On the solution of $x^2 - dy^2 = \pm m$

By Julius M. BASILLA[*)] and Hideo WADA[**)]

(Communicated by Shigefumi MORI, M. J. A., Oct. 12, 2005)

Abstract: An improvement of the Gauss' algorithm for solving the diophantine equation $x^2 - dy^2 = \pm m$ is presented. As an application, multiple continued fraction method is proposed.

Key words: Quadratic form; diophantine equation; continued fraction method; prime decomposition.

1. Introduction. For solving a given quadratic diophantine equation

$$AX^2 + BXY + CY^2 + DX + EY + F = 0,$$

all we have to do is to solve one of the diophantine equations

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

$$x^2 - dy^2 = \pm m \tag{2}$$

where d and m are suitable positive integers and $\sqrt{d} \notin \mathbf{Q}$ because the degenerate cases $\sqrt{d} \in \mathbf{Q}$ and $m = 0$ are easy (cf. [7, § 34, § 53]). There is a very efficient algorithm for solving (1) even if m is very large (cf. [1]). So in this paper, we shall treat the equation (2). Gauss gave an efficient algorithm (cf. [3, 7, § 35]). Our algorithm is essentially the same as Gauss' one, but a little more efficient and simpler.

Let x and y be a primitive solution of (2), namely a solution such that $\gcd(x, y) = 1$. Then $\gcd(y, m) = 1$. So there exists an integer t such that

$$x \equiv -ty \pmod{m}. \tag{3}$$

From (2) and (3) we have $\pm m \equiv t^2y^2 - dy^2 \pmod{m}$. From $\gcd(y, m) = 1$, we have

$$t^2 \equiv d \pmod{m}. \tag{4}$$

Let α be $x + \sqrt{d}y$ and $\vec{\alpha}$ be $(\alpha, \alpha') = (x + \sqrt{d}y, x - \sqrt{d}y)$. Then $\alpha\alpha' = x^2 - dy^2 = \pm m$. From (3) there exists an integer z such that $x = mz - ty$. So

$$\alpha = (mz - ty) + \sqrt{d}y = mz + (-t + \sqrt{d})y.$$

Let α_{-1} be $-t + \sqrt{d}$ and α_0 be m. Then $\alpha = y\alpha_{-1} + z\alpha_0$ and $\vec{\alpha} = y\vec{\alpha}_{-1} + z\vec{\alpha}_0$. Let L_t be

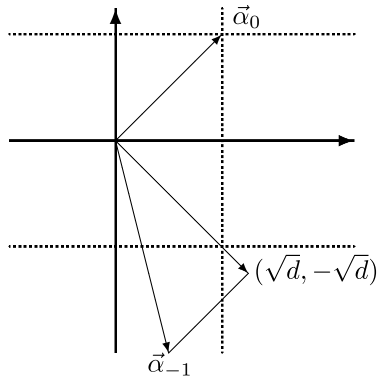

Fig. 1. $m < \sqrt{d}$.

$$\begin{aligned} L_t &= \langle (m, m), (-t + \sqrt{d}, -t - \sqrt{d}) \rangle_{\mathbf{Z}} \\ &= \{ y\vec{\alpha}_{-1} + z\vec{\alpha}_0 \mid y, z \in \mathbf{Z} \}. \end{aligned}$$

Then $\vec{\alpha}$ is an element of L_t and for all $\vec{\beta} \in L_t$, there exist y, z such that $\vec{\beta} = y\vec{\alpha}_{-1} + z\vec{\alpha}_0$ and from (4)

$$\begin{aligned} \beta\beta' &= (mz - ty)^2 - dy^2 \\ &\equiv (t^2 - d)y^2 \pmod{m}, \end{aligned}$$

$$\beta\beta' \equiv 0 \pmod{m}. \tag{5}$$

Therefore for solving the equation (2), we first calculate all t which satisfy (4). If we have a prime decomposition of m, we can calculate t very efficiently (cf. [2]). Secondly we search $\vec{\alpha} \neq \vec{0} = (0, 0)$ in L_t such that $|\alpha\alpha'|$ is the smallest. From (5), $\alpha\alpha'$ is a multiple of m. If $\alpha\alpha' = \pm m$, then we get a solution. If $|\alpha\alpha'| \geq 2m$, then there is no solution in L_t.

