Accepted by Bull. Pol. Acad. Sci. Math. See also arXiv:2104.02520.

$\mathbb{Q} \setminus \mathbb{Z}$ IS DIOPHANTINE OVER $\mathbb{Q}$ WITH 32 UNKNOWNS

GENG-RUI ZHANG AND ZHI-WEI SUN*

Abstract. In 2016 J. Koenigsmann refined a celebrated theorem of J. Robinson by proving that $\mathbb{Q} \setminus \mathbb{Z}$ is diophantine over $\mathbb{Q}$, i.e., there is a polynomial $P(t, x_1, \ldots, x_n) \in \mathbb{Z}[t, x_1, \ldots, x_n]$ such that for any rational number t we have

$$t \notin \mathbb{Z} \iff \exists x_1 \cdots \exists x_n [P(t, x_1, \ldots, x_n) = 0]$$

where variables range over $\mathbb{Q}$, equivalently

$$t \in \mathbb{Z} \iff \forall x_1 \cdots \forall x_n [P(t, x_1, \ldots, x_n) \neq 0].$$

In this paper we prove further that we may even take $n = 32$. Combining this with a result of Sun, we get that there is no algorithm to decide for any $f(x_1, \ldots, x_{41}) \in \mathbb{Z}[x_1, \ldots, x_{41}]$ whether

$$\forall x_1 \cdots \forall x_9 \exists y_1 \cdots \exists y_{32} [f(x_1, \ldots, x_9, y_1, \ldots, y_{32}) = 0],$$

where variables range over $\mathbb{Q}$.

1. Introduction

Let $\mathbb{Z}$ be the ring of integers. Hilbert's Tenth Problem (HTP), the tenth one of his 23 famous mathematical problems presented in the 1900 ICM, asks for an algorithm to determine for any given polynomial $P(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ whether the diophantine equation $P(x_1, \ldots, x_n) = 0$ has solutions $x_1, \ldots, x_n \in \mathbb{Z}$. This was solved negatively by Yu. Matiyasevich [10] in 1970, on the basis of the important work of M. Davis, H. Putnam and J. Robinson [6]; see also Davis [5] for a nice introduction. Z.-W. Sun [17] proved his 11 unknowns theorem which states that there is no algorithm to determine for any $P(x_1, \ldots, x_{11}) \in \mathbb{Z}[x_1, \ldots, x_{11}]$ whether the equation $P(x_1, \ldots, x_{11}) = 0$ has solutions over $\mathbb{Z}$.

Let $\mathbb{Q}$ be the field of rational numbers. It remains open whether HTP over $\mathbb{Q}$ is undecidable. However, J. Robinson [16] used the theory of quadratic forms to prove that one can characterize $\mathbb{Z}$ by using the language of $\mathbb{Q}$ in the following way: For any $t \in \mathbb{Q}$ we have

$$t \in \mathbb{Z} \iff \forall x_1 \forall x_2 \exists y_1 \cdots \exists y_7 \forall z_1 \cdots \forall z_6 [f(t, x_1, x_2, y_1, \ldots, y_7, z_1, \ldots, z_6) = 0],$$

where f is a polynomial with integer coefficients. (Throughout this paper, variables always range over $\mathbb{Q}$.) In 2009 B. Poonen [15] improved this by

Key words and phrases. Undecidability, definability, diophantine sets, Hilbert's tenth problem over $\mathbb{Q}$, mixed quantifiers.

2020 *Mathematics Subject Classification.* Primary 03D35, 11U05; Secondary 03D25, 11D99, 11S99.

* Corresponding author, supported by the National Natural Science Foundation of China (grant no. 11971222).

finding a polynomial $F(t, x_1, x_2, y_1, \ldots, y_7)$ with integer coefficients such that for any $t \in \mathbb{Q}$ we have

$$t \in \mathbb{Z} \iff \forall x_1 \forall x_2 \exists y_1 \cdots \exists y_7 [F(t, x_1, x_2, y_1, \ldots, y_7) = 0].$$

In 2016 J. Koenigsmann [9] improved B. Poonen's result by proving that $\mathbb{Q} \setminus \mathbb{Z}$ is diophantine over $\mathbb{Q}$, i.e., there is a polynomial $P(t, x_1, \ldots, x_n) \in \mathbb{Q}[t, x_1, \ldots, x_n]$ such that for any $t \in \mathbb{Q}$ we have

$$t \notin \mathbb{Z} \iff \exists x_1 \cdots \exists x_n [P(t, x_1, \ldots, x_n) = 0],$$

i.e.,

$$t \in \mathbb{Z} \iff \forall x_1 \cdots \forall x_n [P(t, x_1, \ldots, x_n) \neq 0].$$

The number n of unknowns in Koenigsmann's diophantine representation of $\mathbb{Q} \setminus \mathbb{Z}$ over $\mathbb{Q}$ is over 400 but below 500. In 2018 N. Daans [3] significantly simplified Koenigsmann's approach and proved that $\mathbb{Q} \setminus \mathbb{Z}$ has a diophantine representation over $\mathbb{Q}$ with 50 unknowns. The number 50 could be reduced to 38 by applying a recent result [4, Theorem 1.4] obtained by model theory.

In this paper we establish the following new result.

Theorem 1.1. *$\mathbb{Q} \setminus \mathbb{Z}$ has a diophantine representation over $\mathbb{Q}$ with* 32 *unknowns, i.e., there is a polynomial $P(t, x_1, \ldots, x_{32}) \in \mathbb{Z}[t, x_1, \ldots, x_{32}]$ such that for any $t \in \mathbb{Q}$ we have*

$$t \notin \mathbb{Z} \iff \exists x_1 \cdots \exists x_{32} [P(t, x_1, \ldots, x_{32}) = 0]. \tag{1.1}$$

Furthermore, the polynomial P can be constructed explicitly with $\deg P < 2.1 \times 10^{11}$.

