On Cornacchia's algorithm for solving the diophantine equation $u^2 + dv^2 = m$

F. Morain [*†]
J.-L. Nicolas [‡]

September 12, 1990

Abstract

We give a new proof of the validity of Cornacchia's algorithm for finding the primitive solutions (u, v) of the diophantine equation $u^2 + dv^2 = m$, where d and m are two coprime integers. This proof relies on diophantine approximation and an algorithmic solution of Thue's problem.

1 Introduction

The first step in the Elliptic Curve Primality Proving algorithm [1] consists of finding the representation of a prime p as a norm in an imaginary quadratic field. In other words, we want to solve the diophantine equation

$$4p = x^2 + dy^2. \tag{1}$$

The most straightforward approach is to use reduction of quadratic forms [9] or lattice reduction [11]. In 1908, Cornacchia [3] gave a faster algorithm, using continued fractions. Since the original is neither easy to find nor easy to understand, we decided to give a more modern proof of his results, using diophantine approximation. (Another proof, quite unillimunating, can be found in [5].)

Cornacchia's algorithm is easy to describe. Let m and d two coprime integers. The solution of the problem

$$u^2 + dv^2 = m$$

in coprime integers u and v, if any, is given by the Euclidean algorithm applied to the pair (x_0, m) where x_0 is any root of $x^2 \equiv -d \bmod m$. Define the two sequences (a_n) and (r_n) as follows

$$\begin{array}{rcl} x_0 & = & a_0 \times m + r_0 \\ m & = & a_1 \times r_0 + r_1 \\ & \cdots & \\ r_i & = & a_{i+2} r_{i+1} + r_{i+2} \\ & \cdots & \end{array}$$

[*] Projet ALGO, Institut National de Recherche en Informatique et en Automatique, Domaine de Voluceau, B. P. 105, 78153 LE CHESNAY CEDEX (France) & Département de Mathématique, Université Claude Bernard, 69622 Villeurbanne CEDEX
[†] On leave from the French Department of Defense, Délégation Générale pour l'Armement.
[‡] Département de Mathématique, Université Claude Bernard, 69622 Villeurbanne CEDEX

and stop when $r_k^2 < m \leq r_{k-1}^2$. If the equation has a solution, it is

$$u = r_k \text{ and } v = \sqrt{\frac{m - r_k^2}{d}}.$$

The paper is organized as follows. Section 2 describes the successive reductions to a generalized version of Thue's problem and then to a problem related to diophantine approximation using continued fractions. Therefore, Section 3 reviews the classical theory of continued fractions as well as diophantine approximation. In Section 4, we give an algorithmic solution to Thue's problem. We then prove the validity of Cornacchia's algorithm in Section 5.

2 Statement of the problem

Let d and m be two coprime integers. We want to solve the following

Problem $\mathcal{P}$: find two coprime integers u and v such that

$$u^2 + dv^2 = m. \tag{2}$$

Let (u, v) be a solution. First, we remark that (2) implies that v is prime to m. Therefore

$$(u/v)^2 \equiv -d \bmod m$$

implies that $-d$ is a quadratic residue modulo m. Let x_0 be any squareroot of $-d$ modulo m. We deduce that

$$u + x_0 v \equiv 0 \bmod m, \tag{3}$$

and

$$0 < |u| < \sqrt{m}, 0 < v < \sqrt{\frac{m}{d}}. \tag{4}$$

In turn, this is related to the following problem.

Problem $\mathcal{T}$: given an integer m, find two coprime integers u and v such that

$$u + x_0 v \equiv 0 \bmod m, \text{ and } 0 < |u| < \sqrt{dm}, 0 < v < \sqrt{m/d}. \tag{5}$$

This problem is a generalized version of Thue's problem which was stated in [10] for the case $d = 1$. Suppose that (u, v) is a solution of (5). Then

$$u + x_0 v = km$$

for some integer k. (Note that k is prime to v.) Condition (5) implies

$$\left| v\frac{x_0}{m} - k \right| < \frac{1}{\sqrt{m/d}}.$$

So we are led to solve the following problem.

