#A25 INTEGERS 24 (2024)

FINDING SUMS OF FOUR SQUARES VIA COMPLEX CONTINUED FRACTIONS

Zhaonan Wang
Key Laboratory of Math. Mechanization, NCMIS, Academy of Math. and Systems Science, Chinese Academy of Sciences, Beijing, People's Republic of China
and
School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing, People's Republic of China
znwang@amss.ac.cn

Yingpu Deng
Key Laboratory of Math. Mechanization, NCMIS, Academy of Math. and Systems Science, Chinese Academy of Sciences, Beijing, People's Republic of China
and
School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing, People's Republic of China
dengyp@amss.ac.cn

Received: 11/2/22, Accepted: 2/16/24, Published: 3/15/24

Abstract

The problem of representing a given positive integer as a sum of four squares of integers has been widely studied for a long time. Given a positive odd integer n, one can find a representation of n by some computation in a maximal order of a quaternion algebra, once a pair of (positive) integers x, y that satisfy $x^2 + y^2 \equiv -1 \bmod n$ is given. In this paper, we introduce a new approach to finding a representation of an odd integer w, given x, y that meet the above requirement. This method can avoid the complicated non-commutative structure in the quaternion algebra, which is similar to the method used to obtain a representation of a prime $p \equiv 1 \bmod 4$ as a sum of two squares, employing continued fraction expansions. However, in this case, we use the Hurwitz algorithm for complex number expansions.

1. Introduction

In 1770 Lagrange proved in [4] that all positive integers can be written as a sum of four squares. In 1986, three randomized algorithms were presented by Rabin

DOI: 10.5281/zenodo.10821681

and Shallit[14], which were used to obtain a representation for any given (positive) integer n under the assumption of the Extended Riemann Hypothesis. Among all the methods, one used a maximal order called the *Hurwitz order*

$$\mathbf{H} = \left\{ \frac{h_1 + h_2 i + h_3 j + h_4 k}{2} \mid \textit{all } h_n \in \mathbb{Z},\ h_1 \equiv h_2 \equiv h_3 \equiv h_4 \bmod 2 \right\},$$

which is contained in the restriction of Hamiltonians from $\mathbb{R}$ to $\mathbb{Q}$, namely the quaternion algebra $\left(\frac{-1,-1}{\mathbb{Q}}\right)$, where i, j and k are the coordinates satisfying

$$i^2 = j^2 = k^2 = -1 \text{ and } ij = k, jk = i, ki = j.$$

By [12], once a solution to $x^2 + y^2 \equiv -1 \bmod n$ has been found, one can write n as a sum of four squares by computing the greatest common right divisor of $x + yi + j$ and n in $\mathbf{H}$, i.e., the greatest common divisor by computing on the right-hand side.

However, this method is less effective compared to the approach for solving the sum-of-two-squares problem, which aims to write certain positive integers as a sum of two square integers. The intricate structure of $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ will bring much trouble to the calculation in this algebra, primarily due to its non-commutative property. Therefore, in this paper, we present an algorithm designed to work in a commutative ring. Specifically, our method allows operation in the Gaussian integer ring $\mathbb{Z}[i]$, and avoids the need for cumbersome arithmetic in the Hurwitz order.

To help understand the basic idea of this paper, we illustrate firstly the method employed by Hermite in 1848 [7] to represent a given prime $p \equiv 1 \bmod 4$ as a sum of two squares (one can also see [1] for additional reference):

1. Find x_0 with $0 < x_0 < \frac{p}{2}$ such that $x_0^2 \equiv -1 \bmod p$.

2. Expand $\frac{x_0}{p}$ into a simple continued fraction expansion till the denominator of the convergents $\frac{P_n}{Q_n}$ satisfies $Q_n < \sqrt{p} < Q_{n+1}$. Then we have

$$p = (x_0 Q_n - pP_n)^2 + Q_n^2.$$

This method has inspired us to consider the sum-of-four-squares problem using continued fraction expansions. However, our focus lies in utilizing continued fraction expansions of complex numbers, instead of the classical continued fractions.

Hurwitz first introduced the concept of complex continued fractions in [8]. He developed an expanding algorithm that chooses the nearest Gaussian integers at each step, demonstrating properties akin to those in the classical scenario. Subsequently, in [6], Hensley further detailed properties of Hurwitz continued fraction expansions. These included aspects such as the growth of absolute values of denominator terms in approximations and the distribution of remainders. Although their focus centered on infinite expansions rather than the finite expansions of rational complex numbers, most of the theorems and properties they developed are still applicable in finite cases.

The paper is organized as follows. In Section 2, we present an overview of properties related to Hurwitz continued fractions. Additionally, we introduce definitions and theorems concerning lattices, which will be used in the proof of the main theorem. The theorem and its proof are illustrated in Section 3, followed by the presentation of an algorithm detailing the entire process. Finally, we provide an illustrative example demonstrating the representation of a large odd prime $p \equiv 3 \bmod 4$ as a sum of four squares in Section 4.

2. Preliminaries of Complex Continued Fractions and Lattices

First we present some basic facts about complex continued fractions and Hurwitz's algorithm about complex expansions. Some notation in this paper is adopted from [5], and the readers can also refer to Section 5.2 in [6] for more details.

