Journal of Integer Sequences, Vol. 20 (2017),
Article 17.10.5

Extending Theorems of Serret and Pavone

Keith R. Matthews
School of Mathematics and Physics
University of Queensland
Brisbane 4072
Australia
keithmatt@gmail.com

John P. Robertson
Actuarial and Economic Services Division
National Council on Compensation Insurance
Boca Raton, FL 33487
USA
jpr2718@gmail.com

Anitha Srinivasan
Department of Mathematics
Saint Louis University-Madrid Campus
Avenida del Valle 34
28003 Madrid
Spain
rsrinivasan.anitha@gmail.com

Abstract

We extend theorems of Serret and Pavone for solving $f(x,y) = ax^2 + bxy + cy^2 = \mu$, where $a > 0$, $\gcd(x,y) = 1, y > 0$. Here $d = b^2 - 4ac > 0$ is not a perfect square and $0 < |\mu| < \sqrt{d}/2$. If $\mu > 0$, Serret proved that x/y is a convergent to $\rho = (-b + \sqrt{d})/2a$ or $\sigma = (-b - \sqrt{d})/2a$. If $\mu < 0$, we are able to modify Pavone's approach and show that with at most one exception, the solutions are convergents to ρ or σ.

1 Introduction

In 1885, Serret [13] studied the quadratic diophantine equation

$$f(x,y) = ax^2 + bxy + cy^2 = \mu, \tag{1}$$

where $a > 0, \gcd(a,b,c) = 1, d = b^2 - 4ac$ is positive and nonsquare and $0 < |\mu| < \sqrt{d}/2$. Serret showed that if $\mu > 0$, then any relatively prime solution (x,y) with $y > 0$ is a convergent to $\rho = (-b+\sqrt{d})/2a$ or $\sigma = (-b-\sqrt{d})/2a$. However he was unable to deal conclusively with the case $\mu < 0$. This was done by Pavone [11] in the special case when $|\mu| = m(f)$ is the least of the absolute values of integers represented by f for integers x and y, not both zero. We remark that Lagrange [3, Thm. 86] proved $m(f) < \sqrt{d}/2$.

We modify Pavone's proof when $-\sqrt{d}/2 < \mu < 0$, to show that either x/y is a convergent to ρ or σ, or has the form $(p_m - p_{m-1}, q_m - q_{m-1})$ or $(P_r - P_{r-1}, Q_r - Q_{r-1})$, where

$$\rho = [a_0, \ldots, a_m, \overline{b_1, \ldots, b_n}], \quad \sigma = [c_0, \ldots, c_r, \overline{d_1, \ldots, d_n}],$$

where $a_m \neq b_n, c_r \neq d_n$ and p_h/q_h and P_k/Q_k denote convergents of ρ and σ, respectively.

Barnes [1, Lemma 16] gave a result that overlaps with Serret's theorem when $a > 0 > c$.

Finally, we remark that there is a continued fraction algorithm [8] for solving (1), irrespective of the size of μ.

2 Definitions and Lemmas

Definition 1. We call an indefinite form $g(x,y) = Ax^2 + Bxy + Cy^2$ *Hermite reduced* if the roots θ_1 and θ_2 of $g(x,1) = 0$ satisfy $\theta_1 > 1$ and $-1 < \theta_2 < 0$. Equivalently, $\theta_1 = [\overline{b_1, \ldots, b_n}]$ and $\theta_2 = -[0, \overline{b_n, \ldots, b_1}]$, where the b_i are positive integers. See [12, pp. 73–76].

Remark 2. The term *Hermite reduced* was introduced in [4]. Markov had previously used the concept in his Master's dissertation [2] and [7].

The following sequences were introduced in [4] and [11].

Definition 3. Let $\theta_1 = [a_0, a_1, \ldots,]$ and $\theta_2 = -[0, a_{-1}, a_{-2}, \ldots,]$ be as in Definition 1 and let the doubly-infinite sequences $(S_k), (T_k)$ be defined as follows:

$$\begin{aligned} S_0 = T_{-1} = 1, &\quad S_{-1} = T_0 = 0, \\ S_{k+1} = a_k S_k + S_{k-1}, &\quad T_{k+1} = a_k T_k + T_{k-1}, \quad k \geq 0, \\ S_{-k-1} = -a_{-k} S_{-k} + S_{-k+1}, &\quad T_{-k-1} = -a_{-k} T_{-k} + T_{-k+1}, \quad k \geq 1. \end{aligned} \tag{2}$$

.