To obtain this theorem, we start from Daans' work [3], and mainly use a new relation-combining theorem on diophantine representations over $\mathbb{Q}$ (which is an analogue of Matiyasevich and Robinson's relation-combining theorem [11, Theorem 1]) as an auxiliary tool. Now we state our relation-combining theorem for diophantine representations over $\mathbb{Q}$.

Theorem 1.2. *Let $\mathcal{J}_k(x_1, \ldots, x_k, x)$ denote the expression*

$$\prod_{s=1}^{k} x_s^{(k-1)2^{k+1}} \times \prod_{\varepsilon_1, \ldots \varepsilon_k \in \{\pm 1\}} \left(x + \sum_{s=1}^{k} \varepsilon_s \sqrt{x_s}\, W(x_1, \ldots, x_k)^{s-1} \right),$$

where

$$W(x_1, \ldots, x_k) = \left(k + \sum_{s=1}^{k} x_s^2 \right) \left(1 + \sum_{s=1}^{k} x_s^{-2} \right).$$

Then $\mathcal{J}_k(x_1, \ldots, x_k, x)$ is a polynomial with integer coefficients. Moreover, for any $A_1, \ldots, A_k \in \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, we have

$$A_1, \ldots, A_k \in \square \iff \exists x [\mathcal{J}_k(A_1, \ldots, A_k, x) = 0], \tag{1.2}$$

where $\square = \{r^2 : \ r \in \mathbb{Q}\}$.

Remark 1.1. In view of its proof, Theorem 1.2 can be generalized via replacing $\mathbb{Q}$ by any subfield of the real field $\mathbb{R}$ or any ordered field.

When $\rho_s \in \{\forall, \exists\}$ for all $s = 1, \ldots, k$, we say that $\rho_1 \cdots \rho_k$ over $\mathbb{Q}$ is undecidable if there is no algorithm to decide for any polynomial $P(x_1, \ldots, x_k)$ over $\mathbb{Q}$ whether

$$\rho_1 x_1 \cdots \rho_k x_k [P(x_1, \ldots, x_k) = 0]$$

or not. For convenience we adopt certain abbreviation, for example, $\forall^2\exists^3$ denotes $\forall\forall\exists\exists\exists$.

Combining Theorem 1.1 and its proof with a result of Sun [17, Theorem 1.1], we obtain the following theorem.

Theorem 1.3. *$\forall^9\exists^{32}$ over $\mathbb{Q}$ is undecidable, i.e., there is no algorithm to determine for any $P(x_1, \ldots, x_{41}) \in \mathbb{Z}[x_1, \ldots, x_{41}]$ whether*

$$\forall x_1 \cdots \forall x_9 \exists y_1 \cdots \exists y_{32} [P(x_1, \ldots, x_9, y_1, \ldots, y_{32}) = 0].$$

Also, $\exists^9\forall^{32}\exists$ over $\mathbb{Q}$ and $\exists^{10}\forall^{31}\exists$ over $\mathbb{Q}$ are undecidable.

We remark that Sun [18] obtained some undecidability results on mixed quantifier prefixes over diophantine equations with integer variables; for example, he proved that $\forall^2\exists^4$ over $\mathbb{Z}$ is undecidable.

In the next section we will prove Theorem 1.2. Sections 3 and 4 are devoted to our proofs of Theorems 1.1 and 1.3 respectively.

2. Proof of Theorem 1.2

Proof of Theorem 1.2. Clearly,

$$I_k(x_1, \ldots, x_k, x, y) = \prod_{\varepsilon_1, \ldots, \varepsilon_k \in \{\pm 1\}} (x + \varepsilon_1 x_1 + \varepsilon_2 x_2 y + \cdots + \varepsilon_k x_k y^{k-1}).$$

is a polynomial with integer coefficients. As

$$I_k(x_1, \ldots, x_k, x, y) = \prod_{\varepsilon_i \in \{\pm 1\} \text{ for } i \neq t} \left(\left(x + \sum_{\substack{s=1 \\ s \neq t}}^{k} \varepsilon_s x_s y^{s-1} \right)^2 - x_t^2 y^{2(t-1)} \right)$$

for all $t = 1, \ldots, k$, we see that

$$I_k(x_1, \ldots, x_k, x, y) = I_k^*(x_1^2, \ldots, x_k^2, x, y)$$

for some polynomial I_k^* with integer coefficients. Note that

$$\mathcal{J}_k(x_1, \ldots, x_k, x) = \prod_{s=1}^{k} x_s^{(k-1)2^{k+1}} \times I_k^*\left(x_1, \ldots, x_k, x, \left(k + \sum_{j=1}^{k} x_j^2 \right) \left(1 + \sum_{j=1}^{k} x_j^{-2} \right) \right)$$

is a polynomial with integer coefficients.

Now let $A_1, \ldots, A_k \in \mathbb{Q}^*$. We claim that for any rational number

$$W_k \geq \frac{1 + \sum_{s=1}^{k} |\sqrt{A_s}|}{\min\{|\sqrt{A_1}|, \ldots, |\sqrt{A_k}|\}}, \tag{2.1}$$

we have

$$A_1,\dots,A_k\in\square \iff \exists x[I_k^*(A_1,\dots,A_k,x,W_k)=0].$$

The "⇒" direction is easy. If $A_1=a_1^2,\dots,A_k=a_k^2$ for some $a_1,\dots,a_k\in\mathbb{Q}$, then, for $x=a_1+a_2W_k+\dots+a_kW_k^{k-1}\in\mathbb{Q}$ we have $I_k^*(A_1,\dots,A_k,x,W_k)=0$.