Let $\mathfrak{G}$ denote the Gaussian integer ring $\mathbb{Z}[i]$, and $\{a_n\}$ be a sequence in $\mathfrak{G}$, which can be finite or infinite. Define the $\mathcal{Q}$-pair $\{P_n\}$ and $\{Q_n\}$ of sequences associated to $\{a_n\}$ recursively as

$$P_{-1} = 1,\ P_0 = a_0,\ P_{n+1} = a_{n+1}P_n + P_{n-1}\ (n \geq 0),$$

$$Q_{-1} = 0,\ Q_0 = 1,\ Q_{n+1} = a_{n+1}Q_n + Q_{n-1}\ (n \geq 0).$$

It is easy to verify that

$$P_nQ_{n-1} - Q_nP_{n-1} = (-1)^{n-1}$$

and

$$\frac{P_n}{Q_n} = a_0 + \frac{1}{a_1 + \frac{1}{\cdots + \frac{1}{a_n}}}$$

for all $n \geq 0$. $\frac{P_n}{Q_n}$ can be regarded as the n-th convergent defined by the sequence $\{a_n\}$. If the number of elements in $\{a_n\}$ is infinite and $\frac{P_n}{Q_n}$ converges when $n \to \infty$, we may say that the complex number $z := a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}$ has a continued fraction expansion $[a_0; a_1, a_2, \cdots]$ as in the classical continued fraction case.

However, establishing a continued fraction expansion for a given complex number z requires more definitions and notation. Since we do not focus on the details concerning the continued fraction expansion algorithm, we solely introduce the Hurwitz algorithm relevant to this paper.

We denote by $[z]$ the Gaussian integer nearest z, i.e., rounding both real and imaginary parts of z. The Hurwitz algorithm is more likely to be an improvement of the classical centered continued fraction algorithm for real numbers, which proceeds by defining the sequences recursively as

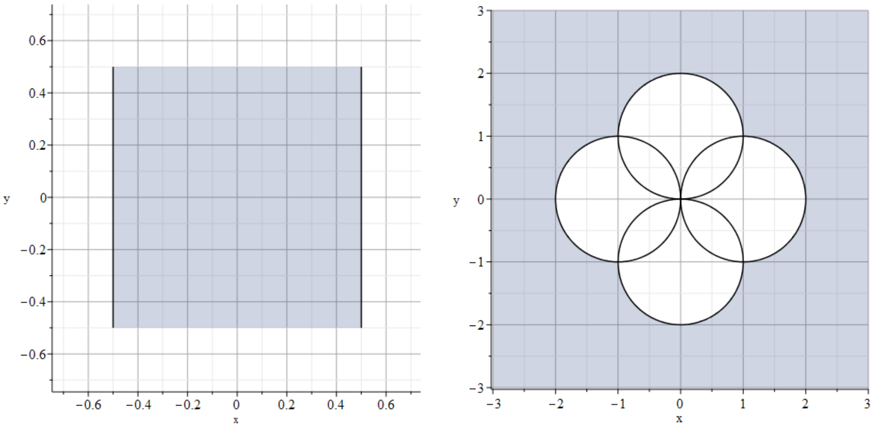
$$\begin{cases} z_0 = z, \\ a_n = [z_n], \\ z_{n+1} = (z_n - a_n)^{-1}. \end{cases}$$

We call $\{z_n\}$ the *iteration sequence* and $\{a_n\}$ the *partial quotients* of z. Again we can define the $\mathcal{Q}$-pair $\{P_n\}$ and $\{Q_n\}$ as above, and they still satisfy the recursive equations.

Since $z_n - a_n$ lies in $\Phi := \left\{x + yi \mid -\frac{1}{2} \leq x, y \leq \frac{1}{2}\right\}$, which can be inferred from the definition of a_n, we have

$$z_n \in \Phi^{-1} = \{x + yi \mid (|x| - 1)^2 + y^2 \geq 1,\ x^2 + (|y| - 1)^2 \geq 1\} \setminus \{(0, 0)\}$$

for $n \geq 1$. Consequently, $|\Re(z_n)| \geq 1$, $|\Im(z_n)| \geq 1$, and $a_n \in \mathfrak{G}\backslash\{0, \pm 1, \pm i\}$ for all $n \geq 1$. In Figure 1, one can find the regions of Φ and Φ^{-1}, highlighted in blue.



(a) Φ (b) Φ^{-1}

Figure 1: The region of Φ and Φ^{-1}

Proposition 1 ([5])**.** *Let $z \in \mathbb{C}$, and let $\{z_n\}$, $\{a_n\}$ be the iteration sequence and partial quotients of z under the Hurwitz algorithm, respectively. Let $\{P_n\}$ and $\{Q_n\}$ be the $\mathcal{Q}$-pair associated to $\{a_n\}$. Then we have $Q_n z - P_n = (-1)^n (z_1 \cdots z_{n+1})^{-1}$ for all legal n, and $z_{n+1} = -\frac{Q_{n-1}z - P_{n-1}}{Q_n z - P_n}$.*

In this context, the term “legal” signifies that $n \geq -1$ is an integer, and can be chosen arbitrarily if z allows for an infinite continued fraction expansion, or smaller than m if $z = [a_0; a_1, \cdots, a_m]$. One can see Proposition 3.3 in [5] for the proof.