Remark 4. For $k \geq 1$, the convergents to θ_1 are given by

$$S_k/T_k = A_{k-1}/B_{k-1} = [a_0, \ldots, a_{k-1}].$$

To determine the convergents to θ_2, we note that

$$S_{-k-1}/T_{-k-1} = -[0, a_{-1}, \ldots, a_{-k}]$$

and use the following result from [5].

$$\theta_2 = \begin{cases} [-1, 1, a_{-1} - 1, a_{-2}, \ldots], & \text{if } a_{-1} > 1; \\ [-1, a_{-2} + 1, a_{-3}, \ldots], & \text{if } a_{-1} = 1. \end{cases}$$

Then for $k \geq 0$, the convergents to θ_2 are given by

$$\begin{aligned} &(A_0, B_0) = (-1, 1) \text{ and } (A_k, B_k) = (-1)^{k+1}(S_{-k}, T_{-k}), k \geq 1 \text{ if } a_{-1} > 1, \\ &(A_k, B_k) = (-1)^{k+1}(S_{-k-2}, T_{-k-2}), k \geq 0, \text{ if } a_{-1} = 1. \end{aligned} \tag{3}$$

We note that for $k \geq 1$, S_{-k-1} is positive exactly when k is odd, and T_{-k-1} is negative exactly when k is odd.

We now give a simple proof of Serret's theorem.

Proposition 5. *Assume $0 < \mu < \sqrt{d}/2$. Let (p, q) be a relatively prime solution of $f(x, y) = ax^2 + bxy + cy^2 = \mu$, with $q > 0$, where $a > 0$. Then p/q is a convergent to $\rho = (-b + \sqrt{d})/2a$ or $\sigma = (-b - \sqrt{d})/2a$.*

Proof. We have

$$a\left(\frac{p}{q} - \rho\right)\left(\frac{p}{q} - \sigma\right) = \frac{\mu}{q^2}.$$

We cannot have $\sigma < p/q < \rho$. First assume $p/q > \rho$. Then

$$\begin{aligned} \frac{p}{q} - \rho &= \frac{\mu}{a(\frac{p}{q} - \rho + \rho - \sigma)q^2} \\ &< \frac{\sqrt{d}}{2a(\rho - \sigma)q^2} = \frac{1}{2q^2}. \end{aligned}$$

Hence p/q is a convergent $p_k/q_k, k \geq 0$, to ρ by Lagrange [6, Thm. 184]. There is a similar argument if $p/q < \sigma$. □

We replace Pavone's Lemma 2 by a more general result:

Lemma 6. *Let $g(x, y)$ be a Hermite reduced form $Ax^2 + Bxy + Cy^2$, $D = B^2 - 4AC$ with roots $\theta_1 = [\overline{b_1, \ldots, b_n}]$ and $\theta_2 = -[0, \overline{b_n, \ldots, b_1}]$ and let $(S_k), (T_k)$ be the sequences defined in (2). Suppose $g(p, q) = \mu$, where $0 < |\mu| < \sqrt{D}/2$, with $\gcd(p, q) = 1$. Then there exists a k such that*

$$(p, q) = \pm(S_k, T_k).$$

Proof. If $(p, q) = (\pm 1, 0)$, we can take $k = 0$, whereas if $(p, q) = (0, \pm 1)$, we can take $k = -1$. So we assume p and q are nonzero. Then p/q is a convergent to θ_1 or θ_2. For if A and μ have the same sign, the result follows from Serret's theorem. If A and μ have opposite signs, then as A and C have opposite sign, C and μ have the same sign and we instead consider the equation $Cq^2 + Bqp + Ap^2 = \mu$. We know by Serret's theorem that q/p is a convergent to one of $1/\theta_1$ or $1/\theta_2$, so p/q will be a convergent $A_h/B_h, h \geq 0$, to one of θ_1 or θ_2. In the former case, $(p, q) = \pm(S_k, T_k)$ for some $k \geq 1$. From Remark 4, the only convergent to θ_2 that is not S_k/T_k is $A_0/B_0 = -1/1$, and this occurs when $b_n > 1$. We show that this is impossible here.

