#A3 INTEGERS 15 (2015)

# CONTINUANTS AND SOME DECOMPOSITIONS INTO SQUARES

**Charles Delorme**
cd@lri.fr

**Guillermo Pineda-Villavicencio**
*Centre for Informatics and Applied Optimisation, Federation University Australia*
work@guillermo.com.au

*Received: 2/24/14, Revised: 11/13/14, Accepted: 12/24/14, Published: 1/19/15*

**Abstract**

In 1855, H. J. S. Smith proved Fermat's two-square theorem using the notion of palindromic continuants. In his paper, Smith constructed a proper representation of a prime number $p$ as a sum of two squares, given a solution of $z^2+1 \equiv 0 \pmod{p}$, and vice versa. In this paper, we extend the use of continuants to proper representations by sums of two squares in rings of polynomials over fields of characteristic different from 2. New deterministic algorithms for finding the corresponding proper representations are presented.

Our approach will provide a new constructive proof of the four-square theorem and new proofs for other representations of integers by quaternary quadratic forms.

## 1. Introduction

Fermat's two-square theorem has always captivated the mathematical community. Equally captivating are the known proofs of this theorem; see, for instance, [53, 21, 39, 8, 5, 4]. Among these proofs we were delighted by Smith's elementary approach [8], which is well within the reach of undergraduates. We remark that Smith's proof is very similar to Hermite's [21], Serret's [39], and Brillhart's [5].

Two main ingredients of Smith's proof are the notion of continuant (Definition 2 for arbitrary rings) and the famous Euclidean algorithm.

Let us recall here, for convenience, a definition taken from [25, Section 2.15].

**Definition 1.** *Euclidean rings* are rings $R$ with no zero divisors which are endowed with a Euclidean function N from $R$ to the nonnegative integers such that for all $\tau_1, \tau_2 \in R$ with $\tau_1 \neq 0$, there exist $q, r \in R$ such that $\tau_2 = q\tau_1 + r$ and $\mathrm{N}(r) < \mathrm{N}(\tau_1)$.

Among well-known examples, we are going to use the integers with $\mathrm{N}(u) = |u|$, and polynomials over a field with $\mathrm{N}(P) = 2^{\mathrm{degree}(P)}$ and $\mathrm{N}(0) = 0$.

**Definition 2** (Continuants in arbitrary rings, [17, Section 6.7])**.** Let $Q$ be a sequence of elements $(q_1, q_2, \ldots, q_n)$ of a ring $R$. We associate with $Q$ an element $[Q]$ of $R$ via the following recurrence formula

$$[\,] = 1, [q_1] = q_1, [q_1, q_2] = q_1q_2 + 1, \text{ and}$$
$$[q_1, q_2, \ldots, q_n] = [q_1, \ldots, q_{n-1}]q_n + [q_1, \ldots, q_{n-2}] \text{ if } n \geq 3.$$

The value $[Q]$ is called the *continuant* of the sequence $Q$.

A sequence $(q_1, q_2, \ldots, q_n)$ of quotients given by the Euclidean algorithm on $\tau_1$ and $\tau_2$, with $\tau_1$ and $\tau_2$ in $R$, is called a *continuant representation* of $(\tau_1, \tau_2)$ as we have the equalities $\tau_1 = [q_1, q_2, \ldots, q_n]h$ and $\tau_2 = [q_2, \ldots, q_n]h$, unless $\tau_2 = 0$. If $\tau_2 \neq 0$, then $h$ is a gcd of $(\tau_1, \tau_2)$, otherwise $h = \tau_1$; in other words $R\tau_1 + R\tau_2 = Rh$, where $R\tau$ denotes the left ideal generated by $\tau$.

Continuants have featured prominently in the literature. For commutative rings many continuant properties are given in [17, Section 6.7], while for non-commutative rings a detailed study is presented in [44]. For applications of continuants to representations of integers by quadratic forms, see [5, **?**, 46, 45, 20]. In all these papers, continuants have featured as numerators (and denominators) of continued fractions. For instance, the continuant $[q_1, q_2, q_3]$ equals the numerator of the continued fraction $q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}$, while the continuant $[q_2, q_3]$ equals its denominator.

Let $p$ be a prime number of the form $4k + 1$. Smith's approach [8] relies on the existence of a palindromic sequence $Q = (q_1, \ldots, q_s, q_s, \ldots, q_1)$ of even length such that $p = [Q]$. He then derives a solution $z_0$ for $z^2 + 1 \equiv 0 \pmod p$ with $2 \leq z_0 \leq p/2$, namely $[q_2, \ldots, q_s, q_s, \ldots, q_1]$. On the other hand, from $z_0$ one can retrieve the palindromic sequence by applying the Euclidean algorithm to $p$ and $z_0$, and then $p = x^2 + y^2$ where $x = [q_1, \ldots, q_s]$ and $y = [q_1, \ldots, q_{s-1}]$.

With regards to the question of finding square roots modulo a prime $p$, a deterministic algorithm can be found in [38]. The paper [43] also discusses the topic.

Brillhart's optimisation [5] of Smith's construction took full advantage of the palindromic structure of the sequence

$$(q_1, \ldots, q_{s-1}, q_s, q_s, q_{s-1}, \ldots, q_1)$$

given by the Euclidean algorithm on $p$ and $z_0$, a solution of $z^2 + 1 \equiv 0 \pmod p$. He noted that the Euclidean algorithm gives the remainders

$$\begin{aligned} r_i &= [q_{i+2}, \ldots, q_{s-1}, q_s, q_s, q_{s-1}, \ldots, q_1] \; (i = 1, \ldots, s-2), \\ r_i &= [q_{2s-1-i}, \ldots, q_1] \; (i = s-1, \ldots, 2s-2), \\ r_{2s-1} &= [\,], \text{and} \\ r_{2s} &= 0. \end{aligned}$$

So, in virtue of Smith's construction, rather than computing the whole sequence we only need to obtain

$$\begin{cases} x &= r_{s-1} = [q_s, q_{s-1}, \ldots, q_1] \\ y &= r_s = [q_{s-1}, \ldots, q_1]. \end{cases}$$

In this case, we have $y < x < \sqrt{p}$, Brillhart's stopping criterion.

### 1.1. Previous Extensions of Fermat's Two-Square Theorem to Other Rings

The question of extending Fermat's two-square theorem to other rings has been extensively considered in the literature; see, for instance, [35, 23, 16, 15, 7, 27, 33, 19].

Quadratic fields have naturally received a lot of attention. Niven [35] considered imaginary quadratic fields and studied the problem of expressing an integer $a + 2b\sqrt{-h}$ as a sum of two squares of integers in the field. Alternative proofs for the case of Gaussian integers (i.e., $h = 1$) appeared in [28, 34, 52]. The number of representations of non-zero Gaussian integers as sums of two Gausssian integers was obtained by Pall [36], and later by Williams [48, 50]. Elia [15] proved that a totally positive integer $m$ in $\mathbb{Q}(\frac{1+\sqrt{5}}{2})$ is a sum of two squares if and only if in the prime decomposition of $m$ each of its prime factors of field norm congruent to $11, 19$ modulo 20 occurs with an even exponent. Recall that an integer in a quadratic field is called *totally positive* if it and its conjugate are positive. Later, Elia and Monico [16] obtained a similar result for totally positive integers in $\mathbb{Q}(\sqrt{2})$. Deutsch [12] also considered the field $\mathbb{Q}(\frac{1+\sqrt{5}}{2})$ and proved that a prime with $-1$ as a quadratic residue has a representation, up to multiplication by a unit, as a sum of two squares of integers in $\mathbb{Q}(\frac{1+\sqrt{5}}{2})$.

Many results in this area rely on theorems about binary quadratic forms. For instance, Niven's proof of the aforementioned result depends heavily on a theorem by Mordell [33]. In [33] Mordell gave necessary and sufficient conditions for a positive binary quadratic form $ax^2+2hxy+by^2$ with integral coefficients to be representable as a sum of the squares of two linear forms $a_1x + b_1y$ and $a_2x + b_2y$ with integral coefficients. The number of representations of $ax^2+2hxy+by^2$ in the aforementioned manner was given in [36, 51]. Mordell's result was subsequently extended by Hardy [19] to forms with Gaussian integer coefficients. See also [29, 49, 30].

