Journal de Théorie des Nombres de Bordeaux

Keith Matthews

The diophantine equation $ax^2 + bxy + cy^2 = N$, $D = b^2 - 4ac > 0$

Journal de Théorie des Nombres de Bordeaux, tome 14, nº 1 (2002), p. 257-270

<http://www.numdam.org/item?id=JTNB_2002__14_1_257_0>

Journal de Théorie des Nombres
de Bordeaux **14** (2002), 257–270

The Diophantine equation $ax^2 + bxy + cy^2 = N,\ D = b^2 - 4ac > 0$

par KEITH MATTHEWS

RÉSUMÉ. Nous revisitons un algorithme dû à Lagrange, basé sur le développement en fraction continue, pour résoudre l'équation $ax^2 + bxy + cy^2 = N$ en les entiers x, y premiers entre eux, où $N \neq 0$, $\text{pgcd}(a, b, c) = \text{pgcd}(a, N) = 1$ et $D = b^2 - 4ac > 0$ n'est pas un carré.

ABSTRACT. We make more accessible a neglected simple continued fraction based algorithm due to Lagrange, for deciding the solubility of $ax^2 + bxy + cy^2 = N$ in relatively prime integers x, y, where $N \neq 0, \gcd(a, b, c) = \gcd(a, N) = 1$ and $D = b^2 - 4ac > 0$ is not a perfect square. In the case of solubility, solutions with least positive y, from each equivalence class, are also constructed.

Our paper is a generalisation of an earlier paper by the author on the equation $x^2 - Dy^2 = N$. As in that paper, we use a lemma on unimodular matrices that gives a much simpler proof than Lagrange's for the necessity of the existence of a solution.

Lagrange did not discuss an exceptional case which can arise when $D = 5$. This was done by M. Pavone in 1986, when $N = \pm\mu$, where $\mu = \min_{(x,y)\neq(0,0)} |ax^2+bxy+cy^2|$. We only need the special case $\mu = 1$ of his result and give a self-contained proof, using our unimodular matrix approach.

1. Introduction

The standard approach to solving the equation

$$ax^2 + bxy + cy^2 = N \tag{1.1}$$

in relatively prime integers x, y, is via reduction of quadratic forms, as in Mathews ([6, p 97]). There is a parallel approach in Faisant's book ([2, pp 106–113]) which uses continued fractions.

However, in a memoir of 1770, Lagrange ([11, Oeuvres II, pp 655–726]), gave a more direct method for solving (1.1) when $\gcd(a, b, c) = \gcd(a, N) = 1$ and $D = b^2 - 4ac > 0$ is not a perfect square. This paper seems to have

Manuscrit reçu le 23 janvier 2001.

been largely overlooked. (Admittedly, the necessity part of his proof is long and not easy to follow.)

M. Pavone ([10, p 271]) solved (1.1) when $N = \pm\mu$, where

$$\mu = \min_{(x,y)\neq(0,0)} |ax^2 + bxy + cy^2|.$$

He had essentially solved (1.1) in general, as Lagrange showed how to reduce the problem to the case $N = \pm 1$. (See (4.2) and (4.6)).

Strangely Pavone made no mention of Lagrange's paper, referring instead to Serret ([12, p 80]), who had earlier drawn attention to the possibility of an exceptional case.

A. Nitaj has also discussed the equation in his thesis, ([9, pp 57–88]), using a standard convergent sufficiency condition of Lagrange, which resulted in a restriction $D \geq 16$, thus making rigorous the necessity part of Lagrange's discussion. Nitaj discussed only the case $b = 0$ in detail, along the lines of Cornacchia ([1, pp 66–70]).

Our contribution in this paper is to use the convergent criterion of Lemma 2, which results in no restriction on D, while allowing us to deal with the non–convergent case, without having to appeal to the case $\mu = 1$ of Pavone, whose proof is somewhat complicated.

The continued fractions approach also has the attraction that it produces the solution (x, y) with least positive y from each class, if $\gcd(a, N) = 1$.

Our treatment generalises an earlier paper by the author on the equation $x^2 - Dy^2 = N$ (See Matthews [7]).

