A LOOK AT QUADRATIC FORM REPRESENTATIONS VIA MODIFICATIONS OF CONTINUANTS

CHARLES DELORME AND GUILLERMO PINEDA-VILLAVICENCIO

ABSTRACT. In 1855 H. J. S. Smith [4] proved Fermat's Two Squares using the notion of palindromic continuants. In this paper we extend Smith's approach to proper binary quadratic form representations in some commutative Euclidean rings, including rings of integers and rings of polynomials over fields of odd characteristic. New deterministic algorithms for finding the corresponding proper representations are presented.

1. INTRODUCTION

Fermat's Two Square Theorem is with no doubt a remarkable result. Many proofs of the theorem have been provided; see, for instance, [24, 10, 19, 4, 1]. It is also true that most proofs have much in common, for instance, Smith's proof is very similar to Hermite's [10], Serret's [19], and Brillhart's [1].

We first give a definition of continuant, a concept around which our paper revolves.

Definition 1 (Continuants in arbitrary rings, [8, Sec. 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*

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

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

Properties of continuants in commutative rings are given in [8, Sec. 6.7]. Here we restrict ourselves to presenting three properties.

Date: May 6, 2014.

1991 *Mathematics Subject Classification.* Primary 11E25, Secondary 11D85, 11A05.

Key words and phrases. Fermat's two square theorem; continuant; integer representation.

Lemma 1 (Lewis Carroll identity, [7]). *Let C be an $n \times n$ matrix in a commutative ring. Let $C_{i_1,\ldots,i_s;j_1,\ldots,j_s}$ denote the matrix obtained from C by omitting the rows $i_1, \ldots, i_s$ and the columns $j_1, \ldots, j_s$. 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 $\det(M)$ *denotes the determinant of a matrix M and the determinant of the* 0×0 *matrix is 1 for convenience.*

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

Given two elements m_1 and m_2 in an Euclidean ring R, the Euclidean algorithm outputs a sequence $(q_1, q_2, \ldots, q_n)$ of quotients and a gcd h of m_1 and m_2. A sequence of quotients given by the Euclidean algorithm is called a *continuant representation* of m_1 and m_2 as we have the equalities $m_1 = [q_1, q_2, \ldots, q_n]h$ and $m_2 = [q_2, \ldots, q_n]h$ unless $m_2 = 0$.

A representation of an element m by the form $Q(x, y) = \alpha x^2 + \gamma xy + \beta y^2$ is called *proper* if $\gcd(x, y) = 1$. In this paper we are mostly concerned with proper representations.

For us the quadratic forms $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = Ax^2 + Bxy + Cy^2$ are *equivalent* if there is a 2×2 matrix $M = (a_{ij})$ with determinant 1 such that $g(x, y) = f(a_{11}x + a_{12}y, a_{21}x + a_{22}y)$. For equivalent forms f and g it follows that an element m is (properly) represented by f iff m is (properly) represented by g.

Let p be a prime number of the form $4k + 1$. In his proof of Fermat's Two Squares Theorem, Smith [4] first shows the existence of a palindromic sequence $Q = (q_1, \ldots, q_s, q_s, \ldots, q_1)$ such that $p = [Q]$ through an elegant parity argument. This sequence then allows him to derive a solution for $z^2 + 1 \equiv 0 \pmod{p}$ and a representation $x^2 + y^2$ for p.

With regards to the question of finding square roots modulo a prime p, Schoof presented a deterministic algorithm in [18] and Wagon discussed the topic in [20].

Brillhart's optimisation [1] on 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

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

so, in virtue of Smith's construction, rather than computing the whole sequence we 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 criterium.

In the ring of integers, Cornacchia [5] first extended Smith's ideas to cover forms $x^2 + hy^2$. Further extensions of Smith's and Brillhart's ideas were presented in [9, 21, 22], where the authors provided algorithms, at the expense of the palindromic nature of the continuant, for finding proper representations of natural numbers as primitive, positive-definite, integral and binary quadratic forms. Mathews [13] provided representations of certain integers as $x^2 - hy^2$, where $h = 2, 3, 5, 6, 7$. In all these works 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 $q_1 + \dfrac{1}{q_2 + \dfrac{1}{q_3}}$, while the continuant $[q_2, q_3]$ equals its denominator.

For us the set of natural numbers $\mathbb{N}$ includes the zero.

Concerning other rings, one of the most important works is by Choi, Lam, Reznick and Rosenberg [3]. In [3] Choi *et al.* proved the following theorem.

Theorem 1 ([3, Thm. 2.5])**.** *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 UFDs (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 by $x^2 + hy^2$ for all j.*

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

1.1. **Our work.** This paper can be considered as a follow-up to our earlier paper [6]. In [6] we studied the use of continuants in some integer representations (e.g. sums of four squares) and sums of two squares in rings of polynomials over fields of characteristic different from 2. Here we deal with the following problems. We denote a unit in the ring by u.

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

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

In this paper we introduce the notion of modified continuants, an extension of continuants, and use them to produce proper representations $Q(x, y) = x^2 + gxy + hy^2$, up to multiplication by a unit u, of an element m in some Euclidean rings. This extension allows us to present the following new deterministic algorithms.

(1) Algorithm 1: for every m in a commutative Euclidean ring, it 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, it finds a proper representation $u(x^2 + hy^2)$ of m, given a solution z_0 of $Q(z, 1) \equiv 0 \pmod{m}$. Here h is a polynomial in $\mathbb{F}[X]$ of degree at most one.
(3) Algorithm 3: for all negative discriminants of class number one, it finds a representation $uQ(x, y)$ of an integer m, given a solution z_0 of $Q(z, 1) \equiv 0 \pmod{m}$.

A simple modification of Algorithm 3 produces representations $uQ(x, y)$ for some positive discriminants of class number one, including all the determinants studied by Mathews [13]. This modification is discussed in Section 5.

Recall the *class number* of a determinant Δ [2, pp. 7] gives the number of equivalence classes of integral binary quadratic forms with discriminant Δ.