Problem $\mathcal{D}$: Let x be a real number. Compute the irreducible fractions p/q such that

$$|qx - p| < \frac{1}{Q}, \tag{6}$$

where Q is any positive real number and where we impose $q \leq Q$.

In Section 3, we will produce an efficient algorithm to solve Problem $\mathcal{D}$. This is to be compared with [6] which uses the same ideas but in a less understandable way. Before we do so, we must recall some properties of continued fractions.

3 Continued fractions

The material found below is taken form [7, Chapter 1] (see also [4, Chapter X]). Let x be a positive real number. Let us develop x as a continued fraction. Define the sequences (a_n) and (x_n) by

1. $a_0 = \lfloor x \rfloor$;
2. $x = a_0 + x_1$, $0 \le x_1 < 1$;
3. $\frac{1}{x_i} = a_i + x_{i+1}$ with $a_i = \lfloor \frac{1}{x_i} \rfloor$ and $0 \le x_{i+1} < 1$ for all i for which $x_i \neq 0$.

When $x = x_0/m$ is a rational number, these notations are coherent with that of the Euclidean algorithm applied to (x_0, m). For any integer n, we write

$$[a_0, a_1, \ldots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{\cdots + \frac{1}{a_n}}} = \frac{p_n}{q_n},$$

where (p_n) and (q_n) are two sequences defined recursively by

1. $p_{-2} = 0, p_{-1} = 1, p_n = a_n p_{n-1} + p_{n-2}$ for $n \ge 0$;
2. $q_{-2} = 1, q_{-1} = 0, q_n = a_n q_{n-1} + q_{n-2}$ for $n \ge 0$.

The rational p_n/q_n is said to be the *n-th convergent* of x. We define also the *intermediate convergents* $p_{n,r}/q_{n,r}$ for $1 \le r \le a_{n+2} - 1$

$$\begin{aligned} p_{n,r} &= r p_{n+1} + p_n, \\ q_{n,r} &= r q_{n+1} + q_n. \end{aligned}$$

From this it follows easily that for all n

$$\begin{aligned} p_n < p_{n,1} < \cdots < p_{n,a_{n+2}-1} < p_{n+2}, \\ q_n < q_{n,1} < \cdots < q_{n,a_{n+2}-1} < q_{n+2}. \end{aligned} \tag{7}$$

One can prove the following lemmas.

Lemma 3.1 (§1, pp. 4) *For all n, $q_n p_{n-1} - p_n q_{n-1} = (-1)^{n-1}$.*

From this, we conclude that p_n and q_n are prime together, making the fraction p_n/q_n irreducible.

If x is a rational number, then $a_n = 0$ for $n \ge n_0(x)$ and if x is not rational, then (a_n) is infinite. In each case, we put

$$a'_n = [a_n, \ldots, a_{n_0}]$$

if x is rational and

$$a'_n = [a_n, \ldots]$$

otherwise. With this notation, one has

$$a'_n = a_n + \frac{1}{a'_{n+1}}. \tag{8}$$

It is convenient to introduce the quantity

$$q'_n = a'_n q_{n-1} + q_{n-2}.$$

Using (8) and the recurrence relation for q_n, we see that

$$q'_{n+1} = a'_{n+1} q'_n, \tag{9}$$

for all n.

Let us now estimate the approximation of x by $p_{n,r}/q_{n,r}$.

Lemma 3.2 (§4, pp. 17) *For all n and all r, $0 \le r \le a_{n+2} - 1$*

$$q_{n,r}x - p_{n,r} = \frac{(-1)^n (a'_{n+2} - r)}{a'_{n+2} q_{n+1} + q_n}. \tag{10}$$

Moreover

Lemma 3.3 (§2, pp. 8) *For all n, put $\delta_n = q_n x - p_n$. Then*

$$\delta_{n+1} = \frac{(-1)^{n+1}}{a'_{n+2} q_{n+1} + q_n} = -\frac{\delta_n}{a'_{n+2}}. \tag{11}$$

We will need the following theorems.

