On the solution of $x^2 + dy^2 = m$

By Julius Magalona BASILLA*)

Department of Mathematics, Sophia University
7-1, Kioicho, Chiyoda-ku, Tokyo 102-8554

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 2004)

Abstract: A simple proof of the validity of Cornacchia's algorithm for solving the diophantine equation $x^2 + dy^2 = m$ is presented. Furthermore, the special case $d = 1$ is solved completely.

Key words: Cornacchia's algorithm; quadratic forms; diophantine equations.

In 1908, G. Cornacchia gave an algorithm for solving the diophantine equation $x^2 + dy^2 = 4p$, for p prime (cf. [1]). The same algorithm can be used to solve the diophantine equation

$$x^2 + dy^2 = m \tag{1}$$

where $1 \leq d < m$, m may not be prime. The algorithm is briefly described as follows:

1. Put $r_0 = m$ and $r_1^2 \equiv -d \pmod{m}$, where $0 \leq r_1 \leq (m/2)$.
2. Using Euclidean algorithm, compute $r_{i+2} \equiv r_i \pmod{r_{i+1}}$ recursively until we arrive at $r_k^2 < m$.
3. If $(m - r_k^2/d)$ is a square integer, say s^2, we get the solution (r_k, s).

A proof of the validity of this algorithm relying on Diophantine Approximation was given by F. Morain and J.-L. Nicolas (cf. [2]). In this paper, we give a simpler proof. Moreover, we claim that if $r_0 = m$, $r_1^2 \equiv -1 \pmod{m}$, $1 \leq r_1 < (m/2)$, then $m = r_k^2 + r_{k+1}^2$, when $r_{k-1}^2 > m > r_k^2$.

1. A simple proof.

Let d and m be integers such that $1 \leq d < m$.

Lemma 1. *If (x_0, y_0) is a primitive solution of (1), then there exists an integer t, $0 < t < m$, $t^2 \equiv -d \pmod{m}$ such that $(x_0, y_0) \in \langle (m, 0), (t, 1) \rangle_{\mathbf{Z}}$.*

Proof. Clearly, $\gcd(y_0, m) = 1$. Choose t, $0 < t < m$ such that $y_0 t \equiv x_0 \pmod{m}$. We have $0 \equiv x_0^2 + dy_0^2 \equiv y_0^2(t^2 + d) \pmod{m}$. Thus, $t^2 \equiv -d \pmod{m}$. Also, for some integer l, $(x_0, y_0) = l(m, 0) + y_0(t, 1) \in \langle (m, 0), (t, 1) \rangle_{\mathbf{Z}}$. □

Define $L_t := \langle (m, 0), (t, 1) \rangle_{\mathbf{Z}}$. Clearly, if the solutions (x_0, y_0) and $(-x_0, -y_0)$ are in L_t, the solutions $(-x_0, y_0)$ and $(x_0, -y_0)$ are in L_{m-t}. This suggests that, to find all the primitive solutions of (1), it is enough to consider all square roots t of $-d$ modulo m, where $1 \leq t \leq (m/2)$ and compute for all the vectors (x, y) in L_t with $x^2 + dy^2 = m$. We will discuss how to find these vectors.

Lemma 2. *Let $\overrightarrow{u} = \langle u_1, u_2 \rangle$, $\overrightarrow{v} = \langle v_1, v_2 \rangle$ be generators of a lattice such that $0 \leq u_2$, $0 \leq v_2$, $|v_1| < |u_1|$, $u_1 v_1 < 0$. Then the vector $\overrightarrow{w} = \langle w_1, w_2 \rangle$ with the least w_2 such that $0 < w_2$, $|w_1| < |v_1|$ is given by $\overrightarrow{w} = \overrightarrow{u} + q\overrightarrow{v}$, where $q = \lfloor -(u_1/v_1) \rfloor$. Moreover, $\langle \overrightarrow{u}, \overrightarrow{v} \rangle_{\mathbf{Z}} = \langle \overrightarrow{v}, \overrightarrow{u} + q\overrightarrow{v} \rangle_{\mathbf{Z}}$.*

For the proof (cf. [3]).