We can assume $A > 0$ and that $g(-1, 1) = \mu$, where $|\mu| < \sqrt{d}/2$. Then $A(-1-\theta_1)(-1-\theta_2) = \mu$, so $(1+\theta_1)(1+\theta_2) = \mu/A$. Then as $\theta_1 > 1$ and $-1 < \theta_2 < 0$, we have $\mu > 0$. Hence

$$1 + \theta_2 = \frac{\mu}{A(1+\theta_1)} < \frac{1}{2},$$

as $1+\theta_1 = 1+\theta_2+\theta_1-\theta_2 > \theta_1-\theta_2 = \sqrt{d}/A$. Hence $1/1$ is a convergent to $-\theta_2 = [0, \overline{b_n, \ldots, b_1}]$, which means that $b_n = 1$. □

We replace Pavone's Lemma 4 by the following result:

Lemma 7. *Let $g(x, y)$ be a Hermite reduced form with roots $\theta_1 = [\overline{b_1, \ldots, b_n}]$ and $\theta_2 = -[0, \overline{b_n, \ldots, b_1}]$. Suppose $b_n > 1, b_{n-1} = 1$ and that $g(S_{-2}, T_{-2}) = \mu$, where $|\mu| < \sqrt{d}/2$. Then $b_{n-2} = 1$.*

Proof. For $1 \leq i \leq n$, let

$$W_i = [\overline{b_i, b_{i+1}, \ldots, b_n, b_1, \ldots, b_{i-1}}] + [0, \overline{b_{i-1}, \ldots, b_1, b_n, \ldots, b_i}].$$

Then $W_i = \sqrt{d}/|g(S_{i-1}, T_{i-1})$ (see [7, p. 385]). Hence, as the W_i are periodic with period n, we have

$$\begin{aligned} W_{n-1} &= [b_{n-1}, b_n, b_1, \ldots, b_{n-2}] + [0, b_{n-2}, \ldots, b_1, b_n, b_{n-1}] \\ &= \sqrt{d}/|g(S_{-2}, T_{-2})| \\ &= \sqrt{d}/|\mu| > 2. \end{aligned}$$

Hence if $b_{n-1} = 1$, we have

$$\begin{aligned} W_{n-1} &= [1, b_n, b_1, \ldots, b_{n-2}] + [0, b_{n-2}, \ldots, b_1, b_n, b_{n-1}] \\ &< 1 + 1/b_n + 1/b_{n-2}. \end{aligned}$$

So if $b_n > 1$, we have

$$2 < W_{n-1} < 1 + 1/b_n + 1/b_{n-2} \leq 1 + 1/2 + 1/b_{n-2}.$$

Hence $1/2 < 1/b_{n-2}$ and so $b_{n-2} < 2$, giving $b_{n-2} = 1$. □

The next result is due to Pavone [11].

Lemma 8. *Let $f(x, y) = ax^2 + bxy + cy^2$ and let $\rho = [a_0, \dots, a_m, \overline{b_1, \dots, b_n}]$ and $\sigma = [c_0, \dots, c_r, \overline{d_1, \dots, d_n}]$ be the roots of $f(x, 1) = 0$. Also let p_h/q_h and P_h/Q_h denote the convergents of ρ and σ, respectively. We do not require the periods to have minimal lengths, but assume m and r are minimal, i.e., $a_m \neq b_n$ and $c_r \neq d_n$. It is also convenient to assume $n \geq 4$.*

Let $\theta_1 = [\overline{b_1, \dots, b_n}], \theta_2 = -[0, \overline{b_n, \dots, b_1}]$ and let S_k, T_k be the sequences (2) for θ_1 and θ_2. Then

$$\begin{pmatrix} p_m & p_{m-1} \\ q_m & q_{m-1} \end{pmatrix} \begin{pmatrix} S_k \\ T_k \end{pmatrix} = \begin{pmatrix} p_{m+k} \\ q_{m+k} \end{pmatrix}, \quad k \geq -1. \tag{4}$$

Moreover, there exists $i, 1 \leq i \leq 3$, such that

$$\sigma = [c_0, \dots, c_r, \overline{b_{n-i}, \dots, b_1, b_n, b_{n-1}, \dots, b_{n-i+1}}], \tag{5}$$

and

$$\begin{pmatrix} p_m & p_{m-1} \\ q_m & q_{m-1} \end{pmatrix} \begin{pmatrix} S_{-k} \\ T_{-k} \end{pmatrix} = \pm \begin{pmatrix} P_{r+k-(i+1)} \\ Q_{r+k-(i+1)} \end{pmatrix}, \quad k \geq i. \tag{6}$$

Also $i = 3$ implies $b_{n-1} = 1$, while $b_n = b_{n-1} = 1$ implies $i = 3$.