Theorem 3.1 (Theorem 5) *Let p_n/q_n be a convergent of x. Then*

$$\frac{1}{2q_{n+1}} < \frac{1}{q_{n+1} + q_n} < |q_n x - p_n| < \frac{1}{q_{n+1}} < \frac{1}{q_n}. \tag{12}$$

For z any real, we note $||z||$ the distance of z to the nearest integer. A *best approximation* to z is a fraction p/q ($q > 0$) such that $||qx|| = |qx - p|$ and for q', $1 \le q' < q$, $||q'x|| > ||qx||$. Then

Theorem 3.2 ("Best approximation", Theorem 6) *For $n \ge 1$, q_n is the smallest integer $q > q_{n-1}$ such that $||qx|| < ||q_{n-1}x||$.*

Corollary 3.1 *The best approximations to x are the principal convergents to x.*

Theorem 3.3 (Theorem 10) *Let p and q be two coprime integers such that*

$$|qx - p| < \frac{1}{q}.$$

Then p/q is either a primary convergent of x or an intermediate convergent $p_{n,r}/q_{n,r}$ with $r = 0, 1$ or $a_{n+2} - 1$.

4 Solving Problem $\mathcal{D}$

If p/q satisfies (6), it is clear that

$$|qx - p| < \frac{1}{q}$$

and so Theorem 3.3 applies. We deduce that p/q is an intermediate convergent $p_{n,r}/q_{n,r}$ for some n and $r \in \{0, 1, a_{n+2} - 1\}$.

We can select the candidates as follows.

Proposition 4.1 *Let n be such $q_n \le Q < q_{n+1}$. Then, for all $q < q_{n-1}$, for all p, p/q cannot satisfy (6).*

Proof: Using (12), one has

$$|q_{n-2}x - p_{n-2}| > \frac{1}{q_{n-2} + q_{n-1}} \ge \frac{1}{q_n} \ge \frac{1}{Q},$$

so that p_{n-2}/q_{n-2} is not a solution of (6) and it follows by Theorem (3.2) that any p/q with $q < q_{n-2}$ cannot be a solution either. □

Corollary 4.1 *The only possible solutions to (6) are*

$$q_{n-2,1} = q_{n-1} + q_{n-2} < q_{n-2,a_n-1} = q_n - q_{n-1} < q_n$$

and

$$q_{n-1} < q_{n-1,1} = q_n + q_{n-1} < q_{n-1,a_{n+1}-1} = q_{n+1} - q_n.$$

We must now distinguish two cases.

Case 1: $q_n + q_{n-1} \leq Q$. Let r be the integer defined by

$$rq_n + q_{n-1} \leq Q < (r+1)q_n + q_{n-1}$$

i.e.

$$r = \left\lfloor \frac{Q - q_{n-1}}{q_n} \right\rfloor,$$

where $\lfloor z \rfloor$ denotes the greatest integer less than or equal to z. We now prove

Proposition 4.2 *1. The only possible q's are q_n, $q_{n-1,1}$, and $q_{n-1,a_{n+1}-1}$.*
2. Moreover, if $r \geq 2$, then $q_{n-1,1}$ is not possible.

Proof: The first point is proven as follows. We use (12) to get

$$|q_{n-1}x - p_{n-1}| > \frac{1}{q_n + q_{n-1}} \geq \frac{1}{Q},$$

and so q_{n-1} cannot be a solution. This implies that $q_{n-2,1}$ and q_{n-2,a_n-1} cannot be solutions by the best approximation theorem.

On the other hand, we have (using (10))

$$|q_{n-1,1}x - p_{n-1,1}| = \frac{a'_{n+1} - 1}{a'_{n+1}q_n + q_{n-1}} = \frac{a'_{n+1} - 1}{rq_n + (a'_{n+1} - r)q_n} > \frac{a'_{n+1} - 1}{Q(a'_{n+1} - r + 1)} \geq \frac{1}{Q},$$

since $r \geq 2$. □

Case 2: $q_n + q_{n-1} > Q$. We immediately see that the only candidates are: q_{n-1}, $q_{n-2,1}$, q_{n-2,a_n-1}. We prove

Proposition 4.3 *Suppose $a_n \geq 2$. Then $rq_{n-1} + q_{n-2}$ is not possible for r such that $1 \leq r \leq a_n - 1$.*