Lemma 3. *Let r_0, r_1 be positive integers. Construct the finite sequences $\{r_i\}$, $\{q_i\}$, $\{P_i\}$, and $\{Q_i\}$ as follows:*

$$\begin{aligned}
&r_i = q_i r_{i+1} + r_{i+2}, \quad && q_i = \left\lfloor \tfrac{r_i}{r_{i+1}} \right\rfloor \\
&P_{-1} = 0; P_0 = 1; && P_{i+1} = q_i P_i + P_{i-1} \\
&Q_{-1} = 1; Q_0 = 0; && Q_{i+1} = q_i Q_i + Q_{i-1}
\end{aligned}$$

for $0 \leq i \leq n-1$, where $r_n = \gcd(r_0, r_1)$ and $r_{n+1} = 0$. Then, for $0 \leq i \leq n$,

$$r_0 = P_i r_i + P_{i-1} r_{i+1}, \tag{2}$$

$$r_{i+1} = (-1)^i (P_i r_1 - Q_i r_0). \tag{3}$$

The proof is by induction on i.

Putting $r_0 = m$ and $r_1^2 \equiv -d \pmod{m}$, from (3) we get,

$$r_i^2 + dP_{i-1}^2 \equiv 0 \pmod{m} \tag{4}$$

for $0 \leq i \leq n+1$.

Proposition 4. *Let $r_0 = m$ and $r_1 = t$ where $t^2 \equiv -d \pmod{m}$. Construct the sequence $\{r_i\}$,*

2000 Mathematics Subject Classification. Primary 11Y16; Secondary 11D09.

*) On study leave from the Department of Mathematics, University of the Philippines, Diliman, Quezon City Philippines.

$\{P_i\}$ *as in Lemma* 3. *The diophantine equation* (1) *has a solution in* L_t *if and only if* $dP_{k-1}^2 < m$, *when* $r_{k-1}^2 > m > r_k^2$.

Proof. ($\Rightarrow$) Let (x_0, y_0) be a solution of (1) in L_t. Without loss of generality, we can change the sign of x_0 and assume $y_0 > 0$. If $r_{k-1}^2 > m > r_k^2$, we have $|x_0|^2 < x_0^2 + dy_0^2 = m < r_{k-1}^2$. That is $|x_0| < |r_{k-1}|$.

Put $\overrightarrow{u_0} = (-m, 0)$ and $\overrightarrow{u_1} = (t, 1)$. By Lemma 2, the vector $\overrightarrow{u_2} = (-r_2, q)$ is the vector $\overrightarrow{w} = (w_1, w_2)$ with the least $w_2 > 0$ such that $|w_1| < |t|$. Note that the pair $\overrightarrow{u_1}$, $\overrightarrow{u_2}$ satisfies the premises of Lemma 2. Thus we can apply the Lemma repeatedly. Inductively, we can show that the vector $\overrightarrow{w} = (w_1, w_2)$ with the least $w_2 > 0$ such that $|w_1| < r_{i-1}$ is $\overrightarrow{u_i} = ((-1)^{i-1} r_i, P_{i-1})$.

In particular, the vector $\overrightarrow{w} = (w_1, w_2)$ with the least w_2 such that $|w_1| < |(-1)^{k-2} r_{k-1}|$ is $((-1)^{k-1} r_k, P_{k-1})$. Since $|x_0| < r_{k-1}$, it follows that $P_{k-1} \leq y_0$ and hence, $dP_{k-1}^2 \leq dy_0^2 < m$.

($\Leftarrow$) From (4), we have $dP_{k-1}^2 \equiv -r_k^2 \equiv m - r_k^2 \pmod{m}$. We get the solution (r_k, P_{k-1}). □

We now consider the special case $d = 1$.

Proposition 5. *Let* $t^2 \equiv -1 \pmod{m}$, $0 < t < (m/2)$. *Set* $r_0 = m$ *and* $r_1 = t$ *and construct the finite sequence* $\{r_i\}$, $r_i = q_i r_{i+1} + r_{i+2}$, *for* $0 \leq i \leq n-1$, *where* $r_0 > r_1 > \cdots > r_n = 1 > r_{n+1} = 0$. *If* $r_{k-1}^2 > m > r_k^2$ *then* $m = r_k^2 + r_{k+1}^2$.