Polynomial rings have also attracted a lot of attention. Hsia [23] studied the representation of cyclotomic polynomials as the sum of two squares in $K[X]$, where $K$ is an algebraic field. Leahey [27] proved a theorem in the same vein as Fermat's two-square theorem for polynomials in $\mathbb{F}[X]$, where $\mathbb{F}$ is a finite field of characteristic different from 2 and $-1$ is a non-square in $\mathbb{F}$. Leahey's theorem reads as follows:

**Theorem 3** ([27])**.** *Let $m \in \mathbb{F}[X]$ be a monic polynomial, then any associate of $m$ is a sum of two squares if and only if in the prime decomposition of $m$ each of its* *prime factors of odd degree occurs with an even exponent.*

Perhaps one of the most important extensions of Fermat's two-square theorem was given by Choi, Lam, Reznick and Rosenberg [7]. In [7] Choi et al. proved the following theorem.

**Theorem 4** ([7])**.** *Let $R$ be an integral domain, $\mathbb{F}_R$ its field of fractions, $-h$ a non-square in $\mathbb{F}_R$ and $R[\sqrt{-h}]$ the smallest ring containing $R$ and $\sqrt{-h}$.*

*If both $R$ and $R[\sqrt{-h}]$ are unique factorisation domains, then the following assertions hold.*

1. *Any element $m \in R$ representable by the form $x'^2 + hy'^2$ with $x', y' \in \mathbb{F}_R$ is also representable by the form $x^2 + hy^2$ with $x, y \in R$.*

2. *Any element $m \in R$ representable by the form $x^2 + hy^2$ can be factored into $p_1^2 \cdots p_k^2 q_1 \cdots q_l$, where $p_i, q_j$ are irreducible elements in $R$ and $q_j$ is representable as $x^2 + hy^2$ for all $j$.*

3. *Some associate of a non-null prime element $p \in R$ is representable as $x^2+hy^2$ if and only if $-h$ is a square in $\mathbb{F}_{R/Rp}$, where $\mathbb{F}_{R/Rp}$ denotes the field of fractions of the quotient ring $R/Rp$.*

### 1.2. Our Work

In this paper we study *proper* representations $x^2 + y^2$ (that is, with $x$ and $y$ coprime) in some Euclidean rings via continuants. Specifically, we concentrate on the following problems. In the following, a unit in the ring is denoted by $u$.

**Problem 5** (From $x^2 + y^2$ to $z^2 + 1$)**.** If $m = u(x^2 + y^2)$ and $x, y$ are coprime, can we find $z$ such that $z^2 + 1$ is a multiple of $m$ using continuants?

**Problem 6** (From $z^2 + 1$ to $x^2 + y^2$)**.** If $m$ divides $z^2 + 1$, can we find $x, y$ such that $m = u(x^2 + y^2)$ using continuants?

As far as we know, this paper presents for the first time the application of continuants to representations in Euclidean rings other than the integers. Specifically, we present the following new deterministic algorithms for the form $Q(x, y) = x^2 + y^2$.

1. Algorithm 1: for every $m$ in a commutative Euclidean ring, the algorithm finds a solution $z_0$ of $Q(z, 1) \equiv 0 \pmod{m}$, given a representation $uQ(x, y)$ of $m$.

2. Algorithm 2: for every polynomial $m \in \mathbb{F}[X]$, where $\mathbb{F}$ is a field of odd characteristic, the algorithm finds a proper representation $uQ(x, y)$ of $m$, given a solution $z_0$ of $Q(z, 1) \equiv 0 \pmod{m}$.

As an application of continuants, we provide a new constructive proof of the four-square theorem (Section 4). Many proofs of this theorem can be found in the literature; see, for instance, [18, Sections 20.5, 20.9 and 20.12] and [22, 40, 3, 41, 1].

Furthermore, we use continuants to prove a number of other results about quaternary forms which represent all integers (Section 5).

From the outset we emphasise that Smith's approach depends heavily on the existence of a Euclidean-like division algorithm and that, if one tries to extend it to other Euclidean rings $R$, the uniqueness of the continuant representation may be lost. The uniqueness of the continuant representation boils down to the uniqueness of the quotients and the remainders in the division algorithm. This uniqueness is achieved only when $R$ is a field or $R = \mathbb{F}[X]$, the polynomial algebra over a field $\mathbb{F}$ (considering the degree as the Euclidean function) [26]. Note that in $\mathbb{Z}$ the uniqueness is guaranteed by requiring the remainder to be nonnegative.

The rest of the paper is structured as follows. In Section 2 we study properties of continuants in arbitrary rings. Section 3 is devoted to studying proper representations $x^2 + y^2$ in some Euclidean rings. We examine later some representations $x\overline{x} + y\overline{y}$ using rings with an anti-automorphism $x \mapsto \overline{x}$ (Sections 4 and 5).

## 2. Continuants

In this section we derive some properties of continuants from Definition 2, which we will refer to as continuant properties. Many of these properties are already known (see [17, Section 6.7] and [44]).

P–1 The first property is the so-called "Euler's rule" [10, Chapter IV]: Given a sequence $Q$, compute all the products of subsequences of $Q$ obtained by removing disjoint pairs of consecutive elements of $Q$. Then the continuant $[Q]$ is given by the sum of all such products. The empty product is 1, as usual.

**Example 7.** Consider $Q = (q_1, q_2, q_3, q_4, q_5)$. Then the products of relevant subsequences are: $q_1q_2q_3q_4q_5$, $q_3q_4q_5$, $q_1q_4q_5$, $q_1q_2q_5$, $q_1q_2q_3$, $q_5$, $q_3$, and $q_1$. Thus, the continuant is

$$\begin{aligned}[Q] =& q_1q_2q_3q_4q_5 + q_3q_4q_5 + q_1q_4q_5 + q_1q_2q_5 + q_1q_2q_3 + \\ &+ q_5 + q_3 + q_1.\end{aligned}$$

P–2 If in a ring $R$ we find a unit $\tau$ commuting with every $q_i$, then

$$[\tau^{-1}q_1, \tau q_2, \ldots, \tau^{(-1)^k}q_k, \ldots, \tau^{(-1)^n}q_n] = \begin{cases} [q_1, \ldots, q_n] & \text{if } n \text{ even} \\ \tau^{-1}[q_1, \ldots, q_n] & \text{if } n \text{ odd.} \end{cases}$$

P–3 $[q_1,\dots,q_n] = [q_1,\dots,q_{i-1}][q_{i+2},\dots,q_n] + [q_1,\dots,q_i][q_{i+1},\dots,q_n]$. To obtain this equality, it suffices to divide the products of subsequences of $Q = (q_1,q_2,\dots,q_n)$ obtained by removing disjoint pairs of consecutive elements of $Q$ into two groups, depending on whether the pair $q_iq_{i+1}$ $(1 \le i < n)$ has been removed or not.

P–4 From the previous points it follows that

$$[-q_h,-q_{h-1},\dots,-q_1,0,q_1,q_2,\dots,q_n] = \begin{cases} [q_{h+2},q_{h+3},\dots,q_n] & \text{for } 0 \le h \le n-2 \\ 1 & \text{if } h = n-1 \\ 0 & \text{if } h = n. \end{cases}$$

P–5 $[q_1,\dots,q_n]$ and $[q_1,\dots,q_{n-1}]$ are coprime.

From Properties P–2 and P–4 we can derive more identities, for instance, the following.

P–6 $[-q_{n-1},\dots,-q_1,0][q_1,\dots,q_n] + [-q_{n-1},\dots,-q_1][q_2,\dots,q_n] = 1$.

P–7 Property P–6 is equivalent to

$$[-q_{n-1},\dots,-q_2][q_1,\dots,q_n] + [-q_{n-1},\dots,-q_1][q_2,\dots,q_n] = 1,$$

which is in turn equivalent to

$$[q_{n-1},\dots,q_2][q_1,\dots,q_n] - [q_{n-1},\dots,q_1][q_2,\dots,q_n] = (-1)^n.$$

This last property first appeared in Theorem 3 of [44], where other variants were also presented.

If the ring $R$ is commutative, then we have some additional properties:

P–8 $[q_1,q_2,\dots,q_n] = [q_n,\dots,q_2,q_1]$.

