically decidable whether a system $S \subseteq E_n$ has a real (complex) solution $(x_1, \dots, x_n)$ with $|x_1|, \dots, |x_n| \le 2^{2^{n-2}}$. It is also algorithmically decidable whether a system $S \subseteq E_n$ is consistent over $\mathbb{R}$ ($\mathbb{C}$). For the final problem, an appropriate algorithm follows from the theorem known as effective Hilbert Nullstellensatz. The expected complexity of such an algorithm is related to Steven Smale's conjecture, which we now recall.

For an integer m denote by $\tau(m)$ the smallest positive integer s for which there exist integers $x_0, x_1, \dots, x_s$ such that $x_0 = 1$, $x_s = m$, and for each $t \in \{1, \dots, s\}$ there are $i, j \in \{0, \dots, t-1\}$ with $x_i \circ x_j = x_t$. Here $\circ$ denotes addition, subtraction or multiplication. Smale's conjecture states that for every sequence $\{m_k\}_{k=3}^\infty$

---

* This paper is a shortened version of [19].
** e-mail: rttyszka@cyf-kr.edu.pl

of non-zero integers, there is no constant c such that $\tau(m_k \cdot k!) \le (\log_2(k))^c$ for all $k \in \{3,4,5,\ldots\}$, see [2, p. 126]. This conjecture implies that there is no polynomial time algorithm for Hilbert Nullstellensatz over $\mathbb{C}$, see [2, p. 126, Theorem 2].

Concerning Conjecture 1.1, for $n = 1$ estimation by $2^{2^{n-2}}$ can be replaced by estimation by 1. For $n > 1$ estimation by $2^{2^{n-2}}$ is the best estimation. Indeed, let $n > 1$ and $\widetilde{x_1} = 1$, $\widetilde{x_2} = 2^{2^0}$, $\widetilde{x_3} = 2^{2^1}, \ldots, \widetilde{x_n} = 2^{2^{n-2}}$. In any ring $\boldsymbol{K}$ of characteristic 0, from the system of all equations belonging to E_n and which are satisfied under the substitution $[x_1 \to \widetilde{x_1}, \ldots, x_n \to \widetilde{x_n}]$, it follows that $x_1 = \widetilde{x_1}, \ldots, x_n = \widetilde{x_n}$.

Theorem 1.2 *If* $n \in \{1,2,3\}$, *then Conjecture* 1.1 *holds true for each subring* $\boldsymbol{K} \subseteq \mathbb{C}$.

Proof. If a system $S \subseteq E_1$ is consistent over $\boldsymbol{K}$, then S has a solution $\widehat{x_1} \in \{0,1\}$. If a system $S \subseteq E_2$ is consistent over $\boldsymbol{K}$ and $\frac{1}{2} \notin \boldsymbol{K}$, then S has a solution $(\widehat{x_1}, \widehat{x_2}) \in \{(0,0),(0,1),(1,0),(1,1),(1,2),(2,1)\}$. If a system $S \subseteq E_2$ is consistent over $\boldsymbol{K}$ and $\frac{1}{2} \in \boldsymbol{K}$, then $(\widehat{x_1}, \widehat{x_2}) \in \{(0,0),(0,1),(1,0),(\frac{1}{2},1),(1,\frac{1}{2}),(1,1),(1,2),(2,1)\}$ is a solution for S. To reduce the number of studied systems $S \subseteq E_3$, we may assume that the equation $x_1 = 1$ belongs to S, as when all equations $x_1 = 1$, $x_2 = 1$, $x_3 = 1$ do not belong to S, then S has the solution $(0,0,0) \in \boldsymbol{K}^3$. Let

$$A_2 = \{\widehat{x_2} \in \mathbb{C} : \text{ there exists } \widehat{x_3} \in \mathbb{C} \text{ for which } (1, \widehat{x_2}, \widehat{x_3}) \text{ solves } S\},$$

$$A_3 = \{\widehat{x_3} \in \mathbb{C} : \text{ there exists } \widehat{x_2} \in \mathbb{C} \text{ for which } (1, \widehat{x_2}, \widehat{x_3}) \text{ solves } S\}.$$

We may assume that $A_2 \not\subseteq \{z \in \mathbb{C} : |z| \le 4\}$ or $A_3 \not\subseteq \{z \in \mathbb{C} : |z| \le 4\}$.

Case 1: $A_2 \not\subseteq \{z \in \mathbb{C} : |z| \le 4\}$ and $A_3 \subseteq \{z \in \mathbb{C} : |z| \le 4\}$. If $(1, \widehat{x_2}, \widehat{x_3}) \in \boldsymbol{K}^3$ solves S, then $(1, 1, \widehat{x_3}) \in \boldsymbol{K}^3$ solves S.

Case 2: $A_2 \subseteq \{z \in \mathbb{C} : |z| \le 4\}$ and $A_3 \not\subseteq \{z \in \mathbb{C} : |z| \le 4\}$. If $(1, \widehat{x_2}, \widehat{x_3}) \in \boldsymbol{K}^3$ solves S, then $(1, \widehat{x_2}, 1) \in \boldsymbol{K}^3$ solves S.

Case 3: $A_2 \not\subseteq \{z \in \mathbb{C} : |z| \le 4\}$ and $A_3 \not\subseteq \{z \in \mathbb{C} : |z| \le 4\}$. If $(1, \widehat{x_2}, \widehat{x_3}) \in \boldsymbol{K}^3$ solves S, then $(1,0,1) \in \boldsymbol{K}^3$ solves S or $(1,1,0) \in \boldsymbol{K}^3$ solves S or $(1,1,1) \in \boldsymbol{K}^3$ solves S. □

The following Observation borrows the idea from the proof of Theorem 1.2.

Observation 1.3 *Let* $n \in \{1,2,3,4\}$, *and let a system* $S \subseteq E_n$ *be consistent over the subring* $\boldsymbol{K} \subseteq \mathbb{C}$. *If* $(x_1, \ldots, x_n) \in \boldsymbol{K}^n$ *solves* S, *then* $(\widehat{x_1}, \ldots, \widehat{x_n})$ *solves* S, *where each* $\widehat{x_i}$ *is suitably chosen from the set* $\{x_i, 0, 1, 2, \frac{1}{2}\} \cap \{z \in \boldsymbol{K} : |z| \le 2^{2^{n-2}}\}$.

