Scientific Research Publishing

Applied Mathematics, 2024, 15, 614-629
https://www.scirp.org/journal/am
ISSN Online: 2152-7393
ISSN Print: 2152-7385

Representation of an Integer by a Quadratic Form through the Cornacchia Algorithm

Moumouni Djassibo Woba

Training and Research Unit/Sciences and Technology, University of Ouahigouya, Mèra, Burkina Faso
Email: moumouniabdoulwoba@gmail.com

How to cite this paper: Woba, M.D. (2024) Representation of an Integer by a Quadratic Form through the Cornacchia Algorithm. *Applied Mathematics*, **15**, 614-629.
https://doi.org/10.4236/am.2024.159037

Received: August 1, 2024
Accepted: September 9, 2024
Published: September 12, 2024

Abstract

Cornachia's algorithm can be adapted to the case of the equation $x^2+dy^2=n$ and even to the case of $ax^2+bxy+cy^2=n$. For the sake of completeness, we have given modalities without proofs (the proof in the case of the equation $x^2+y^2=n$). Starting from a quadratic form with two variables $f(x,y)=ax^2+bxy+cy^2$ and n an integer. We have shown that a primitive positive solution (u,v) of the equation $f(x,y)=n$ is admissible if it is obtained in the following way: we take α modulo n such that $f(\alpha,1)\equiv 0 \bmod n$, u is the first of the remainders of Euclid's algorithm associated with n and α that is less than $\sqrt{4cn/|D|}$) (possibly α itself) and the equation $f(x,y)=n$. has an integer solution u in *y*. At the end of our work, it also appears that the Cornacchia algorithm is good for the form $n=ax^2+bxy+cy^2$ if all the primitive positive integer solutions of the equation $f(x,y)=n$ are admissible, *i.e.* computable by the algorithmic process.

Keywords

Quadratic Form, Cornacchia Algorithm, Associated Polynomials, Euclid's Algorithm, Prime Number

1. Introduction

Quadratic forms are used in many fields of mathematics: different results for the classification of conics and then generally quadratics, search for local minimum or maximum of a function of several variables from a limited expansion, introduction of surface curvature, principal component analysis in statistics. Integer quadratic forms are used in number theory and topology [1].

Let p be an odd prime. -1 is a square modulo p if and only if $p\equiv 1 \bmod 4$. Thus, if p is a prime number that can be written as the sum of two squares (of integers), it is congruent to 1 mod 4: indeed, if $p = x^2 + y^2$,x and y are necessarily prime to p and we have $(x/y)^2 \equiv -1 \bmod p$. The converse is true, which we will demonstrate by giving algorithms that compute integers x. and y such that $x^2 + y^2 = p$ [2].

In mathematics, the Cornacchia algorithm is a procedure for solving certain Diophantine equations generalizing the Pell-Fermat equation. This algorithm is named after the Italian mathematician Giuseppe Cornacchia who introduced it in 1908 and sometimes also attributed to the Vilandic mathematician Henry Smith, under the name of the Cornacchia-Smith algorithm [3].

More specifically, the algorithm provides a solution between (x, y) of the equation $x^2 + dy^2 = m$, where $1 \ll d \ll m$, and the integers d and m are prime to each other. This algorithm is of major practical interest, because it makes it possible to find a representation of a first P as the norm of an element of a quadratic extension, an essential step for example in the proof of primality by elliptic curves [4].

Another important use of the Cornacchia algorithm is the generation of elliptic curves with complex multiplication [5].

For this task, the Cornacchia algorithm is more efficient than generic methods based on quadratic forms or Euclidean lattice reduction to [François Morain “Implementing the asymptotically fast version of thé elliptie curve primalty proving algorithme”].

We will then look at the more general problem of “representing” a prime number by a two-variable quadratic form. Before we start, let’s notice that our problem is not empty, there are prime numbers ≡1 mod 4. There are even an infinity of them because if n is an integer, a prime factor of $n!^2+1$ (which exists!) is necessarily greater than n and congruent to 1 mod 4; So there is an arbitrarily large prime number ≡1 mod 4.

2. Writing a Prime Number ≡ 1 Mod 4 as the Sum of Two Squares

Let’s fix a prime number $p \equiv 1$ mod 4. Let us give a first algorithm for finding integers x and y such that

$$x^2 + y^2 = p \tag{1}$$

We start from an integer a such that $a^2 + 1 = mp$ with m a positive integer that we can assume < p (for example by taking $a \le (p-1)/2$, we even then have $m \le (p-1)/4$. Let us suppose $m \ne 1$. Let $x_0 = a$ and $y_0 = 1$. Let x_1 and y_1 represent them of minimum x_0 and y_0 modulo m in absolute value. As
$x_1^2 + y_1^2 \equiv 0 \bmod m$, we write $x_1^2 + y_1^2 = mm'$ with $m' \le m/2$, hence

$$\left(x_0^2 + y_0^2\right)\left(x_1^2 + y_1^2\right) = m'm^2 p. \tag{2}$$

We check using $|z_0 z_1| = |z_0||z_1|$ remarkable identity

$$\left(x_0^2 + y_0^2\right)\left(x_1^2 + y_1^2\right) = \left(x_0 x_1 + y_0 y_1\right)^2 + \left(x_0 y_1 - x_1 y_0\right)^2.$$

The terms of the right-hand side checking

$$x_0x_1 + y_0y_1 \equiv x_0^2 + y_0^2 \equiv 0 \bmod m.$$

$$x_0y_1 - x_1y_0 \equiv 0 \bmod m \qquad (3)$$

So if $x_2 = (x_0x_1 + y_0y_1)/m$ and if $y_2 = (x_0y_1 - x_1y_0)/m$, we have a $x_1^2 + y_1^2 = m'p$ with $m' \le m/2$. All that remains is to start again by replacing *m* by *m*' and x_0, y_0 by x_2, y_2. We have obtained a solution of the equation $x^2 + y^2 = p$ if we obtain the value $m = 1$. Let's check it out. Since the *m* (and *m*') form a strictly decreasing sequence of positive integers, we necessarily obtain $m' = 1$ or $m' = 0$.