P–9 The continuant $[q_1,\dots,q_n]$ is the determinant of the tridiagonal $n \times n$ matrix $A = (a_{ij})$ with $a_{i,i} = q_i$ for $1 \le i \le n$, $a_{i,i+1} = 1$ and $a_{i+1,i} = -1$ for $1 \le i < n$.

The following identity, due to Charles Lutwidge Dodgson (alias Lewis Carroll), plays an important role in our study of continuants.

**Lemma 8** (Lewis Carroll's identity, [14])**.** *Let $C$ be an $n\times n$ matrix in a commutative ring. Let $C_{i_1,\dots,i_s;j_1,\dots,j_s}$ denote the matrix obtained from $C$ by omitting the rows $i_1,\dots,i_s$ and the columns $j_1,\dots,j_s$. Then*

$$\det(C)\det(C_{i,j;i,j}) = \det(C_{i;i})\det(C_{j;j}) - \det(C_{i;j})\det(C_{j;i})$$

*where the determinant of the $0\times 0$ matrix is 1 for convenience.*

The use of Lewis Carroll's identity and Property P–9 provides more properties:

P–10 $[q_1, q_2, \ldots, q_n][q_2, \ldots, q_{n-1}] = [q_1, \ldots, q_{n-1}][q_2, \ldots, q_n] + (-1)^n$ (when $n \geq 2$).

P–11 In the case of even $n$ with $q_i = q_{n+1-i}$ for $1 \leq i \leq n$ (i.e., if the sequence is *palindromic*), we have

$$[q_1, \ldots, q_{n/2}, q_{n/2}, \ldots, q_2]^2 + 1 =$$
$$[q_1, \ldots, q_{n/2}, q_{n/2}, \ldots, q_1][q_2, \ldots, q_{n/2}, q_{n/2}, \ldots, q_2] =$$
$$([q_1, \ldots, q_{n/2}]^2 + [q_1, \ldots, q_{n/2-1}]^2)([q_2, \ldots, q_{n/2}]^2 + [q_2, \ldots, q_{n/2-1}]^2).$$

Note that Property P-10 also follows from Properties P–7 and P–8. More properties and proof techniques for the commutative case are given in [17, Section 6.7].

### 2.1. Quasi-Palindromic Sequences

Here again the rings are not necessarily commutative.

**Definition 9.** An *anti-automorphism* of a ring $R$ is an involution $\tau \mapsto \overline{\tau}$ such that $\overline{\tau + \sigma} = \overline{\tau} + \overline{\sigma}$ and $\overline{\tau\sigma} = \overline{\sigma}\,\overline{\tau}$ for all elements $\tau$, $\sigma$ of $R$.

**Definition 10.** Let $R$ be a ring endowed with an anti-automorphism $\tau \mapsto \overline{\tau}$. A *quasi-palindromic* sequence of length $n$ satisfies $q_i = \overline{q_{n+1-i}}$ for $1 \leq i \leq n$; in particular, if $n$ is odd the element $q_{(n+1)/2}$ satisfies $q_{(n+1)/2} = \overline{q_{(n+1)/2}}$.

We have an obvious relation.

P–12 $[\overline{q_n}, \ldots, \overline{q_1}] = \overline{[q_1, \ldots q_n]}$,

and counterparts of Properties P–10 and P–11.

**Lemma 11** (Noncommutative Lewis Carroll-like identity)**.** *Let $\tau \mapsto \overline{\tau}$ be an anti-automorphism in a ring $R$, which also satisfies the conditions*

$$\begin{cases} \tau\overline{\tau} = \overline{\tau}\tau, \text{ and} \\ \text{if } \overline{\tau} = \tau \text{ then } \tau \text{ belongs to the center of } R. \end{cases} \qquad (1)$$

*Let $(q_1, \ldots q_n)$ be a quasi-palindromic sequence of length $n \geq 2$ in $R$. The following relation holds*

$$\begin{aligned}[q_1, \ldots, q_n][q_2, \ldots, q_{n-1}] &= [q_2, \ldots, q_n][q_1, \ldots, q_{n-1}] + (-1)^n \\ &= [q_1, \ldots, q_{n-1}][q_2, \ldots, q_n] + (-1)^n.\end{aligned}$$

*Proof.* We proceed by induction on $n$. Our basic cases are $n = 2, 3$. The result is clearly true for $n = 2$.

For $n = 3$, since $q_2$ is in the center of $R$ and $q_1$ commutes with $q_3$, from

$$\begin{aligned}[q_1, q_2][q_2, q_3] - 1 &= (q_1q_2 + 1)(q_2q_3 + 1) - 1\\ &= q_1q_2q_2q_3 + q_1q_2 + q_2q_3\\ &= q_1q_2q_2q_3 + q_1q_2 + q_2q_3,\end{aligned}$$

we obtain $q_1q_2q_2q_3 + q_1q_2 + q_2q_3 = [q_2, q_3][q_1, q_2] - 1 = [q_1, q_2, q_3]q_2$.

For larger $n$, write $E = [q_2, \dots, q_{n-1}]$ and $F = [q_3, \dots, q_{n-2}]$. We want to prove that $[q_1, \dots, q_n]E = [q_1, \dots, q_{n-1}][q_2, \dots, q_n] + (-1)^n$.

Observe that $E$ and $F$ belong to the center of $R$, and that the following results come from the definition of continuant and Property P–3.

On one hand, we have that

$$\begin{aligned}[q_1, \dots, q_{n-1}][q_2, \dots, q_n] &= (q_1E + [q_3, \dots, q_{n-1}])(Eq_n + [q_2, \dots, q_{n-2}])\\ &= q_1E^2q_n + q_1E[q_2, \dots, q_{n-2}] + [q_3, \dots, q_{n-1}]Eq_n\\ &\quad + [q_3, \dots, q_{n-1}][q_2, \dots, q_{n-2}].\end{aligned}$$

On the other hand, we have that

$$\begin{aligned}[q_1, q_2, \dots, q_{n-1}, q_n]E &= (q_1[q_2, \dots, q_{n-1}, q_n] + [q_3, \dots, q_n])E\\ &= (q_1(Eq_n + [q_2, \dots, q_{n-2}]) + [q_3, \dots, q_{n-1}]q_n + F)\,E\\ &= q_1Eq_nE + q_1[q_2, \dots, q_{n-2}]E + [q_3, \dots, q_{n-1}]q_nE\\ &\quad + FE.\end{aligned}$$

First note that $[q_2, \dots, q_n][q_1, \dots, q_{n-1}] = [q_1, \dots, q_{n-1}][q_2, \dots, q_n]$ because of the equality $[q_1, \dots, q_{n-1}] = \overline{[q_2, \dots, q_n]}$.

Since $E = \overline{E}$, $E$ commutes with the whole $R$ and we have

$$\begin{aligned}q_1E^2q_n &= q_1Eq_nE\\ q_1E[q_2, \dots, q_{n-2}] &= q_1[q_2, \dots, q_{n-2}]E, \text{ and}\\ [q_3, \dots, q_{n-1}]Eq_n &= [q_3, \dots, q_{n-1}]q_nE.\end{aligned}$$

It only remains to check that

$$\begin{aligned}EF &= [q_2, \dots, q_{n-2}][q_3, \dots, q_{n-1}] + (-1)^n\\ &= [q_3, \dots, q_{n-1}][q_2, \dots, q_{n-2}] + (-1)^n,\end{aligned}$$

but these equalities follow from the inductive hypothesis. □

**Remark 12.** For a quasi-palindromic sequence $Q$ of length $n \geq 3$, we have

$$\begin{aligned}[q_1, q_2, \dots, q_{n-1}] &= q_1[q_2, \dots, q_{n-1}] + [q_3, \dots, q_{n-1}]\\ &= q_1[q_2, \dots, q_{n-1}] + \overline{[q_2, \dots, q_{n-2}]}.\end{aligned}$$

## 3. Proper Representations in Euclidean Rings

As said before, if one tries to extend Smith's approach to other Euclidean rings $R$, the uniqueness of the continuant representation may be lost. Given two elements $m, z \in R$, the uniqueness of the continuant representation of $(m, z)$ is necessary to recover representations $m = x\overline{x} + y\overline{y}$ from a multiple $z\overline{z} + 1$ of $m$.