Theorem 1.4 *Conjecture* 1.1 *holds true for each* $n \in \{1,2,3,4\}$ *and each subring* $\boldsymbol{K} \subseteq \mathbb{C}$.

Proof. It follows from Observation 1.3. □

Let

$$\begin{aligned}\mathcal{W} = \{ \ & \{1\}, \{0\}, \{1,0\}, \{1,2\}, \{1,\tfrac{1}{2}\}, \{1,2,\tfrac{1}{2}\}, \{1,0,2\}, \{1,0,\tfrac{1}{2}\}, \\ & \{1,0,-1\}, \{1,2,-1\}, \{1,2,3\}, \{1,2,4\}, \{1,\tfrac{1}{2},-\tfrac{1}{2}\}, \{1,\tfrac{1}{2},\tfrac{1}{4}\}, \{1,\tfrac{1}{2},\tfrac{3}{2}\}, \\ & \{1,-1,-2\}, \{1,\tfrac{1}{3},\tfrac{2}{3}\}, \{1,2,\sqrt{2}\}, \{1,\tfrac{1}{2},\tfrac{1}{\sqrt{2}}\}, \{1,\sqrt{2},\tfrac{1}{\sqrt{2}}\}, \\ & \{1,\tfrac{\sqrt{5}-1}{2},\tfrac{\sqrt{5}+1}{2}\}, \{1,\tfrac{\sqrt{5}+1}{2},\tfrac{\sqrt{5}+3}{2}\}, \{1,\tfrac{-\sqrt{5}-1}{2},\tfrac{\sqrt{5}+3}{2}\}\}.\end{aligned}$$

For each $a, b, c \in \mathbb{R}$ ($\mathbb{C}$) we define $S(a,b,c)$ as

$$\{\mathcal{E} \in E_3 : \ \mathcal{E} \text{ is satisfied under the substitution } [x_1 \to a, \ x_2 \to b, \ x_3 \to c]\}.$$

If $a, b, c \in \mathbb{R}$ and $\{a\} \cup \{b\} \cup \{c\} \in \mathcal{W}$, then the system $S(a,b,c)$ is consistent over $\mathbb{R}$, has a finite number of real solutions, and each real solution of $S(a,b,c)$ belongs to $[-4,4]^3$. The family

$$\{S(a,b,c) : \ a,b,c \in \mathbb{R} \ \wedge \ \{a\} \cup \{b\} \cup \{c\} \in \mathcal{W}\}$$

equals the family of all systems $S \subseteq E_3$ which are consistent over $\mathbb{R}$ and maximal with respect to inclusion.

If $a, b, c \in \mathbb{C}$ and $\{a\} \cup \{b\} \cup \{c\} \in \mathcal{W} \cup \{\{1, \frac{-1+\sqrt{-3}}{2}, \frac{1+\sqrt{-3}}{2}\}, \{1, \frac{1-\sqrt{-3}}{2}, \frac{1+\sqrt{-3}}{2}\}\}$, then the system $S(a, b, c)$ is consistent over $\mathbb{C}$, has a finite number of solutions, and each solution of $S(a, b, c)$ belongs to $\{(z_1, z_2, z_3) \in \mathbb{C}^3 : \ |z_1| \le 4 \ \wedge \ |z_2| \le 4 \ \wedge \ |z_3| \le 4\}$. The family

$$\{S(a,b,c) : \ a, b, c \in \mathbb{C} \ \wedge \ \{a\} \cup \{b\} \cup \{c\} \in \mathcal{W} \cup \{\{1, \frac{-1+\sqrt{-3}}{2}, \frac{1+\sqrt{-3}}{2}\}, \{1, \frac{1-\sqrt{-3}}{2}, \frac{1+\sqrt{-3}}{2}\}\}\}$$

equals the family of all systems $S \subseteq E_3$ which are consistent over $\mathbb{C}$ and maximal with respect to inclusion.

Let us consider the following four conjectures; analogous statements seem to be true for $\mathbb{R}$.

Conjecture 1.5

(a) *If a system $S \subseteq E_n$ is consistent over $\mathbb{C}$ and maximal with respect to inclusion, then each solution of S belongs to $\{(x_1, \dots, x_n) \in \mathbb{C}^n : \ |x_1| \le 2^{2^{n-2}} \ \wedge \ \cdots \ \wedge \ |x_n| \le 2^{2^{n-2}}\}$.*

(b) *If a system $S \subseteq E_n$ is consistent over $\mathbb{C}$ and maximal with respect to inclusion, then S has a finite number of solutions $(x_1, \dots, x_n)$.*

(c) *If the equation $x_1 = 1$ belongs to $S \subseteq E_n$ and S has a finite number of complex solutions $(x_1, \dots, x_n)$, then each such solution belongs to $\{(x_1, \dots, x_n) \in \mathbb{C}^n : \ |x_1| \le 2^{2^{n-2}} \ \wedge \ \cdots \ \wedge \ |x_n| \le 2^{2^{n-2}}\}$.*

(d) *If a system $S \subseteq E_n$ has a finite number of complex solutions $(x_1, \dots, x_n)$, then each such solution belongs to $\{(x_1, \dots, x_n) \in \mathbb{C}^n : \ |x_1| \le 2^{2^{n-1}} \ \wedge \ \cdots \ \wedge \ |x_n| \le 2^{2^{n-1}}\}$.*

Conjecture 1.5(a) strengthens Conjecture 1.1 for $\mathbb{C}$. The conjunction of Conjectures 1.5(b) and 1.5(c) implies Conjecture 1.5(a).

Concerning Conjecture 1.5(d), for $n = 1$ estimation by $2^{2^{n-1}}$ can be replaced by estimation by 1. For $n > 1$ estimation by $2^{2^{n-1}}$ is the best estimation. Indeed, the system

$$x_1 + x_1 = x_2 \quad x_1 \cdot x_1 = x_2 \quad x_2 \cdot x_2 = x_3 \quad x_3 \cdot x_3 = x_4 \quad \dots \quad x_{n-1} \cdot x_{n-1} = x_n$$

has precisely two complex solutions, $(0, \dots, 0)$, and $(2, 4, 16, 256, \dots, 2^{2^{n-2}}, 2^{2^{n-1}})$.