Remark 9. A list of the possible continued fraction expansions (5) for σ is given at [9].

3 Extending Pavone's theorem

Theorem 10. *Let $f(x, y) = ax^2 + bxy + cy^2, a > 0, d = b^2 - 4ac > 0$ and not square. Let p and $q > 0$ be relatively prime integers, such that $f(p, q) = \mu$. Let the roots of $f(x, 1) = 0$ be $\rho = [a_0, \dots, a_m, \overline{b_1, \dots, b_n}]$ and $\sigma = [c_0, \dots, c_r, \overline{d_1, \dots, d_n}]$, where $a_m \neq b_n$ and $c_r \neq d_n$. Let the convergents of ρ and σ be denoted by p_h/q_h and P_h/Q_h, respectively.*

(i) If $0 < \mu < \sqrt{d}/2$, then p/q is a convergent to ρ or σ.

(ii) If $-\sqrt{d}/2 < \mu < 0$, then p/q is a convergent to ρ or σ, or

$$(p, q) = (p_m - p_{m-1}, q_m - q_{m-1}) \text{ or } (P_r - P_{r-1}, Q_r - Q_{r-1}). \tag{7}$$

Proof. We assume $f(p, q) = ap^2 + bpq + cq^2 = \mu$, where $0 < |\mu| < \sqrt{d}/2$ and $\gcd(p, q) = 1$. We follow Pavone's argument closely and define $g(x, y)$ by

$$g(x, y) = f(p_m x + p_{m-1} y, q_m x + q_{m-1} y).$$

Then g is Hermite reduced with roots $\theta_1 = [\overline{b_1, \dots, b_n}]$ and $\theta_2 = -[0, \overline{b_n, \dots, b_1}]$ and with sequences S_k, T_k for θ_1 and θ_2 defined in (2). Define integers α and β by

$$p_m \alpha + p_{m-1} \beta = p, \quad q_m \alpha + q_{m-1} \beta = q.$$

Then $g(\alpha,\beta)=\mu$ and by Lemma 6, there exists an integer k such that $(\alpha,\beta)=\pm(S_k,T_k)$. Hence

$$\begin{pmatrix} p \\ q \end{pmatrix} = \pm \begin{pmatrix} p_m & p_{m-1} \\ q_m & q_{m-1} \end{pmatrix} \begin{pmatrix} S_k \\ T_k \end{pmatrix}.$$

Let i be the integer satisfying equations (5) and (6). If $i=1$ or 2, then by (4) and (6)

$$\begin{pmatrix} p \\ q \end{pmatrix} = \pm \begin{pmatrix} p_h \\ q_h \end{pmatrix} \text{ or } \pm \begin{pmatrix} P_h \\ Q_h \end{pmatrix}$$

for some h, and p/q is a convergent to ρ or σ. If $i=3$, then the pair $\begin{pmatrix} S_k \\ T_k \end{pmatrix}$ occurs in (4) or (6) for all $k \neq -2$. Hence either p/q is a convergent to ρ or σ, or

$$\begin{pmatrix} p \\ q \end{pmatrix} = \pm \begin{pmatrix} p_m & p_{m-1} \\ q_m & q_{m-1} \end{pmatrix} \begin{pmatrix} S_{-2} \\ T_{-2} \end{pmatrix} = \pm \begin{pmatrix} p_m & p_{m-1} \\ q_m & q_{m-1} \end{pmatrix} \begin{pmatrix} 1 \\ -b_n \end{pmatrix}$$

and

$$(p,q) = \pm(p_m - b_n p_{m-1}, q_m - b_n q_{m-1}).$$

However we can interchange ρ and σ and similarly deduce that

$$(p,q) = \pm(P_r - b_{n-2}P_{r-1}, Q_r - b_{n-2}Q_{r-1}).$$

If $b_n = 1$, we have $q_m - b_n q_{m-1} = q_m - q_{m-1} > 0$ and

$$(p,q) = (p_m - p_{m-1}, q_m - q_{m-1}).$$

If $b_n > 1$, then $b_{n-1} = 1$ by Lemma 8, and as $g(S_{-2},T_{-2}) = \mu$, it follows from Lemma 7 that $b_{n-2} = 1$. Hence $Q_r - b_{n-2}Q_{r-1} = Q_r - Q_{r-1} > 0$ and

$$(p,q) = (P_r - P_{r-1}, Q_r - Q_{r-1}).$$

□

Definition 11. A solution (p,q) of (1) with $\gcd(p,q)=1$ and $q>0$ that is not a convergent to ρ or σ is called an *exceptional* solution.