Throughout this paper, our focus is on scenarios where $z \in \mathbb{Q}[i]$, indicating z as a rational complex number, thereby ensuring the termination of the algorithm. If the length of the expansion sequence of z is m, then by the m-th step, we achieve $z_m = 0$ and $\frac{P_m}{Q_m} = z$. It is noteworthy that, if $z \in \mathbb{Q}[i]$, and z possesses a Hurwitz expansion $[a_0; a_1, \cdots, a_m]$, then for any $n \geq 0$, we can derive a Hurwitz expansion of $z_n = [a_n; a_{n+1}, \cdots, a_m]$.

We now illustrate the definition and some fundamental properties of lattices, which will be used in the proof of the main theorem. For further elaboration, one can refer to the first chapter in [3].

Definition 1. Let $\{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_k}\}$ be k linearly independent vectors in $\mathbb{R}^n$. The set of all points $\mathcal{L} = \sum\limits_{i=1}^{k} x_i \mathbf{b_i}$ with integral $x_1, \cdots, x_k$ is called the *lattice* with *basis* $\{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_k}\}$, and the *rank* of the lattice $\mathcal{L}$ is k.

Sometimes we simply use the matrix $(\mathbf{b_1}, \cdots, \mathbf{b_k})$ to denote the lattice generated by vectors $\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_k}$. In this paper, we only consider full rank lattices, i.e., the case where $k = n$.

Definition 2. Given a full-rank lattice $\mathcal{L} = (\mathbf{b_1}, \cdots, \mathbf{b_n})$ in $\mathbb{R}^n$, the *determinant* of $\mathcal{L}$ is defined as

$$\det(\mathcal{L}) := |\mathbb{Z}^n/\mathcal{L}| = |\det(\mathbf{b_1}, \cdots, \mathbf{b_n})|,$$

and it can be verified that this determinant remains unchanged for any basis of $\mathcal{L}$.

Proposition 2 ([3])**.** *Given a full-rank lattice $\mathcal{L}$ in $\mathbb{R}^n$, any convex centrally symmetric body S of volume greater than $2^n|\det(\mathcal{L})|$ contains a nonzero lattice point in $\mathcal{L}$.*

The above proposition is the Minkowski's Theorem, a detailed introduction of which can be found in the third chapter of [3].

3. Representation of Sum of Four Squares

Let us now introduce the main theorem of this paper, which aims at representing an integer w as a sum of four squares. We may assume w is odd. To see this, consider an arbitrary $w' = 2^e w$ with w odd. Given $a^2 + b^2 + c^2 + d^2 = w$, we can derive a', b', c', d' satisfying $a'^2 + b'^2 + c'^2 + d'^2 = w'$ by calculating

$$(1+i)^e(a + bi + cj + dk) = a' + b'i + c'j + d'k$$

in the quaternion algebra.

Our finding serves as an alternative approach, replacing the previous method that necessitates computing the greatest common right divisor of w and $x + yi + j$ in

$\left(\frac{-1,-1}{\mathbb{Q}}\right)$. While our theorem applies to all odd positive integers that are not perfect squares, we only have deterministic polynomial algorithms for finding solutions x, y to $x^2 + y^2 \equiv -1 \bmod p$ for primes $p \equiv 3 \bmod 4$. For more information, refer to [15]. As for general w, Rabin and Shallit have described a randomized algorithm to find x, y in Theorem 3.1 of [14]. Moreover, Pollard and Schnorr [11] have given a more general algorithm for solving $x^2 + Dy^2 \equiv k \bmod w$, which runs quickly in random polynomial time under the assumption of the General Riemann Hypothesis.

We define $|z| := \sqrt{\Im^2(z) + \Re^2(z)} = \sqrt{z\bar{z}}$ to be the *norm* of z when $z \in \mathbb{C}$. For a vector $\mathbf{b} = (b_1, \cdots, b_n)$, $||\mathbf{b}|| := \sqrt{b_1^2 + \cdots + b_n^2}$ denotes the *length* of $\mathbf{b}$.

The main theorem is stated as follows.

Theorem 1. *Given an odd integer w (not a square) and integers x, y $(0 \leq x, y < \frac{w}{2})$ such that $x^2 + y^2 \equiv -1 \bmod w$, let $z := \frac{x+yi}{w}$, and z admits a finite Hurwitz continued fraction (HCF) expansion $[a_0, \cdots, a_m] = [0; a_1, \cdots, a_m]$ with $\mathcal{Q}$-pairs (P_k, Q_k). One can find a unique index $n < m$ such that $|Q_n| \leq \sqrt{w} < |Q_{n+1}|$. If $|Q_n| \neq \sqrt{w}$, then $w = |(x + yi) \cdot Q_n - w \cdot P_n)|^2 + |Q_n|^2$, which is a representation of w as a sum of four squares.*

Proof. We may assume that all Gaussian integers appearing in the context below do not have a norm of $\sqrt{w}$. Otherwise, the problem will be solved by finding a representation of w as a sum of two squares.