The assumption that $\gcd(a, N) = 1$ involves no loss of generality. For as pointed out by Gauss in his Disquisitiones (see [3, p 221] (also see Lemma 2 of Hua [5, pp 311–312]), there exist relatively prime integers α, γ such that $a\alpha^2 + b\alpha\gamma + c\gamma^2 = A$, where $\gcd(A, N) = 1$. Then if $\alpha\delta - \beta\gamma = 1$, the unimodular transformation $x = \alpha X + \beta Y, y = \gamma X + \delta Y$ converts $ax^2 + bxy + cy^2$ to $AX^2 + BXY + CY^2$. Also the two forms represent the same integers.

2. The structure of the solutions

We outline the structure of the integer solutions of (1.1) as given in Skolem ([13, pp 42–45]).

The primitive solutions $x + y\sqrt{D}$ of $ax^2 + bxy + cy^2 = N$ (i.e. with $\gcd(x, y) = 1$) fall into equivalence classes, with $x + y\sqrt{D}$ and $x' + y'\sqrt{D}$ being equivalent if and only if

$$2ax + by + y\sqrt{D} = \frac{(u + v\sqrt{D})}{2}(2ax' + by' + y'\sqrt{D}), \tag{2.1}$$

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

This is equivalent to the equations

$$x = (\frac{u - bv}{2})x' - cvy', \quad y = avx' + (\frac{u + bv}{2})y'. \tag{2.2}$$

It is easy to verify that (2.1) holds if and only if the following congruences hold:

$$2axx' + b(xy' + x'y) + 2cyy' \equiv 0 \pmod{|N|} \tag{2.3}$$

$$xy' - x'y \equiv 0 \pmod{|N|}. \tag{2.4}$$

Each primitive solution gives rise to a root n of the congruence

$$n^2 \equiv D \pmod{4|N|}.$$

In fact if (α, γ) is a solution of (1.1) and $\alpha\delta - \beta\gamma = 1$, then

$$n = (2a\alpha + b\gamma)\beta + (b\alpha + 2c\gamma)\delta. \tag{2.5}$$

Equivalent solutions give rise to congruent $n \pmod{2|N|}$.

Conversely, primitive solutions which give rise to congruent $n \pmod{2|N|}$ are equivalent. This follows from the equations

$$\begin{aligned} -\gamma n + 2N\delta &= 2a\alpha + b\gamma \\ \alpha n - 2N\beta &= b\alpha + 2c\gamma \end{aligned}$$

and congruences (2.3) and (2.4).

It is also straightforward to verify that if $ax^2 + bxy + cy^2$ is replaced by an equivalent form $AX^2 + BXY + CY^2$ under a unimodular transformation, then equivalent primitive representations (x, y) and (x', y') of N map into equivalent primitive representations (X, Y) and (X', Y'). In fact the n of equation (2.5) is replaced by Δn, where Δ is the determinant of the transformation. (See Gauss [3, pp 130–131].)

3. Some lemmas

Lemma 1. *Assume $D > 0$ is not a perfect square and $Q_0 | (P_0^2 - D)$.*

If $(P_n + \sqrt{D})/Q_n$ is the n-th complete convergent in the simple continued fraction for $x = (P_0 + \sqrt{D})/Q_0$ and $G_{n-1} = Q_0 A_{n-1} - P_0 B_{n-1}$, where A_{n-1}/B_{n-1} denotes a convergent to x, then

$$G_{n-1}^2 - DB_{n-1}^2 = (-1)^n Q_0 Q_n, \tag{3.1}$$

or equivalently

$$Q_0 A_{n-1}^2 - 2P_0 A_{n-1} B_{n-1} + \frac{P_0^2 - D}{Q_0} B_{n-1}^2 = (-1)^n Q_n. \tag{3.2}$$

Proof. See Mollin [8, pp 246–248]. □

Lemma 2. *If $\omega = \frac{P\zeta+R}{Q\zeta+S}$, where $\zeta > 1$ and P, Q, R, S are integers such that $Q > 0, S > 0$ and $PS - QR = \pm 1$, or $S = 0$ and $Q = 1 = R$, then P/Q is a convergent A_n/B_n to ω. Moreover if $Q \neq S > 0$, then $R/S = (A_{n-1} + kA_n)/(B_{n-1} + kB_n), k \geq 0$. Also $\zeta + k$ is the $(n+1)$-th complete convergent to ω. Here $k = 0$ if $Q > S$, while $k \geq 1$ if $Q < S$.*

Proof. This is an extension of Theorem 172, Hardy and Wright ([4, pp 140—141]), who dealt with the case $Q > S > 0$. See Matthews [7, pp 325–326]. □

The following result is a special case ($\mu(f) = 1$) of a result due to M. Pavone, [10, p 271]. Pavone's proof is rather complicated and we give a self–contained proof using our Lemma 2 as cases (ii) and (iii)(c) of the proof of Lemma 3 below and in the Appendix.