2. Algorithm. Let t be a solution of (4). If $t' \equiv t \pmod{m}$ then t' also satisfies (4). So we can choose the smallest t such that

$$\alpha_{-1} = -t + \sqrt{d} < \alpha_0 = m,$$

2000 Mathematics Subject Classification. 11D09, 11Y05, 11Y16.

*) Department of Mathematics, University of the Philippines, Diliman, Quezon City 1101, Philippines.

**) Department of Mathematics, Sophia University, 7-1 Kioicho, Chiyoda-Ku, Tokyo 102-8554.

$$\alpha'_{-1} = -t - \sqrt{d} < -\alpha'_0 = -m.$$

Moreover if $m < \sqrt{d}$, then we have $0 < \alpha_{-1}$ (cf. Fig. 1). For example, when $m = 1$, then $\alpha_{-1} = -[\sqrt{d}] + \sqrt{d}$. We define

$$(6) \qquad \alpha_{i+1} = \alpha_{i-1} + \left[-\frac{\alpha'_{i-1}}{\alpha'_i}\right]\alpha_i \quad (i \geq 0),$$

$$(7) \qquad \beta_i = -\frac{\alpha'_{i-1}}{\alpha'_i}, k_i = [\beta_i].$$

Let F_i be the Fibonacci sequence, namely $F_1 = F_2 = 1$, $F_{i+1} = F_i + F_{i-1}$. Then we have next theorem.

Theorem.

$$\beta_0 = \frac{\sqrt{d}+t}{m}, \quad \beta_{i+1} = \frac{1}{\beta_i - k_i}.$$

The continued fraction expansion of β_0 *is*

$$\beta_0 = [k_0, k_1, k_2, \dots]$$

and there exist integers a_i, b_i, *such that*

$$\beta_i = \frac{\sqrt{d}+b_i}{a_i}, \quad \alpha_i\alpha'_i = (-1)^i a_i m.$$

Even if $\alpha_{-1} < 0$, *if* $F_{2k} \geq \sqrt{m}$, *then we have*

$$0 < \alpha_{2k-1} < \alpha_{2k} < \alpha_{2k+1} < \cdots.$$

Moreover there exists positive integer ℓ $(< 2d)$ *such that* $\beta_{2k} = \beta_{2k+\ell}$. *So* a_i *are periodic. If* $a_i = 1$ *for some* i $(2k \leq i < 2k+\ell)$, *then we have a solution* α_i *in* L_t *and all solution in* L_t *are*

$$\pm\alpha_{i+n\ell} = \pm(\alpha_{2k+\ell}/\alpha_{2k})^n\alpha_i, \quad n \in \mathbf{Z}.$$

If $a_i > 1$ *for all* i $(2k \leq i < 2k+\ell)$, *then there is no solution in* L_t.

Example.

$$x^2 - 295y^2 = \pm 5,$$
$$t \equiv 0 \pmod 5,$$
$$0 < \alpha_{-1} = \sqrt{295} - 15 = 2.17\cdots < 5 = \alpha_0,$$
$$\alpha'_{-1} = -\sqrt{295} - 15 < -5 = -\alpha'_0,$$
$$\beta_0 = \frac{\sqrt{295}+15}{5} = [6, 2, 3, 2, 1, 5, \dots],$$
$$\beta_6 = \frac{\sqrt{295}+17}{1},$$
$$\alpha_6 = 2250 + 131\sqrt{295},$$
$$2250^2 - 295 \times 131^2 = 5.$$

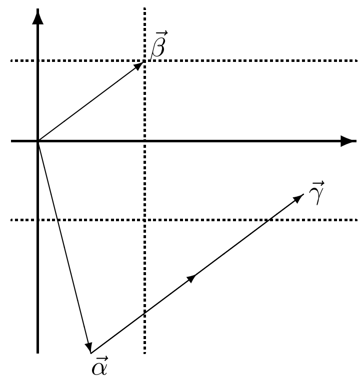

Fig. 2. Next minimal element.

3. Proof of the theorem. We call $\vec{\alpha} \in L_t$ is minimal if there exists no $\vec{\beta} \neq \vec{0}$ in L_t such thet $|\beta| < |\alpha|$, $|\beta'| < |\alpha'|$. If $|\alpha\alpha'|$ is the smallest, then of course $\vec{\alpha}$ is minimal. Therefore we shall search all minimal elements $\vec{\alpha}$ in L_t which are positive (namely $\alpha > 0$).