Let us show that if $m' = 0$, *m* is necessarily equal to 1. Indeed, this implies with the previous notations in the corresponding step that x_0 and y_0 are both divisible by m and therefore since $x_0^2 + y_0^2 = mp$, the integer *m* must divide *p*. If *p* is prime, this implies that $m = 1$ [6].

We have thus obtained an integer solution of the equation $x_0^2 + y_0^2 = p$. (We will call this algorithm *descending algorithm* in the following, it closely follows Euler's proof which is based on Fermat's principle of making "descend" in positive integers). The number of steps is increased by $\log_2(m)$.

3. Representation of a Prime Number by a Quadratic Form with Two Variables

3.1. Definition 1

If $f(x, y)$ is a quadratic form with integer coefficients, *f* is said to *represent p* if there are integers *x* and *y* such that $f(x, y) = p$. All that remains is to persuade yourself that you have verified the following theorem for a prime number $p < 1000$ and different from 2 and 5.

3.2. Theorem 1

-5 is a square modulo *p* if and only if *p* is represented by $x^2 + 5y^2$ or by $2x^2 + 2xy + 3y^2$. The proof of this fact for any prime number, already stated by Fermat, goes back to Euler. There are two parts to the proof: the first part uses *Legendre's quadratic law of reciprocity*: if *p* and *q* are two distinct odd primes, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.

3.3. Example 1

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{(p-1)/2}\left(\frac{5}{p}\right)$$

In the following, **a form will be a quadratic form** $ax^2 + bxy + cy^2$ with *a*, *b*, and *c* integers prime to each other, $a > 0$.

3.4. Definition 2

We say that a form *f* properly represents an integer *m* if there are integers *u* and *v* prime to each other such that $f(u,v)=m$. Such a solution (u,v) is then said to be primitive.

3.5. Definition 3

Two forms $f(x,y)$ and $g(x,y)$ are said to be equivalent (or properly equivalent) if there are integers u,v,w and t such that $f(x,y)=g(ux+vy,wx+ty)$ and $ut-vw=\pm 1$ (resp. $ut-vw=1$). These are equivalence relationships.

3.6. Lemma 1

A form $f(x,y)$ properly represents an integer m if and only if $f(x,y)$ is properly equivalent to a form of the type $mx^2+bxy+cy^2$ for b and c suitable. Indeed, suppose that there are you and v prime to each other such that $f(x,y)=m$. By Bézout's theorem, there exists w and t such that $uw-vt=1$ and $f(ux+ty,vx+wy)$ is of the form $mx^2+axy+cy^2$. The reverse is clear.

3.7. Definition 4

We call the discriminant of the form $ax^2+bxy+cy^2$ the integer $D=b^2-4ac$ [7].

3.8. Remark 1

- Two equivalent forms have even discriminating.
- D is congruent to b^2 modulo 4 and therefore D is congruent to 0 or 1 modulo 4.

3.9. Lemma 2

Let D be an integer $\equiv 0$ or 1 mod 4 and m an odd integer prime to D. Then there is a form of discriminant D properly representing m if and only if D is a square modulo m.

Indeed, if there is a form properly representing m, we can take it of the type $f(x,y)=mx^2+bxy+cy^2$. Its discriminant $=b^2-4mc$ is indeed a square modulo m.

Conversely, suppose that D is a square modulo m: $D\equiv b^2 \bmod m$ with $b\in\mathbb{Z}$ Its discriminant $D=b^2-4mc$ is indeed a square modulo m: $D\equiv b^2 \bmod m$ with $b\in\mathbb{Z}$. Since m is odd, we can take b and D of the same parity (even if it means changing b to $b+m$). Like $D\equiv 0$ or 1 mod 4, we then have
$D\equiv b^2 \bmod 4m$.

Let c be the integer such that $D=b^2-4mc$. Then, $mx^2+bxy+cy^2$ properly represents m and the integers $a=m,b$ and c are prime to each other because m is prime with D. We deduce the result of the following corollary: [8].

3.10. Corollary 1

Let n be an integer and p an odd prime that does not divide n. Then p is represented by a form of discriminant-4m if and only if $\left(\frac{-n}{p}\right)=1$.

Let's go back to the forms $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ of discriminant-20. To show the following theorem, all that remains is to show that the forms of discriminant-20 are all properly equivalent to one of the two forms $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$.

3.11. Theorem 2

-5 is a square modulo p if and only if p is represented by par $x^2 + 5y^2$ or by $2x^2 + 2xy + 3y^2$.