We use induction on k to prove the "⇐" direction of the claim. In the case $k=1$, if $I_1^*(A_1,x,W_1)=x^2-A_1$ is zero for some $x\in\mathbb{Q}$ then we obviously have $A_1\in\square$.

Now let $k>1$ and assume that the "⇐" direction of the claim holds for all smaller values of k. Let W_k be any rational number satisfying the inequality (2.1). Suppose that $I_k^*(A_1,\dots,A_k,x,W_k)=0$ for some $x\in\mathbb{Q}$. Then there are $\varepsilon_1,\dots,\varepsilon_k\in\{\pm1\}$ such that

$$x+\sum_{s=1}^{k}\varepsilon_s\sqrt{A_s}W_k^{s-1}=0.$$

If $A_k=a_k^2$ for some $a_k\in\mathbb{Q}$, then, for $x'=x+\varepsilon_ka_kW_k^{k-1}$ we have

$$x'+\varepsilon_1\sqrt{A_1}+\varepsilon_2\sqrt{A_2}W_k+\dots+\varepsilon_{k-1}\sqrt{A_{k-1}}W_k^{k-2}=0$$

and hence $I_{k-1}^*(A_1,\dots,A_{k-1},x',W_k)=0$. Note that

$$|\sqrt{A_t}|W_k\ge 1+\sum_{s=1}^{k}|\sqrt{A_s}|\ge 1+\sum_{s=1}^{k-1}|\sqrt{A_s}|$$

for each $t=1,\dots,k-1$. So, in the case $A_k\in\square$, we get $A_1,\dots,A_{k-1}\in\square$ by the induction hypothesis.

To finish the induction step, it remains to prove $A_k\in\square$. As the characteristic of $\mathbb{Q}$ is zero, $\mathbb{Q}(\sqrt{A_s})$ is a Galois extension of $\mathbb{Q}$ for any $s=1,\dots,k$. Thus

$$\mathbb{Q}(\sqrt{A_1},\dots,\sqrt{A_k})=\mathbb{Q}(\sqrt{A_1})\cdots\mathbb{Q}(\sqrt{A_k})$$

is also a Galois extension of $\mathbb{Q}$ in view of [12, p. 50, Problem 10(d)]. Suppose that $A_k\notin\square$. Then $\sqrt{A_k}\notin\mathbb{Q}$, and hence there is an automorphism $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$ with $\sigma(\sqrt{A_k})\neq\sqrt{A_k}$, where $K=\mathbb{Q}(\sqrt{A_1},\dots,\sqrt{A_k})$. Recall that

$$0=x+\sum_{s=1}^{k}\varepsilon_s\sqrt{A_s}W_k^{s-1}.$$

Hence

$$0=0-\sigma(0)=\sum_{s=1}^{k}2\varepsilon_s(\sqrt{A_s}-\sigma(\sqrt{A_s}))W_k^{s-1}. \tag{2.2}$$

Note that $\sigma(\sqrt{A_k})=-\sqrt{A_k}$, and $\sigma(\sqrt{A_s})\in\{\pm\sqrt{A_s}\}$ for all $s=1,\dots,k-1$. Thus, by (2.2) we have

$$2|\sqrt{A_k}|W_k^{k-1}=|2\varepsilon_k\sqrt{A_k}W_k^{k-1}|\le\sum_{s=1}^{k-1}2|\sqrt{A_s}|W_k^{s-1}.$$

On the other hand,

$$\begin{aligned}|\sqrt{A_k}|W_k^{k-1} \geq& W_k^{k-2}\left(1+\sum_{s=1}^{k}|\sqrt{A_s}|\right)\\ >& W_k^{k-2}\sum_{s=1}^{k-1}|\sqrt{A_s}| \geq \sum_{s=1}^{k-1}|\sqrt{A_s}|W_k^{s-1}.\end{aligned}$$

So we get a contradiction and this concludes our proof of the claim.

Note that

$$\begin{aligned}W :=& \left(\sum_{s=1}^{k}(1+A_s^2)\right)\left(1+\sum_{s=1}^{k}A_s^{-2}\right)\\ =& \sum_{s=1}^{k}(1+A_s^2)+\sum_{r=1}^{k}\sum_{s=1}^{k}A_r^{-2}(1+A_s^2).\end{aligned}$$

For $0 \leq \alpha \leq 1$ clearly $1+\alpha^4 \geq 1 \geq \alpha$; if $\alpha \geq 1$ then $1+\alpha^4 \geq \alpha^4 \geq \alpha$. So $1+\alpha^4 \geq \alpha$ for all $\alpha \geq 0$, and hence $1+A_s^2 \geq |\sqrt{A_s}|$ for all $s = 1,\dots,k$. Therefore,

$$W \geq \sum_{s=1}^{k}(1+A_s^2)+1 \geq 1+\sum_{s=1}^{k}|\sqrt{A_s}|.$$

If $t \in \{1,\dots,k\}$ and $|A_t| \geq 1$, then

$$|\sqrt{A_t}|W \geq W \geq 1+\sum_{s=1}^{k}|\sqrt{A_s}|.$$

If $1 \leq t \leq k$ and $|A_t| < 1$, then $|\sqrt{A_t}| = |A_t|^{1/2} > A_t^2$ and hence

$$\begin{aligned}|\sqrt{A_t}|W \geq& |\sqrt{A_t}|\left(1+\sum_{s=1}^{k}A_t^{-2}(1+A_s^2)\right)\\ \geq& |\sqrt{A_t}|+\sum_{s=1}^{k}(1+A_s^2) = |\sqrt{A_t}|+(1+A_t^2)+\sum_{\substack{s=1\\ s\neq t}}^{k}(1+A_s^2)\\ \geq& 1+\sum_{s=1}^{k}|\sqrt{A_s}|.\end{aligned}$$