When trying to extend Smith's approach to other Euclidean rings R, one faces the lack of uniqueness of the continuant representation. 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 $R = \mathbb{F}[X]$, polynomial algebra over a field $\mathbb{F}$ [12] (considering the degree as the Euclidean function).

The rest of the paper is structured as follows. In Section 2 we modify the notion of continuant and describe some of their properties. Section 3 is devoted to studying proper representations $x^2 + gxy + hy^2$ in some commutative Euclidean rings, mainly in the ring of polynomials over a field of odd characteristic. In Section 4 we consider proper representations $x^2 + gxy + hy^2$ in the ring of integers. Some final remarks are presented in Section 5.

2. Modified Continuants

With the aim of considering the problem of properly representing an element m as $x^2 + gxy + hy^2$, we extend the notion of continuants.

Definition 2 (Modified Continuants in Arbitrary Rings)**.** *In a ring R associate with the element $[Q; h, s]$ the 3-tuple formed from a sequence Q of elements $q_1, q_2, \ldots, q_n$ of R, an element h of R and an integer s via the following recurrence formula*

$$[q_1, \ldots q_n; h, s] = \begin{cases} [q_1, \ldots q_n] & \text{if } s \geq n \\ [q_1, \ldots q_{n-1}]q_n + [q_1, \ldots q_{n-2}]h & \text{if } s = n-1 \\ [q_1, \ldots q_{n-1}; h, s]q_n + [q_1, \ldots q_{n-2}; h, s] & \text{if } s < n-1 \end{cases}$$

The definition of modified continuant carries several consequences, which we will refer to as Modified Continuant Properties.

- P–3 $[q_1, \ldots, q_n; h, s] = [q_1, \ldots, q_{s-1}]h[q_{s+2}, \ldots, q_n] + [q_1, \ldots, q_s][q_{s+1}, \ldots, q_n]$: Divide the products of subsequences of $Q = (q_1, q_2, \ldots, q_n)$ obtained by removing disjoint pairs of consecutive elements of Q into two groups, depending on whether or not the products remove the pair $q_s q_{s+1}$ ($1 \leq s < n$).
- P–4 If in a ring R we find a unit u commuting with all q_i's, then

$$[u^{-1}q_1, uq_2, \ldots, u^{(-1)^n}q_n; h, s] = \begin{cases} [q_1, \ldots, q_n; h, s] & \text{for even } n \\ u^{-1}[q_1, \ldots, q_n; h, s] & \text{for odd } n \end{cases}$$

P–5 Induction can provide us with the following.

$$[q_1,\dots q_n;h,s]=\begin{cases}[q_1,\dots q_n] & \text{if } s\geq n \text{ or } s=0\\ q_1[q_2,\dots q_{n-1},q_n]+h[q_3,\dots q_n] & \text{if } s=1\\ [q_1,\dots q_{n-1}]q_n+[q_1,\dots q_{n-2}]h & \text{if } s=n-1\\ q_1[q_2,\dots q_n;h,s-1] & \text{if } 2\leq s<n-1\\ \quad +[q_3,\dots q_{n-2};h,s-2] & \end{cases}$$

The next two properties pertain to commutative rings.

P–6 The modified continuant $[q_1,\dots,q_n;h,s]$ is the determinant of the tridiagonal $n\times n$ matrix $A=(a_{ij})$ with $a_{i,i}=q_i$ for $1\leq i\leq n$, $a_{i,i+1}=1$ for $1\leq i<n$, $a_{s+1,s}=-h$ and $a_{i+1,i}=-1$ for $1\leq i<n$ and $i\neq s$. See the determinant of the matrix below for a small example.

$$[q_1,q_2,q_3,q_4,q_5;h,3]=\det\begin{bmatrix} q_1 & 1 & & & \\ -1 & q_2 & 1 & & \\ & -1 & q_3 & 1 & \\ & & -h & q_4 & 1\\ & & & -1 & q_5\end{bmatrix}$$

P–7 $[q_1,q_2,\dots,q_n;h,n-s]=[q_n,\dots,q_2,q_1;h,s]$. This can be seen from applying Property P–3 on both sides of the equality, and then using Property P–2.

3. From $Q(x,y)$ to $Q(z,1)$ and back

In this section, considering the form $Q(x,y)=x^2+gxy+hy^2$, we deal with the problem of going from a representation $Q(x,y)$ of an element m to a multiple $Q(z,1)$ of m and back.

3.1. From $Q(x,y)$ to $Q(z,1)$.

We begin with a general proposition which is valid for every commutative ring.

Proposition 1. *If $Rx+Ry=R$ then there exist $z\in R$ such that $Q(x,y)$ divides $Q(z,1)$, where Rm denotes the ideal generated by m.*

If R is Euclidean, we can explicitly find z and the quotient $Q(z,1)/Q(x,y)$ with modified continuants.

Proof. We have u and v such that $xu + yv = 1$. Then, computation with norms in the ring obtained from R by adjoining formally a root of the polynomial $T^2 - gT + h$ provides the identity

$$Q(x,y)Q(v-ug,u) = Q(xv - xug - yuh, xu + yv),$$

which proves the first assertion. This identity can be interpreted also as a kind of Lewis-Carroll identity.

The determinant of the tridiagonal matrix

$$M = \begin{bmatrix} q_s & 1 & & & & & & \\ -1 & \ddots & \ddots & & & & & \\ & \ddots & q_2 & \ddots & & & & \\ & & -1 & q_1 & \ddots & & & \\ & & & -h & q_1+g & \ddots & & \\ & & & & -1 & q_2 & \ddots & \\ & & & & & \ddots & \ddots & 1 \\ & & & & & & -1 & q_s \end{bmatrix} \tag{1}$$

is $Q(x,y)$ with $x = [q_1, \ldots, q_s]$ and $y = [q_2, \ldots, q_s]$ if $s \geq 1$.