3.12. Theorem 3

An odd prime p prime to 5 is represented by $x^2 + 5y^2$ si and only if $p \equiv 1$ or 9 mod 20, it is represented by $2x^2 + 2xy + 3y^2$ if and only if $p \equiv 3$ or 7 mod 20.

Let's go back to the shape equivalence classes.

3.13. Definition 5

A form $ax^2 + bxy + cy^2$ of a negative discriminant is said to be reduced if $|b| \le a \le c$ and $b \ge 0$ in cases where $|b| = a$ or $a = c$. There is only a finite number of reduced forms of the discriminant $D < 0$ given (we have indeed $-D = 4ac - b^2 \ge 4a^2 - a^2 = 3a^2$ and therefore $a \le \sqrt{\frac{-D}{3}}$, there is a finite number of a and b and therefore of c since $b^2 - 4ac = D$).

3.14. Theorem 3

Any form of negative discriminant is properly equivalent to a single reduced form. Thus, the set of equivalence classes $C(D)$ (for proper equivalence) of the given discriminant forms is finite [9].

The cardinal $h(D)$ of $C(D)$ is called the number of classes of discriminant D.

4. A Look Back at the Algorithms

Cornachia's algorithm can be adapted to the case of the equation $x^2 + dy^2 = n$ and even to the case of $ax^2 + bxy + cy^2 = n$.

Let $f(x, y) = ax^2 + bxy + cy^2$ be a form and n an integer. We say that a primitive positive solution (u, v) of the equation $f(x, y) = n$ is admissible if it is obtained in the following way: we take α modulo n such that $f(\alpha, 1) \equiv 0 \bmod n$, u is the first of the remainders of Euclid's algorithm associated with n and α that is less than $\sqrt{4cn/|D|}$) (possibly α itself) and the equation $f(x, y) = n$ has an integer solution v in y [10].

We will say that Cornacchia's algorithm is good for the form $n = ax^2 + bxy + cy^2$ if all the primitive positive integer solutions of the equation $f(x, y) = n$ are admissible, *i.e.* computable by the algorithmic process we have just described.

Theorem 4

The Cornacchia algorithm is good in the following cases:

1) $n = x^2 + dy^2$ with d and n positive integers;

2) $n = ax^2 + bxy + cy^2$ and $a > 0$, $c > 0$, $D = b^2 - 4ac < 0$, $|D| > 16$ et $|b| \le \dfrac{|D| - 16}{8}$ and n integer ≥ 2sup(a, c).

So, Cornacchia's algorithm is good for f and n and if you can't find any qualifying pairs, The equation $n = f(x, y)$ has no integer solutions.

5. Proof of the Cornacchia Algorithm in the Case of the Equation $x^2 + y^2 = a$

5.1. Theorem 5

Let a be an integer such as −1 or a square mod a. If b is an integer verifying $0 \le b \le a/2$ et $b^2 \equiv -1 \bmod a$, the first two remainder $< \sqrt{a}$ in the algorithm of Euclidean division of a by b give a primitive solution of the equation $x^2 + y^2 = a$. Moreover, all primitive solutions are obtained in this way. A trivial transformation is one of the transformations $(x, y) \mapsto (\pm x; \pm y)$ ou $(x, y) \mapsto (\pm y; \pm x)$. A primitive solution of the equation is a solution (x, y) with x and y primes between them [11].

5.2. Some Polynomials Associated with Euclid's Algorithm

Consider the sequence of equations

$$\begin{cases} r_0 = q_1 r_1 + r_2 \\ r_{i-1} = q_i r_i + r_{i+1} \\ r_{n-1} = q_n r_n + r_{n+1} \end{cases} \tag{4}$$

It is easy to see that by substitution, we can write

$$r_0 = f_n(q_1, \cdots, q_n) r_n + g_{n-1}(q_1, \cdots, q_{n-1}) r_{n+1} \tag{5}$$

where the f_m and g_m are polynomials in $q_1, \cdots, q_n$ of partial degree 1 in relation to each of the q_i.

Relationships

$$r_0 = f_{n-1}(q_1, \cdots, q_{n-1}) r_{n-1} + g_{n-2}(q_1, \cdots, q_{n-1}) r_n$$

$$r_{n-1} = q_n r_n + r_{n+1}$$

Implies that:

$$r_0 = \left(f_{n-1}(q_1, \cdots, q_{n-1}) q_n + g_{n-2}(q_1, \cdots, q_{n-1}) \right) r_n + f_{n-1}(q_1, \cdots, q_{n-1}) r_{n+1} \tag{6}$$

We deduce that $g_{n-1} = f_{n-1}$ and therefore that

$$r_0 = f_n(q_1, \cdots, q_n) r_n + f_{n-1}(q_1, \cdots, q_{n-1}) r_{n+1} \tag{7}$$