Therefore the inequality (2.1) holds if we take $W_k = W$. Applying the proved claim we immediately obtain the desired result. This concludes our proof of Theorem 1.2. □

3. Proof of Theorem 1.1

Let p be any prime. As usual, we let $\mathbb{Q}_p$ and $\mathbb{Z}_p$ denote the p-adic field and the ring of p-adic integers respectively. We also define

$$\mathbb{Z}_{(p)} = \mathbb{Q}\cap\mathbb{Z}_p = \left\{\frac{a}{b}:\ a,b\in\mathbb{Z} \text{ and } p\nmid b\right\}.$$

D. Flath and S. Wagon [8] attributed the following lemma as an observation of J. Robinson, but we cannot find it in any of Robinson's papers.

Lemma 3.1. *Let r be any rational number. Then*

$$r \in \mathbb{Z}_{(2)} \iff \exists x \exists y \exists z [7r^2 + 2 = x^2 + y^2 + z^2]. \tag{3.1}$$

Proof. The Gauss-Legendre theorem on sums of three squares (cf. [13, pp. 17-23])) states that $n \in \mathbb{N} = \{0, 1, \ldots\}$ is a sum of three integer squares if and only if $n \notin \{4^k(8m+7) : k, m \in \mathbb{N}\}$.

If $r = a/b$ with $a, b \in \mathbb{Z}$ and $2 \nmid b$, then $7a^2 + 2b^2 \equiv 2 - a^2 \equiv 1, 2 \pmod 4$ and hence $7a^2 + 2b^2$ is a sum of three squares, thus $7r^2 + 2 = (7a^2 + 2b^2)/b^2$ can be expressed as $x^2 + y^2 + z^2$ with $x, y, z \in \mathbb{Q}$.

Suppose that $r = a/b$ with $a, b \in \mathbb{Z}$, $2 \nmid a$, $b \neq 0$ and $2 \mid b$. If $7r^2 + 2 = x^2 + y^2 + z^2$ for some $x, y, z \in \mathbb{Q}$, then there is a nonzero integer c such that $c^2(7r^2 + 2)$ is a sum of three integer squares and hence $c^2(7r^2 + 2) \notin \{4^k(8m + 7) : k, m \in \mathbb{N}\}$. Note that any odd square is congruent to 1 modulo 8 and $7a^2 + 2b^2 \equiv 7 \pmod 8$ as $2 \nmid a$ and $2 \mid b$. Thus the integer $c^2(7r^2 + 2) = (c/b)^2(7a^2 + 2b^2)$ has the form $(2^k)^2(8m + 7)$ with $k, m \in \mathbb{N}$ which leads to a contradiction.

In view of the above, we have completed the proof of Lemma 3.1.

For any prime p and $t \in \mathbb{Q}$, as usual we denote the p-adic valuation of t by $\nu_p(t)$. For $A \subseteq \mathbb{Q}$ we define $A^\times = \{a \in A \setminus \{0\} : a^{-1} \in A\}$.

Lemma 3.2. *Let p be a prime, and let $t \in \mathbb{Q}$. Then*

$$t \in \mathbb{Z}_{(p)}^\times \iff t \neq 0 \wedge (t + t^{-1} \in \mathbb{Z}_{(p)}). \tag{3.2}$$

Proof. For $t \in \mathbb{Q}^*$, we have $\nu_p(t^{-1}) = -\nu_p(t)$. So the desired result follows. □

Remark 3.1. This easy lemma was used by N. Daans [3].

For first-order formulas $\psi_1, \ldots, \psi_k$, we simply write

$$\psi_1 \vee \cdots \vee \psi_k \quad \text{and} \quad \psi_1 \wedge \cdots \wedge \psi_k$$

as $\bigvee_{s=1}^k \psi_s$ and $\bigwedge_{s=1}^k \psi_s$ respectively.

Definition 3.1. We set $\square^* = \{x^2 : x \in \mathbb{Q}^*\}$. A subset T of $\mathbb{Q}$ is said to be *m-good* if there are polynomials

$$f_s(t, x_1, \ldots, x_m),\ g_{s1}(t, x_1, \ldots, x_m), \ldots, g_{s\ell_s}(t, x_1, \ldots, x_m)\ (s = 1, \ldots, k)$$

with integer coefficients such that a rational number t belongs to T if and only if

$$\exists x_1 \cdots \exists x_m \left[\bigvee_{s=1}^k \left(f_s(t, x_1, \ldots, x_m) = 0 \wedge \bigwedge_{j=1}^{\ell_s} (g_{sj}(t, x_1, \ldots, x_m) \in \square^*) \right) \right].$$

Remark 3.2. (i) Clearly a rational number t is nonzero if and only if $t^2 \in \square^*$. For any polynomial $P(x) \in \mathbb{Z}[x]$ of degree d, we have $x^{2d}P(x^{-1}) \in \mathbb{Z}[x]$, and

$$t^{2d}P(t^{-1}) \in \square^* \iff P(t^{-1}) \in \square^*$$

for all $t \in \mathbb{Q}^*$.

(ii) For any $a, b \in \mathbb{Q}$, clearly $(a = 0 \wedge b = 0) \iff a^2 + b^2 = 0$. In view of this and the distributive law concerning disjunction and conjunction, if $S \subseteq \mathbb{Q}$ is m-good and $T \subseteq \mathbb{Q}$ is n-good then $S \cap T$ is $(m+n)$-good.