### 3.1. Euclidean Rings Not Necessarily Commutative

We first use continuants to obtain a multiple $z\overline{z} + 1$ of an element $m$ of the form $x\overline{x} + y\overline{y}$, with $x, y$ satisfying $Rx + Ry = R$ and $\tau \mapsto \overline{\tau}$ an anti-automorphism in the ring under consideration.

**Theorem 13.** *Let $R$ be a Euclidean ring, and let $\tau \mapsto \overline{\tau}$ be an anti-automorphism of $R$ satisfying the conditions (1) of Lemma 11. If $m \in R$ admits a* proper *representation $m = x\overline{x}+y\overline{y}$ (that is, with $Rx+Ry = R$), then the equation $z\overline{z}+1 \in Rm$ admits solutions.*

*Furthermore, one of these solutions is equal to $[\overline{q_s}, \dots, \overline{q_1}, q_1, \dots, q_{s-1}]$, where $(q_1, q_2, \dots, q_s)$ is a sequence provided by the Euclidean algorithm on $x$ and $y$.*

*Proof.* Let N denote the Euclidean function of $R$ and let $(x, y)$ (with $\mathrm{N}(x) \geq \mathrm{N}(y)$) be a proper representation of $m$.

If $y = 0$ then $x$ is a unit, so $m$ must be a unit and the ideal $Rm$ is the whole ring $R$. Otherwise, the Euclidean algorithm on $x$ and $y$ gives a unit $u$ and a sequence $(q_1, q_2, \dots, q_s)$ such that $x = [q_1, q_2, \dots, q_s]u$ and $y = [q_2, \dots, q_s]u$. Then

$$\begin{aligned}
x\overline{x} &= [q_1, \dots, q_s]u\overline{u}[\overline{q_s}, \dots, \overline{q_1}], \text{ using Property P–12}\\
x\overline{x} &= [\overline{q_s}, \dots, \overline{q_1}][q_1, \dots, q_s]u\overline{u}, \text{ since } u\overline{u} \text{ belongs to the center of } R\\
y\overline{y} &= [\overline{q_s}, \dots, \overline{q_2}][q_2, \dots, q_s]u\overline{u}\\
m &= x\overline{x} + y\overline{y} = [\overline{q_s}, \dots, \overline{q_1}, q_1, \dots, q_s]u\overline{u}, \text{ by Property P–3.}
\end{aligned}$$

Let $z = [\overline{q_s}, \dots, \overline{q_1}, q_1, \dots, q_{s-1}]$. Then applying Lemma 11 we obtain

$$\begin{aligned}
z\overline{z} + 1 = (u\overline{u})^{-1}m[\overline{q_{s-1}}, \dots, \overline{q_1}, q_1, \dots, q_{s-1}]&\\
= (u\overline{u})^{-1}[\overline{q_{s-1}}, \dots, \overline{q_1}, q_1, \dots, q_{s-1}]m&\\
\text{since } m \text{ is in the center of } R.&
\end{aligned}$$

That is, $z$ satisfies $z\overline{z} + 1 \in Rm$, which completes the proof of the theorem. □

### 3.2. Commutative Rings: From $x^2 + y^2$ to $z^2 + 1$

In this subsection we deal with the problem of going from a representation $x^2 + y^2$ of an associate of an element $m$ to a multiple $z^2 + 1$ of $m$. We begin with a very general remark, valid in every commutative ring.

**Corollary 14.** *In a commutative ring $R$, if $Rx + Ry = R$ then there exists some $z \in R$ such that $x^2 + y^2$ divides $z^2 + 1$. Furthermore, if $R$ is Euclidean, we can explicitly find $z$ and the quotient $(z^2 + 1)/(x^2 + y^2)$ with continuants.*

This relation can be interpreted using Lewis Carroll's identity. The determinant of the tridiagonal matrix $A$ associated with the palindromic sequence $(q_s, \ldots, q_1, q_1, \ldots, q_s)$ (see property P–9 of continuants) is $x^2 + y^2$ with $x = [q_1, \ldots, q_s]$ and $y = [q_2, \ldots, q_s]$ if $s \geq 1$.

Moreover, $(x^2 + y^2)([q_1, \ldots q_{s-1}]^2 + [q_2, \ldots q_{s-1}]^2) = z^2 + 1$, where $z$ is the determinant of the matrix formed by the first $2s - 1$ rows and columns of $A$ (see properties P–10 and P–8). These remarks can readily be converted into a deterministic algorithm (see Algorithm 1).

**Algorithm 1:** Deterministic algorithm for constructing a solution $z_0$ of $Q(z, 1) \equiv 0 \pmod{m}$, given a representation $uQ(x, y)$ of an element $m$.

```
input  : A commutative Euclidean ring $R$.
         An element $m \in R$.
         A proper representation $uQ(x, y)$ of $m$, where $Q(x, y) = x^2 + y^2$.
output: A solution $z_0$ of $Q(z, 1) \equiv 0 \pmod{m}$ with $\mathrm{N}(1) \leq \mathrm{N}(z_0)$.
/* Apply the Euclidean algorithm to $x$ and $y$ and obtain a sequence
   $(q_1, \ldots, q_s)$ of quotients.                                   */
$s \leftarrow 0$;
$m_0 \leftarrow m$;
$r_0 \leftarrow z$;
repeat
    $s \leftarrow s + 1$;
    $m_s \leftarrow r_{s-1}$;
    find $q_s, r_s \in R$ such that $m_{s-1} = q_s m_s + r_s$ with $\mathrm{N}(r_s) < \mathrm{N}(m_s)$;
until $r_s = 0$;
$z_0 \leftarrow [q_s, q_{s-1}, \ldots, q_1, q_1, q_2, \ldots, q_{s-1}]$;
return $z_0$
```

### 3.3. Commutative Rings: From $z^2 + 1$ to $x^2 + y^2$

Here we deal with the problem of going from a solution $z_0$ of $z^2 + 1 \equiv 0 \pmod{m}$ to a representation $x^2 + y^2$ of an associate of $m$.

A natural question which arises is: if $m$ divides $z^2 + 1$, do there exist $x, y$ such that $m = x^2 + y^2$? We now give examples showing that no simple answer is to be expected.

In general, we cannot construct a representation $x^2 + y^2$ of an element $m$ from a solution of $z^2 + 1 \equiv 0 \pmod{m}$. As an illustration, consider the Euclidean domain $\mathbb{F}_2[X]$ of polynomials over the field $\mathbb{F}_2$, where $z^2 + 1$ is a multiple of $m = z + 1$ for any polynomial $z$, square or not. Recall that in $\mathbb{F}_2[X]$ the squares, and therefore the sums of squares, are exactly the even polynomials (i.e., the coefficient of $X^t$ is null if $t$ is odd). Thus, the converse of Corollary 14 is false in $\mathbb{F}_2[X]$. Other examples are the ring $\mathbb{Z}[i]$ of Gaussian integers and its quotients by an even integer, since the squares and the sum of squares have an even imaginary part. Thus, no Gaussian integer with an odd imaginary part is a sum of squares, although it obviously divides $0 = i^2 + 1$; see [35].

However, there are cases where the answer is positive. Propositions 15-17 discuss some of these cases.

**Proposition 15.** *Let $R$ be a commutative ring. If 2 is invertible and $-1$ is a square, say $1 + k^2 = 0$, then $x = \left(\frac{x+1}{2}\right)^2 + \left(\frac{x-1}{2k}\right)^2$.*

Results similar to Proposition 15 have appeared previously in the literature. For instance, one such result can be found in [27] in the context of finite fields.