For the complex case of Conjectures 1.1 and 1.5(a), 1.5(b), 1.5(c), 1.5(d), the author prepared two *MuPAD* codes which confirm these conjectures probabilistically, see [19] and [21].

2 Systems of equations over number rings

Hilbert's tenth problem is to give a computing algorithm which will tell of a given polynomial equation with integer coefficients whether or not it has a solution in integers. Yu. V. Matijasevič proved ([13]) that there is no such algorithm, see also [14], [4], [5], [10]. It implies that Conjecture 1.1 is false for $\mathbb{Z}$ instead of $\mathbb{R}$ ($\mathbb{C}$). Moreover, Matijasevič's theorem implies that Conjecture 1.1 for $\mathbb{Z}$ is false with any other computable estimation instead of $2^{2^{n-2}}$.

As we have proved, Conjecture 1.1 for $\mathbb{Z}$ is false. We describe a counterexample showing that Conjecture 1.1 for $\mathbb{Z}$ is false with $n = 21$. Lemma 1 is a special case of the result presented in [18, p. 3].

Lemma 2.1 *For each non-zero integer x there exist integers a, b such that $ax = (2b-1)(3b-1)$.*

P r o o f. Write x as $(2y-1) \cdot 2^m$, where $y \in \mathbb{Z}$ and $m \in \mathbb{Z} \cap [0, \infty)$. Obviously, $\frac{2^{2m+1}+1}{3} \in \mathbb{Z}$. By Chinese Remainder Theorem, we can find an integer b such that $b \equiv y \pmod{2y-1}$ and $b \equiv \frac{2^{2m+1}+1}{3} \pmod{2^m}$. Thus, $\frac{2b-1}{2y-1} \in \mathbb{Z}$ and $\frac{3b-1}{2^m} \in \mathbb{Z}$. Hence

$$\frac{(2b-1)(3b-1)}{x} = \frac{2b-1}{2y-1} \cdot \frac{3b-1}{2^m} \in \mathbb{Z}. \qquad \square$$

Lemma 2.2 ([9, Lemma 2.3, p. 451]) *For each $x \in \mathbb{Z} \cap [2, \infty)$ there exists $y \in \mathbb{Z} \cap [1, \infty)$ such that $1 + x^3(2+x)y^2$ is a square.*

Lemma 2.3 ([9, Lemma 2.3, p. 451]) *For each $x \in \mathbb{Z} \cap [2, \infty)$, $y \in \mathbb{Z} \cap [1, \infty)$, if $1 + x^3(2+x)y^2$ is a square, then $y \geq x + x^{x-2}$.*

Theorem 2.4 *Conjecture* 1.1 *for $\mathbb{Z}$ is false with $n = 21$.*

P r o o f. Let us consider the following system over $\mathbb{Z}$. This system consists of two subsystems.

$$
\begin{array}{llllll}
(\bullet) & x_1 = 1 & x_1 + x_1 = x_2 & x_2 \cdot x_2 = x_3 & x_3 \cdot x_3 = x_4 & x_4 \cdot x_4 = x_5 \\
 & x_5 \cdot x_5 = x_6 & x_6 \cdot x_6 = x_7 & x_6 \cdot x_7 = x_8 & x_2 + x_6 = x_9 & x_8 \cdot x_9 = x_{10} \\
 & x_{11} \cdot x_{11} = x_{12} & x_{10} \cdot x_{12} = x_{13} & x_1 + x_{13} = x_{14} & x_{15} \cdot x_{15} = x_{14}\ , & \\
(\diamond) & x_{16} + x_{16} = x_{17} & x_1 + x_{18} = x_{17} & x_{16} + x_{18} = x_{19} & x_{18} \cdot x_{19} = x_{20} & x_{12} \cdot x_{21} = x_{20}\ .
\end{array}
$$

Since $x_1 = 1$ and $x_{12} = x_{11} \cdot x_{11}$, the subsystem marked with $(\diamond)$ is equivalent to

$$x_{21} \cdot x_{11}^2 = (2x_{16} - 1)(3x_{16} - 1).$$

The subsystem marked with $(\bullet)$ is equivalent to

$$x_{15}^2 = 1 + (2^{16})^3 \cdot (2 + 2^{16}) \cdot x_{11}^2.$$

By Lemma 2.2, the last equation has a solution $(x_{11}, x_{15}) \in \mathbb{Z}^2$ such that $x_{11} \geq 1$. By Lemma 2.1, we can find integers x_{16}, x_{21} satisfying $x_{21} \cdot x_{11}^2 = (2x_{16} - 1)(3x_{16} - 1)$. Thus, the whole system is consistent over $\mathbb{Z}$.

If $(x_1, \ldots, x_{21}) \in \mathbb{Z}^{21}$ solves the whole system, then

$$x_{15}^2 = 1 + (2^{16})^3 \cdot (2 + 2^{16}) \cdot |x_{11}|^2 \quad \text{and} \quad x_{21} \cdot |x_{11}|^2 = (2x_{16} - 1)(3x_{16} - 1).$$

Since $2x_{16} - 1 \neq 0$ and $3x_{16} - 1 \neq 0$, $|x_{11}| \geq 1$. By Lemma 2.3,

$$|x_{11}| \geq 2^{16} + (2^{16})^{2^{16}-2} > (2^{16})^{2^{16}-2} = 2^{2^{20}-32} > 2^{2^{21-2}}. \qquad \square$$

Lemma 2.5 ([22]). *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 solutions in a number ring **K**, then the system S has only finitely many solutions in **K**.*

Since there is a finite number of subsets of E_n, for any ***K*** there is a function $\chi : \{1, 2, 3, \ldots\} \longrightarrow \{1, 2, 3, \ldots\}$ with the property: for each positive integer n, if a system $S \subseteq E_n$ is consistent over the number ring ***K***, then S has a solution whose heights are less than or equal to $\chi(n)$.