Lemma 3. *Suppose $X, y > 0, Q, n, R$ are integers and*

$$QX^2 + nXy + Ry^2 = 1, \tag{3.3}$$

where $D = n^2 - 4QR > 0$ is not a perfect square. Also let $\omega = \frac{-n+\sqrt{D}}{2Q}$ and $\omega^* = \frac{-n-\sqrt{D}}{2Q}$ be the roots of $Q\theta^2 + n\theta + R = 0$. Then either

(i) *X/y is a convergent A_{i-1}/B_{i-1} to ω (resp. ω^*) and if $(P_i + \sqrt{D})/Q_i$ denotes the i-th complete convergent to ω (resp. ω^*), then $Q_i = (-1)^i 2$ (resp. $Q_i = (-1)^{i+1}2$), or*

(ii) *$D = 5$, $Q < 0$ and*

$$X/y = (A_r - A_{r-1})/(B_r - B_{r-1}) = (A'_s - A'_{s-1})/(B'_s - B'_{s-1}),$$

where A_r/B_r and A'_s/B'_s denote convergents to ω and ω^*, respectively and

$$\omega = [a_0, \dots, a_r, \overline{1}],\ \omega^* = [b_0, \dots, b_s, \overline{1}],$$

where $a_r > 1$ if $r > 0$ and $b_s > 1$ if $s > 0$.

Moreover X/y is not a convergent to ω or ω^*.

Conversely, if (i) *or* (ii) *hold, then X/y is a solution of (3.3).*

Remarks. (a) In the Appendix, we prove that if $D = 5$ and $Q < 0$, then $r - 1 \equiv s \pmod 2$ and

$$(A_r - A_{r-1})/(B_r - B_{r-1}) = (A'_s - A'_{s-1})/(B'_s - B'_{s-1}),$$

the latter being obtained directly by an appeal to symmetry by Pavone ([10, p 277]).

(b) As Pavone points out, we have

$$\frac{A_{r-2}}{B_{r-2}} < \frac{A_r - A_{r-1}}{B_r - B_{r-1}} < \frac{A_r}{B_r} < \omega \text{ if } r \text{ is even,}$$

$$\omega<\frac{A_r}{B_r}<\frac{A_r-A_{r-1}}{B_r-B_{r-1}}<\frac{A_{r-2}}{B_{r-2}} \text{ if } r \text{ is odd.}$$

The corresponding equations hold if ω is replaced by ω^*, each A_r is replaced by A'_s and each B_r is replaced by B'_s etc.

Consequently, $\frac{A_r-A_{r-1}}{B_r-B_{r-1}}$ is not a convergent to ω or ω^*.

(c) If n is even, say $n=2P$, then $\omega=(-P+\sqrt{\Delta})/Q$ and $\omega^*=(-P-\sqrt{\Delta})/Q$, where $\Delta=P^2-QR$. If we then denote the n–th complete convergent to ω (resp. ω^*) by $(P_n+\sqrt{\Delta})/Q_n$, condition (i) becomes $Q_i=(-1)^i$ (resp $Q_i=(-1)^{i+1}$).

Proof. Suppose (3.3) holds. Consider the matrix

$$H=\begin{pmatrix} X & t \\ y & QX+Py \end{pmatrix},$$

where $t=-PX-Ry$ if $n=2P$, while $t=-(P+1)X-Ry$ if $n=2P+1$.

Then in both cases,

$$\det H=QX^2+nXy+Ry^2=1. \tag{3.4}$$

Also it is straightforward to verify that

$$\omega=\frac{X\alpha+t}{y\alpha+QX+Py},$$

where

$$\alpha=\begin{cases}\sqrt{\Delta} & \text{if } n=2P,\\ \frac{\sqrt{D}+1}{2} & \text{if } n=2P+1.\end{cases}$$

Case (i). Suppose $QX+Py>0$. Then as $\alpha>1$, Lemma 2 applies and X/y is a convergent to ω.