Proof. Construct the sequence $\{P_i\}$ as in Lemma 3. We get the following relations.

$$\begin{aligned} m = r_0 &= P_n r_n + P_{n-1} r_{n+1} = P_n \\ r_{n-1} &= q_{n-1} r_n + r_{n+1} = q_{n-1} \geq 2 \\ m = P_n &= q_{n-1} P_{n-1} + P_{n-2} > 2P_{n-1}, \end{aligned}$$

since $n \geq 2$ and $P_{n-2} \neq 0$. Also

$$\begin{aligned} 1 = r_n &= (-1)^{n-1}(P_{n-1} r_1 - Q_{n-1} r_0) \\ &\equiv (-1)^{n-1} P_{n-1} t \pmod{m} \\ t &\equiv (-1)^n P_{n-1} \pmod{m}. \end{aligned}$$

It follows that n must be even say $n = 2k$, and $t = P_{n-1}$. Inductively, we can show $P_{n-i} = r_i$ for $0 \leq i \leq n+1$. From Lemma 3, we have $m = r_0 = P_k r_k + P_{k-1} r_{k+1} = r_k^2 + r_{k+1}^2$. Observe that $r_{k-1}^2 = (q_{k-1} r_k + r_{k+1})^2 > r_k^2 + r_{k+1}^2 = m > r_k^2$. This proves the proposition. □

2. A proof of uniqueness. We now show that for a particular square root t modulo m of $-d$, the only primitive solution of (1) belonging to the lattice $\langle (m, 0), (t, 1) \rangle_{\mathbf{Z}}$ is (r_k, P_{k-1}). In the case $d = 1$, because of symmetry we have two: (r_k, r_{k+1}) and (r_{k+1}, r_k).

Assume that (r_k, P_{k-1}) is the solution of (1) obtained by applying Cornacchia's algorithm. When $d = 1$, it is clear that $dP_{k+1}^2 \geq m$.

Lemma 6. *If* $d > 1$, *then* $dP_k^2 \geq m$.

Proof. Suppose that $dP_k^2 < m$. As in the proof of Proposition 4, we get $r_{k+1}^2 + dP_k^2 = m$. From (2), we have

$$\begin{aligned} m = r_0 &= P_k r_k + P_{k-1} r_{k+1} \\ &\leq \frac{r_k^2 + P_k^2}{2} + \frac{r_{k+1}^2 + P_{k-1}^2}{2} \\ &< \frac{r_k^2 + dP_{k-1}^2 + r_{k+1}^2 + dP_k^2}{2} = m. \end{aligned}$$

We have a contradiction. □

Proposition 7. *Let* $d > 1$ *and* $t^2 \equiv -d \pmod{m}$. *If* (x, y), $y > 0$ *is a solution of (1) such that* $(x, y) \in L_t$, *then* $(x, y) = ((-1)^{k-1} r_k, P_{k-1})$.

Proof. Since $x^2 + dy^2 = m$ it follows that $|x|^2 < m$ and $dy^2 < m$. Thus, $|x| < r_{k-1}$. If $|x| < r_k < r_{k-1}$, then $y \geq P_k$, by minimality of P_k. Thus $dy^2 \geq dP_k^2 \geq m$.

If $|x| > r_k$, since $|x| < r_{k-1}$, then $y \geq P_{k-1}$ by minimality of P_{k-1}. Then $x^2 + dy^2 > r_k^2 + dP_{k-1}^2 = m$. □

Proposition 8. *Let* $t^2 \equiv -1 \pmod{m}$. *If* (x, y), $y > 0$ *is a solution of* $x^2 + y^2 = m$ *such that* $(x, y) \in L_t$, *then* $(x, y) = ((-1)^{k-1} r_k, r_{k+1})$ *or* $(x, y) = ((-1)^k r_{k+1}, r_k)$.

The proof is similar to that of Proposition 7.

This proves that using Cornacchia's algorithm on all the square-root t modulo m of $-d$, we can find all the primitive solutions of (1).

References

[1] Cohen, H.: A Course in Computational Number Theory. Grad. Texts in Math., 138. Springer-Verlag, New York, pp. 34–36 (1993).

[2] Morain, F., and Nicolas, J.-L.: On Cornacchia's Algorithm for Solving the Diophantine Equation $u^2 + dv^2 = m$. Courbes elliptiques et tests de primalite These, Universite de Lyon I, 20 September (1990).

[3] Wada, H.: A note on the Pell equation. Tokyo J. Math., **2**, 133–136 (1979).