Proof: One has

$$|q_{n-2,r}x - p_{n-2,r}| = \frac{a'_n - r}{a'_n q_{n-1} + q_{n-2}} = \frac{a'_n - r}{(a'_n - a_n)q_{n-1} + q_n} > \frac{a'_n - r}{Q(1 + a'_n - a_n)} = \frac{a_n - r + \theta}{Q(1+\theta)},$$

with $\theta = a'_n - a_n$. Since $x \rightarrow \frac{\alpha + x}{1+x}$ is decreasing for $\alpha \geq 1$, we have

$$\frac{a_n - r + \theta}{Q(1+\theta)} \geq \frac{a_n + 1 - r}{2Q} \geq \frac{1}{Q},$$

which establishes the proof. □

Using the preceding results, we can build up algorithm THUE that solves problem $\mathcal{D}$.

procedure THUE(x, Q)
(* returns a set $\{p/q\}$ of irreducible solutions of $|qx - p| < 1/q$ *)

1. extract the following quantities from the development of x: $(p_{n-1}, q_{n-1}), (p_n, q_n), a_{n+1}$; put $\mathcal{S} := \{p_n/q_n\}$;
2. compute $r = \lfloor (Q - q_{n-1})/q_n \rfloor$;
3. **if** $r = 0$ **then** test whether p_{n-1}/q_{n-1} is a solution;
4. **if** $r \geq 1$ or $r = a_{n+1} - 1$ then test $p_{n-1,r}/q_{n-1,r}$;
5. **end**.

5 Solving Problem $\mathcal{P}$

We have to find two integers u and v such that

$$0 < |u| < \sqrt{m}, 0 < v < \sqrt{\frac{m}{d}}. \tag{13}$$

We can now solve Problem $\mathcal{D}$ with $Q = \sqrt{m/d}$ and then select the solutions to our initial problem $u^2 + dv^2 = m$.

5.1 An auxiliary algorithm

Theorem 5.1 *If Problem $\mathcal{P}$ has a solution, then it is given by*

$$u = p_n m - x_0 q_n, v = q_n$$

where $x_0^2 \equiv -d \bmod m$ *and* $q_n \leq \sqrt{m/d} < q_{n+1}$.

Proof: The proof follows that of Thue's problem. For each fraction $p_{n,r}/q_{n,r}$, we write $u_{n,r} = p_{n,r}m - x_0 q_{n,r}$, $v_{n,r} = q_{n,r}$ and $N_{n,r} = N(u_{n,r}, v_{n,r})$.

Case 1: in that case, we know that the only possible solutions are p_n/q_n, $(p_{n-1} + p_n)/(q_{n-1} + q_n)$ and $(p_{n+1} - p_n)/(q_{n+1} - q_n)$.

We put $\Delta_1 = N_{n-1,1} - N_n$ and we are going to show that $\Delta_1 > 0$. We have

$$\Delta_1 = ((p_{n-1} + p_n)m - x_0(q_{n-1} + q_n))^2 + d(q_{n-1} + q_n)^2 - (p_n m - x_0 q_n)^2 - dq_n^2.$$

We may rewrite this using $\delta_k = q_k x_0/m - p_k$ and (11) as

$$\Delta_1 = m^2 \delta_{n-1}^2 (1 - 2/a'_{n+1}) + dq_{n-1}(q_{n-1} + 2q_n).$$

We see that this quantity is positive, since

$$q_n + q_{n-1} \leq \sqrt{m/d} < q_{n+1} = a_{n+1}q_n + q_{n-1}$$

implies $a'_{n+1} \geq 2$.

Similarly, we put $\Delta_2 = N_{n-1,a_{n+1}-1} - N_n$. We have

$$\Delta_2 = m^2 \delta_{n+1}^2 (1 + 2a'_{n+2}) + dq_{n+1}(q_{n+1} - 2q_n),$$

which is positive since $q_{n+1} = a_{n+1}q_n + q_{n-1}$ and $a_{n+1} \geq 2$.