Lemma 3.3. *Both* $\mathbb{Z}_{(2)}$ *and* $\mathbb{Z}_{(2)}^{\times}$ *are* 2*-good.*

Proof. For any $t \in \mathbb{Q}$, by Lemma 3.1 we have

$$t \in \mathbb{Z}_{(2)} \iff \exists x \exists y[7t^2 + 2 - x^2 - y^2 \in \square].$$

Note also that

$$t \in \mathbb{Z}_{(2)}^{\times} \iff t \neq 0 \wedge (t + t^{-1} \in \mathbb{Z}_{(2)})$$

by Lemma 3.2. Combining these with Remark 3.2 we immediately get the desired result. $\square$

Let $a, b \in \mathbb{Q}^*$. As in B. Poonen [15], we define

$$S_{a,b} = \{2x_1 \in \mathbb{Q} : \exists x_2 \exists x_3 \exists x_4 [x_1^2 - a x_2^2 - b x_3^2 + ab x_4^2 = 1]\} \tag{3.3}$$

and

$$T_{a,b} = \{x + y : x, y \in S_{a,b}\}. \tag{3.4}$$

Lemma 3.4. *Let* $a, b \in \mathbb{Q}^*$ *with* $a > 0$ *or* $b > 0$. *Then* $T_{a,b}$ *and* $T_{a,b}^{\times}$ *are* 5*-good.*

Proof. Let $r \in \mathbb{Q}$. Note that

$$\left(\frac{r}{2}\right)^2 - a\left(\frac{x}{2}\right)^2 - b\left(\frac{y}{2}\right)^2 + ab\left(\frac{z}{2}\right)^2 = 1 \iff ab(4 - r^2 + ax^2 + by^2) = (abz)^2.$$

So

$$\begin{aligned} r \in S_{a,b} &\iff \exists x \exists y[ab(4 - r^2 + ax^2 + by^2) \in \square] \\ &\iff \exists x \exists y[ab(4 - r^2 + ax^2 + by^2) = 0 \vee ab(4 - r^2 + ax^2 + by^2) \in \square^*] \end{aligned}$$

and hence $S_{a,b}$ is 2-good.

For $t \in \mathbb{Q}$, we obviously have

$$t \in T_{a,b} \iff \exists r(r \in S_{a,b} \wedge t - r \in S_{a,b}).$$

As $S_{a,b}$ is 2-good, $T_{a,b}$ is 5-good by Remark 3.2(ii).

By Koenigsmann [9, Proposition 6],

$$T_{a,b}^{\times} = \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)}^{\times},$$

where

$$\Delta_{a,b} = \{p : p \text{ is prime and } (a,b)_p = -1\}$$

with $(a,b)_p$ the Hilbert symbol. (We view an empty intersection of subsets of $\mathbb{Q}$ as $\mathbb{Q}$, thus $T_{a,b}^{\times} = \mathbb{Q}$ if $\Delta_{a,b} = \emptyset$.) Let $t \in \mathbb{Q}^*$. By Lemma 3.2, we have

$$t \in T_{a,b}^{\times} \iff \forall p \in \Delta_{a,b}(t + t^{-1} \in \mathbb{Z}_{(p)}) \iff t + t^{-1} \in T_{a,b}.$$

In view of Remark 3.2, from the above we see that $T_{a,b}^{\times}$ is 5-good.

The proof of Lemma 3.4 is now complete. $\square$

For $S,T\subseteq\mathbb{Q}$ we set
$$ST=\{st:\ s\in S\text{ and }t\in T\}.$$
For $a,b,c\in\mathbb{Q}^*$ with $a>0$ or $b>0$, we define
$$J^c_{a,b}=T_{a,b}\,\{cy^2:\ y\in\mathbb{Q}\text{ and }1-cy^2\in\Box T^\times_{a,b}\}.\tag{3.5}$$
By Koenigsmann [9, Proposition 6] and Daans [3, Lemma 5.4],
$$J^c_{a,b}=\bigcap_{\substack{p\in\Delta_{a,b}\\ 2\nmid\nu_p(c)}}p\mathbb{Z}_{(p)}.\tag{3.6}$$

Lemma 3.5. *Let $a,b,c\in\mathbb{Q}^*$ with $a>0$ or $b>0$. Then $J^c_{a,b}$ is 12-good.*

Proof. As $0\in J^c_{a,b}$ by (3.6), we have $T^\times_{a,b}\neq\emptyset$. For any $x\in\mathbb{Q}$, clearly
$$x\in\Box T^\times_{a,b}\iff x=0\vee\exists y(xy^2\in T^\times_{a,b}).$$
So $\Box T^\times_{a,b}$ is 6-good in light of Lemma 3.4. As $\pm2\in S_{a,b}$, both $T_{a,b}$ and $J^c_{a,b}$ contain 0. Let $x\in\mathbb{Q}$. Note that
$$x\in J^c_{a,b}\iff x=0\vee\exists y\neq0\left[\frac{x}{cy^2}\in T_{a,b}\wedge(1-cy^2\in\Box T^\times_{a,b})\right].$$
Thus, with the aid of Remark 3.2 and Lemma 3.4, we see that $J^c_{a,b}$ is 12-good. □