Let $\vec{\alpha}$ and $\vec{\beta}$ be generators of L_t such that

$$0 < \alpha < \beta, \quad \alpha'\beta' < 0, \quad |\alpha'| > |\beta'|$$

(cf. Fig. 2). Then $\vec{\alpha}, \vec{\beta}$ are minimal and the next minimal element $\vec{\gamma}$ such that $\beta < \gamma$ is

$$\gamma = \alpha + \left[-\frac{\alpha'}{\beta'}\right]\beta$$

(cf. [8]). The vectors $\vec{\beta}$ and $\vec{\gamma}$ are also generators of L_t and we have

$$0 < \beta < \gamma, \quad \beta'\gamma' < 0, \quad |\beta'| > |\gamma'|.$$

Therefore $\vec{\beta}$ and $\vec{\gamma}$ satisty the same conditions as $\vec{\alpha}$ and $\vec{\beta}$. From (6), we have

$$L_t = \langle\vec{\alpha}_{-1}, \vec{\alpha_0}\rangle = \langle\vec{\alpha_0}, \vec{\alpha_1}\rangle = \langle\vec{\alpha_1}, \vec{\alpha_2}\rangle = \cdots.$$

If we put $r_i = (-1)^i\alpha'_i$, then

$$r_{-1} = t + \sqrt{d} > m = r_0 > 0.$$

From (6), we have

$$r_{i+1} = r_{i-1} - \left[\frac{r_{i-1}}{r_i}\right]r_i.$$

This is just the Euclidian Algorithm. So we have

$$r_{-1} > r_0 > r_1 > r_2 > \cdots > 0,$$

$$(8) \qquad \beta_i = \frac{r_{i-1}}{r_i} > 1, \quad k_i = \left[\frac{r_{i-1}}{r_i}\right] \geq 1,$$

$$(9) \qquad \alpha_{i+1} = \alpha_{i-1} + k_i\alpha_i.$$

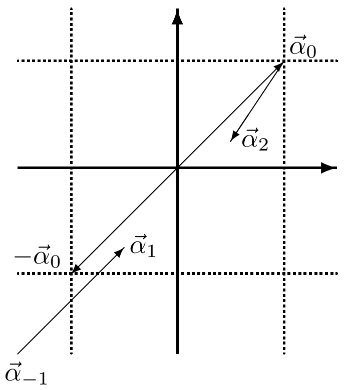

Fig. 3. $\alpha_{-1} < 0, \alpha_1 < 0$.

If $m > \sqrt{d}$, then there is a possibility that $\alpha_{-1} < 0$. We shall examine this case strictly. As $k_0 \geq 1$, we have

$$\alpha_1 = \alpha_{-1} + k_0\alpha_0 \geq \alpha_{-1} + \alpha_0.$$

If $\alpha_1 < 0$, then $\alpha_{-1} < -\alpha_0 < 0$. From $0 < \alpha'_0/\alpha_0 < \alpha'_{-1}/\alpha_{-1}$, we have $0 < \alpha'_{-1}/\alpha_{-1} < \alpha'_1/\alpha_1$ (cf. Fig. 3). From $0 < \alpha'_0/\alpha_0 < \alpha'_1/\alpha_1$ and $-\alpha'_0 < \alpha'_1 < 0$ we have $-\alpha_0 < \alpha_1$. From $\alpha'_0/\alpha_0 < \alpha'_1/\alpha_1$ and $0 < \alpha'_2$ we have $0 < \alpha_2 < \alpha_0$, $\alpha'_0/\alpha_0 > \alpha'_2/\alpha_2$. Therefore if $\alpha_1 < 0$ then we have

$$\alpha_{-1} < -\alpha_0 < \alpha_1 < 0 < \alpha_2, \quad \frac{\alpha'_1}{\alpha_1} > \frac{\alpha'_2}{\alpha_2}.$$

Similarly if $\alpha_{2k-1} < 0$ then we have

$$\alpha_{-1} < -\alpha_0 < \alpha_1 < \cdots < \alpha_{2k-1} < 0 < \alpha_{2k}.$$