Before presenting the proof, we introduce two additional lemmas. Although their original discussion revolved around the infinite expansion case, they are applicable in the context of rational complex numbers, and the proofs remain valid.

Lemma 1 ([8])**.** *For any complex number z with HCF expansion $[a_0; a_1, ..., a_m, ...]$ and Q-pairs (P_k, Q_k), we have*

$$1 = |Q_0| < |Q_1| < \cdots < |Q_m|$$

for all legal m.

Lemma 2 ([10])**.** *For any complex number z with HCF expansion $[a_0; a_1, ..., a_m, ...]$ and any legal k, we have*

$$\left|z - \frac{P_k}{Q_k}\right| \leq \frac{1}{|Q_k|^2}.$$

From Lemma 1, we establish the existence of a unique n less than m such that $|Q_n| < \sqrt{w} < |Q_{n+1}|$. By considering

$$|((x+yi) \cdot Q_k - w \cdot P_k)|^2 + |Q_k|^2 = (x^2+y^2+1)|Q_k|^2 + w^2|P_k|^2 - 2w\Re(\bar{P_k} \cdot (x+yi)Q_k),$$

we observe that this expression is divisible by w for arbitrary k with the condition $w \mid x^2 + y^2 + 1$.

Let $S_k = (x+yi) \cdot Q_k - w \cdot P_k$ for all $-1 \leq k \leq m$. The overall proof idea is as follows. Firstly, we show that $|S_n|^2 + |Q_n|^2$ can only be either w or $2w$, with the specific selection of n as described in the theorem. Then we exclude the $2w$-case, thus substantiating the entire theorem.

If $|S_n| < \sqrt{w}$, then $|S_n|^2 + |Q_n|^2 = w$. This holds true since $|Q_n| < \sqrt{w}$, and hence $|S_n|^2 + |Q_n|^2 < 2w$, which must also be divisible by w. Therefore, we obtain a representation of w as a sum of four squares. From now on, we consider the case where $|S_n| > \sqrt{w}$.

From Proposition 1, we derive that

$$z_{k+1} = -\frac{Q_{k-1} \cdot \frac{x+yi}{w} - P_{k-1}}{Q_k \cdot \frac{x+yi}{w} - P_k} = -\frac{S_{k-1}}{S_k}$$

for all k. By the rules of the Hurwitz algorithm, we know $|z_{k+1}| \geq \sqrt{2}$, and consequently $|S_{k-1}| \geq \sqrt{2}\,|S_k|$.

For any given k, we have

$$S_kQ_{k+1} - S_{k+1}Q_k = ((x+yi)Q_k - wP_k)Q_{k+1} - ((x+yi)Q_{k+1} - wP_{k+1})Q_k = (-1)^k w.$$

Setting $k = n$, we deduce $S_nQ_{n+1} - S_{n+1}Q_n = (-1)^n w$.

Firstly, let us consider the case where n is even, then $S_nQ_{n+1} - S_{n+1}Q_n = w$. We list some facts that can be obtained from the previous content. From Lemma 2 we derive

$$|Q_nS_n| = |Q_n((x+yi) \cdot Q_n - w \cdot P_n)| = \left| w \cdot Q_n^2 \left(\frac{x+yi}{w} - \frac{P_n}{Q_n} \right) \right| \leq w,$$

and

$$|S_{n+1}| = \left| w \cdot Q_{n+1} \left(z - \frac{P_{n+1}}{Q_{n+1}} \right) \right| \leq \frac{w}{|Q_{n+1}|} < \sqrt{w}.$$

Recalling that $|Q_n| < \sqrt{w} < |Q_{n+1}|$, and $|S_n| > \sqrt{w}$, we conclude that

$$|Q_{n+1}S_n| > w > |Q_nS_{n+1}|.$$

Furthermore,

$$\left| \frac{Q_{n+1}S_n}{Q_nS_{n+1}} \right| = \left| \frac{S_n}{S_{n+1}} \right| \cdot \left| \frac{Q_{n+1}}{Q_n} \right| > \sqrt{2} \cdot 1 = \sqrt{2},$$

and

$$|Q_{n+1}S_n| \cdot |Q_nS_{n+1}| = |(Q_nS_n) \cdot (Q_{n+1}S_{n+1})| \leq w^2.$$

Assuming $Q_nS_{n+1} = r + ti$, we have $Q_{n+1}S_n = r + w + ti$. Following our previous analysis, we derive four inequalities:

$$\begin{cases} r^2 + t^2 < w^2, \\ (r+w)^2 + t^2 > w^2, \\ (r+w)^2 + t^2 > 2(r^2+t^2), \\ ((r+w)^2 + t^2) \cdot (r^2+t^2) \leq w^4. \end{cases}$$

We can use these relations to obtain further constraints for $Q_{n+1}S_n$. Let us consider the case $r<0$ and $r\geq 0$ separately to obtain the upper bounds for $|Q_{n+1}S_n|$.

