arXiv:2002.12136v2 [math.NT] 30 Dec 2020

Accepted for publication in Proc. of the 2019 Asian Logic Conf. (World Sci.)

ON DIOPHANTINE EQUATIONS OVER $\mathbb{Z}[i]$ WITH 52 UNKNOWNS

YURI MATIYASEVICH AND ZHI-WEI SUN

Abstract. In this paper we show that there is no algorithm to decide whether an arbitrarily given polynomial equation $P(z_1,\ldots,z_{52}) = 0$ (with integer coefficients) over the Gaussian ring $\mathbb{Z}[i]$ is solvable.

1. Introduction

The original HTP (Hilbert's Tenth Problem) asks for an (effective) algorithm to test whether an arbitrary polynomial Diophantine equation with integer coefficients has solutions over the ring $\mathbb{Z}$ of the integers. This was finally solved by Yu. Matiyasevich [5] negatively in 1970 based on the work of M. Davis, H. Putnam and J. Robinson [2]. Z.-W. Sun [10] showed further that there is no algorithm to decide for any given $P(x_1,\ldots,x_{11}) \in \mathbb{Z}[x_1,\ldots,x_{11}]$ whether the equation $P(x_1,\ldots,x_{11}) = 0$ has integer solutions.

Let K be a number field which is a finite extension of the field $\mathbb{Q}$ of rational numbers. It is natural to ask whether HTP over the ring O_K of algebraic integers in K is unsolvable. Clearly, if $\mathbb{Z}$ is Diophantine over O_K then HTP over O_K is undecidable with the aid of Matiyasevich's theorem. It is known that $\mathbb{Z}$ is Diophantine over O_K if $[K:\mathbb{Q}] = 2$ or K is totally real (cf. J. Denef [3, 4]), or $[K:\mathbb{Q}] \geqslant 3$ and K has exactly two nonreal embeddings into the field of complex numbers (cf. T. Pheidas [7]), or K is an abelian number field (cf. H. N. Shapiro and A. Shlapentokh [8]).

In this paper we study Diophantine equations with few unknowns over the Gaussian ring

$$\mathbb{Z}[i] = O_{\mathbb{Q}(i)} = \{a+bi:\ a,b\in\mathbb{Z}\}.$$

2010 *Mathematics Subject Classification.* Primary 03D35, 11U05; Secondary 03D25, 11B39, 11D99, 11R11.

Key words and phrases. Hilber's Tenth Problem, Diophantine equation, Gaussian ring, undecidability.

The work is supported by the NSFC-RFBR Cooperation and Exchange Program (grants NSFC 11811530072 and RFBR 18-51-53020-GFEN-a). The second author is also supported by the Natural Science Foundation of China (grant no. 11971222).

Our main results are as follows.

Theorem 1.1. *A number $z \in \mathbb{Z}[i]$ is a rational integer if and only if there are $v, w, x, y \in \mathbb{Z}[i]$ with $v \neq 0$ such that*

$$\begin{aligned}&(4(2v(2(2z+1)^2+1)-y)^2-3y^2-1)^2\\&+2(w^2-1-3y^2(2z+1-xy)^2)^2=0.\end{aligned} \tag{1}$$

Theorem 1.2. *For any r.e. (recursively enumerable) set $\mathcal{A} \subseteq \mathbb{N} = \{0, 1, 2, \ldots\}$, there is a polynomial $P(z_0, z_1, \ldots, z_{52})$ with integer coefficients such that for any $a \in \mathbb{N}$ we have*

$$a \in \mathcal{A} \iff P(a, z_1, \ldots, z_{52}) = 0 \text{ for some } z_1, \ldots, z_{52} \in \mathbb{Z}[i]. \tag{2}$$

It is well known (cf. N. Cutland [1]) that there are nonrecursive r.e. subsets of $\mathbb{N}$. Thus Theorem 1.2 has the following corollary.