Remark 12. From the above proof, we see that if a solution is given by a convergent p_k/q_k to ρ, then $k \geq m-1$. Similarly, if a solution is given by a convergent P_j/Q_j to σ, then $j \geq r-1$.

4 Fundamental solutions

We need some definitions and lemmas associated with the diophantine equation

$$ax^2 + bxy + cy^2 = \mu. \tag{8}$$

The integer solutions of (8) divide into equivalence classes under the relation (x_1, y_1) and (x_2, y_2) are equivalent if and only if

$$x_2 = \frac{x_1(u - bv)}{2} - cvy_1, \quad y_2 = \frac{y_1(u + bv)}{2} + avx_1,$$

where u and v are integers satisfying $u^2 - dv^2 = 4$.

Definition 13. A *fundamental* solution (u, v) of a class of solutions K of (8), is one where v has least non-negative value when (u, v) belongs to K. Let $u' = -(au + bv)/a$ be the conjugate solution to u. If u' is not integral, or if (u', v) is not equivalent to (u, v), this determines (u, v). If u' is integral and (u', v) is equivalent to (u, v), where $u \neq u'$, we choose $u > u'$. There are finitely many equivalence classes, each indexed by a fundamental solution.

Reference [10] contains more information about the fundamental solutions.

Lemma 14. ([14, p. 383]). *Solutions (x_1, y_1) and (x_2, y_2) of (8) are equivalent if and only if $x_1y_2 - x_2y_1 \equiv 0 \pmod{|\mu|}$.*

We find the fundamental solutions when $|\mu| < \sqrt{d}/2$, by examining the continued fractions for ρ and σ. It can be proved that the different classes will be represented in the first period (and second period if the period is odd). We first check to see if an exceptional solution exists. Then we examine the the convergents $p_m/q_m, \ldots$ and $P_r/Q_r, \ldots$ of the first period of ρ and σ, and additionally the second period, if the period-length is odd, using the equations

$$aA_{n-1}^2 + bA_{n-1}B_{n-1} + cB_{n-1}^2 = \begin{cases} (-1)^n Q_n/2, & \text{with } \rho = (-b + \sqrt{d})/2a; \\ (-1)^{n+1} Q_n/2, & \text{with } \sigma = (-b - \sqrt{d})/2a, \end{cases}$$

to check if for ρ, we have $\mu = (-1)^n Q_n/2$, or for σ, we have $\mu = (-1)^{n+1} Q_n/2$.

We then use Lemma 14 to test for equivalence of solutions using (p_{m-1}, q_{m-1}), (P_{r-1}, Q_{r-1}) and any exceptional solution.

Proposition 15. *If (p, q) is an exceptional solution of (1), then it is a fundamental solution if $|\mu| > 1$.*

Proof. Suppose (p, q) is an exceptional solution of (1). Then from the proof of Theorem 10, we have

$$(p, q) = (p_m - b_n p_{m-1}, q_m - b_n q_{m-1}) = (P_r - b_{n-2} P_{r-1}, Q_r - b_{n-2} Q_{r-1}).$$

We have to compare (p,q) with the convergents p_h/q_h and P_k/Q_k of ρ and σ that give solutions of (1). By Remark 12, we know that $h \geq m-1$ and $k \geq r-1$.

Now $q = q_m - b_n q_{m-1} < q_m \leq q_k$ if $k \geq m$ and $q = Q_r - b_{n-2}Q_{r-1} < Q_r \leq Q_j$ if $j \geq r$. Also (p,q) is not equivalent to (p_{m-1}, q_{m-1}) or (P_{r-1}, Q_{r-1}) if $|\mu| > 1$. For

$$\begin{aligned}
(p,q) \sim (p_{m-1}, q_{m-1}) &\iff p_{m-1}(q_m - b_n q_{m-1}) - q_{m-1}(p_m - b_n p_{m-1}) \equiv 0 \pmod{|\mu|} \\
&\iff p_{m-1}q_m - q_{m-1}p_m \equiv 0 \pmod{|\mu|} \\
&\iff (-1)^m \equiv 0 \pmod{|\mu|}.
\end{aligned}$$

Similarly with (P_{r-1}, Q_{r-1}). $\square$

Remark 16. If $\mu = -1$, the situation is more complicated. For example, the equation $x^2 + xy - y^2 = -1$ has one solution class, with fundamental solution $(0,1)$ and an exceptional solution $(-1,1)$.