Proof of Theorem 1.1. Let $t\in\mathbb{Q}$. Clearly,
$$t\in\mathbb{Q}\setminus\mathbb{Z}\iff t\neq0\wedge t^{-1}\in\bigcup_{p\in\mathbb{P}}p\mathbb{Z}_{(p)},$$
where $\mathbb{P}$ is the set of all primes. By Daans [3, (1)], we have
$$\bigcup_{p\in\mathbb{P}}p\mathbb{Z}_{(p)}=2\mathbb{Z}_{(2)}\cup\bigcup_{(a,b)\in\Phi}(J^a_{a,b}\cap J^{2b}_{a,b}),\tag{3.7}$$
where
$$\Phi=\{(1+4u^2,2v):\ u,v\in\mathbb{Z}^\times_{(2)}\}.\tag{3.8}$$
In view of this and Lemma 3.1, when $t\neq0$ we have
$$\begin{aligned}t\notin\mathbb{Z}&\iff\frac{1}{2t}\in\mathbb{Z}_{(2)}\vee\exists u\exists v\left[u,v\in\mathbb{Z}^\times_{(2)}\wedge\frac1t\in J^{1+4u^2}_{1+4u^2,2v}\cap J^{4v}_{1+4u^2,2v}\right]\\&\iff\exists u\exists v\left(\frac{7}{4t^2}+2-u^2-v^2\in\Box\right)\\&\qquad\vee\exists u\exists v\left[u,v\in\mathbb{Z}^\times_{(2)}\wedge\frac1t\in J^{1+4u^2}_{1+4u^2,2v}\cap J^{4v}_{1+4u^2,2v}\right]\\&\iff\exists u\exists v\Bigg[8t^2+7-u^2-v^2\in\Box\\&\qquad\vee\left(u,v\in\mathbb{Z}^\times_{(2)}\wedge t^{-1}\in J^{1+4u^2}_{1+4u^2,2v}\wedge t^{-1}\in J^{4v}_{1+4u^2,2v}\right)\Bigg].\end{aligned}$$

Combining this with Lemmas 3.3 and 3.5, we obtain that $\mathbb{Q}\setminus\mathbb{Z}$ is 30-good in view of Remark 3.2.

By the above, there are polynomials

$$f_s(t,x_1,\ldots,x_{30}),\ g_{s1}(t,x_1,\ldots,x_{30}),\ldots,g_{s\ell_s}(t,x_1,\ldots,x_{30})\ (s=1,\ldots,k)$$

with integer coefficients such that a rational number t is not an integer if and only if

$$\exists x_1\cdots\exists x_{30}\Bigg[\bigvee_{s=1}^{k}\Bigg(f_s(t,x_1,\ldots,x_{30})=0\wedge\bigwedge_{j=1}^{\ell_s}(g_{sj}(t,x_1,\ldots,x_{30})\in\square^*)\Bigg)\Bigg].$$

Note that

$$g_{sj}(t,x_1,\ldots,x_{30})\neq 0\quad\text{for all } j=1,\ldots,\ell_s$$

if and only if

$$x_{31}\prod_{j=1}^{\ell_s}g_{sj}(t,x_1,\ldots,x_{30})-1=0$$

for some $x_{31}\in\mathbb{Q}$. By Theorem 1.2, when $\prod_{j=1}^{\ell_s}g_{sj}(t,x_1,\ldots,x_{30})\neq 0$, we have

$$g_{sj}(t,x_1,\ldots,x_{30})\in\square\qquad\text{for all } j=1,\ldots,\ell_s$$

if and only if

$$\mathcal{J}_{\ell_s}\left(g_{s1}(t,x_1,\ldots,x_{30}),\ldots,g_{s\ell_s}(t,x_1,\ldots,x_{30}),x_{32}\right)=0$$

for some $x_{32}\in\mathbb{Q}$. Combining these we see that $t\notin\mathbb{Z}$ if and only if there are $x_1,\ldots,x_{32}\in\mathbb{Q}$ such that the product of all those

$$f_s(t,x_1,\ldots,x_{30})^2+\left(x_{31}\prod_{j=1}^{\ell_s}g_{sj}(t,x_1,\ldots,x_{30})-1\right)^2$$
$$+\mathcal{J}_{\ell_s}(g_{s1}(t,x_1,\ldots,x_{30}),\ldots,g_{s\ell_s}(t,x_1,\ldots,x_{30}),x_{32})^2$$

$(s=1,\ldots,k)$ is zero.

In the spirit of the above proof, we can actually construct an explicit polynomial $P(t,x_1,\ldots,x_{32})$ with integer coefficients satisfying (1.1) with the total degree of P smaller than 2.1×10^{11}. This concludes our proof of Theorem 1.1. □

4. Proof of Theorem 1.3

It is known that each nonnegative integer can be written as a sum of four squares of rational numbers. This result due to Euler (cf. [14]) is weaker than Lagrange's four-square theorem (cf. [13, pp. 5-7]). Clearly, any nonnegative rational number can be written as $a/b=(ab)/b^2$ with $a,b\in\mathbb{N}$ and $b>0$. So we have the following lemma.

Lemma 4.1. *Let $r\in\mathbb{Q}$. Then*

$$r\geq 0\iff\exists w\exists x\exists y\exists z[r=w^2+x^2+y^2+z^2].\tag{4.1}$$

We also need a known result of Sun [17, Theorem 1.1].

Lemma 4.2 (Sun [17]). *Let $\mathcal{A} \subseteq \mathbb{N}$ be an r.e. (recursively enumerable) set.*

(i) *There is a polynomial $P_{\mathcal{A}}(x_0, x_1, \ldots, x_9)$ with integer coefficients such that for any $a \in \mathbb{N}$ we have $a \in \mathcal{A}$ if and only if $P_{\mathcal{A}}(a, x_1, \ldots, x_9) = 0$ for some $x_1, \ldots, x_9 \in \mathbb{Z}$ with $x_9 \geq 0$.*

(ii) *There is a polynomial $Q_{\mathcal{A}}(x_0, x_1, \ldots, x_{10})$ with integer coefficients such that for any $a \in \mathbb{N}$ we have $a \in \mathcal{A}$ if and only if $Q_{\mathcal{A}}(a, x_1, \ldots, x_{10}) = 0$ for some $x_1, \ldots, x_{10} \in \mathbb{Z}$ with $x_{10} \neq 0$.*

Proof of Theorem 1.3. It is well known that there are nonrecursive r.e. sets (see, e.g., [2, pp. 140-141]). Let us take any nonrecursive r.e. set $\mathcal{A} \subseteq \mathbb{N}$.