Corollary 1.1. *There is no algorithm to decide for any polynomial $P(z_1, \ldots, z_{52})$ with integer coefficients whether the equation*

$$P(z_1, \ldots, z_{52}) = 0$$

has solutions in $\mathbb{Z}[i]$.

We will provide some lemmas in the next section and then show Theorems 1.1-1.2 in Section 3.

2. Some Lemmas

For $A, B \in \mathbb{Z}$, the Lucas sequence $(u_n(A, B))_{n \geqslant 0}$ is given by $u_0(A, B) = 0$, $u_1(A, B) = 1$, and

$$u_{n+1}(A, B) = Au_n(A, B) - Bu_{n-1}(A, B) \quad (n = 1, 2, 3, \ldots).$$

Sun [9] studied arithmetic properties of such sequences as well as related Diophantine representations over $\mathbb{Z}$.

Lemma 2.1. *Let $A, B \in \mathbb{Z}$.*

(i) *For any $k, n, r \in \mathbb{N}$, we have the identity*

$$u_{kn+r}(A, B) = \sum_{j=0}^{n} \binom{n}{j} (u_{k+1}(A, B) - Au_k(A, B))^{n-j} u_k^j u_{j+r}.$$

(ii) *Let $A, B, M \in \mathbb{Z}$ with $M \neq 0$. Then B is relatively prime to M if and only if $u_n(A, B) \equiv 0 \pmod{M}$ and $u_{n+1}(A, B) \equiv 1 \pmod{M}$ for some $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.*

(iii) *If $A > B \geqslant 0$, then $(A - B)^n \leqslant u_{n+1}(A, B) \leqslant A^n$ for all $n \in \mathbb{N}$.*

Remark 2.1. Parts (i)-(iii) are Lemmas 2, 6, 8 of Sun [9].

Lemma 2.2. *Let $A \in \{2,3,\ldots\}$. Then*

$$x^2 - Axy + y^2 = 1 \text{ with } x, y \in \mathbb{N} \text{ and } x \geqslant y$$

if and only if

$$x = u_{n+1}(A,1) \text{ and } y = u_n(A,1) \text{ for some } n \in \mathbb{N}.$$

Remark 2.2. This is a known result, see, e.g., Sun [9, Lemma 9].

Lemma 2.3. *If $x, y \in \mathbb{Z}[i]$ and $x^2 - 4xy + y^2 = 1$, then $x, y \in \mathbb{Z}$.*

Remark 2.3. This follows from a more general result of Denef [3]; a proof for this particular case was also presented in Matiyasevich [6, Section 7.3].

Lemma 2.4. *For $x, y \in \mathbb{Z}[i]$, we have*

$$x = 0 \wedge y = 0 \iff x^2 + 2y^2 = 0.$$

Proof. Though the result is known, here we provide a simple proof.

Suppose that $x^2 + 2y^2 = 0$ but $x \neq 0$ or $y \neq 0$. Then $xy \neq 0$ and $x/y \in \{\sqrt{2}\,i, -\sqrt{2}\,i\}$. As $x/y \in \mathbb{Q}(i) = \{r + si : \ r, s \in \mathbb{Q}\}$, and $\sqrt{2}$ is irrational, we obtain a contradiction. This ends the proof. □

Lemma 2.5. *An integer m is nonzero if and only if $m = (2x+1)(3y+1)$ for some $x, y \in \mathbb{Z}$.*

Remark 2.4. This is a useful observation of S.-P. Tung [11].

3. Proofs of Theorems 1.1 and 1.2

Proof of Theorem 1.1. (i) We first show the "if" direction.