Case 2: This case is more intricate. We know that the only possible values of v are q_n or q_{n-1}. We delay the case $d = 1$ to the end, since it appears as a particular case. We first concentrate on $d > 1$ and we will show that N_{n-1} is always greater than m.

Case 2.1: $d > 1$. We have

$$N_{n-1} = m^2 \delta_{n-1}^2 + dq_{n-1}^2.$$

Using (11), one has

$$|\delta_{n-1}| = \frac{1}{a'_n q_{n-1} + q_{n-2}}.$$

We know that

$$a'_n q_{n-1} + q_{n-2} \leq (a_n + 1)q_{n-1} + q_{n-2} = q_n + q_{n-1}.$$

Together with $q_n < \sqrt{m/d}$, one gets

$$N_{n-1} > \frac{m^2}{\left(\sqrt{m/d} + q_{n-1}\right)^2} + dq_{n-1}^2.$$

The idea is now to study the function

$$f : x \mapsto \frac{m^2}{(x + \sqrt{m/d})^2} + dx^2$$

for $x \in I = [0, \sqrt{m/d}]$ and to show that f is always greater than m. We write $x = \lambda\sqrt{m/d}$ and study instead

$$g(\lambda) = \frac{1}{m} f\left(\lambda\sqrt{m/d}\right) = \lambda^2 + \frac{d}{(1+\lambda)^2}$$

on the interval $J = [0, 1]$.

We remark that it is enough to consider the case $d = 2$. We have

$$g'(\lambda) = 2\lambda - \frac{4}{(1+\lambda)^3}$$

and g'' is clearly positive. Hence g' is increasing on J. In particular

$$g'(0) = -4, g'(1) = 3/2.$$

Therefore, g' has a unique root λ_0 in J, satisfying

$$\lambda_0(\lambda_0 + 1)^3 = 2.$$

Moreover, λ_0 is in $]1/2, 1]$ since

$$g'(1/2) = 1 - \frac{32}{27} < 0.$$

Now g is minimum for λ_0 for which

$$g(\lambda_0) = \lambda_0(2\lambda_0 + 1) > 1,$$

since λ_0 is greater than $1/2$.

As a conclusion, f is always greater than m on I and we have proven the theorem.

Case 2.2: $d = 1$. Let us come back to the Euclidean algorithm as applied to (x_0, m). We keep the notations of the introduction. The following result is easily shown by induction.

Lemma 5.1 *For all i, $u_i = p_i m - x_0 q_i = (-1)^{i+1} r_i$.*

We follow [2]. From [8], we extract the following results. Since m is an integer greater than x_0 that divides $x_0^2 + 1$, the continued fraction of m/x_0 is symmetric

$$\frac{m}{x_0} = [b_0, b_1, \dots, b_k, b_k, \dots, b_0].$$

Denote the i-th convergent of m/x_0 by p'_i/q'_i and note that with our notations

$$\frac{p'_i}{q'_i} = \frac{q_{i-1}}{p_{i-1}}. \tag{14}$$

This implies that

$$p'_{2k+1} = m, q'_{2k+1} = x_0 = p'_{2k} \tag{15}$$

and

$$m = p_k'^2 + p_{k-1}'^2 = q_{k-1}^2 + q_{k-2}^2 \tag{16}$$

which is the crucial point. Using the recurrence relations for p_i', we have

$$\begin{aligned} p_{2k+1}' &= b_0 p_{2k}' + p_{2k-1}' = m = a_1 r_0 + r_1 && (17) \\ p_{2k}' &= b_1 p_{2k-1}' + p_{2k-2}' = x_0 = a_2 r_1 + r_2. && (18) \end{aligned}$$

By uniqueness of the remainders of the Euclidean algorithm, we see that for all i

$$p_{2k-i}' = r_i. \tag{19}$$

From all this, we get

$$m = p_k'^2 + p_{k-1}'^2 = r_k^2 + r_{k-1}^2 = q_{k-1}^2 + q_{k-2}^2.$$

As in Case 2.1, we know that the only possible solutions of the problem $m = u^2 + dv^2$ are $(u, v) = ((-1)^{n-1} r_n, q_n)$ or $(u, v) = ((-1)^{n-2} r_{n-1}, q_{n-1})$ where $q_n \leq \sqrt{m} < q_{n+1}$. This implies that $k = n + 1$ and the Theorem is proved. $\square$

5.2 Cornacchia's algorithm

We now prove the following theorem.