(i) Let $P_{\mathcal{A}}$ and P be polynomials as in Lemma 4.2 and Theorem 1.1. In view of Lemmas 4.1-4.2 and Theorem 1.1, for any $a \in \mathbb{N}$ we have

$$\begin{aligned}
a \notin \mathcal{A} &\iff \forall x_1 \cdots \forall x_9 [\neg(x_1, \ldots, x_9 \in \mathbb{Z} \wedge x_9 \geq 0) \vee P_{\mathcal{A}}(a, x_1, \ldots, x_9) \neq 0] \\
&\iff \forall x_1 \cdots \forall x_9 \left[\bigvee_{t=1}^{9} (x_t \notin \mathbb{Z}) \vee x_9 < 0 \vee P_{\mathcal{A}}(a, x_1, \ldots, x_9) \neq 0 \right] \\
&\iff \forall x_1 \cdots \forall x_9 \left[\bigvee_{t=1}^{9} \exists y_1 \cdots \exists y_{32} (P(x_t, y_1, \ldots, y_{32}) = 0) \right. \\
&\qquad \left. \vee -x_9 > 0 \vee \exists y_1 (y_1 P_{\mathcal{A}}(a, x_1, \ldots, x_9) - 1 = 0 \right] \\
&\iff \forall x_1 \cdots \forall x_9 \exists y_1 \cdots \exists y_{32} [P_0(a, x_1, \ldots, x_9, y_1, \ldots, y_{32}) = 0],
\end{aligned}$$

where

$$\begin{aligned}
&P_0(a, x_1, \ldots, x_9, y_1, \ldots, y_{32}) \\
=&(y_1 P_{\mathcal{A}}(a, x_1, \ldots, x_9) - 1) \prod_{t=1}^{9} P(x_t, y_1, \ldots, y_{32}) \\
&\times \left((x_9 y_1 - 1)^2 + (x_9 + y_2^2 + y_3^2 + y_4^2 + y_5^2)^2 \right).
\end{aligned}$$

It follows that for any $a \in \mathbb{N}$ we have

$$a \in \mathcal{A} \iff \exists x_1 \cdots \exists x_9 \forall y_1 \cdots \forall y_{32} \exists y_{33} [y_{33} P_0(a, x_1, \ldots, x_9, y_1, \ldots, y_{32}) - 1 = 0]$$

As both $\mathcal{A}$ and $\mathbb{N} \setminus \mathcal{A}$ are nonrecursive, by the above we get that $\forall^9 \exists^{32}$ over $\mathbb{Q}$ and $\exists^9 \forall^{32} \exists$ over $\mathbb{Q}$ are undecidable.

(ii) Let $Q_{\mathcal{A}}$ be the polynomial in Lemma 4.2(ii). For any $a \in \mathbb{N}$, we have

$$\begin{aligned}
a \notin \mathcal{A} &\iff \forall x_1 \cdots \forall x_{10} [\neg(x_1, \ldots, x_{10} \in \mathbb{Z} \wedge x_{10} \neq 0) \vee Q_{\mathcal{A}}(a, x_1, \ldots, x_9) \neq 0] \\
&\iff \forall x_1 \cdots \forall x_{10} \left[\bigvee_{t=1}^{10} (x_t \notin \mathbb{Z}) \vee x_{10} = 0 \vee Q_{\mathcal{A}}(a, x_1, \ldots, x_{10}) \neq 0 \right].
\end{aligned}$$

By the proof of Theorem 1.1, $\mathbb{Q} \setminus \mathbb{Z}$ is 30-good. Thus, in view of Theorem 1.2, there are polynomials

$$f_s(x, y_1, \ldots, y_{31}) \text{ and } g_s(x, y_1, \ldots, y_{31}) \quad (s = 1, \ldots, k)$$

with integer coefficients such that for any $x \in \mathbb{Q}$ we have

$$x \notin \mathbb{Z} \iff \exists y_1 \cdots \exists y_{31}\Big[\bigvee_{s=1}^{k}(f_s(x,y_1,\ldots,y_{31})=0 \wedge g_s(x,y_1,\ldots,y_{31})\neq 0)\Big]$$

Thus, for any $a \in \mathbb{N}$, we have

$$\begin{aligned} a \notin \mathcal{A} \iff & \forall x_1 \cdots \forall x_{10} \exists y_1 \cdots \exists y_{31} \\ & \Big[\bigvee_{t=1}^{10}\Big(\bigvee_{s=1}^{k}(f_s(x_t,y_1,\ldots,y_{31})=0 \wedge g_s(x_t,y_1,\ldots,y_{31})\neq 0) \\ & \vee x_{10}=0 \vee Q_{\mathcal{A}}(a,x_1,\ldots,x_{10})\neq 0\Big)\Big] \end{aligned}$$

and hence

$$\begin{aligned} a \in \mathcal{A} \iff & \exists x_1 \cdots \exists x_{10} \forall y_1 \cdots \forall y_{31} \\ & \Big[\bigwedge_{t=1}^{10}\Big(\bigwedge_{s=1}^{k}(f_s(x_t,y_1,\ldots,y_{31})\neq 0 \vee g_s(x_t,y_1,\ldots,y_{31})=0) \\ & \wedge x_{10}\neq 0 \wedge Q_{\mathcal{A}}(a,x_1,\ldots,x_{10})=0\Big)\Big]. \end{aligned}$$