The polynomial f_n has the property

$$f_n(q_1, \cdots, q_n) = f_n(q_n, \cdots, q_1)$$

Indeed, we have

$$\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$$

Thus, $f_n(q_1,\cdots,q_n)$ is the coefficient at the top left of the matrix

$$\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}$$

This coefficient is also that of its transpose (in the same place) which is equal to $\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$ and is $f_n(q_1,\cdots,q_n)$. We can explicitly compute $f_1,\cdots,f_7$ with MAPLE using the recurrence relation: $f_n = f_{n-1}q_n + f_{n-2}$. We find

$$\begin{cases} f_1 = q_1 \\ f_2 = q_2q_1 + 1 \\ f_3 = q_3q_2q_1 + q_3 + q_1 \\ f_4 = q_4q_3q_2q_1 + q_4q_3 + q_4q_1 + q_2q_1 + 1 \\ f_5 = q_5q_4q_3q_2q_1 + q_5q_4q_3 + q_5q_4q_1 + q_5q_2q_1 + q_3q_2q_1 + q_5 + q_3 + q_1 \\ f_6 = q_6q_5q_4q_3q_2q_1 + q_6q_5q_4q_3 + q_6q_5q_4q_1 + q_6q_5q_2q_1 + q_6q_3q_2q_1 \\ \qquad + q_4q_3q_2q_1 + q_6q_5 + q_6q_3 + q_6q_1 + q_4q_3 + q_4q_1 + q_2q_1 + 1 \\ f_7 = q_7q_6q_5q_4q_3q_2q_1 + q_7q_6q_5q_4q_3 + q_7q_6q_5q_4q_1 + q_7q_6q_5q_2q_1 \\ \qquad + q_7q_6q_3q_2q_1 + q_7q_4q_3q_2q_1 + q_5q_4q_3q_2q_1 + q_7q_6q_5 + q_7q_6q_3 \\ \qquad + q_7q_6q_1 + q_7q_4q_3 + q_7q_4q_1 + q_7q_2q_1 + q_5q_4q_3 + q_5q_4q_1 \\ \qquad + q_5q_2q_1 + q_3q_2q_1 + q_7 + q_5 + q_5 + q_1 \end{cases}$$ [12]

It will be noted that the monomials involved in f_n are exactly those obtained by removing from $q_1,\cdots,q_n$ a certain number of successive pairs of elements $(q_i,\cdots,q_{i+1})$.

If $1 < m < n$, we have

$$\begin{aligned} r_m &= f_{n-m}(q_{m+1},\cdots,q_n)r_n + f_{n-m-1}(q_{m+1},\cdots,q_{n-1})r_{n+1} \\ r_{m+1} &= f_{n-m-1}(q_{m+2},\cdots,q_n)r_n + f_{n-m-2}(q_{m+2},\cdots,q_{n-1})r_{n+1} \\ r_0 &= f_m(q_1,\cdots,q_m)r_m + f_{m-1}(q_1,\cdots,q_{m-1})r_{m+1} \end{aligned} \tag{8}$$

It is easy to deduce that:

$$\begin{aligned} & f_n(q_1,\cdots,q_n) \\ & = f_m(q_1,\cdots,q_m)f_{n-m}(q_{m+1},\cdots,q_n) + f_{m-1}(q_1,\cdots,q_{m-1})f_{n-m-1}(q_{m+2},\cdots,q_n) \end{aligned} \tag{9}$$

Particular case

Suppose that n is even and that $(q_1,\cdots,q_n) = (q_n,\cdots,q_1)$, that is, that is, $q_i = q_{n+1-i}$.

For $m = \frac{n}{2}$, the equation becomes:

$$\begin{aligned} & f_n(q_1,\cdots,q_n) \\ & = f_{\frac{n}{2}}\left(q_1,\cdots,q_{\frac{n}{2}}\right) f_{\frac{n}{2}}\left(q_{\frac{n}{2}+1},\cdots,q_n\right) + f_{\frac{n}{2}-1}\left(q_1,\cdots,q_{\frac{n}{2}-1}\right) f_{\frac{n}{2}-1}\left(q_{\frac{n}{2}+2},\cdots,q_n\right) \end{aligned}$$

$$f_n(q_1,\cdots,q_n) = f_{\frac{n}{2}}\left(q_1,\cdots,q_{\frac{n}{2}}\right)^2 + f_{\frac{n}{2}-1}\left(q_1,\cdots,q_{\frac{n}{2}-1}\right)^2 = f_{\frac{n}{2}}\left(q_n,\cdots,q_{\frac{n}{2}+2}\right)^2$$

$$\text{Either}\quad f_n\left(q_1,\cdots,q_n\right)=f_{\frac{n}{2}}\left(q_{\frac{n}{2}+1},\cdots,q_n\right)^2+f_{\frac{n}{2}-1}\left(q_{\frac{n}{2}+2},\cdots,q_n\right)^2$$

5.3. Properties of Euclid's Algorithm

Let a and b now be two positive integers prime to each other with $b<a$. The sequence of the quotients associated with (a,b) is the sequence of successive quotients obtained by applying Euclid's algorithm to a and b: we set $r_0=a$, $r_1=b$ and then we define by recurrence

$$q_i=\left[r_{i-1}/r_i\right]\text{ et } r_{i+1}=r_{i-1}q_ir_i \tag{10}$$

We denote n the integer such that $r_n=pgcd(a,b)=1$ and we call it the length of the algorithm. So we have $r_{i-1}=0$.

We define another sequence of integers t_i by:

$$t_0=0,t_1=1\text{ et } t_{i+1}=t_{i-1}-q_it_i\text{ by } i=1,\cdots,n+1$$

We then have the ties:

$$r_i=s_ia+t_ib$$

If s_i is the sequence defined by the same recurrence relation and first terms 1 and 0. By recurrence, it is easy to see that the t_i are of alternating sign, more precisely $|t_i|=(-1)^{i-1}t_i$.