Also, $Q(x,y)Q([q_1, \ldots q_{s-1}], [q_2, \ldots q_{s-1}]) = Q(z,1)$, where $z = (-1)^{s+1}c$ and c is the determinant of the matrix formed by the $2s-1$ first rows and columns of M. □

The proof of Proposition 1 can be readily converted into a deterministic algorithm which finds a solution z_0 of $Q(z,1) \equiv 0 \pmod{m}$, given a representation $uQ(x,y)$ of an element m in an Euclidean ring R. See Algorithm 1.

3.2. **From $Q(z,1)$ to $Q(x,y)$.** We begin the subsection with the following remark.

Remark 1. *Let R be a commutative ring.*

If 2 is invertible, the form $x^2 + gxy + hy^2$ can be rewritten as $(x + gy/2)^2 + (h - g^2/4)y^2$. We may then assume $g = 0$ without loss of generality.

If moreover $-h$ is an invertible square, say $h + k^2 = 0$, then $x = \left(\frac{x+1}{2}\right)^2 + h\left(\frac{x-1}{2k}\right)^2$

Below we provide a proposition which can be considered as an extension of [6, Prop. 16]. In the case of m being prime, Proposition 2 is embedded in Theorem

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 $Q(x,y) = x^2 + gxy + hy^2$.
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,...,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 $r_s = 0$;
$z_0 \leftarrow (-1)^{s+1}[q_s, q_{s-1}, \ldots, q_1, q_1 + g, q_2, \ldots, q_{s-1}; h, s]$;
return z_0

2.5 of [3]. Note that in Propositions 2 and 3 we implicitly invoke the uniqueness of the quotients and the remainders in the division algorithm.

Proposition 2. *Let $R = \mathbb{F}[X]$ be the ring of polynomials over a field $\mathbb{F}$ with characteristic different from 2, and $-h$ a (non-null) non-square of $\mathbb{F}$.*

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

Proof. We introduce the extension $\mathbb{G}$ of $\mathbb{F}$ by a square root ω of $-h$. The ring $\mathbb{G}[X]$ is principal and $z^2 + ht^2$ factorises as $(z - \omega t)(z + \omega t)$, with the two factors being coprime. Introduce $x + \omega y = \gcd(m, z + \omega t)$; then $x - \omega y$ is a gcd of m and $z - \omega t$, using 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 $(x - \omega y)(x + \omega y) = x^2 + hy^2$. On the other hand, m divides $(z - \omega t)(z + \omega t)$. Consequently, m is an associate of $x^2 + hy^2$. Since $x - \omega y$ and $x + \omega y$ are coprime, x and y are coprime. □

Proposition 3. *Let $R = \mathbb{F}[X]$ be the ring of polynomials over a field $\mathbb{F}$ with characteristic different from 2, and let h be a polynomial of degree 1.*

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

Proof. Consider the extension of the ring $R = \mathbb{F}[X]$ by a root of $T^2 + h$; this extension of R is isomorphic to $\mathbb{F}[T]$.

If m is a multiple of h, then m is an associate of $(hy)^2 + hx^2$, with hy and x coprime. This representation of m follows from a representation $x^2 + hy^2$ of m/h.

We may now assume that h and z are coprime. Then, $z^2 + ht^2$ factors as $(z - Tt)(z + Tt)$, with the two factors being coprime. Reasoning as in Proposition 2, we let $x + Ty$ be the gcd of m and $z + Tt$ and we obtain that $x - Ty$ is the gcd of m and $z - Tt$ and that m is an associate of $x^2 + hy^2$ with x, y coprime. □

The next remark generalises [6, Rem. 19].

Remark 2 (Algorithmic considerations)**.** *For the cases covered in Propositions 2 and 3, given an element m and a solution z_0 of $z^2 + h \equiv 0 \pmod{m}$, we can obtain a representation $x^2 + hy^2$ of an associate of m via modified continuants and Brillhart's* [1] *optimisation. Divide m by z_0 and stop when a remainder r_{s-1} with degree at most $\deg(m)/2$ is encountered. This will be the $(s-1)$-th remainder, and $(uq_s, u^{-1}q_{s-1}, \ldots, u^{(-1)^{s-2}}q_2)$ are the quotients so far obtained. Then*

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

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

This remark follows from dividing

$$m/u = [q_s, \ldots, q_1, q_1, \ldots, q_s; h, s] \quad \text{by}$$
$$z_0 = [q_{s-1}, \ldots, q_1, q_1, \ldots, q_s; h, s-1]$$

using modified continuant properties.

Remark 2 can be readily translated into a deterministic algorithm for computing representations $Q(x, y)$; see Algorithm 2.

The argument brought forward in [6, Prop. 17] can be applied to the form $x^2 + hy^2$ in polynomials over a field $\mathbb{F}$ of characteristic different from 2, where h is either a non-square $\in \mathbb{F}$ or a polynomial in $\mathbb{F}[X]$ of degree 1.

Corollary 1 (of Proposition 2: h non-square unit in $\mathbb{F}[X]$)**.** *Let m be a non-unit of $\mathbb{F}[X]$ and a divisor of $z^2 + h$ for some $z \in \mathbb{F}[X]$ with $\deg(z) < \deg(m)$. Then, $m = (x^2 + hy^2)u$ for some unit u and the Euclidean algorithm on m and z gives the unit u and the sequence*

$$(uq_s, u^{-1}q_{s-1}, \ldots, u^{(-1)^{s+1}}q_1, u^{(-1)^s}h^{-1}q_1, \ldots, u^{-1}h^{(-1)^s}q_s)$$

such that $x = [q_1, \ldots q_s]$ and $y = [q_2, \ldots, q_s]$.