Theorem 2.6 *If $\mathbb{Z}$ has a Diophantine definition in a number ring **K**, then any such χ is not computable.*

P r o o f. Let

$$(\triangle) \qquad (\forall x \in \boldsymbol{K})(x \in \mathbb{Z} \Leftrightarrow \exists t_1 \ldots \exists t_m\, W(x, t_1, \ldots, t_m) = 0)$$

where $W(x, t_1, \ldots, x_m) \in \mathbb{Z}[x, t_1, \ldots, x_m]$. Assume, on the contrary, that χ is computable. We show that it would imply a positive solution to Hilbert's tenth problem for $\mathbb{Z}$. Let us consider an arbitrary Diophantine equation $D(x_1, \ldots, x_p) = 0$. According to $(\triangle)$, for each $i \in \{1, \ldots, p\}$ we construct the polynomial equation $W(x_i, t_{(1,i)}, \ldots, t_{(m,i)}) = 0$. Applying Lemma 2.5, we write the system

$$
\begin{aligned}
0 &= D(x_1, \ldots, x_p) \\
0 &= W(x_1, t_{(1,1)}, \ldots, t_{(m,1)}) \\
&\ \vdots \\
0 &= W(x_p, t_{(1,p)}, \ldots, t_{(m,p)})
\end{aligned}
$$

as an equivalent system $T \subseteq E_n$, where T and n are algorithmically determinable. Since χ is computable, we can decide whether T has a solution in ***K***. Therefore, we can decide whether the equation $D(x_1, \ldots, x_p) = 0$ has an integer solution. We get the contradiction to Matijasevič's theorem. $\square$

The rings considered in Theorems 2.7 – 2.9 and 2.11 have the property that they allow Diophantine definitions for $\mathbb{Z}$. The number $2 + 273^2$ is prime.

Theorem 2.7 *If $k \in \mathbb{Z} \cap [273, \infty)$ and $2 + k^2$ is prime, then Conjecture* 1.1 *fails for $n = 6$ and the ring* $\mathbb{Z}\left[\dfrac{1}{2+k^2}\right] = \left\{\dfrac{x}{(2+k^2)^m} : x \in \mathbb{Z}, m \in \mathbb{Z} \cap [0, \infty)\right\}$.

Proof. $\left(1, 2, k, k^2, 2+k^2, \dfrac{1}{2+k^2}\right)$ solves the system

$$x_1 = 1 \quad x_1 + x_1 = x_2 \quad x_3 \cdot x_3 = x_4 \quad x_2 + x_4 = x_5 \quad x_5 \cdot x_6 = x_1.$$

Assume that $(x_1, x_2, x_3, x_4, x_5, x_6) \in \left(\mathbb{Z}\left[\dfrac{1}{2+k^2}\right]\right)^6$ solves the system. Let $x_5 = \dfrac{a}{(2+k^2)^p}$, $x_6 = \dfrac{b}{(2+k^2)^q}$, $a, b \in \mathbb{Z}$, $p, q \in \mathbb{Z} \cap [0, \infty)$. Since $2 + k^2$ is prime and $1 = |x_1| = |x_5 \cdot x_6| = \dfrac{|a| \cdot |b|}{(2+k^2)^{p+q}}$, we conclude that $|a| = (2+k^2)^{\widetilde{p}}$ for some $\widetilde{p} \in \mathbb{Z} \cap [0, \infty)$. Hence $|x_5| = (2+k^2)^{\widetilde{p}-p}$. On the other hand, $|x_5| = |x_2 + x_4| = |x_1 + x_1 + x_3 \cdot x_3| = |1 + 1 + x_3^2| \geq 2$. Therefore, $\widetilde{p} - p \geq 1$. Consequently, $|x_5| = (2+k^2)^{\widetilde{p}-p} \geq 2 + k^2 > 2^{2^{6-2}}$. □

Theorem 2.8 *If a prime number p is greater than 2^{256}, then Conjecture* 1.1 *fails for $n = 10$ and the ring* $\mathbb{Z}\left[\dfrac{1}{p}\right]$.

Proof. Let us consider the system

$$\begin{array}{llll} x_1 = 1 & x_2 \cdot x_3 = x_1 & x_3 + x_4 = x_2 & x_4 \cdot x_5 = x_6 \\ x_7 + x_7 = x_8 & x_1 + x_9 = x_8 & x_7 + x_9 = x_{10} & x_9 \cdot x_{10} = x_6. \end{array}$$

By Lemma 2.1, there exist integers u, s such that $(p^2 - 1) \cdot u = (2s - 1)(3s - 1)$. Hence

$$\left(1,\ p,\ \frac{1}{p},\ p - \frac{1}{p},\ p \cdot u,\ (p^2-1) \cdot u,\ s,\ 2s,\ 2s-1,\ 3s-1\right) \in \left(\mathbb{Z}\left[\frac{1}{p}\right]\right)^{10}$$

solves the system. If $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}) \in \left(\mathbb{Z}\left[\frac{1}{p}\right]\right)^{10}$ solves the system, then we get $(x_2 - x_3) \cdot x_5 = (2x_7 - 1)(3x_7 - 1)$. Since $2x_7 - 1 \neq 0$ and $3x_7 - 1 \neq 0$, we get $x_2 \neq x_3$. Since $x_2 \cdot x_3 = 1$, we get: $|x_2| = p^n$ for some $n \in \mathbb{Z} \cap [1, \infty)$ or $|x_3| = p^n$ for some $n \in \mathbb{Z} \cap [1, \infty)$. Therefore, $|x_2| \geq p > 2^{2^{10-2}}$ or $|x_3| \geq p > 2^{2^{10-2}}$. □

The number $-2^{32} - 2^{16} - 1$ is square-free, because $-3 \cdot 7 \cdot 13 \cdot 97 \cdot 241 \cdot 673$ is the factorization of $-2^{32} - 2^{16} - 1$ into prime numbers.