Hence the relationship

$$|t_{i+1}|=|t_{i-1}|+q_i|t_i| \tag{11}$$

The rest of the $|t_i|$ is therefore increasing. Thus, we can see the $|t_{i+1-i}|$ as the sequence of successive remainders in Euclid's algorithm applied to $|t_{i+1}|$ and $|t_i|$. Since $r_{i+1}=0$ and a and b are prime to each other, for $i=n+1$ indicates that a divides $r_{n+1}=0$. We actually have $|t_{n+1}|=a$ because $|t_{n+i}|=f_n\left(q_n,\cdots,q_1\right)=f_n\left(q_1,\cdots,q_n\right)=a$ What can we say now about $|t_n|$? we have $t_n<a$ et $bt_n\equiv 1\bmod a$.

5.4. Theorem 6

Let a and b be two integers with $b<a/2$. The sequence of successive quotients in Euclid's algorithm (of length n) starting with a and b is symmetric if and only if $b^2\equiv\pm 1\bmod a$ and we then have $b^2\equiv(-1)^{n+1}\bmod a$ [13].

Let's prove the lemma. We have just seen that the sequence of $|t_i|$ is increasing, that the t_i are of alternating sign, with t_n of the sign of $(-1)^{n+1}$, and that $|t_{i+1}|=a$.

Suppose $b^2\equiv\varepsilon\bmod a$ with $\varepsilon=\pm 1$.

Show that $|t_n|=\varepsilon b$. We notice that $t_nb\equiv 1\bmod a$. Like $b^2\equiv\varepsilon\bmod a$, we deduce that $t_n\equiv\varepsilon b\bmod a$. Moreover, $|t_n|<|t_{n+1}|=a$, therefore $|t_n|=\varepsilon b$ where $|t_n|=\varepsilon(b-a)$.

Suppose $t_n=\varepsilon(b-a)$. Wich means $|t_n|=a-b$. The euclidian division of $|t_{n+i}|=a$ par $|t_n|=a-b$ gives

$$|t_{n+i}|=|t_n|+b$$

Since $b < a - b$. So $\left|t_{n+i}\right| = b$ and we have

$$a = (a-b) + \left|t_{n-i}\right|$$

$$a - b = q_{n-1} b + \left|t_{n-2}\right|$$

$$b = q_{n-2}\left|t_{n-2}\right| + \left|t_{n-3}\right|$$

From where

$$a = (q_{n-1}+1)b + \left|t_{n-2}\right|$$

$$b = q_{n-2}\left|t_{n-2}\right| + \left|t_{n-3}\right|$$

Euclid's algorithm of *a* by *b* would be of length $n-1$. Contradiction, so $t_n = \varepsilon b$. It is then clear that the sequences $(q_1,\cdots,q_n)$ and $(q_n,\cdots,q_1)$ are equa. In addition, we have $\varepsilon = (-1)^{n+1}$. Let us now suppose the sequences $(q_1,\cdots,q_n)$ and $(q_n,\cdots,q_1)$ equal. So we have $\left|t_{n+1}\right| = a$ and $t_n = (-1)^{n+1} b$. We also always have $t_n b \equiv 1 \bmod a$ which implies that $b^2 \equiv (-1)^{n+1} \bmod a$ and ends the proof of the lemma. Let's use the above to prove the theorem. A necessary condition for a primitive solution of the equation $x^2 + y^2 = a$ to exist is that 4 does not divide a and that all odd primes dividing a are congruent to 1 mod 4 (this is a condition for −1 to be a square mod a). We now assume so. There is then an integer $b < \frac{a}{2}$ such that $b^2 \equiv -1 \bmod a$; Let's choose one.

By applying $f_n(q_1,\cdots,q_n) = f_{\frac{n}{2}}\left(q_{\frac{n}{2}+1},\cdots,q_n\right)^2 + f_{\frac{n}{2}-1}\left(q_{\frac{n}{2}+2},\cdots,q_n\right)^2$ and by denoting r_i the successive remainders as before, we obtain that the roots $r_{\frac{n}{2}}$ and $r_{\frac{n}{2}+1}$ check

$$a = r_{\frac{n}{2}}^2 + r_{\frac{n}{2}+1}^2$$

Although of course $0 \le r_{\frac{n}{2}} \le \sqrt{a}$.

Let us show that $r_{\frac{n}{2}}$ is the first remainder less than $\sqrt{a}$. Let us first note that for any integer *i*, we have

$$r_i^2 + r_{n+1-i}^2 \equiv 0 \bmod a$$

Indeed, as $t_i b \equiv r_i \bmod a$ and $b^2 \equiv -1 \bmod a$, by squaring, $t_i^2 + r_i^2 \equiv \bmod a$; since $t_i = r_{n+1-i}$, the congruence can be deduced from this. Suppose that there exists $m < \frac{n}{2}$ such that $r_m \le \sqrt{a}$. Then, $r_{n+1-m}^2 \le a$ and we necessarily have $r_m^2 + r_{n+1-m}^2 = a$. On the other hand, $r_m / r_{n+1-m}^2 \equiv b \bmod a \equiv r_{\frac{n}{2}} \big/ r_{\frac{n}{2}+1}$. All that remains is to show that with the nearest transformation by $(x,y) \mapsto (\pm x, \pm y)$ and $(x,y) \mapsto (\pm y, \pm x)$, there is only one solution (x,y) to the equation $x^2 + y^2 = a$ of quotient *x*/*y* mod has given, which will imply that $r_m = r_{\frac{n}{2}-1}$ and therefore $m = \frac{n}{2} - 1$. To do this, let's take two pairs (x,y) and (x',y') with $x < y$,