When $r<0$, the first and the second inequalities indicate

$$(r+w)^2+t^2<2w^2+2wr\leq 2w^2,$$

hence $|Q_{n+1}S_n|^2<2w^2$. When $r\geq 0$, the second inequality naturally holds, and the third one holds if the first does. Thus, we may assume $r=w\epsilon\cos\theta$, $t=w\epsilon\sin\theta$, where $\epsilon\in(0,1)$ from the first inequality and $\theta\in\left[-\frac{\pi}{2},\frac{\pi}{2}\right]$ considering the assumption that $r\geq 0$. Now, we have

$$|Q_{n+1}S_n|^2=(r+w)^2+t^2=w^2\epsilon^2+w^2+2w^2\epsilon\cos\theta,$$

and the last inequality suggests $\epsilon^2(\epsilon^2+1+2\epsilon\cos\theta)\leq 1$.

Recall that our goal is to derive the upper bound of $|Q_{n+1}S_n|$, equivalently, the upper bound of $w^2\epsilon^2+w^2+2w^2\epsilon\cos\theta$. The last inequality implies

$$\cos\theta\leq\frac{1}{2\epsilon}\left(\frac{1}{\epsilon^2}-\epsilon^2-1\right).$$

On one hand, $\cos\theta\geq 0$, hence

$$\frac{1}{2\epsilon}\left(\frac{1}{\epsilon^2}-\epsilon^2-1\right)\geq 0,$$

yielding $\epsilon^2\leq\frac{\sqrt{5}-1}{2}$, i.e., $0\leq\epsilon\leq\sqrt{\frac{\sqrt{5}-1}{2}}$. On the other hand, $\cos\theta\leq 1$ implies that, if we require

$$\frac{1}{2\epsilon}\left(\frac{1}{\epsilon^2}-\epsilon^2-1\right)\geq 1,$$

then $\cos\theta\leq\frac{1}{2\epsilon}\left(\frac{1}{\epsilon^2}-\epsilon^2-1\right)$ would always hold. Notably, when

$$\frac{1}{2\epsilon}\left(\frac{1}{\epsilon^2}-\epsilon^2-1\right)\geq 0,$$

the value decreases when ϵ increases, hence $\epsilon=\frac{\sqrt{5}-1}{2}$ is the unique root of

$$\frac{1}{2\epsilon}\left(\frac{1}{\epsilon^2}-\epsilon^2-1\right)=1.$$

Therefore, when $\epsilon\leq\frac{\sqrt{5}-1}{2}$, $\cos\theta$ can be chosen arbitrarily.

Next, let us determine the upper bounds separately for $0<\epsilon\leq\frac{\sqrt{5}-1}{2}$ and $\frac{\sqrt{5}-1}{2}<\epsilon\leq\sqrt{\frac{\sqrt{5}-1}{2}}$ when $r\geq 0$. For $0<\epsilon\leq\frac{\sqrt{5}-1}{2}$, $\cos\theta$ can assume any value between $(0,1)$. To maximize $w^2\epsilon^2 + w^2 + 2w^2\epsilon\cos\theta$, we choose $\cos\theta = 1$ and $\epsilon = \frac{\sqrt{5}-1}{2}$. Consequently,

$$\max\left\{w^2\epsilon^2 + w^2 + 2w^2\epsilon\cos\theta \mid 0 < \epsilon \le \frac{\sqrt{5}-1}{2}\right\} = (\frac{\sqrt{5}+1}{2})^2 w^2.$$

For $\frac{\sqrt{5}-1}{2} < \epsilon \le \sqrt{\frac{\sqrt{5}-1}{2}}$, we recall the inequality $\epsilon^2(\epsilon^2+1+2\epsilon\cos\theta) \le 1$. Therefore,

$$\begin{aligned}&\max\left\{w^2\epsilon^2 + w^2 + 2w^2\epsilon\cos\theta \mid \frac{\sqrt{5}-1}{2} < \epsilon \le \sqrt{\frac{\sqrt{5}-1}{2}}\right\}\\ &\le \max\left\{\frac{1}{\epsilon^2}w^2 \mid \frac{\sqrt{5}-1}{2} < \epsilon \le \sqrt{\frac{\sqrt{5}-1}{2}}\right\} = \left(\frac{\sqrt{5}+1}{2}\right)^2 w^2.\end{aligned}$$

Hence we always have $|Q_{n+1}S_n| \le \frac{\sqrt{5}+1}{2}w$ when n is even.

As for the case where n is odd, the equation $S_nQ_{n+1} - S_{n+1}Q_n = -w$ holds. The previous analysis in the even n scenario remains valid. Assuming that

$$Q_nS_{n+1} = r + ti, Q_{n+1}S_n = r - w + ti,$$

we obtain another four inequalities:

$$\begin{cases} r^2 + t^2 < w^2, \\ (r-w)^2 + t^2 > w^2, \\ (r-w)^2 + t^2 > 2(r^2+t^2), \\ ((r-w)^2+t^2)\cdot(r^2+t^2) \le w^4. \end{cases}$$

By separately analyzing cases where $r > 0$ and $r \le 0$, we find that the upper bounds for $|Q_{n+1}S_n|^2$ are identical to those in the even n scenario.