Theorem 2.9 *Conjecture* 1.1 *fails for $n = 6$ and the ring*

$$\mathbb{Z}\left[\sqrt{-2^{32} - 2^{16} - 1}\right] = \left\{x + y \cdot \sqrt{-2^{32} - 2^{16} - 1} : x, y \in \mathbb{Z}\right\}.$$

Proof. $(1, 2^{16} + 1, -2^{16}, -2^{32} - 2^{16}, \sqrt{-2^{32} - 2^{16} - 1}, -2^{32} - 2^{16} - 1)$ solves the system

$$x_1 = 1 \qquad x_2 + x_3 = x_1 \qquad x_2 \cdot x_3 = x_4 \qquad x_5 \cdot x_5 = x_6 \qquad x_1 + x_6 = x_4$$

which has no integer solutions. For each $z \in \mathbb{Z}[\sqrt{-2^{32} - 2^{16} - 1}]$, if $|z| \leq 2^{2^{6-2}}$, then $z \in \mathbb{Z}$. □

Observation 2.10 *If $q, a, b, c, d \in \mathbb{Z}$, $b \neq 0$ or $d \neq 0$, $q \geq 2$, q is square-free, and $(a + b\sqrt{q}) \cdot (c + d\sqrt{q}) = 1$, then*

$$(a \geq 1 \wedge b \geq 1) \vee (a \leq -1 \wedge b \leq -1) \vee (c \geq 1 \wedge d \geq 1) \vee (c \leq -1 \wedge d \leq -1).$$

The number $4 \cdot 13^4 - 1$ is square-free, because $3 \cdot 113 \cdot 337$ is the factorization of $4 \cdot 13^4 - 1$ into prime numbers.

Theorem 2.11 *If $p \in \mathbb{Z} \cap [13, \infty)$ and $4p^4 - 1$ is square-free, then Conjecture* 1.1 *fails for $n = 5$ and the ring $\mathbb{Z}[\sqrt{4p^4-1}] = \{x + y \cdot \sqrt{4p^4-1} : \ x, y \in \mathbb{Z}\}$.*

Proof. $(1, 2p^2 + \sqrt{4p^4-1}, 2p^2 - \sqrt{4p^4-1}, 4p^2, 2p)$ solves the system

$$x_1 = 1 \qquad x_2 \cdot x_3 = x_1 \qquad x_2 + x_3 = x_4 \qquad x_5 \cdot x_5 = x_4.$$

Assume that $(x_1, x_2, x_3, x_4, x_5) \in (\mathbb{Z}[\sqrt{4p^4-1}])^5$ solves the system. Let $x_2 = a + b\sqrt{4p^4-1}$ and let $x_3 = c + d\sqrt{4p^4-1}$, $a, b, c, d \in \mathbb{Z}$. Since

$$\neg((\exists x_2 \in \mathbb{Z})(\exists x_3 \in \mathbb{Z})(\exists x_5 \in \mathbb{Z}[\sqrt{4p^4-1}])\ (x_2 \cdot x_3 = 1 \wedge x_2 + x_3 = x_5^2)),$$

we get $b \neq 0$ or $d \neq 0$. Since $x_2 \cdot x_3 = 1$, Observation 2.10 implies that $|x_2| \geq 1 + \sqrt{4p^4-1} > 2^{2^{5-2}}$ or $|x_3| \geq 1 + \sqrt{4p^4-1} > 2^{2^{5-2}}$. □

3 Systems of equations over number fields

Julia Robinson proved that $\mathbb{Z}$ is definable in $\mathbb{Q}$ by a first order formula in the language of rings. Bjorn Poonen proved ([15]) that $\mathbb{Z}$ is definable in $\mathbb{Q}$ by a formula with 2 universal quantifiers followed by 7 existential quantifiers. It is unknown whether $\mathbb{Z}$ is existentially definable in $\mathbb{Q}$. If it is, Hilbert's tenth problem for $\mathbb{Q}$ is undecidable. The author conjectures that if a system $S \subseteq E_n$ has at most finitely many integer (rational) solutions, then their heights are less than or equal to $2^{2^{n-1}}$, see [22]. This conjecture and Lemma 2.5 imply that Hilbert's tenth problem for $\mathbb{Z}$ ($\mathbb{Q}$) has a positive solution for Diophantine equations which have at most finitely many integer (rational) solutions.

Theorem 3.1 *If $\mathbb{Z}$ is definable in $\mathbb{Q}$ by an existential formula, then Conjecture* 1.1 *fails for $\mathbb{Q}$.*

Proof. If $\mathbb{Z}$ is definable in $\mathbb{Q}$ by an existential formula, then $\mathbb{Z}$ is definable in $\mathbb{Q}$ by a Diophantine formula. Let

$$(\forall x_1 \in \mathbb{Q})(x_1 \in \mathbb{Z} \Leftrightarrow (\exists x_2 \in \mathbb{Q}) \ldots (\exists x_m \in \mathbb{Q})\Phi(x_1, x_2, \ldots, x_m))$$

where $\Phi(x_1, x_2, \ldots, x_m)$ is a conjunction of formulae of the form $x_i = 1$, $x_i + x_j = x_k$, $x_i \cdot x_j = x_k$, where $i, j, k \in \{1, \ldots, m\}$. We find an integer n with $2^n \geq m + 10$. Now we are ready to describe a counterexample to Conjecture 1.1 for $\mathbb{Q}$, this counterexample uses $n + m + 11$ variables. Considering all equations over $\mathbb{Q}$, we can equivalently write down the system

(1) $$\Phi(x_1, x_2, \ldots, x_m)$$

(2) $$x_{m+2}^2 = 1 + \left(2^{2^n}\right)^3 \cdot (2 + 2^{2^n}) \cdot x_1^2$$

(3) $$x_1 \cdot x_{m+1} = 1$$

as a conjunction of formulae of the form $x_i = 1$, $x_i + x_j = x_k$, $x_i \cdot x_j = x_k$, where $i, j, k \in \{1, \ldots, n+m+11\}$. The system is consistent over $\mathbb{Q}$. Assume that $(x_1, \ldots, x_{n+m+11}) \in \mathbb{Q}^{n+m+11}$ solves the system. Formula (1) implies that $x_1 \in \mathbb{Z}$. By this and equation (2), $x_{m+2} \in \mathbb{Z}$. Equation (3) implies that $x_1 \neq 0$, so by Lemma 2.3

$$|x_1| \geq 2^{2^n} + (2^{2^n})^{2^{2^n}} - 2 > 2^{2^{n} + 2^n} - 2^{n+1} \geq 2^{2^{n+2^n-1}} \geq 2^{2^{n+m+11-2}}. \qquad \square$$

Theorem 3.2 *Let $f(x, y) \in \mathbb{Q}[x, y]$ and the equation $f(x, y) = 0$ defines an irreducible algebraic curve of genus greater than* 1*. Let some $r \in \mathbb{R}$ satisfy*

(∗) $$(-\infty, r) \subseteq \{x \in \mathbb{R} : (\exists y \in \mathbb{R}) f(x, y) = 0\} \ \vee \ (r, \infty) \subseteq \{x \in \mathbb{R} : (\exists y \in \mathbb{R}) f(x, y) = 0\}$$