In the next example we illustrate Remark 2 and the method of Corollary 1, in this order. Let $h = 3$ and $m = 1 + 2X + 3X^2 + 2X^3 + X^4$, then m divides $((5 + 12X + 6X^2 + 4X^3)/3)^2 + 3$. The Euclidean division gives

$$\begin{aligned} 1 + 2X + 3X^2 + 2X^3 + X^4 =&((5 + 12X + 6X^2 + 4X^3)/3)(3X/4 + 3/8) \\ &+ 3/8 - 3X/4 - 3X^2/4 \end{aligned}$$

Here the first remainder has degree at most $\deg(m)/2$, thus we stop the division process and obtain $s = 2$, $x = (3/8 - 3X/4 - 3X^2/4)/u$ and $y = [3X/4 + 3/8]/u$. It is now plain to get $u = 9/16$.

If instead we use the method of Corollary 1, then we obtain the unit $u = 9/16$ and the sequence $(9/16 \cdot 2/3 \cdot (1 + 2X), 16/9 \cdot (-1/2 - X), 9/16 \cdot 1/3 \cdot (-1/2 - X), 16/9 \cdot 3 \cdot 2/3 \cdot (1 + 2X))$. From this sequence we know that

$$\begin{aligned} x &= [2/3 \cdot (1 + 2X), -1/2 - X] \\ y &= [2/3 \cdot (1 + 2X)] \end{aligned}$$

Corollary 2 (of Proposition 3: h of degree 1 in $\mathbb{F}[X]$)**.** *Let m be a polynomial over $\mathbb{F}[X]$ and a divisor of $z^2 + h$ for some $z \in \mathbb{F}[X]$ with $\deg(z) < \deg(m)$ and z, h coprime. Then, $m = (x^2 + hy^2)u$ for some unit u and the values of x and y can be obtained by Remark 2.*

Consider the following example, let $h = X$, $m = 1 + X + X^3 + X^4$ and $z = (X^3 + 2X^2 + 1)/2$. Then, the division gives

$$1 + X + X^3 + X^4 = (X^3 + 2X^2 + 1)/2 \cdot (-2 + 2X) + 2 + 2X^2$$

Algorithm 2: Deterministic algorithm for constructing a proper representation $uQ(x,y) = u(x^2 + hy^2)$ 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 square-free element $h \in \mathbb{F}$ or a polynomial $h \in R$ of degree 1.
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.

assumptions: The polynomials z and h are coprime.

/* Divide m by z using the Euclidean algorithm until a remainder r_{s-1} until we find a remainder 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 $m = u(x_{temp}^2 + hy_{temp}^2)$ for u

else Solve $um = x_{temp}^2 + hy_{temp}^2$ for u

/* We obtain (x,y) so that $m = (x^2 + hy^2)u$. */

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)

At this step we should stop the division process as the first remainder has at most half the degree of m. Now we know that $s = 2$, $x = (2 + 2X^2)/u$ and $y = u^{-1}[-2 + 2X]$ for a unit u. It plainly follows that $u = 4$.

We now may wonder how far can we push this method for polynomials over a field of characteristic different from 2? That is, will the method work for h with $\deg(h) > 1$ over any such field?

We first note that the property

"$m|z^2 + h \Rightarrow \exists x, y, u\ (m = u(x^2 + y^2 h) \wedge u \text{ unit})$"

does not hold in general for h reducible. Consider $h = X^3 + X^2 + X$ in polynomials over a field of characteristic $\neq 3$. Then, $X^2 + X + 1$ divides $0^2 + 1^2 h$ and is certainly not of the form $x^2 + y^2 h$. Indeed, here we have either $y^2 h$ null or of odd degree ≥ 3. In the former case, it follows that $x^2 + y^2 h = x^2$ is a square, but $X^2 + X + 1$ is not a square in a field of characteristic $\neq 3$, while in the latter case $x^2 + y^2 h$ has degree $\geq 3 >$ degree$(X^2 + X + 1)$.

What about irreducible h with $\deg(h) \geq 2$? Already for degree 2 the property does not hold in general. Indeed, consider in $\mathbb{Q}[X]$ the polynomials $h = X^2 - 2$, $z = X^2$ and $m = X - 1$. Observe that $X - 1$ divides $X^4 + X^2 - 2$ and that $X - 1$ is not of the form $u(x^2 + y^2(X^2 - 2))$. To see this note that the degree of $x^2 + y^2(X^2 - 2)$ is either $2\deg(x)$ or $2 + 2\deg(y)$.

For specific fields we find situations where the property holds. Take, for instance, the field $\mathbb{R}$ of reals, $h = X^2 + 1$ and every real polynomial m taking only positive values over $\mathbb{R}$. It is known that the polynomials m over $\mathbb{R}$ that take at every point of $\mathbb{R}$ a positive value has the form $\prod(a_k X^2 + 2b_k X + c_k)$, where $a_k, b_k, c_k \in \mathbb{R}$ and $b_k^2 - a_k c_k < 0$. Thus, it suffices to consider the case of $m = aX^2 + 2bX + c$ with $a > 0, c > 0$ and $b^2 - ac < 0$. If $b = 0$, then

$$m = \begin{cases} (\sqrt{a - c}X)^2 + \sqrt{c}^2(X^2 + 1) & \text{if } a \geq c \\ \sqrt{c - a}^2 + \sqrt{a}^2(X^2 + 1) & \text{if } a \leq c. \end{cases}$$

If instead $b \neq 0$, then, setting $d = \sqrt{(a + c - \sqrt{(a - c)^2 + 4b^2})/2}$, we obtain $m = (\sqrt{a - d^2}X + e\sqrt{c - d^2})^2 + d^2(X^2 + 1)$, where $e = \pm 1$ has the sign of b.