Therefore, $|Q_{n+1}S_n| \le \frac{\sqrt{5}+1}{2}w$ holds in all cases. Given $|Q_{n+1}| > \sqrt{w}$, we find that

$$|S_n| < \frac{\sqrt{5}+1}{2}\sqrt{w}, \quad |S_n|^2 + |Q_n|^2 < \frac{3+\sqrt{5}+1}{2}w < 4w,$$

consequently allowing for only $2w$ or $3w$.

The assertion that $|S_n|^2 + |Q_n|^2 = 3w$ is impossible can be demonstrated as follows. From Lemma 2, we deduce

$$\left|\frac{w}{Q_n}\right|^2 + |Q_n|^2 \ge |S_n|^2 + |Q_n|^2 \ge 3w.$$

Therefore, $|Q_n|^2 \le \frac{3-\sqrt{5}}{2}w$, implying $|S_n|^2 \ge \frac{3+\sqrt{5}}{2}w$ (i.e., $|S_n| \ge \frac{\sqrt{5}+1}{2}\sqrt{w}$) for the equation $|S_n|^2 + |Q_n|^2 = 3w$ to hold, which contradicts the condition $|S_n| < \frac{\sqrt{5}+1}{2}\sqrt{w}$ derived in the preceding paragraph.

Finally, we conclude that $|S_n|^2 + |Q_n|^2$ can only equal $2w$ when $|S_n| > \sqrt{w}$, thus having

$$|S_{n+1}| \leq \frac{|S_n|}{\sqrt{2}} < \frac{\sqrt{2w}}{\sqrt{2}} = \sqrt{w}.$$

Employing the concept of lattices, we shall demonstrate the impossibility of this scenario. Notice that the two pairs (S_n, Q_{n+1}), (S_{n+1}, Q_n) exhibit some form of symmetry, given their shared relative magnitudes. Therefore, for the same reason as discussed above, we also have the equation $|S_{n+1}|^2 + |Q_{n+1}|^2 = 2w$ under the assumption that $|S_n| > \sqrt{w}$. Next we prove that these two equations for $|S_n|$, $|Q_n|$, $|S_{n+1}|$ and $|Q_{n+1}|$ cannot hold simultaneously.

Let us begin by considering a full-rank lattice $\mathcal{L} = (\mathbf{b_1}, \mathbf{b_2}, \mathbf{b_3}, \mathbf{b_4})$ in $\mathbb{R}^4$:

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -w & y & -x \\ -w & 0 & x & y \end{pmatrix}.$$

By straightforward computation, we have $\det(\mathcal{L}) = w^2$. For any $\mathbf{b} \in \mathcal{L}$, write $\mathbf{b} = \sum_{i=1}^{4} \mu_i \mathbf{b_i}$; then

$$||\mathbf{b}||^2 = (-w\mu_1 + x\mu_3 + y\mu_4)^2 + (-w\mu_2 + y\mu_3 - x\mu_4)^2 + \mu_3^2 + \mu_4^2.$$

Thus $||\mathbf{b}||^2 \equiv (x^2 + y^2 + 1)(\mu_3^2 + \mu_4^2) \equiv 0 \bmod w$, i.e., $w \mid ||\mathbf{b}||^2$ for any $\mathbf{b} \in \mathcal{L}$.

Consider the ball centered at the origin in $\mathbb{R}^4$ with a radius of $\sqrt{2w - \epsilon}$ for some small $\epsilon > 0$, denoted by $B(\sqrt{2w - \epsilon})$. When ϵ is sufficiently small,

$$\mathrm{Vol}(B(\sqrt{2w - \epsilon})) = \frac{\pi^2}{2}(2w - \epsilon)^2 > 2^4 w^2 = 2^4 \det(\mathcal{L}),$$

hence by Proposition 2, $B(\sqrt{2w - \epsilon})$ must contain a nonzero point $\mathbf{u}$ in $\mathcal{L}$. Write $\mathbf{u} = \sum_{i=1}^{4} x_i \mathbf{b_i}$. It follows that

$$w \mid ||u||^2 = (-x_1 w + x_3 x + x_4 y)^2 + (-x_2 w + x_3 y - x_4 x)^2 + x_3^2 + x_4^2 < 2w,$$

which implies that

$$(-x_1 w + x_3 x + x_4 y)^2 + (-x_2 w + x_3 y - x_4 x)^2 + x_3^2 + x_4^2 = w.$$

Alternatively speaking, we have discovered two Gaussian integers $x_1 + x_2 i$ and $x_3 - x_4 i$ satisfying

$$|x_3 - x_4 i|^2 + |(x_1 + x_2 i)w - (x_3 - x_4 i)(x + yi)|^2 = w. \tag{1}$$

On the other hand, if we take $(x_1+x_2i)w-(x_3-x_4i)(x+yi)=x_3'-x_4'i$, by direct calculation we have

$$(x_3+x_4i)-(x_3'+x_4'i)(x+yi)=(x^2+y^2+1)(x_3+x_4i)+(x_1-x_2i)(x+yi)w,$$

which is divisible by w. Therefore, there also exists a Gaussian integer $x_1'+x_2'i$ such that

$$|x_3'+x_4'i|^2+|(x_3'+x_4'i)(x+yi)-(x_1'+x_2'i)w|^2=w, \tag{2}$$

where

$$x_3'+x_4'i=\overline{((x_1+x_2i)w-(x_3-x_4i)(x+yi))},$$

and

$$(x_3'+x_4'i)(x+yi)-(x_1'+x_2'i)w=x_3+x_4i.$$

Here, we denote $\overline{a+bi}=a-bi$ for any $a+bi\in\mathbb{C}$. In other words, Equation (1) and Equation (2) essentially represent the same equation, just interpreted in two different ways.