**Proposition 16.** *Let $R = \mathbb{F}[X]$ be the ring of polynomials over a field $\mathbb{F}$ with characteristic different from 2 and let $-1$ be a non-square in $\mathbb{F}$.*

*If $m$ divides $z^2 + t^2$ with $z, t$ coprime, then $m$ is an associate of some $x^2 + y^2$ with $x, y$ coprime.*

*Proof.* We introduce the extension $\mathbb{G}$ of $\mathbb{F}$ by a square root $\omega$ of $-1$. The ring $\mathbb{G}[X]$ is principal and $z^2 + t^2$ factorises as $(z - \omega t)(z + \omega t)$. The two factors are coprime, since their sum and difference are respectively $2z$ and $2\omega t$, and 2 and $\omega$ are units. Introduce $\gcd(m, z+\omega t) = x+\omega y$, then $x-\omega y$ is a gcd of $m$ and $z-\omega t$ owing to the natural automorphism of $\mathbb{G}$. The polynomials $x - \omega y$ and $x + \omega y$ are coprime and both divide $m$. Thus, $m$ is divisible by $(x - \omega y)(x + \omega y) = x^2 + y^2$. On the other hand, $m$ divides $(z - \omega t)(z + \omega t)$. Consequently, $(x - \omega y)(x + \omega y)$ is an associate of $m$. Since $x - \omega y$ and $x + \omega y$ are coprime, we have $x$, $y$ are coprime. □

On one hand, Corollary 14 and Proposition 16 somehow generalise the main theorem of [27]. On the other hand, in the case of $m$ being prime, Proposition 16 is embedded in Theorem 2.5 of [7].

**Proposition 17.** *Let $m$ be a non-unit of $\mathbb{F}[X]$ and a divisor of $z^2 + 1$ for some $z \in \mathbb{F}[X]$ with $\deg(z) < \deg(m)$.*

*If $\mathbb{F}$ is a field of characteristic different from 2, where $-1$ is a non-square, then continuants provide a method for representing $m$ as a sum of squares.*

*Specifically, the Euclidean algorithm on $m$ and $z$ gives the unit $u$ and the sequence $(uq_s, u^{-1}q_{s-1}, \ldots, u^{(-1)^{s-1}}q_1, u^{(-1)^s}q_1, \ldots, u^{-1}q_s)$ such that $x = [q_1, \ldots, q_s]$ and $y = [q_2, \ldots, q_s]$.*

*Proof.* Having a divisor $m$ of $z^2 + 1$, we already know from Proposition 16 that the degree of $m$ is even. We may assume that degree$(z) <$ degree$(m)$ as we may divide $z$ by $m$.

From Proposition 16 we also know that, for this given $z$, $m/u = x^2 + y^2$ for some coprime $x, y$. Consequently, the Euclidean algorithm on these $x$ and $y$ will give the unit 1 and the sequence $(q_1, \dots, q_s)$ such that $x = [q_1, \dots q_s]$, $y = [q_2, \dots, q_s]$ and $m/u = [q_s, \dots, q_1, q_1, \dots, q_s]$. Theorem 13 tells that, given these $x$ and $y$, the element $z$ has the form $[q_s, \dots, q_1, q_1, \dots, q_{s-1}]$, which, by Property P8, is equivalent to $[q_{s-1}, \dots, q_1, q_1, \dots, q_s]$. Note that the uniqueness of the continuant representation of $(x, y)$ has implicitly been invoked.

We may also assume degree$(x) >$ degree$(y)$; otherwise, if $x = \lambda y + t$ with $\lambda$ a unit and $t$ a polynomial of degree smaller than the degree of $x$ and $y$, then $m = \left(((1+\lambda^2)y + \lambda t)^2 + t^2\right) \frac{u}{1+\lambda^2}$. As a result, we consider only the case where each $q_i$ has degree at least 1 in the continuant representation of $(x, y)$.

We then apply the Euclidean algorithm to $m$ and $z$, and obtain, by virtue of the uniqueness of the division in polynomials, a sequence whose last non-null remainder is $u$. Consequently, $m/u = x^2 + y^2$ (see Property P–2 of continuants). □

We illustrate this proposition through some examples. First take $m = 2X^4 - 2X^3 + 3X^2 - 2X + 1$, then $m$ divides $(2X^3 + X)^2 + 1$. The Euclidean divisions give successively

$$\begin{aligned} 2X^4 - 2X^3 + 3X^2 - 2X + 1 =& (2X^3 + X)(X - 1) + 2X^2 - X + 1 \\ 2X^3 + X =& (2X^2 - X + 1)(X + 1/2) + (X/2 - 1/2) \\ 2X^2 - X + 1 =& (X/2 - 1/2)(4X + 2) + 2 \\ X/2 - 1/2 =& 2(X/4 - 1/4). \end{aligned}$$

Here we have $m/2 = [2 \cdot (X-1)/2, 2^{-1} \cdot (2X+1), 2 \cdot (2X+1), 2^{-1} \cdot (X-1)/2]$ with $u = 2$, which gives $m/2 = (X^2 - X/2 + 1/2)^2 + (X/2 - 1/2)^2 = x^2 + y^2$. Since 2 is also a sum of two squares, we obtain $m = (x+y)^2 + (x-y)^2 = X^4 + (X^2 - X + 1)^2$.

We find other examples among the cyclotomic polynomials. The cyclotomic polynomial $\Phi_{4n} \in \mathbb{Q}[X]$ divides $X^{2n} + 1$. Thus, $\Phi_{4n}$ is, up to a constant, a sum of two squares; see, for instance, [37]. Since $\Phi_{4n}(0) = 1$, the constant can be chosen equal to 1. For an odd prime $p$, it is easy to check

$$\Phi_{4p}(X) = \sum_{k=0}^{p-1} (-1)^k X^{2k} = \left( \sum_{k=0}^{(p-1)/2} (-1)^k X^{2k} \right)^2 + \left( X \sum_{k=0}^{(p-3)/2} (-1)^k X^{2k} \right)^2 .$$

For the small composite odd number 15, the computation gives

$$\begin{aligned}
\Phi_{60}(X) &= X^{16} + X^{14} - X^{10} - X^8 - X^6 + X^2 + 1\\
&= [X, X, X^3 - X, -X, -X, X, X, -X, -X, X^3 - X, X, X]\\
X^{15} &= [X, X^3 - X, -X, -X, X, X, -X, -X, X^3 - X, X, X]\\
x &= [X, -X, -X, X^3 - X, X, X]\\
&= X^8 - X^4 + 1\\
y &= [-X, -X, X^3 - X, X, X]\\
&= X^7 + X^5 - X^3 - X\\
\Phi_{60}(X) &= x^2 + y^2.
\end{aligned}$$

At this stage the following remark is important.

**Remark 18.** If a polynomial with integer coefficients is the sum of squares of two polynomials with rational coefficients, it is also the sum of squares of two polynomials with integer coefficients.

For example, we see that $50X^2 + 14X + 1 = (5X + 3/5)^2 + (5X + 4/5)^2$, but it is also $X^2 + (7X + 1)^2$.

This remark follows from Theorem 2.5 of [7]. Other proofs can be found in [42] and [11].

**Remark 19** (Algorithmic considerations)**.** For the cases covered in Proposition 17, given an element $m$ and a solution $z_0$ of $z^2 + 1 \equiv 0 \pmod{m}$, we can recover a representation $x^2 + y^2$ of an associate of $m$ via continuants and Brillhart's [5] optimisation. We divide $m$ by $z_0$ and stop when we first encounter a remainder $r_{s-1}$ with degree at most $\deg(m)/2$. This will be the $(s-1)$-th remainder, and the quotients so far obtained are $(uq_s, u^{-1}q_{s-1}, \ldots, u^{-1^{(s-2)}}q_2)$. In this context,

$$x = \begin{cases} r_{s-1} & \text{for odd } s\\ u^{-1}r_{s-1} & \text{for even } s \end{cases}$$

and

$$y = \begin{cases} [uq_s, u^{-1}q_{s-1}, \ldots, u^{(-1)^{s-2}}q_2] & \text{for odd } s\\ u^{-1}[uq_s, u^{-1}q_{s-1}, \ldots, u^{(-1)^{s-2}}q_2] & \text{for even } s. \end{cases}$$

This observation follows from dividing $m/u = [q_s, \ldots, q_1, q_1, \ldots, q_s]$ by $z_0 = [q_{s-1}, \ldots, q_1, q_1, \ldots, q_s]$ using continuant properties.

Algorithm 2 implements Remark 19.