For $h = -X^2 - 1$ and every real polynomial m over $\mathbb{R}$, we have another situation where the property holds. Observe that the form $Q(x, y) = x'^2 + (-X^2 - 1)y'^2$ is equivalent to the form $Q(x, y) = x^2 + 2Xxy - y^2$ (by Remark 1). Any polynomial of degree 1 is an associate of some $a^2 - b^2 + 2abX$ with units a and b. We now take care of polynomials $m = k(X^2 + 2vX + w)$ with no real zeros and $k, v, w \in \mathbb{R}$. Here note that $v^2 < w$. Set $p(X) = (X + a)^2 + 2b(X + a)X - b^2$. We solve the

equation $p(X) = m$ in (a, b, k). We first find that $k = 1 + 2b$, $a = kv/(1 + b)$ (if $b \neq -1$) and $w = (a^2 - b^2)/k = -X^2 - 2vX$. If $b = -1$ then $v = 0$, $k = -1$ and $a = \pm\sqrt{1 - w}$ with $0 < w \leq 1$. If instead $b \neq -1$, then, substituting $a = kv/(1 + b)$ into $-(1 + b)^2 p(X)$, we obtain

$$b^4 + 2(w + 1)b^3 + (5w - 4v^2 + 1)b^2 + 4(w - v^2)b + w - v^2 = 0.$$

This equation in b is $1/16$ when $b = -1/2$ and $-v^2$ when $b = -1$. Hence there is a solution b in the open interval $(-1, -1/2)$ for $w > 1$. Consequently, each real polynomial is an associate of some polynomial $x^2 + 2xyX - y^2 = (x + Xy)^2 + (-1 - X^2)y^2$.

Using the automorphisms of $\mathbb{R}[x]$, both previous approaches can easily be applied to any real polynomial of degree 2 with no real roots.

4. From $Q(z, 1)$ to $Q(x, y)$: integral quadratic forms

In this section, given integers m, z such $m|Q(z, 1)$, we provide an algorithm that proves the existence of representations $Q(x, y)u$ of m for a unit u and certain forms Q.

Since 2 is not invertible in $\mathbb{Z}$, we have to consider the rings of algebraic integers of $\mathbb{Q}[\sqrt{-h}]$, that is, the rings $\mathbb{Z}[\sqrt{-h}]$ for forms $x^2 + hy^2$ with $|h|$ square-free and $h \not\equiv -1 \pmod 4$, and the ring $\mathbb{Z}[(1 + \sqrt{1 - 4h})/2]$ for forms $x^2 + xy + hy^2$ with $|1 - 4h|$ square-free; see [17, pp. 35].

What are those rings of integers for which the following property holds?

"$m|Q(z, 1) \Rightarrow \exists x, y, u\ (m = uQ(x, y) \wedge u$ unit)."

The answer is given by the rings whose corresponding forms have class number $H(\Delta)$ equal to one [2, pp. 6–7,81–84]. Here Δ denotes the form discriminant. In the case of $\Delta < 0$, all the principal rings satisfy the property; these Δ's are the following: $-3, -4, -7, -8, -11, -19, -43, -67, -163$; see [14] and [2, pp. 81]. In this context, modified continuants provide a constructive proof of the property. For the case of $\Delta > 0$, while we do not even know whether the list of such determinants is infinite, it is conjectured this is likely the case; see [2, pp. 81–82] and [15].

Recall the class number $H(\Delta)$ [2, pp. 7] gives the number of equivalence classes of integral binary quadratic forms with discriminant Δ.

Next we recall the following well-known result by Rabinowitsch.

Theorem 2 ([16]). *For a discriminant $\Delta = 1 - 4\kappa \leq -7$, it follows that $H(\Delta) = 1$ iff $x^2 + x + \kappa$ attains only prime values for $-(\kappa - 1) \leq x \leq \kappa - 2$.*

Below we present a division algorithm (Algorithm 3) which, for any negative discriminant of class number one, gives a proper representation $Q(x, y)$ of m assuming m divides $Q(z, 1)$.

Since $m = 1$ trivially admits proper representation $(1, 0)$ of $Q(x, y) = x^2 + gxy + hy^2$, Algorithm 3 assumes $|m| > 1$.

Algorithm 3: Deterministic algorithm for constructing a proper representation $Q(x, y) = x^2 + gxy + hy^2$ of an element m

input : A negative discriminant Δ of class number one.
An integer m_0 with $1 < |m_0|$.
A solution z_0 of $Q(z, 1) \equiv 0 \pmod{m_0}$ with $1 < |z_0| < |m_0|$.

output: A proper representation $Q(x, y)$ of m_0/u ($u = \pm 1$).

$s \leftarrow 0$;
while $|m_s| \neq 1$ **do**
  $s \leftarrow s + 1$;
  $m_s \leftarrow Q(z_{s-1}, 1)/m_{s-1}$;
  find $k_s, z_s \in R$ such that $z_{s-1} = k_s m_s + z_s$ with $|z_s| < |m_s|$;
  /* We prioritise non-null quotients k_s. */
end
/* Here we have the unit m_s and sequence $(k_1, \ldots, k_s)$. */
/* To keep consistency with the previous sections of the paper we reverse the subscripts of the quotients */
$(q_1, q_2, \ldots, q_s) \leftarrow (k_s, k_{s-1}, \ldots, k_1)$;
$x \leftarrow [m_s q_1, m_s^{-1} q_2, \ldots, m_s^{(-1)^{s-2}} q_{s-1}, m_s^{(-1)^{s-1}} q_s]$;
$y \leftarrow [m_s^{-1} q_2, \ldots, m_s^{(-1)^{s-2}} q_{s-1}, m_s^{(-1)^{s-1}} q_s]$;
return (x, y)

Remark 3 (Algorithm 3: Prioritising non-null quotients)**.** *In the Euclidean division of z_{s-1} by m_s with $|z_{s-1}| < |m_s|$, a valid quotient k_s could be ± 1 or 0. By "prioritising non-null quotients k_s" we mean that, in this situation, we always choose the non-null k_s.*

Proposition 4 (Algorithm 3 Correctness)**.** *Let $h, g, \Delta, u, m_0, z_0$, and m_i, z_i, q_i $(i = 1, \ldots, s)$ be as in Algorithm 3. Then, Algorithm 3 produces a proper representation $Q(x, y)$ of m_0/u.*

Proof. In the ring $\mathbb{Z}[(1+\sqrt{1-4h})/2]$ we consider the form $Q(x,y) = x^2 + xy + hy^2$, while in the ring $\mathbb{Z}[\sqrt{-h}]$ we consider the form $Q(x,y) = x^2 + hy^2$. As the proof method is the same in both cases, we restrict ourselves to the former case, that is, to the case of $\Delta = -3, -7, -11, -19, -43, -67, -163$ and $h = 1, 2, 3, 5, 11, 17, 41$.