We may assume that $|x_3+x_4i|^2>\frac{w}{2}>|x_3'+x_4'i|^2$, i.e.,

$$w>|x_3+x_4i|^2>\frac{w}{2}>|(x_1+x_2i)w-(x_3-x_4i)(x+yi)|^2.$$

Here we still omit the case where some Gaussian integers have norm $\sqrt{w}$, since finding such an element allows us to represent w as a sum of two squares, thus solving the problem.

Now we introduce another lemma and its related concept, which was originally proved by Lakein.

Definition 3 ([9])**.** Let $z\in\mathbb{C}$ be a complex number. A rational complex $\frac{p}{q}$ $(p,q\in\mathbb{Z}[i])$ is a *good approximation* to z if for any $p',q'\in\mathbb{Z}[i]$ with $|q'|\le|q|$, $|q'z-p'|\le|qz-p|$.

Lemma 3 ([9])**.** *If $z\in\mathbb{C}$ admits a HCF expansion, then any HCF convergent $\frac{P_k}{Q_k}$ of z is a good approximation to z.*

Apart from [9], one can refer to [13] for the proofs of all three lemmas mentioned in the proof of this theorem.

Consider the index k_1 where $|Q_{k_1}|<|x_3+x_4i|\le|Q_{k_1+1}|$. Note that such k_1 must exist due to the specific properties of the sequence. This is evident because $|Q_{-1}|=0$, $|Q_m|=w$, and $|Q_k|$ increases monotonically with increasing index k.

Recall our current conditions of $|Q_n|<\sqrt{w}<|Q_{n+1}|$ and $|S_n|>\sqrt{w}>|S_{n+1}|$. Since $|x_3+x_4i|\le|Q_{k_1+1}|$, let $q'=x_3+x_4i$ and $p'=x_1+x_2i$. By Lemma 3, we have

$$|S_{k_1+1}|\le|q'(x+yi)-p'w|,$$

i.e.,

$$|S_{k_1+1}| \leq |x_3' + x_4' i| < \sqrt{\frac{w}{2}}.$$

This allows us to conclude that $k_1 + 1 \geq n + 1$, based on our choice of n. Simultaneously, considering $|Q_{k_1}| < |x_3 + x_4 i| < \sqrt{w}$, we derive that $k_1 \leq n$. Combining these two results, we have $k_1 = n$.

Similarly we consider the index k_2 such that $|Q_{k_2}| < |x_3' + x_4' i| \leq |Q_{k_2+1}|$, and by the same discussion as above, we obtain $k_2 = n$. Recall that $|x_3' + x_4' i| < \sqrt{\frac{w}{2}}$, hence now we have

$$|Q_n| < \sqrt{\frac{w}{2}} < \sqrt{w} < |Q_{n+1}|, \quad |S_n| > \sqrt{w} > \sqrt{\frac{w}{2}} > |S_{n+1}|.$$

Given $|S_n|^2 + |Q_n|^2 = |S_{n+1}|^2 + |Q_{n+1}|^2 = 2w$, it follows that $|S_n|^2 > \frac{3w}{2}$, and $|Q_{n+1}|^2 > \frac{3w}{2}$. Therefore,

$$|S_n Q_{n+1}| > \frac{3w}{2}, \tag{3}$$

and

$$|S_{n+1} Q_n| < \frac{w}{2}. \tag{4}$$

However, we already have

$$S_n Q_{n+1} - S_{n+1} Q_n = (-1)^n w, \tag{5}$$

and the triangular inequality reveals that Inequality (3), Inequality (4) and Equation (5) cannot hold simultaneously. Therefore, the assumption $|S_n| > \sqrt{w}$ is not true, and we complete the proof of the theorem. □

4. Algorithms and Examples

Now we summarize the content in Section 3 as the Algorithm 1 to obtain a representation as a sum of four squares for odd w.

According to [15], for a prime $p = 4k + 1$ for some k, there already exist several algorithms running in polynomial time that find x, y such that $p = x^2 + y^2$. Hence, we mainly consider the odd w that is not a prime in the form $4k + 1$.

The following proposition can be easily observed.