**Algorithm 2:** Deterministic algorithm for constructing a proper representation $uQ(x, y) = u(x^2 + y^2)$ of an element $m$

```
input  : A field $\mathbb{F}$ with characteristic different from 2.
         The ring $R = \mathbb{F}[X]$ of polynomials over $\mathbb{F}$.
         A polynomial $m$ with $\mathrm{N}(1) < \mathrm{N}(m)$.
         A solution $z_0$ of $Q(z, 1) \equiv 0 \pmod{m}$ with $\mathrm{N}(1) < \mathrm{N}(z_0) < \mathrm{N}(m_0)$.
output: A unit $u$ and a proper representation $uQ(x, y)$ of $m$.
/* Divide $m$ by $z$ using the Euclidean algorithm until we find a
   remainder $r_{s-1}$ with degree at most $\deg(m)/2$.                  */
$s \leftarrow 1$;
$m_0 \leftarrow m$;
$r_0 \leftarrow z$;
repeat
    $s \leftarrow s + 1$;
    $m_{s-1} \leftarrow r_{s-2}$;
    find $k_{s-1}, r_{s-1} \in R$ such that $m_{s-2} = k_{s-1}m_{s-1} + r_{s-1}$ with
    $\mathrm{N}(r_{s-1}) < \mathrm{N}(m_{s-1})$;
until $\deg(r_{s-1}) \leq \deg(m)/2$;
/* Here we have a sequence $(k_1, \ldots, k_{s-1})$ of quotients.        */
$x_{temp} \leftarrow r_{s-1}$;
$y_{temp} \leftarrow [k_1, \ldots, k_{s-1}]$;
/* We obtain a unit $u$.                                                 */
if $s$ is odd then
    Solve $m = u(x_{temp}^2 + y_{temp}^2)$ for $u$
end
else
    Solve $um = x_{temp}^2 + y_{temp}^2$ for $u$
end
/* We obtain $(x, y)$ so that $m = (x^2 + y^2)u$.                        */
if $s$ is odd then $x \leftarrow x_{temp}$else $x \leftarrow u^{-1}x_{temp}$;
if $s$ is odd then $y \leftarrow y_{temp}$else $y \leftarrow u^{-1}y_{temp}$;
return $(x, y, u)$
```

## 4. Four-Square Theorem

The four-square theorem has been proved in a number of ways. Hardy and Wright [18, Sections 20.5, 20.9 and 20.12] present three proofs: one based on the "method of descent," one based on quaternions, and one based on elliptic functions. We are aware of five other proofs [22, 40, 3, 41, 1]. The proofs in [22, 3, 1] are based on the triple-product identity, the paper [41] gives an arithmetic proof based on the number of representations of a positive number as the sum of two squares, and the proof in [40] is based on factorizations of $2 \times 2$ matrices over the ring $\mathbb{Z}[i]$ of

Gaussian integers.

In this section, we provide a new constructive proof of the four-square theorem. Our proof is based on continuants over $\mathbb{Z}[i]$.

We start by stating the following formula, which was already known to Euler; see [13, Chapter VIII].

**Lemma 20** (Product formula)**.** *Let $R$ be a commutative ring endowed with an anti-automorphism. Let $x, y, z, u$ be elements of $R$. Then*

$$(x\overline{x}+y\overline{y})(z\overline{z}+u\overline{u}) = (xz-y\overline{u})(\overline{xz-y\overline{u}}) + (xu+y\overline{z})(\overline{xu+y\overline{z}}).$$

*Proof.* This can be seen by looking at the determinants in the equality

$$\begin{bmatrix} x & y \\ -\overline{y} & \overline{x} \end{bmatrix} \begin{bmatrix} z & u \\ -\overline{u} & \overline{z} \end{bmatrix} = \begin{bmatrix} xz-y\overline{u} & xu+y\overline{z} \\ -\overline{xu+y\overline{z}} & \overline{xz-y\overline{u}} \end{bmatrix}.$$

□

We use Lemma 20 for the case of $R$ being the ring of Gaussian integers, with its conjugation. This product formula allows us to reduce the proof of the four-square theorem to the case of primes.

We recall that each prime $p$ is either of the form $z\overline{z}$ or divides $z\overline{z}+1$, for some $z \in \mathbb{Z}[i]$ [9, Section 4]. If $p = z\overline{z}$ then $p$ is trivially a sum of four squares. Assume the equation $z\overline{z}+1 \equiv 0 \pmod{p}$ admits a solution $z_0$ over $\mathbb{Z}[i]$. Given this solution $z_0$, we prove the four-square theorem by constructing a representation of $p$ as $x\overline{x}+y\overline{y}$, with $x, y \in \mathbb{Z}[i]$.

By reducing $z_0$ modulo $p$, we may assume $|z_0| \leq p/\sqrt{2}$, and thus $z_0\overline{z}_0 + 1 < p^2$ (if $p = 2$, a parity argument shows the inequality remains valid). Here $|z_0|$ denotes the *complex norm* of $z_0$.

Let $p_0 := p$. Then, we produce a succession of $s$ equalities $p_i p_{i+1} = z_i\overline{z_i} + 1$ and $z_i = q_{i+1}p_{i+1} + z_{i+1}$, where the sequence of positive integers $p = p_0, p_1, \ldots, p_s = 1$ is decreasing. At the end, we have $p_{s-1}p_s = z_{s-1}\overline{z_{s-1}} + 1$ and $q_s = z_{s-1}$.

We now build a continuant representation of $q$. The equation $p_{s-1}p_s = z_{s-1}\overline{z_{s-1}} + 1$ can be written as $p_{s-1} = [q_s, \overline{q_s}] = [\overline{q_s}, q_s]$, since $p_s = 1$, $z_{s-1} = q_s$, and $q_s$ and $\overline{q_s}$ commute; see Lemma 11. From the equation $z_{s-2} = q_{s-1}p_{s-1} + z_{s-1}$ and Remark 12, it follows that $z_{s-2} = [q_{s-1}, \overline{q_s}, q_s]$. The equation $p_{s-2}p_{s-1} = z_{s-2}\overline{z_{s-2}} + 1$ can therefore be written as

$$\begin{aligned} p_{s-2}[\overline{q_s}, q_s] =& [q_{s-1}, \overline{q_s}, q_s]\overline{[q_{s-1}, \overline{q_s}, q_s]} + 1 \\ p_{s-2}[\overline{q_s}, q_s] =& [q_{s-1}, \overline{q_s}, q_s][\overline{q_s}, q_s, \overline{q_{s-1}}] + 1 \qquad \text{(by Property P–12).} \end{aligned}$$

Hence, $p_{s-2} = [q_{s-1}, \overline{q_s}, q_s, \overline{q_{s-1}}]$ (by Lemma 11). Continuing this process, we obtain continuant representations for $p_{s-3}, \ldots, p_0$. The representation for $p_0 = p$ is the quasi-palindromic continuant $[q_1, \overline{q_2}, \ldots, q_2, \overline{q_1}]$, where the central pair is $q_s, \overline{q_s}$ if $s$

is odd and $\overline{q_s}, q_s$ if $s$ is even. Thus, we have a representation of $p = x\overline{x} + y\overline{y}$, with $x$ and $y$ being as follows:

$$x = \begin{cases} [q_1, \overline{q_2}, \ldots, \overline{q_{s-1}}, q_s] & \text{if } s \text{ is odd} \\ [q_1, \overline{q_2}, \ldots, q_{s-1}, \overline{q_s}] & \text{if } s \text{ is even} \end{cases}$$

$$y = \begin{cases} [q_1, \overline{q_2}, \ldots, \overline{q_{s-1}}] & \text{if } s \text{ is odd} \\ [q_1, \overline{q_2}, \ldots, q_{s-1}] & \text{if } s \text{ is even.} \end{cases}$$

This completes the proof of the four-square theorem.