5 Examples

Example 17. Consider the equation $x^2 + xy - 100y^2 = -10$. Here $d = 401$, $|\mu| = 10 < \sqrt{d}/2$. Also

$$\rho = (-1+\sqrt{401})/2 = [9, \overline{1, 1, 19}], \quad \sigma = (-1-\sqrt{401})/2 = [-11, 2, \overline{19, 1, 1}].$$

The double periods for ρ and σ give the solutions

$(p_0, q_0) = (9, 1)$	$(P_3, Q_3) = (-431, 41)$
$(p_4, q_4) = (390, 41)$	$(P_5, Q_5) = (-16410, 1561)$

Also $(-10, 1) = (P_1 - P_0, Q_1 - Q_0)$ is an exceptional solution, where $P_1/Q_1 = -21/2$ and $P_0/Q_0 = -11/1$; also neither $(p_{m-1}, q_{m-1}) = (p_{-1}, q_{-1}) = (1, 0)$ nor $(P_{r-1}, Q_{r-1}) = (P_0, Q_0) = (-11, 1)$ is a solution of $x^2 + xy - 100y^2 = -10$. We also have

$$\begin{aligned}
(9,1) \sim (-431, 41) &\not\sim (-10, 1), \\
(390, 41) \sim (-16410, 1561) &\sim (-10, 1).
\end{aligned}$$

Hence the fundamental solutions are $(9,1)$ and $(-10,1)$, and the complete solution is

$$x = (9u + 191v)/2; \quad x = (-10u + 210v)/2, \tag{9}$$
$$y = (u + 19v)/2; \quad y = (u - 19v)/2, \tag{10}$$

where $u^2 - 401v^2 = 4$.

Example 18. Consider the equation $69x^2 + 71xy + 15y^2 = -13$. Here $d = 901, |\mu| = 13 < \sqrt{d}/2$. Then

$$\rho = (-71 + \sqrt{901})/138 = [-1, 1, 2, \overline{2, 1, 2, 1, 1, 1, 1}],$$
$$\sigma = (-71 - \sqrt{901})/138 = [-1, 3, \overline{1, 2, 1, 2, 1, 1, 1}],$$

and we have the exceptional solution

$$(-1, 2) = (P_1 - P_0, Q_1 - Q_0) = (p_2 - p_1, q_2 - q_1),$$

where $P_1/Q_1 = -2/3, P_0/Q_0 = -1/1$ and $p_2/q_2 = -1/3, p_1/q_1 = 0/1$.

The double periods for ρ and σ give the solutions

$(p_6, q_6) = (-11, 37)$	$(P_7, Q_7) = (-71, 97)$
$(p_{14}, q_{14}) = (-1141, 3842)$	$(P_{13}, Q_{13}) = (-2461, 3362)$

Also neither $(p_{m-1}, q_{m-1}) = (p_1, q_1) = (0, 1)$ nor $(P_{r-1}, Q_{r-1}) = (P_0, Q_0) = (-1, 1)$ is a solution of $69x^2 + 71xy + 15y^2 = -13$ and

$$(-11, 37) \sim (-71, 97) \not\sim (-1, 2),$$
$$(-1141, 3842) \sim (-2461, 3362) \sim (-1, 2).$$

Hence the fundamental solutions are $(-1, 2)$ and $(-11, 37)$, and the complete solution is given by

$$x = (-u + 11v)/2; \qquad x = (-11u - 329v)/2, \tag{11}$$
$$y = (2u + 4v)/2; \qquad y = (37u + 1109v)/2, \tag{12}$$

where $u^2 - 901v^2 = 4$.

Example 19. Consider the equation $2x^2 + 5xy + y^2 = -2$. Here $d = 17, |\mu| = 2 < \sqrt{d}/2$. Then

$$\rho = (-5 + \sqrt{17})/4 = [-1, \overline{1, 3, 1}], \quad \sigma = (-5 - \sqrt{17})/4 = [-3, 1, 2, \overline{1, 1, 3}].$$

There is no exceptional solution, as $i = 2$ here.