Proposition 3. *For a given odd w, steps 2 to 5 in Algorithm 1 require $O(\log w)$ operations.*

It can be seen that Steps 2 to 5 in our algorithm are essentially the same as the method of calculating the greatest common right divisor of w and $x + yi$ in

Algorithm 1 Finding a representation of odd w as a sum of four squares

```
**Input**: An odd positive integer $w$ not a prime $p \equiv 1 \bmod 4$ or a perfect square;
**Output**: Four integers $a, b, c, d$ such that $a^2 + b^2 + c^2 + d^2 = w$;
1. If $w$ is an odd prime $p \equiv 3 \bmod 4$, use the method in [2] to obtain a pair of integers $0 < x, y < \frac{w}{2}$ such that $x^2 + y^2 \equiv -1 \bmod w$ in polynomial time. Otherwise, use the method in [14] and derive $0 \leq x, y < \frac{w}{2}$ such that $x^2 + y^2 \equiv -1 \bmod w$ in random polynomial time.
2. Compute the Hurwitz expansion $\{a_k\}$ of $\frac{x+yi}{w}$ and $Q_k$ until $|Q_{k+1}|^2 - w \geq 0$;
3. If $|Q_{k+1}|^2 = w$, take $a = \Re(Q_{k+1})$, $b = \Im(Q_{k+1})$, $c = d = 0$;
4. If $|Q_{k+1}|^2 > w$, take $a = \Re(Q_k)$, $b = \Im(Q_k)$, $c = \Re(S_k)$, $d = \Im(S_k)$;
5. Return $a, b, c, d$.
```

the Hurwitz order after finding satisfying x, y. Hence they share the same time complexity.

We take $w = 98787853334822666555522223331179$ as an example, which is a prime in the form of $4k + 3$. One can check that

$$(x, y) = (32929284444940888851840744443726, 2902967144089498477004731971911)$$

is a pair of solution to the congruence equation $x^2 + y^2 \equiv -1 \bmod w$. Expanding $\frac{x+yi}{w}$ under the Hurwitz algorithm, we have the results as shown in Table 1.

n	a_n	P_n	Q_n
-1		1	0
0	0	0	1
1	2 - i	1	2 - i
2	-1 + i	-1 + i	3i
3	-2i	3 + 2i	8 - i
...	...	...	...
36	3 + i	393331037760940 - 446167971615681i	-1338503914847043i
37	-2i	-805083291726049 - 974048629634780i	-2808580912939087 - 446167971615681i
38	2i	2341428297030500 - 2056334555067779i	892335943231362 - 6955665740725217i

Table 1: The expansion of $\frac{x+yi}{w}$

By calculation we have $|Q_{37}| < \sqrt{w} < |Q_{38}|$, hence

$$w = |Q_{37}(x + yi) - P_{37}w|^2 + |Q_{37}|^2,$$

and we obtain a representation of 98787853334822666555522223331179 as sum of squares

$$1338503914847043^2 + 2808580912939087^2 + 446167971615681^2.$$

Here we actually obtain a representation of w as a sum of three squares, due to the fact that $Q_{37}(x+yi)-P_{37}w$ is a pure imaginary number. From the Gauss-Legendre's three-square theorem, we know that the positive integers n can be written as a sum of three integer squares if and only if n is not in the form of $4^k(8m+7)$ for any non-negative integers k, m. Therefore, the w we choose does admit a three-square representation, and luckily we have obtained one. If we choose another pair of solutions x, y, we may obtain a four-square representation as usual. For example, if $(x, y) = (24696963333705666638880558327\!90, 38682456944339879707851152433\!0)$, then we can represent w as

$$807068241548931^2+2301810491935532^2+1089926588442075^2+1655643282228363^2.$$

Acknowledgement. This work was supported by National Key R&D Program of China (No.2020YFA0712300) and National Natural Science Foundation of China (No.12271517).

References

[1] J. Brillhart, Note on representing a prime as a sum of two squares, *Math. Comp.* **26** (1972), no. 120, 1011-1013.

[2] R. T. Bumby, Sums of four squares, in *Number Theory: New York Seminar 1991-1995*, Springer, New York, 1996.

[3] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer Science & Business Media, Berlin, 2012.

[4] J. L. de Lagrange, Démonstration d'un théorème d'arithmétique, *Nouv. Mém. Acad. Berlin.* **3** (1770), 189-201.

[5] S. Dani and A. Nogueira, Continued fractions for complex numbers and values of binary quadratic forms, *Trans. Amer. Math. Soc.* **366** (2014), no. 7, 3553-3583.

[6] D. Hensley, *Continued Fractions*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2006.

[7] C. Hermite, Note au sujet de l'article précédent, *J. Math. Pures Appl.* **13** (1848), 15.

[8] A. Hurwitz, Über die entwicklung complexer grössen in kettenbrüche, *Acta Math.* **11** (1900), 187-200.

[9] R. B. Lakein, Approximation properties of some complex continued fractions, *Monatsh. Math.* **77** (1973), 396-403.

[10] R. B. Lakein, A continued fraction proof of Ford's theorem on complex rational approximations, *J. Reine Angew. Math.* **272** (1975), 1-13.

[11] J. Pollard and C. Schnorr, An efficient solution of the congruence $x^2 + ky^2 \equiv m \bmod n$, *IEEE Trans. Inform. Theory* **33** (1987), no. 5, 702-709.

[12] P. Pollack and E. Treviño, Finding the four squares in Lagrange's theorem, *Integers* **18A** (2018), #A15.

[13] G. G. Robert, *Complex Continued Fractions: Theoretical Aspects of Hurwitz's Algorithm*, Ph.D. thesis, Aarhus University, 2018.

[14] M. O. Rabin and J. O. Shallit, Randomized algorithms in number theory, *Comm. Pure Appl. Math.* **39** (1986), no. S, suppl., S239-S256.

[15] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* **44** (1985), 483-494.