Suppose that there are $v, w, x, y \in \mathbb{Z}[i]$ with $v \neq 0$ satisfying (1). In view of Lemma 2.4, we have

$$4(2v(2(2z+1)^2+1) - y)^2 - 3y^2 - 1 = 0 \tag{3}$$

and

$$w^2 - 1 - 3y^2(2z+1-xy)^2 = 0. \tag{4}$$

Let $y_* = 4v(2(2z+1)^2+1)$ and $w_* = w + 2(2z+1-xy)y$. Then

$$y_*^2 - 4y_*y + y^2 = (y_* - 2y)^2 - 3y^2 = 1$$

and

$$\begin{aligned}&w_*^2 - 4w_*y(2z+1-xy) + y^2(2z+1-xy)^2\\ =&(w_* - 2y(2z+1-xy))^2 - 3y^2(2z+1-xy)^2\\ =&w^2 - 3y^2(2z+1-xy)^2 = 1.\end{aligned}$$

Applying Lemma 2.3, we see that $y, y_*, w_*, y(2z+1-xy) \in \mathbb{Z}$. Thus both $2z+1-xy$ and w are rational integers.

Note that

$$\frac{|y_*|}{4} \geqslant 2|2z+1|^2 - 1 = |2z+1|(2|2z+1|-1) + (|2z+1|-1) \geqslant |2z+1|$$

and

$$(y-2y_*)^2 = 3y_*^2 + 1 \leqslant 3y_*^2 + \frac{y_*^2}{16} = \left(\frac{7}{4}y_*\right)^2.$$

If $(y-2y_*)^2 = (\frac{7}{4}y_*)^2$, then we must have $|y_*|/4 = 1 = |2z+1|$, hence $z \in \{0,-1\}$ and $|y_*| = |12v| > 4$. Therefore

$$|y| > 2|y_*| - \frac{7}{4}|y_*| = \frac{|y_*|}{4} \geqslant |2z+1|.$$

Recall that $2z+1-xy \in \mathbb{Z}$, and write $x = a+bi$ with $a, b \in \mathbb{Z}$. Then

$$|y|^2 > |2z+1|^2 = |(2z+1-xy)+(a+bi)y|^2 = (2z+1-xy+ay)^2 + b^2y^2,$$

hence $b = 0$ and $x \in \mathbb{Z}$. Thus $2z+1 \in \mathbb{Z}$ and hence $z \in \mathbb{Z}$.

(ii) Below we show the "only if" direction. For $n \in \mathbb{N}$ we simply write u_n to denote $u_n(4,1)$.

Let $z \in \mathbb{Z}$ and $k = |2z+1|$. By Lemma 2.1(ii), for some $n \in \mathbb{N}$ we have $u_{n+1} \equiv 0 \pmod{4(2k^2+1)}$. In view of Lemma 2.1(iii), $u_{kn} \geqslant 3^{kn-1}$ and $u_{n+1} \geqslant 3^n$. Write $u_{n+1} = 4(2k^2+1)v$ with $v \in \mathbb{Z}^+$ and set $y = u_n$. Then

$$4(2v(2k^2+1)-y)^2 = (u_{n+1}-2u_n)^2 = 3u_n^2 + 1 = 3y^2 + 1$$

with the aid of Lemma 2.2. By Lemma 2.1(i),

$$u_{nk} \equiv k(u_{n+1}-4u_n)^{k-1}u_n \pmod{u_n^2}.$$

Let $q = u_{kn}/u_n \in \mathbb{Z}^+$. Then

$$q \equiv ku_{n+1}^{k-1} \equiv k \pmod{u_n}$$

since $k \equiv 1 \pmod 2$ and $u_{n+1}^2 = 1 - u_n^2 + 4u_nu_{n+1} \equiv 1 \pmod{u_n}$. Define $\varepsilon = 1$ if $z \geqslant 0$, and $\varepsilon = -1$ if $z < 0$. Then $\varepsilon u_{kn} = u_n(\varepsilon k + xu_n) = y(2z+1-xy)$ for some $x \in \mathbb{Z}$. Let $w_* = \varepsilon u_{kn+1}$ and $w = w_* - 2\varepsilon u_{kn}$. Then

$$w^2 - 3y^2(2z+1-xy)^2 = (u_{kn+1}-2u_{kn})^2 - 3u_{kn}^2 = 1$$

by Lemma 2.2. Now it is clear that (1) holds.