Let s_i be $(-1)^i\alpha_i$. Then,

$$s_{-1} > s_0 > s_1 > s_2 > \cdots > s_{2k-1} > 0.$$

Recalling (9), we see

$$s_{i+1} = s_{i-1} - k_i s_i < s_i.$$

This is again the Euclidean Algorithm and

$$s_{2k-3} = k_{2k-2}s_{2k-2} + s_{2k-1} > 2s_{2k-1} = F_3 \cdot s_{2k-1}.$$

Using induction we have

$$m = s_0 > F_{2k} \cdot s_{2k-1}.$$

Similarly we have

$$m = r_0 > F_{2k} \cdot r_{2k-1}.$$

As $r_{2k-1}s_{2k-1} = \alpha_{2k-1}\alpha'_{2k-1} \equiv 0 \pmod{m}$, we have $mF_{2k}^2 < m^2$. Therefore if $F_{2k} \geq \sqrt{m}$, we have

$$(10) \qquad 0 < \alpha_{2k-1} < \alpha_{2k} < \alpha_{2k+1} < \cdots.$$

When $\alpha_{-1} > 0$, we define $k = 0$. Then (10) is always valid. From (5) we have integers a_i such that

$$(11) \qquad \alpha_i\alpha'_i = (-1)^i a_i m.$$

We shall prove next Lemma.

Lemma. *There are integers b_i such that*

$$(12) \qquad \alpha'_{i-1}\alpha_i = (-1)^{i-1}(\sqrt{d} + b_i)m.$$

Proof. When $i = 0$,

$$\alpha'_{i-1}\alpha_i = \alpha'_{-1}\alpha_0 = (-1)^{-1}(\sqrt{d} + t)m.$$

So $b_0 = t$. If (12) is valid, then from (9)

$$\begin{aligned} \alpha'_i\alpha_{i+1} &= \alpha'_i(\alpha_{i-1} + k_i\alpha_i) \\ &= (\alpha'_{i-1}\alpha_i)' + k_i\alpha_i\alpha'_i \\ &= (-1)^{i-1}(-\sqrt{d} + b_i)m + (-1)^i k_i a_i m \\ &= (-1)^i(\sqrt{d} - b_i + k_i a_i)m. \end{aligned}$$

So $b_{i+1} = k_i a_i - b_i$. □

From (7), (11), (12) we have

$$\beta_i = -\frac{\alpha'_{i-1}\alpha_i}{\alpha'_i\alpha_i} = \frac{\sqrt{d} + b_i}{a_i}.$$

From (9) we have

$$\begin{aligned} -\frac{\alpha'_{i+1}}{\alpha'_i} &= -\frac{\alpha'_{i-1}}{\alpha'_i} - k_i, \\ \frac{1}{\beta_{i+1}} &= \beta_i - [\beta_i], \\ \beta_0 &= -\frac{\alpha'_{-1}}{\alpha'_0} = \frac{\sqrt{d} + t}{m}. \end{aligned}$$

If $i \geq 2k$, then $\alpha_i > 0$. So $a_i > 0$ follows from (11),

$$1 < \beta_i, \quad -1 < \beta'_i = -\frac{\alpha_{i-1}}{\alpha_i} < 0$$

follow from (8) and (10). Therefore we have

$$0 < \frac{\sqrt{d} - b_i}{a_i} < 1 < \frac{\sqrt{d} + b_i}{a_i}, \quad (i \geq 2k).$$

From $a_i > 0$, we have

$$0 < b_i < \sqrt{d}, \quad 0 < a_i < \sqrt{d} + b_i < 2\sqrt{d}.$$

Using pegion-hole principle, we can find i, j $(2k \leq i < j < 2k + 2d)$ such that $\beta_i = \beta_j$. From (9), we have

$$\frac{\alpha_{i+1}}{\alpha_i} = \frac{\alpha_{i-1}}{\alpha_i} + k_i.$$

If $2k \le i$, then $0 < \alpha_{i-1} < \alpha_i < \alpha_{i+1}$. So we have

$$k_i = \left[\frac{\alpha_{i+1}}{\alpha_i}\right],$$

$$\alpha_{i-1} = \alpha_{i+1} - \left[\frac{\alpha_{i+1}}{\alpha_i}\right]\alpha_i \quad (i \ge 2k), \tag{13}$$

$$\beta_i' = -\frac{\alpha_{i-1}}{\alpha_i} = -\frac{\alpha_{i+1}}{\alpha_i} + \left[\frac{\alpha_{i+1}}{\alpha_i}\right],$$

$$\beta_i' = \frac{1}{\beta_{i+1}'} + \left[-\frac{1}{\beta_{i+1}'}\right], \quad (i \ge 2k). \tag{14}$$

If $2k < i$, then from (14) we have $\beta_{i-1} = \beta_{j-1}$. So for some ℓ $(1 \le \ell < 2d)$ we have $\beta_{2k} = \beta_{2k+\ell}$. So $a_{i+\ell} = a_i (2k \le i)$, namely a_i are periodic.