$x' < y'$ et $x/y \equiv x'/y' \bmod a$. So we have the equations $x^2 + y^2 = a$, $x'^2 + y'^2 = a$ and $xy' - x'y = ar$, for r an integer. Let us eliminate x' in the second equation. We easily obtain the equation $y'^2 - 2rxy' + ar^2 - y^2 = 0$ whose discriminant must be positive (and even a square in $\mathbb{Z}$); it is $\left(1-r^2\right)\beta^2$. We therefore necessarily have $r = 0$, or $r = \pm 1$. For $r = 0$, we get $y^2 = y'^2$, for $r = \pm 1$, we get $y' \pm x = 0$, which proves our assertion. In conclusion, we have shown that the different choices of b verifying $0 < b < a/2$ and $b^2 \equiv -1 \bmod a$ give the different primitive solutions of the equation $x^2 + y^2 = a$, with the nearest transformation by $(x, y) \mapsto (\pm x, \pm y)$ and $(x, y) \mapsto (\pm y, \pm x)$, in the following way: the solution is given by the first pair of remainders less than $\sqrt{a}$ in Euclid's algorithm of a by such a b. For an odd divisible only by prime numbers congruent to à 1 mod 4, we find $4 \cdot 2^{\lambda}$ solutions, where λ is the number of prime factors in the decomposition of n (if p is odd, -1 is a square in $\mathbb{Z}/p^S\mathbb{Z}$ if and only if $p \equiv 1 \bmod 4$ and then there are exactly two solutions; then use the Chinese remainder theorem).

6. What Is the Motivation for Adapting the Cornacchia Algorithm to More Complex Cases?

The adaptation of the Cornacchia algorithm for complex cases allows to gain in efficiency and speed during the calculations involved in various fields of Cryptography, which makes it an interesting tool to strengthen the security and performance of Cryptographic systems.

Examples 2

- Increased efficiency: The Cornacchia algorithm offers a more efficient approach than traditional methods to solving some complex problems related to number theory, such as calculating square roots modulo a composite number. This results in reduced computation times.
- Public Key Cryptography: This algorithm has its application in Public Key Cryptography schemes, such as RSA encryption and discrete logarithm-based digital signatures. Its use makes it possible to speed up these operations.
- Primality verification: it can be used to effectively test the primality of certain numbers, which is essential in many cryptographic protocols that rely on the use of prime numbers.
- Integer factorization: To ensure that factorization itself remains a complex computational challenge, the Cornacchia algorithm can help improve some factorization techniques, such as the known fraction method.

6.1. Some Examples of Applications of Cornacchia's Algorithm for Specific Quadratic Forms

- Quadratic form $x^2 + y^2$: The cornacchia algorithm can be used to find integers x and y that satisfy Fermat's equation $x^2 + y^2 = z^2$ where z is an integer.

This algorithm has been used to solve some such Fermat equations, such as $x^2 + y^2 = 61$.

- Quadratic form $ax^2 + by^2$: Cornacchia's algorithm can be adapted to solve equations of the form $ax^2 + by^2 = c$ where *a*, *b*, and *c* are integers. For example: *p* find solutions to the equation: $3x^2 + 5y^2 = 17$, we can use a modified version of Cornacchia's algorithm.
- Ternary binary quadrancy forms: The Cornacchia algorithm can also be used to solve equations of the form $ax^2 + by^2 + cy^2 = d$ where *a*, *b*, and *c* are integers. For example: we can use it to find solutions to the equation $2x^2 + xy + 3y^2 = 13$.
- Quadratic forms with Gaussian coefficients: The Cornacchia algorithm can be extended to quadratic forms defined on the ring of Gaussian integers, of the form $(a+b)^2$, where *a* and *b* are integers. This solves equations like $(3+2i)x^2 + (1-i)y^2 = (5+3i)$.

In any case, Cornacchia's algorithm provides a systematic way to find integer solutions to quadratic equations, exploiting the particular properties of each quadratic form. It is a very powerful tool in number theory. In any case, Cornacchia's algorithm provides a systematic way to find integer solutions to quadratic equations, exploiting the particular properties of each quadratic form. It is a very powerful tool in number theory.

6.2. Let's Discuss the Computational Complexity of the Cornacchia Algorithm

The Cornacchia algorithm is an efficient method for solving the Pell-Fermat equation, which has the following form: $x^2 - dy^2 = 1$ where *D* is a positive non-square integer. The computational complexity of the adapted Cornacchia algorithm depends mainly on two factors:

1) The size of the numbers involved in the calculation:

- The larger the numbers, the more time arithmetic operations (multiplication, division, etc.) take.
- The algorithmic complexity for basic operations on large numbers is usually logarithmic in the size of the numbers.

2) The number of iterations needed to find a solution:

- Cornacchia's algorithm proceeds by successive iterations until a solution is found.
- The number of iterations depends on the value of *D* and can vary greatly depending on the case.
- In general, the larger the *D*, the number of iterations will be large.

In conclusion, the complexity of the adapted Cornacchia algorithm can be characterized as follows:

➢ Complexity of arithmetic operations: $O(\log n)$, where *n* is the size of the manipulated numbers.