Let $\Gamma=\{1,\ldots,k\}\times\{1,\ldots,10\}$. By the distributive law concerning disjunction and conjunction,

$$\bigwedge_{t=1}^{10}\bigwedge_{s=1}^{k}(f_s(x_t,y_1,\ldots,y_{31})\neq 0 \vee g_s(x_t,y_1,\ldots,y_{31})=0)$$

is equivalent to

$$\bigvee_{\Delta\subseteq\Gamma}\Big(\bigwedge_{(s,t)\in\Delta}(f_s(x_t,y_1,\ldots,y_{31})\neq 0)\wedge\bigwedge_{(s',t')\in\Gamma\setminus\Delta}(g_{s'}(x_{t'},y_1,\ldots,y_{31})=0)\Big).$$

Thus, for any $a \in \mathbb{N}$, we have

$$\begin{aligned} a \in \mathcal{A} \iff & \exists x_1 \cdots \exists x_{10} \forall y_1 \cdots \forall y_{31} \\ & \Big[\bigvee_{\Delta\subseteq\Gamma}\Big(x_{10}\prod_{(s,t)\in\Delta} f_s(x_t,y_1,\ldots,y_{31})\neq 0 \\ & \wedge \bigwedge_{(s',t')\in\Gamma\setminus\Delta}(g_{s'}(x_{t'},y_1,\ldots,y_{31})=0)\wedge Q_{\mathcal{A}}(a,x_1,\ldots,x_{10})=0\Big)\Big] \\ \iff & \exists x_1 \cdots \exists x_{10} \forall y_1 \cdots \forall y_{31} \exists z \\ & \Big[\bigvee_{\Delta\subseteq\Gamma}\Big(1-zx_{10}\prod_{(s,t)\in\Delta} f_s(x_t,y_1,\ldots,y_{31})=0 \\ & \wedge \bigwedge_{(s',t')\in\Gamma\setminus\Delta}(g_{s'}(x_{t'},y_1,\ldots,y_{31})=0)\wedge Q_{\mathcal{A}}(a,x_1,\ldots,x_{10})=0\Big)\Big] \end{aligned}$$

and hence

$$a \in \mathcal{A} \iff \exists x_1 \cdots \exists x_{10} \forall y_1 \cdots \forall y_{31} \exists z [P_1(a, x_1, \ldots, x_{10}, y_1, \ldots, y_{31}, z) = 0],$$

where we view an empty product as 1, and $P_1(a, x_1, \ldots, x_{10}, y_1, \ldots, y_{31}, z)$ stands for the product of

$$\Big(1 - z x_{10} \prod_{(s,t)\in\Delta} f_s(x_t, y_1, \ldots, y_{31})\Big)^2 + \sum_{(s',t')\in\Gamma\setminus\Delta} g_{s'}(x_{t'}, y_1, \ldots, y_{31})^2 + Q_{\mathcal{A}}(a, x_1, \ldots, x_{10})^2$$

over $\Delta \subseteq \Gamma$. As $\mathcal{A}$ is nonrecursive, we obtain that $\exists^{10}\forall^{31}\exists$ over $\mathbb{Q}$ is undecidable.

In view of the above, we have completed the proof of Theorem 1.3. □

Acknowledgment. The authors would like to thank the referee for helpful comments.

References

[1] A. S. Besicovich, *On the linear independence of fractional powers of integers*, J. London Math. Soc. **15** (1940), 3–6.

[2] N. Cutland, Computability, Cambridge Univ. Press, Cambridge, 1980.

[3] N. Daans, *Universally defining finite generated subrings of global fields*, Doc. Math. **26** (2021), 1851–1869.

[4] N. Daans, P. Dittmann and A. Fehm, *Existential rank and essential dimension of Diophantine sets*, preprint, arXiv:2102.06941, 2021.

[5] M. Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly **80** (1973), 233–269.

[6] M. Davis, H. Putnam and J. Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. **74(2)** (1961), 425–436.

[7] B. Dubuque, Answer to Question 30687 at Mathematics Stack Exchange, 2011. `https://math.stackexchange.com/questions/30687`.

[8] D. Flath and S. Wagon, *How to pick out the integers in the rationals: an application of number theory to logic?* Amer. Math. Monthly **98** (1991), 812–823.

[9] J. Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Annals of Math. **183** (2016), 73–93.

[10] Yu. Matiyasevich, *Enumerable sets are diophantine*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282; English translation with addendum, Soviet Math. Doklady **11** (1970), 354–357.

[11] Yu. Matiyasevich and J. Robinson, *Reduction of an arbitrary diophantine equation to one in 13 unknowns*, Acta Arith. **27** (1975), 521–553.

[12] P. Morandi, Fields and Galois Theory, Grad. Texts Math., vol. 167, Springer, New York, 1996.

[13] M. B. Nathanson, Additive Number Theory: The Classical Bases, Grad. Texts in Math., vol. 164, Springer, New York, 1996.

[14] H. Pieper, *On Euler's contributions to the four-squares theorem*, Historia Math. **20** (1993), 12–18.

[15] B. Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131** (2009), 675–682.

[16] J. Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114.

[17] Z.-W. Sun, *Further results on Hilbert's Tenth Problem*, Sci. China Math. **64** (2021), 281–306.

[18] Z.-W. Sun, *Mixed quantifier prefixes over Diophantine equations with integer variables*, preprint, arXiv:2103.08302, 2021.

(Geng-Rui Zhang) School of Mathematics, Peking University, Beijing 100871, People's Republic of China

E-mail address: grzhang@stu.pku.edu.cn

(Zhi-Wei Sun, corresponding author) Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

E-mail address: zwsun@nju.edu.cn