Consider the following example, where $p_0 = 431$ and $z_0 = 54 + 10i$.

$$\begin{aligned} 431 \cdot 7 &= (54+10i)(54-10i)+1 & &\rightarrow & 54+10i &= (8+i)7 + (-2+3i) \\ 7 \cdot 2 &= (-2+3i)(-2-3i)+1 & &\rightarrow & -2+3i &= (-1+i)2 + i \\ 2 \cdot 1 &= (i)(-i)+1 & &\rightarrow & i &= i \cdot 1. \end{aligned}$$

Hence $(q_1, q_2, q_3) = (8+i, -1+i, i)$, $x = [8+i, -1-i, i]$ and $y = [8+i, -1-i]$. Thus,

$$\begin{aligned} 431 &= [8+i, -1-i, i, -i, -1+i, 8-i] \\ &= [8+i, -1-i, i]\overline{[8+i, -1-i, i]} + [8+i, -1-i]\overline{[8+i, -1-i]} \\ &= (17-5i)(17-5\overline{i}) + (-6-9i)(-6-9\overline{i}) \\ &= 17^2 + 5^2 + 6^2 + 9^2. \end{aligned}$$

**Remark 21** (Number of representations by the form $x^2+y^2+z^2+u^2$)**.** The number of representations of positive numbers by this form is given by Jacobi's theorem [47]. See also [18, Section 20.12] and [22, 1, 3, 41].

## 5. Some Quadratic Forms Representing Integers

Using the techniques of Section 4 we may construct other forms representing either all positive integers or all integers. Examples of forms representing all positive integers are $x^2 - xy + y^2 + z^2 - zu + u^2$ and $x^2 + 3y^2 + z^2 + 3u^2$, while the form $x^2 - 3y^2 + z^2 - 3u^2$ is an example of a form representing all integers. Some of these results have already appeared in the literature; see, for instance, [1], [2], [6] and [24].

**Proposition 22.** *Each positive integer has the form $x^2 - xy + y^2 + z^2 - zu + u^2$ with $x, y, z, u$ integers.*

*Proof.* Consider the ring $\mathbb{Z}[j]$ of Eisenstein integers, with $j = \exp(2i\pi/3)$, endowed with its natural anti-automorphism. We note that $v^2 - vw + w^2$ is the norm of

$v + wj$. As in Section 4, Lemma 20 for the case $R = \mathbb{Z}[j]$ reduces the task to primes. Again, as in Section 4, every prime $p$ is either of the form $z\overline{z}$ or divides some $z\overline{z} + 1$, with $z \in \mathbb{Z}[j]$. See [9, Section 4].

Assume the equation $z\overline{z} + 1 \equiv 0 \pmod{p}$ admits a solution $z_0$ over $\mathbb{Z}[i]$. Then, reasoning as in Section 4, the division process provides a deterministic algorithm to find a representation $p = x\overline{x} + y\overline{y}$. Here again we reduce $z_0$ modulo $p$ and assume $z_0\overline{z}_0 \leq 3p^2/4$. Thus, we only have to be careful if $p_{s-1} = 2$ to avoid the trap $2 \cdot 2 = (1 - j)(1 - \overline{j}) + 1$, where $p_{s-1} = p_s = 2$. This problem is avoided by choosing a convenient quotient $q_{s-1}$. □

Next we exhibit an example with the aforementioned trap, that is, where the sequence $p_0, \ldots, p_s$ is not decreasing. Take $p_0 = 47$ and $z_0 = 11 + 7j$, then $94 = 47 \cdot 2 = (11 + 7j)(11 + 7\overline{j}) + 1$. Here we have $p_1 = 2$. The equation $11 + 7j = q_1 p_1 + z_1$ with the quotient $q_1 = 5 + 4j$ would produce $z_1 = 1 - j$ and $p_2 = 2$, that is, $2 \cdot 2 = (1 - j)(1 - \overline{j}) + 1$. However, with the quotient $q_1 = 5 + 3j$, we get $z_1 = 1 + j$ and $p_2 = 1$, that is, $2 \cdot 1 = (1 + j)(1 + \overline{j}) + 1$ and $q_2 = 1 + j$. Hence, $(q_1, q_2) = (5 + 3j, 1 + j)$ and

$$\begin{aligned} 47 &= [5 + 3j, 1 + \overline{j}, 1 + j, 5 + 3\overline{j}] \\ &= [5 + 3j, 1 + \overline{j}]\overline{[5 + 3j, 1 + \overline{j}]} + [5 + 3j]\overline{[5 + 3j]} \\ &= (4 - 2j)(4 - 2\overline{j}) + (5 + 3j)(5 + 3\overline{j}) \\ &= 4^2 - (4)(-2) + (-2)^2 + 5^2 - 5 \cdot 3 + 3^2. \end{aligned}$$

Previous proofs of Proposition 22 appeared in [2], [6], and [24]. The proof in [24] is perhaps the first elementary proof.

**Remark 23** (Number of representations by the form $x^2 - xy + y^2 + z^2 - zu + u^2$**).** The number of representations is given by Liouville's theorem [47]. See also [2], [6], and [24].

**Corollary 24.** *Every positive integer has the form $x^2 + 3y^2 + z^2 + 3u^2$.*

*Proof.* By Proposition 22 we only need to prove that $x^2 - xy + y^2$ has the form $p^2 + 3q^2$. Indeed,

1. If $x$ is even, say $x = 2t$, then $x^2 - xy + y^2 = 4t^2 - 2ty + y^2 = (y - t)^2 + 3t^2$.

2. If $y$ is even, say $y = 2t$, then $x^2 - xy + y^2 = (x - t)^2 + 3t^2$.

3. If $x$ and $y$ are both odd, then $x^2 - xy + y^2 = ((x + y)/2)^2 + 3((y - x)/2)^2$.

□

A proof of Corollary 24 appeared in [1].

**Remark 25** (Number of representations by the form $x^2 + 3y^2 + z^2 + 3u^2$)**.** The number of representations was stated without proof by Liouville [31, 32] and it is proved in [1].

**Proposition 26.** *Each integer has the form $x^2 - 3y^2 + z^2 - 3u^2$.*

*Proof.* This can be proved by reasoning as in Proposition 22. The necessary ring is $\mathbb{Z}[\sqrt{3}]$ endowed with its natural anti-automorphism. □

In the following example we will represent 19 and $-19$, noticing that $19 \cdot 2 = 7^2 - 3 \cdot 2^2 + 1$.

$$\begin{aligned} 19 \cdot 2 &= (7+\sqrt{3})(7-\sqrt{3}) + 1 \\ &\qquad q_1 = 3+\sqrt{3} \\ 2 \cdot 1 &= (1+0\sqrt{3})(1-0\sqrt{3}) + 1 \\ &\qquad q_2 = 1+0\sqrt{3}. \end{aligned}$$

Hence

$$\begin{aligned} 19 &= [3+\sqrt{3}, 1-0\sqrt{3}][3-\sqrt{3}, 1+0\sqrt{3}] + [3+\sqrt{3}][3-\sqrt{3}] \\ &= (4+\sqrt{3})(4-\sqrt{3}) + (3+\sqrt{3})(3-\sqrt{3}) \\ &= 4^2 - 3 \cdot 1^2 + 3^2 - 3 \cdot 1^2. \end{aligned}$$

Then, to represent $-19$, we use $-1 = 1 \cdot 1 + (1+\sqrt{3})(1-\sqrt{3})$ and the product formula (Lemma 20) to get

$$\begin{aligned} -19 &= ((4+\sqrt{3})(1+\sqrt{3}) + (3+\sqrt{3}))\overline{(4+\sqrt{3})(1+\sqrt{3}) + (3+\sqrt{3})} \\ &\quad + ((4+\sqrt{3}) - (3+\sqrt{3})(1-\sqrt{3}))\overline{(4+\sqrt{3}) - (3+\sqrt{3})(1-\sqrt{3})} \\ &= (10+6\sqrt{3})(10-6\sqrt{3}) + (4+3\sqrt{3})(4-3\sqrt{3}) \\ &= 10^2 - 3 \cdot 6^2 + 4^2 - 3 \cdot 3^2. \end{aligned}$$

**Remark 27.** If continuants over new rings are considered, the approach presented in Sections 4 and 5 is likely to provide more quaternary quadratic forms representing either all positive integers or all integers.

**Acknowledgment** The authors would like to thank the anonymous referee for his/her helpful comments.

## References

[1] A. Alaca, Ş. Alaca, M. F. Lemire, and K. S. Williams, *Nineteen quaternary quadratic forms*, Acta Arith. **130** (2007), no. 3, 277–310.

[2] A. Alaca, Ş. Alaca, and K. S. Williams, *On the two-dimensional theta functions of the Borweins*, Acta Arith. **124** (2006), no. 2, 177–195.