*and let **K** denote the function field over $\mathbb{Q}$ defined by $f(x, y) = 0$. Then Conjecture* 1.1 *fails for some subfield of $\mathbb{R}$ that is isomorphic to **K**.*

P r o o f. By Faltings' finiteness theorem ([7], cf. [12, p. 12]) the set

$$\{u \in \boldsymbol{K} :\ \exists v \in \boldsymbol{K}\ f(u,v) = 0\}$$

is finite. Let card $\{u \in \boldsymbol{K} :\ \exists v \in \boldsymbol{K}\ f(u,v) = 0\} = n \geq 1$, and let $\mathcal{U}$ denote the following system of equations

$$\begin{aligned} f(x_i, y_i) &= 0 \qquad (1 \leq i \leq n) \\ x_i + t_{i,j} &= x_j \quad (1 \leq i < j \leq n) \\ t_{i,j} \cdot s_{i,j} &= 1 \qquad (1 \leq i < j \leq n) \\ x_{n+1} &= \textstyle\sum_{i=1}^{n} x_i^2. \end{aligned}$$

For some integer $m > n$ there exists a set $\mathcal{G}$ of m variables such that

$$\{x_1, \ldots, x_n\, x_{n+1}, y_1, \ldots, y_n\} \cup \{t_{i,j}, s_{i,j} :\ 1 \leq i < j \leq n\} \subseteq \mathcal{G}$$

and the system $\mathcal{U}$ can be equivalently written down as a system $\mathcal{V}$ which contains only equations of the form $X = 1$, $X + Y = Z$, $X \cdot Y = Z$, where $X, Y, Z \in \mathcal{G}$. By $(*)$, we find $\widetilde{x}, \widetilde{y} \in \mathbb{R}$ such that $f(\widetilde{x}, \widetilde{y}) = 0$, $\widetilde{x}$ is transcendental over $\mathbb{Q}$, and $|\widetilde{x}| > 2^{2^{m-3}}$. If $(\widehat{x_1}, \ldots, \widehat{x_m}) \in (\mathbb{Q}(\widetilde{x}, \widetilde{y}))^m$ solves $\mathcal{V}$, then

$$\widehat{x_{n+1}} = \textstyle\sum_{i=1}^{n} \widehat{x_i}^{\,2} \geq \widetilde{x}^2 > (2^{2^{m-3}})^2 = 2^{2^{m-2}}.$$

Obviously, $\boldsymbol{K}$ is isomorphic to $\mathbb{Q}(\widetilde{x}, \widetilde{y})$. □

Theorem 3.3 *Conjecture* 1.1 *fails for some subfield of* $\mathbb{R}$ *and* $n = 7$.

P r o o f. (sketch) We find $\alpha, \beta \in \mathbb{R}$ such that $\alpha^2 \cdot \beta \cdot (1 - \alpha^2 - \beta) = 1$, α is transcendental over $\mathbb{Q}$, and $|\alpha| > 2^{2^{7-2}}$. It is known ([16]) that the equation $x + y + z = xyz = 1$ has no rational solution. Applying this, we prove: if $(x_1, x_2, x_3, x_4, x_5, x_6, x_7) \in \mathbb{Q}(\alpha, \beta)^7$ solves the system

$$x_1 = 1 \quad x_2 \cdot x_2 = x_3 \quad x_3 + x_4 = x_5 \quad x_5 + x_6 = x_1 \quad x_3 \cdot x_4 = x_7 \quad x_6 \cdot x_7 = x_1,$$

then $|x_2| = |\alpha| > 2^{2^{7-2}}$. □

4 Systems of linear equations

For a positive integer n we define the set of equations W_n by

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

Conjecture 4.1 *Let $\boldsymbol{G}$ be an additive subgroup of $\mathbb{C}$. If a system $S \subseteq W_n$ is consistent over $\boldsymbol{G}$, then S has a solution $(x_1, \ldots, x_n) \in (\boldsymbol{G} \cap \mathbb{Q})^n$ in which $|x_j| \leq 2^{n-1}$ for each j.*

Concerning Conjecture 4.1, estimation by 2^{n-1} is the best estimation. Indeed, if $1 \in \boldsymbol{G}$, then the system

$$x_1 = 1 \quad x_1 + x_1 = x_2 \quad x_2 + x_2 = x_3 \quad x_3 + x_3 = x_4 \quad \ldots \quad x_{n-1} + x_{n-1} = x_n$$

has a unique solution $(1, 2, 4, 8, \ldots, 2^{n-2}, 2^{n-1}) \in \boldsymbol{G}^n$.

Observation 4.2 *Let $n \in \{1, 2, 3, 4\}$, and let a system $S \subseteq W_n$ be consistent over the additive subgroup $\boldsymbol{G} \subseteq \mathbb{C}$. If $(x_1, \ldots, x_n) \in \boldsymbol{G}^n$ solves S, then $(\widehat{x_1}, \ldots, \widehat{x_n})$ solves S, where each $\widehat{x_i}$ is suitably chosen from $\{x_i, 0, 1, 2, \frac{1}{2}\} \cap \{z \in \boldsymbol{G} :\ |z| \leq 2^{n-1}\}$.*

Theorem 4.3 *Conjecture* 4.1 *holds true for each* $n \in \{1, 2, 3, 4\}$ *and each additive subgroup* $\boldsymbol{G} \subseteq \mathbb{C}$.

Proof. It follows from Observation 4.2. □

Conjecture 4.1 restricted to the case when $\boldsymbol{G} \supseteq \mathbb{Q}$ was probabilistically confirmed by various algorithms written in *MuPAD*, see [19] and [21]. In [11], a code in *Mathematica* illustrates the validity of Conjecture 4.1 restricted to the case when $\boldsymbol{G} \supseteq \mathbb{Q}$.

In the case when $\boldsymbol{G} \supseteq \mathbb{Q}$, we will prove a weaker version of Conjecture 4.1 with the estimation given by $(\sqrt{5})^{n-1}$.