In view of the above, we have completed the proof of Theorem 1.1. □

Remark 3.1. In view of Lemma 2.5 and the proof of Theorem 1.1, a number $z \in \mathbb{Z}[i]$ is an rational integer if and only if there are $s, t, w, x, y \in \mathbb{Z}[i]$ such that (1) holds with $v = (2s+1)(3t+1)$.

Proof of Theorem 1.2. By Sun [10, Theorem 1.1(ii)], there is a polynomial $f(z_0, \ldots, z_{10}) \in \mathbb{Z}[z_0, \ldots, z_{10}]$ such that $a \in \mathbb{N}$ belongs to $\mathcal{A}$ if and only if $f(a, z_1, \ldots, z_{10}) = 0$ for some $z_1, \ldots, z_{10} \in \mathbb{Z}$ with $z_{10} \neq 0$.

Let $F(v, w, x, y, z)$ denote the left-hand side of (1). For $z_k \in \mathbb{Z}[i]$, by Theorem 1.1, $z_k \in \mathbb{Z}$ if and only if $F(v_k, w_k, x_k, y_k, z_k) = 0$ for some $v_k, w_k, x_k, y_k \in \mathbb{Z}[i]$ with $v_k \neq 0$. Thus, $a \in \mathcal{A}$ if and only if there are

$$v_k, w_k, x_k, y_k, z_k \in \mathbb{Z}[i] \ (k = 1, \ldots, 10)$$

with $F(v_k, w_k, x_k, y_k, z_k) = 0$ for all $k = 1, \ldots, 10$ such that $z_{10} \prod_{k=1}^{10} v_k \neq 0$. By the proof of Theorem 1.1, when $a \in \mathcal{A}$ we can actually choose $z_{10}, v_1, \ldots, v_{10} \in \mathbb{Z} \setminus \{0\}$ to meet the requirements. Therefore, in view of Lemma 2.5, $a \in \mathcal{A}$ if and only if there are

$$v_k, w_k, x_k, y_k, z_k \in \mathbb{Z}[i] \ (k = 1, \ldots, 10)$$

such that $F(v_k, w_k, x_k, y_k, z_k) = 0$ for all $k = 1, \ldots, 10$ and $z_{10} \prod_{k=1}^{10} v_k = (2s+1)(2t+1)$ for some $s, t \in \mathbb{Z}[i]$. Thus, in light of Lemma 2.4, (2) holds for some polynomial $P(z_0, z_1, \ldots, z_{52}) \in \mathbb{Z}[z_0, z_1, \ldots, z_{52}]$. This concludes the proof. □

References

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

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

[3] J. Denef, *Hilbert's Tenth Problem for quadratic rings*, Proc. Amer. Math. Soc. **48** (1975), 214–220.

[4] J. Denef, *Diophantine sets of algebraic integers, II*, Trans. Amer. Math. Soc. **257 (1980)**, 227–236, 1980.

[5] 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.

[6] Yu. Matiyasevich, Hilbert's Tenth Problem, MIT Press, Cambridge, Massachusetts, 1993.

[7] T. Pheidas, *Hilbert's Tenth Problem for a class of rings of algebraic integers*, Proc. Amer. Math. Soc. **104** (1988), 611–620.

[8] H. N. Shapiro and A. Shlapentokh, *Diophantine relationships between algebraic number fields*, Comm. Pure Appl. Math. **42** (1989), 1113–1122.

[9] Z.-W. Sun, *Reduction of unknowns in Diophantine representations*, Sci. China Ser. A **35** (1992), no. 3, 257–269.

[10] Z.-W. Sun, *Further results on Hilbert's tenth problem*, preprint, arXiv:1704.03504, 2017.

[11] S. P. Tung, *On weak number theories*, Japan. J. Math. (N.S.) **11** (1985), 203–232.

(Yuri Matiyasevich) St. Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences, Fontanka 27, 191023, St. Petersburg, Russia
Email address: yumat@pdmi.ras.ru

(Zhi-Wei Sun, corresponding author) Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China
Email address: zwsun@nju.edu.cn