Redefine α_{i-1} for $i < 2k$ by (13). Then all positive minimal elements in L_t are $\vec{\alpha_i}$, $i \in \mathbf{Z}$. Similarly we can prove for all $i \in \mathbf{Z}$

$$\beta_i = -\frac{\alpha_{i-1}'}{\alpha_i'} = \frac{\sqrt{d} + b_i}{a_i} = \beta_{i+\ell}, \quad \alpha_i \alpha_i' = (-1)^i a_i m.$$

Therefore if $a_i = 1$ for some i $(2k \le i < 2k + \ell)$, we have a solution α_i, and all solutions in L_t are $\pm\alpha_{i+n\ell}$, $n \in \mathbf{Z}$. From $\beta_i = \beta_{i+\ell}$, we have

$$\alpha_{i+n\ell} = \frac{-1}{\beta_{i+n\ell}'} \cdots \frac{-1}{\beta_{i+1}'}\alpha_i = \left(\frac{\alpha_{2k+\ell}}{\alpha_{2k}}\right)^n \alpha_i, \quad n \in \mathbf{Z}.$$

If $a_i > 1$ for all i such that $2k \le i < 2k + \ell$, then there is no solution in L_t. Therefore the theorem is completely proved.

4. The case $m < \sqrt{d}$. If m is less than $\sqrt{d}$, then we have $0 < \alpha_{-1}$. Therefore we can take $k = 0$. If $m = 1$, then $a_\ell = a_0 = 1$, namely we have always solutions. If $m > 1$ and (2) has a solution, then there exists i $(0 < i < \ell)$ such that $a_i = 1$. Then we have $\beta_i = (\sqrt{d} + b_i)/1$, $-1 < \beta_i' < 0$. Therefore $b_i = [\sqrt{d}]$ and $\beta_\ell = \beta_0 = (\sqrt{d} + t)/m$. This means that if we start from $\beta_0 = \sqrt{d} + [\sqrt{d}]$, then for some i, a_i becomes m (Lagrange, cf. [4, 6, § 27]). If there does not exist such i, then (2) has no solution. We need not calculate t. For example

$$x^2 - 295y^2 = \pm 3$$

has no solution, because $\beta_0 = \sqrt{295} + 17$ and a_i are $1, 6, 21, 11, 9, 14, 5, 14, 9, 11, 21, 6, 1, \ldots$.

5. Multiple continued fraction method. We shall propose an improvement of continued fraction metod (cf. [5]). When we want to decompose a large number d into prime factors, we expand $\sqrt{d}$ into continued fraction. Namely from $\beta_0 = \sqrt{d} + [\sqrt{d}]$, we calculate β_i. We want to get many a_i which are products of small primes. When some a_i is $(\prod p_i)m$, where p_i are small primes but m is a product of large primes, then we start from $\tilde{\beta}_0 = (\sqrt{d} + t)/m$ in parallel with β_i. There are many such m. From (11), (12), we have $a_{i-1}a_i = d - b_i^2$. So we can use b_i as t. From the continued fraction expansion of $\tilde{\beta}_0$, we get $\tilde{\beta}_j = \left(\sqrt{d} + \tilde{b}_j\right)/\tilde{a}_j$. We get many $\tilde{a}_j$ which are products of small primes. So some product of a_i, $\tilde{a}_j m$ becomes a square number and we can get a decomposition of d.

Acknowledgement. The authors thank the referee who suggested the use of the Fibonacci sequence for estimating k such that $0 < \alpha_{2k-1}$.

References

[1] J.M. Basilla, On the solution of $x^2 + dy^2 = m$, Proc. Japan Acad., **80A** (2004), no. 5, 40–41.

[2] H. Cohen, *A course in computational algebraic number theory*, Springer, Berlin, 1993.

[3] C.F. Gauss, *Disquisiones Arithmeticae*, Fleischer, Leipzig, 1801.

[4] L.K. Hua, *Introduction to number theory*, Translated from the Chinese by Peter Shiu, Springer, Berlin, 1982.

[5] M.A. Morrison and J. Brillhart, A method of factoring and the factorization of F_7, Math. Comp. **29** (1975), 183–205.

[6] O. Perron, *Die Lehre von dem Kettenbrüchen I*, Teubner, Stuttgart, 1954.

[7] T. Takagi, *Lectures on the elementary theory of numbers*, 2nd ed., Kyoritsu-publication, Tokyo, 1971. (In Japanese).

[8] H. Wada, A note on the Pell equation, Tokyo J. Math. **2** (1979), no. 1, 133–136.