Claim 1. Algorithm 3 terminates with the last m_j being ± 1.

As a general approach we show that the sequence $|m_i|$ $(i = 0, \ldots, s-1)$ is decreasing, that is, $|m_{i+1}| < |m_i|$. Once this decreasing character fails, we show that the algorithm anyway stops with the last m_i being a unit.

Recall we have $|m_i| \geq |z_i| + 1$ for $i = 1, \ldots, s-1$.

Case $(\Delta, h) = (-3, 1), (-7, 2)$**:** $|m_i||m_i| \geq z_i^2 + 2|z_i| + 1 > |z_i^2 + z_i + h| = |m_i||m_{i+1}|$, and thus $|m_i| > |m_{i+1}|$ for $|z_i| > 1$. Assume that for a certain z_i, say z_{s-1}, $|z_{s-1}| = 1$. If $h = 1$ then Line 4 ($z_{s-1}^2 + z_{s-1} + 1 = m_{s-1}m_s$) gives that $|m_s| = 1$, as desired. In the case of $h = 2$ and $z_{s-1} = -1$, we have that $z_{s-1}^2 + z_{s-1} + 2 = 2$ and $|m_s| = 1$. If $h = 2$ and $z_{s-1} = 1$, we have that Line 4 gives $1 + 1 + 2 = m_{s-1}m_s$. From this we get that either $|m_{s-1}| = 2$ and $|m_s| = 2$ or $|m_{s-1}| = 4$ and $|m_s| = 1$. The configuration $|m_{s-1}| = 4$ and $|m_s| = 1$ will cause the algorithm to stop with m_s being a unit. In the case of $|m_{s-1}| = 2$ and $|m_s| = 2$, in Line 5 we have $z_{s-1} = k_s m_s + z_s$ and the algorithm would obtain $z_s = -1$, which implies $|m_{s+1}| = 1$.

Consequently, in these two cases Algorithm 3 terminates with the last m_j being a unit.

Case $(\Delta, h) = (-11, 3), (-19, 5), (-43, 11), (-67, 17), (-163, 41)$**:** Reasoning as in the previous case, we have that $|m_i||m_i| \geq z_i^2 + 2|z_i| + 1 > |z_i^2 + z_i + h| = |m_i||m_{i+1}|$, unless $|z_i| \leq h - 1$. Suppose $|z_{s-1}| \leq h - 1$. Note that $|m_{s-1}| > 1$, otherwise the algorithm would have stopped. By Theorem 2, the polynomial $Q(z_{s-1}, 1) = z_{s-1}^2 + z_{s-1} + h$ is prime for $-(h-1) \leq z_{s-1} \leq h - 2$. Thus, we have that $|m_{s-1}| > |m_s|$ with $|m_s| = 1$.

If instead $z_{s-1} = h - 1$, then $|m_{s-1}| = |m_s| = h$, which implies that $z_s = -1$ and $|m_{s+1}| = 1$, causing the algorithm to stop.

Claim 2. Algorithm 3 produces a proper representation $Q(x, y)$.

It only remains to prove that x and y have the claimed expression. First we reverse the subscripts of the quotients, that is, the quotient k_s becomes q_1, the quotient k_{s-1} becomes q_2, and so on. Thus, after the while loop we have that $z_{s-1} = m_s q_1$, where m_s is a unit. We know that $Q(m_s q_1, 1) = m_{s-1} m_s$. Consequently, $m_{s-1} m_s = [m_s q_1 + 1, m_s q_1; h, 1]$. Then, by Property P–7 and Property P–3 it follows

$$z_{s-2} = [m_s^{-1} q_2, m_s q_1 + 1, m_s q_1; h, 2].$$

Then, from the equation $m_{s-2} m_{s-1} = Q(z_{s-2}, 1)$ we obtain

$$m_{s-2} m_s^{-1} = [m_s^{-1} q_2, m_s q_1 + 1, m_s q_1, m_s^{-1} q_2; h, 2] = Q([m_s q_1, m_s^{-1} q_2], [m_s^{-1} q_2]).$$

Continuing this process, we have

$$\begin{aligned} z_0 &= [m_s^{(-1)^{s-1}} q_s, K, m_s q_1 + 1, m_s q_1, K^{-1}; h, s] \\ m_0 m_s^{(-1)^{s+1}} &= [m_s^{(-1)^{s-1}} q_s, K, m_s q_1 + 1, m_s q_1, K^{-1}, m_s^{(-1)^{s-1}} q_s; h, s] \end{aligned}$$

where $K = m_s^{(-1)^{s-2}} q_{s-1}, \ldots, m_s^{-1} q_2$ and $K^{-1} = m_s^{-1} q_2, \ldots, m_s^{(-1)^{s-2}} q_{s-1}$.

Consequently, from Property P–4 it follows that $m_0 m_s^{(-1)^{s+1}} = Q(x, y)$, where

$$\begin{aligned} x =& [m_s q_1, m_s^{-1} q_2, \ldots, m_s^{(-1)^{s-2}} q_{s-1}, m_s^{(-1)^{s-1}} q_s] \\ y =& [m_s^{-1} q_2, \ldots, m_s^{(-1)^{s-2}} q_{s-1}, m_s^{(-1)^{s-1}} q_s] \end{aligned}$$

Using Property P–7 we could write $m_0 m_s^{(-1)^{s+1}}$ as follows; see Equation (1).

$$m_0 m_s^{(-1)^{s+1}} = [m_s^{(-1)^{s-1}} q_s, K, m_s q_1, m_s q_1 + 1, K^{-1}, m_s^{(-1)^{s-1}} q_s; h, s].$$

Remark 4. *Note that we require all numbers m_i to be represented by the form $Q(x', y')$. This is assured by the fact that Q has class number one.*