➢ Overall complexity: $O(k\log n)$, where *k* is the number of iterations needed to find a solution.

The actual complexity therefore depends heavily on the value of D and the size of the numbers involved. For relatively small D values, the adapted Cornacchia algorithm is usually very efficient and can be used to solve reasonably sized Pell-Fermat equations [14].

6.3. How Does Cornacchia's Algorithm Compare to the Algecta of Cornacchia Origin in Terms of Efficiency and Practice?

Let's go through a comparison between the adapted Cornacchia algorithm and the original one.

- ➢ Original Cornacchia algorithm
  - ▪ This algorithm was proposed by Giuseppe Cornacchia in 1908 to solve the Pell-Fermat equation.
  - ▪ It uses operations on integers and cont9inue fractions to find a solution.
  - ▪ Complexity of calculation: $O\left(\sqrt{D \log D}\right)$, where D is the coefficient of the Pell-Fermat equation.
  - ▪ Efficiency: very good for relatively small D values (e.g. $<10^6$).
  - ▪ Disadvantages: can become very slow for very large D values, and requires the calculation of the square root fractional portion of D.
- ➢ Adapted Cornacchia algorithm
  - ▪ This algorithm is an improved variant of the original algorithm, proposed more recently.
  - ▪ It uses operations only on integers, thus avoiding calculations with continuous fractions.
  - ▪ Computational complexity: $O(k \log n)$, where k is the number of iterations and n is the size of the numbers manipulated.
  - ▪ Efficiency: Generally faster than the original algorithm, especially for very large D values
- ❖ The advantages
  - ✓ Avoids calculations with continuous fractions, no more to implement.
  - ✓ Can be faster than the original algorithm, especially for very large D values.
  - ✓ Adaptable to solving other Diophantine equations.

In summary, the adapted Cornacchia algorithm is generally more efficient and more convenient to implement than the original algorithm, especially for very large D values. However, for relatively small D values, the two algorithms have similar performance.

7. Elaborating on the Criteria for Determining Whether a Primitive Positive Solution Is Admissible. Providing Clear Guidance and Rationale for These Criteria

The criteria for determining whether a primitive solution to the Pell-Fermat equation $x^2 - Dy^2 = 1$ is admissible are as follows:

1) Positivities of solutions

- ➢ The solutions (*x*, *y*) must be positive integers.
- ➢ Rationale: The Pell-Fermat equation describes a relationship between geometric quantities that must be positive (length, areas, etc).

2) Minimality of the solution

- Among all the possible solutions, we must identify the smallest solution in absolute value, called the primitive solution.
- Rationale: The original solution is the simplest and most fundamental, from which all other solutions can be generated.

3) Uniqueness of the primitive solution

- ✓ For a given value of *D*, there must be only one primitive solution.
- ✓ Rationale: If there were multiple primitive solutions, this would imply that there are several fundamentally different ways of solving the equation, which is not the case.

4) Pell condition

- The primitive solution (*x*, *y*) must satisfy the Pell condition $x^2 - Dy^2 = 1$.
- Justification: it is the very definition of the Pell-Fermat equation that we are trying to solve [15].

7.1. Guidelines for Verifying Whether a Solution Is Acceptable

1) Verify that the values of *x* and *y* are positive integers.

2) Calculate the product $x^2 - Dy^2$ and check that it is equal to 1.

3) Compare the candidate solution to already known solutions to identify the smallest in value.

4) Make sure that there are no other primitive solutions for the same value of *D*. By following these criteria, it can be guaranteed that the solution identified is the unique and fundamental primitive solution of the Pell-Fermat equation for the value of *D* considered.

7.2. Discussion of the Possible Range of Solutions for Given Quadratic Forms, Are There Any Constraints or Special Cases Where the Adapted Algorithm Does Not Work

The range of possible solutions for the equations of the quadratic form $x^2 - Dy^2 = 1$ (Pell-Fermat equation) depends on several factors.

1) Valeur of *D*

- ✓ For a given value of *D*, there are infinitely many solutions (*x*, *y*) satisfying the equation.
- ✓ However, among these solutions, there is only one primitive solution that is the smallest in value.
- ✓ From this primitive solution, we can generate all the solutions using recurrence formulas.

2) Sign of solutions

- The solutions x and y must be positive integers.
- There are therefore no negative solutions for this solution.

3) Solution size

- The larger the value of D, the larger the primitive solutions x and y can become.
- For example, for $D = 61$, the primitive solution is $(x, y) = (267.37)$.
- The larger D is, the more iterations are needed to find the primitive solution.

7.3. Regarding Constraints or Special Cases or Adapted of Cornacchia May Not Work

1) Ineligible D values.

- The adapted Cornacchia algorithm assumes that D is a positive non-square integer.
- If it is not, the algorithm will not be able to find solutions because the Pell-Fermat equation would have no solutions in this case.

2) Numerical precision problems.

- If the values of the variables of x and y become too large, they may exceed the maximum capacity of the numeric data types used by the implementation.
- This can cause overflow issues and prevent the algorithm from working properly.

To overcome these problems, it may be necessary to use arbitrarily precise calculation libraries or to adapt the algorithm to better handle very large values.

In summary: the range of possible solutions for the Pell-Fermat equations is very wide and depends mainly on the value of D. however, the adapted Cornacchia algorithm may encounter limitations when values become very large, requiring adaptations to ensure its robustness.