Observation 4.4 *If* $\mathcal{A} \subseteq \mathbb{C}^k$ *is an affine subspace and* $\operatorname{card} \mathcal{A} > 1$*, then there exists* $m \in \{1, \ldots, k\}$ *with*

$$\emptyset \neq \mathcal{A} \cap \{(x_1, \ldots, x_k) \in \mathbb{C}^k : \; x_m + x_m = x_m\} \subsetneq \mathcal{A}.$$

Theorem 4.5 *Let a system* $S \subseteq W_n$ *be consistent over* $\mathbb{C}$*. Then* S *has a rational solution* $(x_1, \ldots, x_n)$ *in which* $|x_j| \leq (\sqrt{5})^{n-1}$ *for each* j.

Proof. We shall describe how to find a solution $(x_1, \ldots, x_n) \in \mathbb{Q}^n$ in which $|x_j| \leq (\sqrt{5})^{n-1}$ for each j. We can assume that for a certain $i \in \{1, \ldots, n\}$ the equation $x_i = 1$ belongs to S, as otherwise $(0, \ldots, 0)$ is a solution. Without loss of generality we can assume that the equation $x_1 = 1$ belongs to S. Each equation belonging to S has the form

$$a_1 x_1 + \ldots + a_n x_n = b,$$

where $a_1, \ldots, a_n, b \in \mathbb{Z}$. Since $x_1 = 1$, we can equivalently write this equation as

$$a_2 x_2 + \ldots + a_n x_n = b - a_1.$$

We receive a system of equations whose set of solutions is a non-empty affine subspace $\mathcal{A} \subseteq \mathbb{C}^{n-1}$. If $\operatorname{card} \mathcal{A} > 1$, then by Observation 4.4 we find $m \in \{2, \ldots, n\}$ for which

$$\emptyset \neq \mathcal{A} \cap \{(x_2, \ldots, x_n) \in \mathbb{C}^{n-1} : \; x_m + x_m = x_m\} \subsetneq \mathcal{A}.$$

The procedure described in the last sentence is applied to the affine subspace

$$\mathcal{A} \cap \{(x_2, \ldots, x_n) \in \mathbb{C}^{n-1} : \; x_m + x_m = x_m\}$$

and repeated until one point is achieved. The maximum number of procedure executions is $n - 1$. The received one-point affine subspace is described by equations belonging to a certain set

$$\mathcal{U} \subseteq \{x_i = 1 : \; i \in \{2, \ldots, n\}\} \cup \{x_i + x_j = x_k : \; i, j, k \in \{1, \ldots, n\}, \; i + j + k > 3\}.$$

Each equation belonging to $\mathcal{U}$ has the form

$$a_2 x_2 + \ldots + a_n x_n = c,$$

where $a_2, \ldots, a_n, c \in \mathbb{Z}$. Among these equations, we choose $n - 1$ linearly independent equations. We can do this because the equations belonging to $\mathcal{U}$ describe one-point affine subspace. Let $\mathbf{A}$ be the matrix of the system, and the system of equations has the following form

$$\mathbf{A} \cdot \begin{bmatrix} x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} c_2 \\ \vdots \\ c_n \end{bmatrix}.$$

Let $\mathbf{A}_j$ be the matrix formed by replacing the j-th column of $\mathbf{A}$ by the column $c_2, \ldots, c_n$. Clearly, $\det(\mathbf{A}) \in \mathbb{Z}$, and $\det(\mathbf{A}_j) \in \mathbb{Z}$ for each $j \in \{1, \ldots, n-1\}$. By Cramer's rule $x_j = \dfrac{\det(\mathbf{A}_{j-1})}{\det(\mathbf{A})} \in \mathbb{Q}$ for each $j \in \{2, \ldots, n\}$.

When the row of matrix $\mathbf{A}$ corresponds to the equation $x_i = 1$ ($i > 1$), then the entries in the row are 1, 0 ($n-2$ times), while the right side of the equation is 1.

When the row of matrix $\mathbf{A}$ corresponds to the equation $x_1 + x_1 = x_i$ ($i > 1$), then the entries in the row are 1, 0 ($n-2$ times), while the right side of the equation is 2.

When the row of matrix $\mathbf{A}$ corresponds to one of the equations: $x_1 + x_i = x_1$ or $x_i + x_1 = x_1$ ($i > 1$), then the entries in the row are 1, 0 ($n-2$ times), while the right side of the equation is 0.

When the row of matrix $\mathbf{A}$ corresponds to one of the equations: $x_1 + x_i = x_j$ or $x_i + x_1 = x_j$ ($i > 1$, $j > 1$, $i \neq j$), then the entries in the row are 1, -1, 0 ($n-3$ times), while the right side of the equation is 1.

When the row of matrix $\mathbf{A}$ corresponds to the equation $x_i + x_i = x_1$ ($i > 1$), then the entries in the row are 2, 0 ($n-2$ times), while the right side of the equation is 1.

When the row of matrix $\mathbf{A}$ corresponds to the equation $x_i + x_j = x_1$ ($i > 1$, $j > 1$, $i \neq j$), then the entries in the row are 1, 1, 0 ($n-3$ times), while the right side of the equation is 1.

From now on we assume that $i, j, k \in \{2, \dots, n\}$.

When the row of matrix $\mathbf{A}$ corresponds to the equation $x_i + x_j = x_k$ ($i \neq j$, $i \neq k$, $j \neq k$), then the entries in the row are 1, 1, -1, 0 ($n-4$ times), while the right side of the equation is 0.

When the row of matrix $\mathbf{A}$ corresponds to the equation $x_i + x_i = x_k$ ($i \neq k$), then the entries in the row are 2, -1, 0 ($n-3$ times), while the right side of the equation is 0.

When the row of matrix $\mathbf{A}$ corresponds to the equation $x_i + x_j = x_k$ ($k = i$ or $k = j$), then the entries in the row are 1, 0 ($n-2$ times), while the right side of the equation is 0.