As a result, each root z_0 of $Q(z, 1) \equiv 0 \pmod{m_0}$ with $1 < |z_0| < |m_0|$ gives rise to a proper representation of $m_0 m_s^{(-1)^{s+1}}$ as $Q(x, y)$. The coprimality of x and y follows from Property P–1. □

Let us see now an example. For the ring $\mathbb{Z}[(1+\sqrt{-19})/2]$ the form is $x^2+xy+5y^2$. Noticing $251\cdot 11 = 52^2+52+5$, the division gives

$$\begin{aligned} 251\cdot 11 = 52^2+52+5 &\quad\to\quad 52 = 4\cdot 11+8\\ 11\cdot 7 = 8^2+8+5 &\quad\to\quad 8 = 1\cdot 7+1\\ 7\cdot 1 = 1^2+1+5 &\quad\to\quad 1 = 1\cdot 1. \end{aligned}$$

Thus, we have $m_3 = 1$ and $(q_3, q_2, q_1) = (4, 1, 1)$. From this we recover the continuant representation of $m_0 = 251$

$$251 = \det\begin{bmatrix} 4 & 1 & & & & \\ -1 & 1 & 1 & & & \\ & -1 & 1 & 1 & & \\ & & -5 & 1+1 & 1 & \\ & & & -1 & 1 & 1\\ & & & & -1 & 4 \end{bmatrix}$$

concluding that $251 = x^2+xy+5y^2$ with $x = [1,1,4] = 9$ and $y = [1,4] = 5$.

5. Final remarks

In Algorithm 3 we require m_s to be ± 1. However, this may be an unnecessarily strong restriction. If in Algorithm 3 we replace the condition of the while loop by $z_s \neq 0$, then this modified Algorithm 3 may also end with the last m_j, say m_s, being different from ± 1. Further, if such m_s admits a representation as $Q(x,y)$, then the formula

$$\begin{aligned} (2)\qquad (x^2+gxy+hy^2)(z^2+gzw+hw^2) =& (xz-hyw)^2+g(xz-hyw)\times\\ &\times(xw+yz+gyw)+\\ &+h(xw+yz+gyw)^2 \end{aligned}$$

will provide a desired representation of $m = m_0$ for a larger number of forms $Q(x,y)$. First recall that in Algorithm 3

$$m_0 m_s^{(-1)^{s+1}} = x^2+gxy+hy^2.$$

where

$$\begin{aligned} x =& [m_s q_1, m_s^{-1}q_2, \ldots, m_s^{(-1)^{s-2}}q_{s-1}, m_s^{(-1)^{s-1}}q_s]\\ y =& [m_s^{-1}q_2, \ldots, m_s^{(-1)^{s-2}}q_{s-1}, m_s^{(-1)^{s-1}}q_s] \end{aligned}$$

Then, to recover the representation of m_0 (associated with z_0) we just need to expressed m_s or $-m_s$ as $Q(x,y)$. This simple modification of Algorithm 3 will provide proper representations $Q(x,y)$ of $\pm m$ for some forms Q with discriminant $\Delta > 0$ and $H(\Delta) = 1$ (see [15]). The following two examples illustrate this idea. Recall the condition of the while loop is now $z_s \neq 0$.

For the ring $\mathbb{Z}[(1+\sqrt{17})/2]$ the form is $x^2 + xy - 4y^2$. Take $m_0 = 3064$ and $z_0 = 564$. Noticing $3064 \cdot 104 = 564^2 + 564 - 4$, the division gives

$$\begin{aligned} 3064 \cdot 104 = 564^2 + 564 - 4 \quad &\rightarrow \quad 564 = 5 \cdot 104 + 44 \\ 104 \cdot 19 = 44^2 + 44 - 4 \quad &\rightarrow \quad 44 = 2 \cdot 19 + 6 \\ 19 \cdot 2 = 6^2 + 6 - 4 \quad &\rightarrow \quad 6 = 3 \cdot 2. \end{aligned}$$

Thus, we have $s = 3$, $m_3 = 2$ and $(q_3, q_2, q_1) = (5, 2, 3)$. From this we recover the continuant representation of $m_0 \cdot 2 = 6128$

$$6128 = \det \begin{bmatrix} 10 & 1 & & & & \\ -1 & 1 & 1 & & & \\ & -1 & 6 & 1 & & \\ & & 4 & 6+1 & 1 & \\ & & & -1 & 1 & 1 \\ & & & & -1 & 10 \end{bmatrix}$$

The representation $Q(x,y)$ of 6128 is given by $x = [2 \cdot 3, 2^{-1} \cdot 2, 2 \cdot 5] = 76$ and $y = [2^{-1} \cdot 2, 2 \cdot 5] = 11$. Note that $2 = 2^2 + 2 \cdot 1 - 4 \cdot 1^2$. Using Equation (2) in the form $3064 \cdot (2^2 + 2 \cdot 1 - 4 \cdot 1) = 76^2 + 76 \cdot 11 - 4 \cdot 11^2$, we conclude that $3064 = 92^2 + 92 \cdot (-27) - 4(-27)^2$.

For the ring $\mathbb{Z}[\sqrt{6}]$ the form is $Q(x,y) = x^2 - 6y^2$. Take $m_0 = 37410$ and $z_0 = 1326$. Noticing $37410 \cdot 47 = 1326^2 - 6$, the division gives

$$\begin{aligned} 37410 \cdot 47 = 1326^2 - 6 \quad &\rightarrow \quad 1326 = 28 \cdot (47) + 10 \\ 47 \cdot 2 = 10^2 - 6 \quad &\rightarrow \quad 10 = 5 \cdot 2. \end{aligned}$$

Thus, we have $s = 2$, $m_2 = 2$ and $(q_2, q_1) = (28, 5)$. The representation $Q(x,y)$ of $37410 \cdot 2^{-1}$ is $x = [2 \cdot 5, 2^{-1} \cdot 28] = 141$ and $y = [2^{-1} \cdot 28] = 14$. Note that $-2 = 2^2 - 6 \cdot 1^2$. Using Equation (2) in the form $(141^2 - 6 \cdot 14^2)(2^2 - 6 \cdot 1^2) = -37410$, we have that $-37410 = 366^2 - 6 \times 169^2$.