[3] G. E. Andrews, S. B. Ekhad, and D. Zeilberger, *A short proof of Jacobi's formula for the number of representations of an integer as a sum of four squares*, Amer. Math. Monthly **100** (1993), no. 3, 274–276.

[4] C. W. Barnes, *The representation of primes of the form* $4n+1$ *as the sum of two squares*, Enseignement Math. (2) **18** (1972), 289–299 (1973).

[5] J. Brillhart, *Note on representing a prime as a sum of two squares*, Math. Comp. **26** (1972), 1011–1013.

[6] R. Chapman, *Representations of integers by the form* $x^2+xy+y^2+z^2+zt+t^2$, Int. J. Number Theory **4** (2008), no. 5, 709–714.

[7] M. D. Choi, T. Y. Lam, B. Reznick, and A. Rosenberg, *Sums of squares in some integral domains*, J. Algebra **65** (1980), no. 1, 234–256.

[8] F. W. Clarke, W. N. Everitt, L. L. Littlejohn, and S. J. R. Vorster, *H. J. S. Smith and the Fermat two squares theorem*, Amer. Math. Monthly **106** (1999), no. 7, 652–665, doi:10.2307/2589495.

[9] D. A. Cox, *Primes of the Form* $x^2+ny^2$*: Fermat, Class Field Theory and Complex Multiplication*, John Wiley & Sons Inc., New York, 1989.

[10] H. Davenport, *The Higher Arithmetic-An Introduction to the Theory of Numbers*, 8th ed., Cambridge University Press, Cambridge, 2008, Editing and additional material by J. H. Davenport.

[11] H. Davenport, D. J. Lewis, and A. Schinzel, *Polynomials of certain special types*, Acta Arith. **9** (1964), 107–116.

[12] Jesse Ira Deutsch, *Geometry of numbers proof of Götzky's four-squares theorem*, J. Number Theory **96** (2002), no. 2, 417–431.

[13] L. E. Dickson, *History of the Theory of Numbers, Vol. II*, Chelsea Publishing Company, New York, 1971.

[14] C. L. Dodgson, *Condensation of determinants, being a new and brief method for computing their arithmetical values*, Proc. R. Soc. Lond. **15** (1866), pp. 150–155.

[15] M. Elia, *Representation of primes as the sums of two squares in the golden section quadratic field*, J. Discrete Math. Sci. Cryptogr. **9** (2006), no. 1, 25–37.

[16] M. Elia and C. Monico, *On the representation of primes in* $\mathbb{Q}(\sqrt{2})$ *as sums of squares*, JP J. Algebra Number Theory Appl. **8** (2007), no. 1, 121–133.

[17] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, 2nd ed., Addison-Wesley, New York, 1994.

[18] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed., Oxford University Press, Oxford, 2008, Revised by D. R. Heath-Brown and J. H. Silverman.

[19] J. Hardy, *A note on the representability of binary quadratic forms with Gaussian integer coefficients as sums of squares of two linear forms*, Acta Arith. **15** (1968), 77–84.

[20] K. Hardy, J. B. Muskat, and K. S. Williams, *A deterministic algorithm for solving* $n=fu^2+gv^2$ *in coprime integers* $u$ *and* $v$, Math. Comp. **55** (1990), no. 191, 327–343, doi:10.2307/2008809.

[21] C. Hermite, *Note au sujet de l'article précédent*, J. Math. Pures Appl. **5** (1848), 15.

[22] M. D. Hirschhorn, *A simple proof of Jacobi's four-square theorem*, Proc. Amer. Math. Soc. **101** (1987), no. 3, 436–438.

[23] J. S. Hsia, *On the representation of cyclotomic polynomials as sums of squares*, Acta Arith.**25** (1973/74), 115–120.

[24] J. G. Huard, Z. M. Ou, B. K. Spearman, and K. S. Williams, *Elementary evaluation of certain convolution sums involving divisor functions*, Number theory for the millennium, II (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 229–274.

[25] N. Jacobson, *Basic Algebra I*, 2nd. ed., W. H. Freeman and Co., New York, 1985.

[26] M. A. Jodeit, Jr., *Uniqueness in the division algorithm*, Amer. Math. Monthly **74** (1967), 835–836.

[27] W. Leahey, *Sums of squares of polynomials with coefficients in a finite field*, Amer. Math. Monthly **74** (1967), 816–819.

[28] W. J. Leahey, *A note on a theorem of I. Niven*, Proc. Amer. Math. Soc. **16** (1965), 1130–1131.

[29] P. A. Leonard and K. S. Williams, *Representability of binary quadratic forms over a Bézout domain*, Duke Math. J. **40** (1973), 533–539.

[30] P. A. Leonard and K. S. Williams, *Forms representable by integral binary quadratic forms*, Acta Arith. **26** (1974/75), 1–9.

[31] J. Liouville, *Sur la forme $x^2 + y^2 + 3(z^2 + t^2)$*, J. Math. Pures Appl. **5** (1860), 147–152.

[32] J. Liouville, *Remarque nouvelle sur la forme $x^2 + y^2 + 3(z^2 + t^2)$*, J. Math. Pures Appl. **8** (1863), 296.

[33] L. J. Mordell, *On the representation of a binary quadratic form as a sum of squares of linear forms*, Math. Z. **35** (1932), no. 1, 1–15.

[34] L. J. Mordell, *The Representation of a Gaussian integer as a Sum of two Squares*, Math. Mag. **40** (1967), no. 4, 209.

[35] I. Niven, *Integers of quadratic fields as sums of squares*, Trans. Amer. Math. Soc. **48** (1940), 405–417.

[36] G. Pall, *Sums of two squares in a quadratic field*, Duke Math. J. **18** (1951), 399–409.

[37] Y. Pourchet, *Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques*, Acta Arith. **19** (1971), 89–104.

[38] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod $p$*, Math. Comp. **44** (1985), no. 170, 483–494.

[39] J. A. Serret, *Sur un théorème relatif aux nombres entieres*, J. Math. Pures Appl. **5** (1848), 12–14.

[40] C. Small, *A simple proof of the four-squares theorem*, Amer. Math. Monthly **89** (1982), no. 1, 59–61.

[41] B. K. Spearman and K. S. Williams, *The simplest arithmetic proof of Jacobi's four squares theorem*, Far East J. Math. Sci. (FJMS) **2** (2000), no. 3, 433–439.

[42] G. Zaimi (`http://mathoverflow.net/users/2384/`), *About integer polynomials which are sums of squares of rational polynomials*, Mathoverflow, `http://mathoverflow.net/questions/82046/`, accessed Dec 16 2011.

[43] S. Wagon, *Editor's corner: the Euclidean algorithm strikes again*, Amer. Math. Monthly **97** (1990), no. 2, 125–129, doi:10.2307/2323912.

[44] J. H. M. Wedderburn, *On continued fractions in non-commutative quantities*, Ann. of Math. **15** (1913/14), no. 1-4, 101–105.

[45] K. S. Williams, *On finding the solutions of* $n = au^2 + buv + cv^2$ *in integers* $u$ *and* $v$, Util. Math. **46** (1994), 3–19.

[46] K. S. Williams, *Some refinements of an algorithm of Brillhart*, Number theory (Halifax, NS, 1994), CMS Conf. Proc., vol. 15, Amer. Math. Soc., Providence, RI, 1995, pp. 409–416.

[47] K. S. Williams, *Number Theory in the Spirit of Liouville*, London Mathematical Society Student Texts, vol. 76, Cambridge University Press, Cambridge, 2011.

[48] K. S. Williams, *On a theorem of Niven*, Canad. Math. Bull. **10** (1967), 573–578.

[49] K. S. Williams, *Forms representable by an integral positive-definite binary quadratic form*, Math. Scand. **29** (1971), 73–86.

[50] K. S. Williams, *Note on a theorem of Pall*, Proc. Amer. Math. Soc. **28** (1971), 315–316.

[51] K. S. Williams, *Representation of a binary quadratic form as a sum of two squares*, Proc. Amer. Math. Soc. **32** (1972), 368–370.

[52] K. S. Williams, *Another proof of a theorem of Niven*, Math. Mag. **46** (1973), 39.

[53] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares*, Amer. Math. Monthly **97** (1990), no. 2, 144, doi:10.2307/2323918.