The double periods for ρ and σ give the solutions

$(p_0, q_0) = (-1, 1)$	$(P_3, Q_3) = (-9, 4)$
$(p_2, q_2) = (-1, 4)$	$(P_5, Q_5) = (-57, 25)$

Also $(p_{m-1}, q_{m-1}) = (p_{-1}, q_{-1}) = (1, 0)$ and $(P_{r-1}, Q_{r-1}) = (P_1, Q_1) = (-2, 1)$ are not solutions of $2x^2 + 5xy + y^2 = -2$. We also have

$$(-1, 1) \sim (-57, 25) \not\sim (-1, 4) \sim (-9, 4).$$

Hence the fundamental solutions are $(-1, 1)$ and $(-1, 4)$ and the complete solution is given by

$$x = (-u + 3v)/2; \qquad x = (-u - 3v)/2, \tag{13}$$
$$y = (u + v)/2; \qquad y = (4u + 16v)/2, \tag{14}$$

where $u^2 - 17v^2 = 4$.

If instead we consider the equation $2x^2 + 5xy + y^2 = -1$, again there are no exceptional solutions. Also the double periods for ρ and σ now give the solutions

$(p_4, q_4) = (-2, 9)$	$(P_1, Q_1) = (-130, 57)$

Here $(P_{r-1}, Q_{r-1}) = (P_1, Q_1) = (-2, 1)$ is a solution of $2x^2 + 5xy + y^2 = -1$, whereas $(p_{m-1}, q_{m-1}) = (p_{-1}, q_{-1}) = (1, 0)$ is not a solution. Also

$$(-2, 9) \sim (-130, 57) \sim (-2, 1).$$

Hence the fundamental solution is $(-2, 1)$ and the complete solution is given by

$$x = -u + 4v, \quad y = (u - 3v)/2,$$

where $u^2 - 17v^2 = 4$.

References

[1] E. S. Barnes, The minimum of the product of two values of a quadratic form (I), *J. London Math. Soc.* (2) **1** (1951) 257–283.

[2] B. N. Delone, *The St. Petersburg School of Number Theory*, History of Mathematics **26**, Amer. Math. Soc., 2005.

[3] L. E. Dickson, *Introduction to the Theory of Numbers*, Dover, 1957.

[4] M. E. Gbur, The Markoff spectrum and minima of indefinite binary quadratic forms, *Proc. Amer. Math. Soc.* **63** (1977) 17–22.

[5] F. Halter–Koch, Principal ideals in quadratic orders, continued fractions and Diophantine equations, *J. Comb. Number Theory* **6** (2014) 17–30.

[6] G. H. Hardy and E. M. Wright, *An Introduction to Theory of Numbers*, Oxford University Press, 1962.

[7] A. A. Markov, Sur les formes binaires indéfinies, *Math. Ann.* **15** (1879) 381–406.

[8] K. R. Matthews, The Diophantine equation $ax^2 + bxy + cy^2 = N, D = b^2 - 4ac > 0$, *J. Théor. Nombres Bordeaux* **14** (2002) 257–270.

[9] K. R. Matthews, On the continued fractions of conjugage quadratic irrationalities, `http://www.numbertheory.org/pdfs/appendix.pdf`.

[10] K. R. Matthews, J. P. Robertson, and A. Srinivasan, On fundamental solutions of binary quadratic form equations, *Acta Arith.* **169** (2015) 291–299.

[11] M. Pavone, A remark on a theorem of Serret, *J. Number Theory* **23** (1986) 268–278.

[12] O. Perron, *Die Lehre von den Kettenbrüchen*, Band 1, B. G. Teubner, 1954.

[13] J. A. Serret, *Cours d'Algèbre supérieure*, Tome 1, Gauthier-Villars, 1885.

[14] B. Stolt, On a Diophantine equation of the second degree, *Ark. Mat.* **3** (1957) 381–390.

2000 *Mathematics Subject Classification*: Primary 11A55; Secondary 11A70, 11D09.
Keywords: quadratic diophantine equation, indefinite binary quadratic form, continued fraction, convergent, fundamental solution.

Received July 18 2017; revised version received September 16 2017. Published in *Journal of Integer Sequences*, October 29 2017.

Return to Journal of Integer Sequences home page.