Below we present some of the forms $Q(x,y)$ for which the proposed modification of Algorithm 3 will give the representation of m_0 associated with the given z_0.

The forms are given in the format $(Q, \{\text{list of possible } m_s\text{'s}\})$. Note that m_s is a divisor of h and that, for every case, either m_s or $-m_s$ is represented by the form.

$(x^2 - 2y^2, \{\pm 1, \pm 2\})$	$(x^2 + xy - 4y^2, \{\pm 1, \pm 2, \pm 4\})$
$(x^2 - 3y^2, \{\pm 1, \pm 3\})$	$(x^2 + xy - 7y^2, \{\pm 1, \pm 7\})$
$(x^2 - 6y^2, \{\pm 1, \pm 2, \pm 3, \pm 6\})$	$(x^2 + xy - 9y^2, \{\pm 1, \pm 3, \pm 9\})$
$(x^2 - 7y^2, \{\pm 1, \pm 7\})$	$(x^2 + xy - 10y^2, \{\pm 1, \pm 2, \pm 5, \pm 10\})$
$(x^2 + xy - y^2, \{\pm 1\})$	$(x^2 + xy - 13y^2, \{\pm 1, \pm 13\})$
$(x^2 + xy - 3y^2, \{\pm 1\})$	$(x^2 + xy - 15y^2, \{\pm 1, \pm 3, \pm 5, \pm 15\})$

Recall that Mathews [13] provided representations of certain integers as $x^2 - hy^2$, where $h = 2, 3, 5, 6, 7$. From the previous remarks it follows that the modified Algorithm 3 covers all the cases studied by Mathews [13]. Observe that the form $x^2 - 5y^2$, studied in [13] and associated with the non-principal ring $\mathbb{Z}[\sqrt{5}]$, has been superseded by the form $x^2 + xy - y^2$ associated with the integral closure of $\mathbb{Z}[\sqrt{5}]$, that is, $\mathbb{Z}[(1 + \sqrt{5})/2]$.

Unsatisfactorily, our algorithm does not terminate for every $\Delta > 0$ with $H(\Delta) = 1$. For instance, take $\Delta = 73$, $m_0 = 267$ and $z_0 = 23$. The corresponding quadratic form is $x^2 + xy - 18y^2$, and we have that $267 = (-69)^2 + (-69) \cdot 14 - 18 \cdot 14^2$ and $267 | 23^2 + 23 - 18$.

Furthermore, a minor modification of Algorithm 3 can also provide alternative proofs to Propositions 2 and 3.

The approach presented in the paper is likely to work for other representations if new modified continuants are defined.

Mathematica®[23] implementations of most of the algorithms presented in the paper and other related algorithms are available at

`http://guillermo.com.au/wiki/List_of_Publications`

under the name of this paper.

REFERENCES

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

[2] D. A. Buell, *Binary quadratic forms. Classical theory and modern computations*, Springer-Verlag, New York, 1989.

[3] M. D. Choi, T. Y. Lam, B. Reznick, and A. Rosenberg, *Sums of squares in some integral domains*, Journal of Algebra **65** (1980), 234–256.

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

[5] G. Cornacchia, *Su di un metodo per la risoluzione in numeri interi dell' equazione* $\sum_{h=0}^{n} C_h x^{n-h} = P$, Giornale di Matematiche di Battaglini **46** (1908), 33–90.

[6] C. Delorme and G. Pineda-Villavicencio, *Continuants and some decompositions into squares*, (2012), `http://arxiv.org/abs/1112.4535`.

[7] C. L. Dodgson, *Condensation of determinants, being a new and brief method for computing their arithmetical values*, Proceedings of the Royal Society of London **15** (1866), 150–155.

[8] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A foundation for computer science*, 2nd ed., Addison-Wesley, New York, 1994.

[9] 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, Mathematics of Computation **55** (1990), no. 191, 327–343, doi:10.2307/2008809.

[10] C. Hermite, *Note au sujet de l'article précédent*, Journal de Mathématiques Pures et Appliquées **5** (1848), 15.

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

[12] M. A. Jodeit, Jr., *Uniqueness in the division algorithm*, The American Mathematical Monthly **74** (1967), 835–836.

[13] K. Matthews, *Thue's theorem and the Diophantine equation* $x^2 - Dy^2 = \pm N$, Mathematics of Computation **71** (2002), no. 239, 1281–1286.

[14] OEIS Foundation Inc., *Sequence A014602*, The On-Line Encyclopedia of Integer Sequences, `http://oeis.org/A014602`, 2013.

[15] OEIS Foundation Inc., *Sequence A003655*, The On-Line Encyclopedia of Integer Sequences, `http://oeis.org/A003655`, 2013.

[16] G. Rabinowitsch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*, Journal für die reine und angewandte Mathematik **142** (1913), 153–164.

[17] P. Samuel, *Algebraic Theory of Numbers*, Houghton Mifflin Co., Boston, Mass., 1970, Translated from the French by A. Silberger.

[18] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod* p, Mathematics of Computation **44** (1985), 483–494.

[19] J. A. Serret, *Sur un théorème relatif aux nombres entiers*, Journal de Mathématiques Pures et Appliquées **5** (1848), 12–14.

[20] S. Wagon, *Editor's corner: the Euclidean algorithm strikes again*, The American Mathematical Monthly **97** (1990), 125–129.

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

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

[23] Wolfram Research, Inc., *Mathematica Edition: Version 8.0*, Wolfram Research, Inc., Champaign, IL, 2010.

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

E-mail address: cd@lri.fr

CENTRE FOR INFORMATICS AND APPLIED OPTIMISATION, FEDERATION UNIVERSITY AUSTRALIA

E-mail address: work@guillermo.com.au