Contradictory equations, e.g. $x_1 + x_i = x_i$ do not belong to $\mathcal{U}$, and therefore their description has been neglected. The description presented shows that each row of matrix $\mathbf{A}_j$ ($j \in \{1, \dots, n-1\}$) has the Euclidean length less than or equal to $\sqrt{5}$. Hadamard's inequality states that a determinant of a real matrix is majorized by the product of the Euclidean lengths of its rows. By Hadamard's inequality $|\det(\mathbf{A}_j)| \leq (\sqrt{5})^{n-1}$ for each $j \in \{1, \dots, n-1\}$. Hence, $|x_j| = \dfrac{|\det(\mathbf{A}_{j-1})|}{|\det(\mathbf{A})|} \leq |\det(\mathbf{A}_{j-1})| \leq (\sqrt{5})^{n-1}$ for each $j \in \{2, \dots, n\}$. □

In the case where $\boldsymbol{G} = \mathbb{Z}$, we will prove a weaker version of Conjecture 4.1 with the estimation given by $(\sqrt{5})^{n-1}$.

Lemma 4.6 ([3]). *Let $\mathbf{A}$ be a matrix with m rows, n columns, and integer entries. Let $b_1, \dots, b_m \in \mathbb{Z}$, and the matrix equation*

$$\mathbf{A} \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

defines the system of linear equations with rank m. Denote by δ the maximum of the absolute values of the $m \times m$ minors of the augmented matrix $(\mathbf{A}, b)$. We claim that if the system is consistent over $\mathbb{Z}$, then it has a solution in $(\mathbb{Z} \cap [-\delta, \delta])^n$.

Theorem 4.7 *Let a system $S \subseteq W_n$ be consistent over $\mathbb{Z}$. Then S has an integer solution $(x_1, \dots, x_n)$ in which $|x_j| \leq (\sqrt{5})^{n-1}$ for each j.*

Proof. We shall describe how to find a solution $(x_1, \dots, x_n) \in \mathbb{Z}^n$ in which $|x_j| \leq (\sqrt{5})^{n-1}$ for each j. We can assume that for a certain $i \in \{1, \dots, n\}$ the equation $x_i = 1$ belongs to S, as otherwise $(0, \dots, 0)$ is a solution. Without loss of generality we can assume that the equation $x_1 = 1$ belongs to S. Analogously as in the proof of Theorem 4.5, we construct a system of linear equations with variables $x_2, \dots, x_n$. For the augmented matrix of this system, the Euclidean length of each row is not greater than $\sqrt{5}$. We finish the proof by applying Hadamard's inequality and Lemma 4.6. □

Theorems 4.5 and 4.7 have similar forms, although linear systems over $\mathbb{C}$ and linear systems over $\mathbb{Z}$ have different criteria of consistency. Georg Frobenius proved that a system of linear Diophantine equations has an integer solution if and only if the rank r of the unaugmented matrix of coefficients and the greatest common divisor of the $r \times r$ minors of this matrix do not change when the augmented matrix is taken instead, see [6, p. 84]. In the case where the equations in the system are linearly independent, the reader is referred to [17, Satz 5, p. 10].

Acknowledgements The author would like to thank the anonymous referee for suggesting the formulation of Theorem 2.6 and other comments that have led to better organization of the paper.

References

[1] S. Basu, R. Pollack, and M. F. Roy, Algorithms in Real Algebraic Geometry, Second Edition (Springer-Verlag, 2006).
[2] L. Blum, F. Cucker, M. Shub, and S. Smale, Complexity and Real Computation (Springer-Verlag, 1998).
[3] I. Borosh, M. Flahive, D. Rubin, and B. Treybig, A sharp bound for solutions of linear Diophantine equations. Proc. Amer. Math. Soc. **105**, 844 – 846 (1989).
[4] M. Davis, Hilbert's tenth problem is unsolvable. Amer. Math. Monthly **80** , 233 – 269 (1973).
[5] M. Davis, Computability and Unsolvability (Dover Publications, 1982).
[6] L. E. Dickson, History of the Theory of Numbers, vol. II: Diophantine Analysis (Chelsea Publishing Co., 1966). Reprint of the 1920 ed. published by the Carnegie Institution of Washington.
[7] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. **73**, 349 – 366 (1983). Erratum ibid. **75**, 381 (1984).
[8] D. Yu. Grigor'ev and N. N. Vorobjov, Jr., Solving systems of polynomial inequalities in subexponential time. J. Symbolic Comput. **5**, 37 – 64 (1988).
[9] J. P. Jones, D. Sato, H. Wada, and D. Wiens, Diophantine representation of the set of prime numbers. Amer. Math. Monthly **83**, 449 – 464 (1976).
[10] J. P. Jones and Yu. V. Matijasevič, Proof of recursive unsolvability of Hilbert's tenth problem. Amer. Math. Monthly **98**, 689 – 709 (1991).
[11] A. Kozłowski and A. Tyszka, A Conjecture of Apoloniusz Tyszka on the Addition of Rational Numbers. http://demonstrations.wolfram.com/ AConjectureOfApoloniuszTyszkaOnTheAdditionOfRationalNumbers/, 2008.
[12] S. Lang, Number theory III: Diophantine geometry. Encyclopaedia of Mathematical Sciences 60 (Springer-Verlag, 1991).
[13] Yu. V. Matijasevič, The Diophantineness of enumerable sets. Soviet Math. Dokl. **11**, 354 – 358 (1970).
[14] Yu. V. Matijasevič, Hilbert's Tenth Problem (MIT Press, 1993).
[15] B. Poonen, Characterizing integers among rational numbers with a universal-existential formula. Amer. J. Math **131**, 675 – 682 (2009).
[16] G. Sansone and J .W. S. Cassels, Sur le problème de M. Werner Mnich. Acta Arith. **7**, 187 – 190 (1961/1962).
[17] Th. Skolem, Diophantische Gleichungen (Julius Springer, 1938).
[18] Th. Skolem, Unlösbarkeit von Gleichungen, deren entsprechende Kongruenz für jeden Modul lösbar ist. Avh. Norske Vid. Akad. Oslo. I., no. 4 (1942).
[19] A. Tyszka, Bounds of some real (complex) solution of a finite system of polynomial equations with rational coefficients. http://arxiv.org/abs/math/0702558
[20] A. Tyszka, A system of equations. SIAM Problems and Solutions (electronic only), Problem 07-006, http://www.siam.org/journals/problems/downloadfiles/07-006.pdf (2007).
[21] A. Tyszka, Some conjectures on addition and multiplication of complex (real) numbers. Int. Math. Forum **4**, 521 – 530 (2009).
[22] 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.
[23] N. N. Vorobjov, Jr., Estimates of real roots of a system of algebraic equations. J. Sov. Math. **34**, 1754 – 1762 (1986).