Theorem 5.2 *Denote by k the first integer for which $r_k \leq \sqrt{m} < r_{k-1}$. If Problem $\mathcal{P}$ has a solution, it is given by*

$$u = r_k \text{ and } v = q_k.$$

Proof: This is already proved for $d = 1$, by the last case of the preceding subsection. When $d > 1$, by Theorem (5.1), we know also that the only possible solution is (r_n, q_n) with $q_n \leq \sqrt{m/d} < q_{n+1}$. Let us show that (r_{k+1}, q_{k+1}) cannot be a solution.

First of all, using the notations of Section 3, we have

$$r_i = m|q_i x - p_i| = \frac{m}{q_{i+1}'},$$

for all i. Then, we cannot have $r_{k+1} = 0$, since this would imply $r_k = 1$ and thus $q_{k+1} = m$; in turn: $N_{k+1} > m$. Suppose now that $r_{k+1} \neq 0$. Then we can write

$$a_{k+2}' = \frac{r_k}{r_{k+1}}$$

using (9). We compute

$$q_{k+1}' = a_{k+1}' q_k + q_{k-1} = (a_{k+1} + \frac{1}{a_{k+2}'}) q_k + q_{k-1}$$

which gives

$$q_{k+1}' = q_{k+1} + \frac{1}{a_{k+2}'} q_k \geq \left(1 + \frac{1}{a_{k+2}'}\right) q_k$$

and finally

$$q_{k+1} \geq \frac{a_{k+2}'}{a_{k+2}' + 1} q_{k+1}.$$

From this, we deduce

$$N_{k+1} \geq \left(\frac{m}{q_{k+2}'}\right)^2 + d \left(\frac{a_{k+2}'}{1 + a_{k+2}'}\right)^2 q_{k+1}'^2.$$

We must show that the above quantity is always greater than m, for all $q'_{k+1} > \sqrt{m}$ and $a'_{k+2} \geq 1$. Putting $t = q'_{k+1} = T\sqrt{m}$ and $a = a'_{k+2}$, and noting that $q'_{k+2} = aT$, we must show that

$$F(a,T) = \frac{1}{(aT)^2} + d\left(\frac{aT}{a+1}\right)^2$$

is greater than 1 for T greater than 1. Since $T > 1$, we see that

$$F(a,T) > g\left(\frac{1}{aT}\right)$$

where g is the function studied in the preceding Section. We already know that it is always greater than 1. Hence the Theorem is proved. □

References

[1] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. Research Report 1256, INRIA, June 1990. Submitted to *Math. Comp.*

[2] J. Brillhart. Note on representing a prime as a sum of two squares. *Math. Comp.*, 26(120):1011–1013, 1972.

[3] G. Cornacchia. 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, 1908.

[4] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers.* Clarendon Press, 5th edition, 1985.

[5] 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(191):327–343, July 1990.

[6] E. Kaltofen and H. Rolletschek. Computing greatest common divisors and factorizations in quadratic number fields. *Math. Comp.*, 53(188):697–720, October 1989.

[7] S. Lang. *Introduction to diophantine approximations.* Addison-Wesley Series in Mathematics. Addison-Wesley Publishing Company, 1966.

[8] O. Perron. *Die Lehre von den Kettenbrüchen.* Chelsea, New York, 2nd edition, 1950.

[9] D. Shanks. Five number theoretic algorithms. In R. S. D. Thomas and H.C. Williams, editors, *Proc. 2nd Manitoba Conference on Numerical Mathematics*, pages 51–70, 1972.

[10] A. Thue. Et par antydninger til en taltheoretisk methode. *Vid. Selsk. Forhandlinger Christiania*, (2), 1902.

[11] B. Vallée. Une approche géométrique des algorithmes de réduction des réseaux en petite dimension, 1986. Thèse, Université de Caen.