7.4. Let Us Give More Detailed Examples, Especially for Generalist Generative Forms, Which Could Help Illustrate the Application of the Cornacchia Algorithm. Then Discuss the Potential Applications of These Findings in Other or Related Areas of Mathematics That Can Provide Additional Context and Motivation for Research

1) Quadratic generating forms:

- Consider the quadratic form $Q(x,y)=x^2+xy+y^2$. Cornacchia's algorithm can be used to find all these integers x,y such that $Q(x,y)$ is a perfect square.
- For example, finding the solutions of $Q(x,y)=4$, the algorithm would give solutions $(x,y)=(0,\pm 2);(\pm 1,\pm 1);(\pm 2,0)$.
- This application has links with number theory and number geometry, especially in the study of quadratic forms and their representation by squares.

2) Cubic generating forms.

- ✓ Let the cubic form $C(x,y,z)=x^3+y^3+z^3$. Cornacchia's algorithm can be used to find triples (x,y,z) such that $C(x,y,z)$ is a perfect square.
- ✓ For example, we can find that $C(1,1,-1)=1$ is a perfect square thus giving a non-trivial solution.
- ✓ This application has links to number theories, Diophantine numbers and the search for integer solutions for cubic equations.

3) Higher-order generative forms.

- More generally, we can consider higher-order generative forms such as $f(x,y,z,t)=x^4+y^4+z^4+t^4$.
- Cornacchia's algorithm can also be applied to find quadruplets (x,y,z,t) such that $f(x,y,z,t)$ is a perfect square. These results are part of a broader result of the theory of Diophantine equations and the search for integer solutions for polynomial equations.

7.5. Regarding the Potential Equations of These Results, We Can Mention

1) Number theory and number geometry.

✓ Quadratic, cubic, and order generative forms have direct links to the theory of quadratic and cubic forms, as well as number geometry.

✓ These results can contribute to a better understanding of the arithmetic properties of these forms and their representation by perfect squares.

2) Diophantine équations

- The search for integer solutions for polynomial equations is a central topic in Diophantine number theory.
- Applications of the Cornacchia algorithm to these generative forms can provide new tools and perspectives for the study of Diophantine equations.

3) Additive number theory.

❖ Generating forms can be related to problems in additive number theory, such as the representation of integers by sums of powers.

❖ Results obtained with the Cornacchia algorithm may shed new light on these questions.

4) Cryptography and number theory.

➢ Some cryptographic and code theory applications use arithmetic properties similar to those studied.

➢ The techniques developed by the Cornacchia algorithm could find applications in this field.

8. Conclusions

Cornacchia's algorithm is good for the form $n=ax^2+bxy+cy^2$ if all the primitive positive integer solutions of the equation $f(x,y)=n$ are admissible, *i.e.* computable by the algorithmic process. In addition, the Cornacchia algorithm is good in the following cases:

1) $n=x^2+dy^2$ with d and n positive integers;

2) $n=ax^2+bxy+cy^2$ and $a>0$, $c>0$, $D=b^2-4ac<0$, $|D|>16$ et $|b|\leq\frac{|D|-16}{8}$ and n integer ≥2sup(a, c).

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Serre, J.P. (1973) A Course in Arithmetc, Collection: Graduate Texts in Mathematics. Springer, 115.

[2] Serre, J.P. (1970) Cours d'Arithmétique. P.U.F., 123.

[3] Crandall, R. and Pomerance, C. (2005) Prime Numbers: A Computation Al Perspective. Spinger, 97.

[4] Morain, F. (2007) Implementing the Asymptotically Fast Version of the Elliptic Curve Primality Proving Algorithm. *Mathematics of Computation*, **76**, 493-505. https://doi.org/10.1090/S0025-5718-06-01890-4

[5] Blachut, R.E. (2014) Cryptography and sécure communication. Cambridge University Press, 602.

[6] Cohen, H. (1993) A Course in Computational Algebraic Number Teory. Springer, 234. https://doi.org/10.1007/978-3-662-02945-9

[7] Cox, D.A. (1989) Primes of the Form $x^2 + ny^{22}$, Fermat, Class Field Theory and Complex Multiplication. Wiley, 432.

[8] Hardy, K., Muskat, J.B. and Williams, K.S. (1990) Solving $n = au^2 + buv + cv^2$ Using the Euclidan Algorithm. *Utilitas Mathematica*, **38**, 225-236.

[9] Hardy, G.H. and Wright, E.M. (1969) An Introduction to the Theory of Numbers。5th Edition, Oxford Science Publications, 567。

[10] Wagon, S. (1990) Editor's Corner: The Euclidean Algorithm Strikes again. *The American Mathematical Monthly*, **97**, 125-129. https://doi.org/10.1080/00029890.1990.11995559

[11] Samuel, P. (1970) Théorie algébrique des nombres. Hermann, 282.

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

[13] Séroul, R. (1995) Math-info, Informatique pour mathématiciens. InterEditions, 321.

[14] Smith, H.J.S. (1855) De compositione numerorum primorum formae 4λ + 1 ex duobus qudratis. *Journal für die reine und angewandte Mathematik*, **1855**, 91-92. https://doi.org/10.1515/crll.1855.50.91

[15] Cohen, H. (1993) A Course in Computational Algebraic Number Theory. Spinger, 536. https://doi.org/10.1007/978-3-662-02945-9