Case (ii). Suppose $QX+Py=0$. On substituting for QX in (3.4), we get

$$(-Py)X+nXy+Ry^2=1.$$

Hence $y=1$ and $-PX+nX+R=1$. Also $\omega=X-\frac{1}{\alpha}$.

Hence

$$\omega^*=\begin{cases}X+\frac{1}{\sqrt{\Delta}} & \text{if } n=2P,\\ X+\frac{1}{\frac{\sqrt{D}-1}{2}} & \text{if } n=2P+1.\end{cases}$$

Hence $X/y=\lfloor\omega^*\rfloor$ is a convergent to ω^* if $D\neq5$.

If $D=5$, we see $\omega^*=[X+1,\overline{1}]$ $(s=0)$ and $\omega=[X-1,2,\overline{1}]$ $(r=1)$.

Then

$$\begin{aligned}\frac{A_1 - A_0}{B_1 - B_0} &= \frac{(2X-1)-(X-1)}{2-1} = X,\\ \frac{A'_0 - A'_{-1}}{B'_0 - B'_{-1}} &= \frac{(X+1)-1}{1-0} = X.\end{aligned}$$

Also $QX^2 + (2P+1)X + R = 1$ and $P = -QX$ together give

$$-QX^2 + X + R = 1.$$

Hence

$$\begin{aligned}1 = \frac{D-1}{4} &= P^2 + P - QR = Q^2X^2 - QX - QR\\ &= Q(QX^2 - X - R) = -Q\end{aligned}$$

and hence $Q < 0$.

Case (iii) (a) Suppose $QX + Py < 0$. Then $-(QX+Py) > 0$ and

$$\omega^* = \frac{X(-\alpha^*) - t}{y(-\alpha^*) - (QX+Py)},$$

where $-\alpha^* > 1$ if $D \neq 5$.

Hence X/y is a convergent to ω^*, unless $D = 5$.

(b) If $D = 5$ and $-(QX+Py) \geq y$, then

$$\omega^* = \frac{X - t\alpha}{y - (QX+Py)\alpha} \tag{3.5}$$

and again X/y is a convergent to ω^* by Lemma 2.

In all cases where X/y is the convergent A_{n-1}/B_{n-1} to ω (resp. ω^*), it follows from (3.3) and equation (3.2) of Lemma 1, with $P_0 = -n, Q_0 = 2Q$ (resp. $P_0 = n, Q_0 = -2Q$), that

$$\begin{aligned}(-1)^n Q_n &= Q_0A_{n-1}^2 - 2P_0A_{n-1}B_{n-1} + \frac{P_0^2 - D}{Q_0}B_{n-1}^2\\ &= \begin{cases} 2QX^2 + 2nXy + 2Ry^2 = 2 & \text{for } \omega,\\ -2QX^2 - 2nXy - 2Ry^2 = -2 & \text{for } \omega^*\end{cases}\end{aligned}$$

and consequently $(-1)^nQ_n = 2$ (resp. -2) in all cases.

(c) Now suppose $D = 5$ and $y > -(QX+Py) > 0$.

Now, from (3.5), Lemma 2 tells us that

$$\begin{aligned}\frac{X}{y} &= \frac{A_{i-1} + kA_i}{B_{i-1} + kB_i} \qquad (3.6)\\ (P+1)X + Ry &= -t = A_i\\ -(QX+Py) &= B_i,\end{aligned}$$

where $k \geq 1$. Moreover $\omega^*_{i+1} = \alpha + k = [k+1, \overline{1}]$.

Hence $\omega^* = [a_0, \ldots, a_s, \overline{1}]$, where $s = i+1$ and $a_s = k+1$.
Hence (3.6) gives

$$\begin{aligned}\frac{X}{y} &= \frac{A_{s-2}+(a_s-1)p_{s-1}}{B_{s-2}+(a_s-1)B_{s-1}}\\ &= \frac{A_s-A_{s-1}}{B_s-B_{s-1}}.\end{aligned}$$

Next we prove that $Q<0$. We have from equation (1.1)),

$$\begin{aligned}1 &= QX^2+(2P+1)Xy+Ry^2\\ Q &= Q^2X^2+(2P+1)QXy+QRy^2\\ &= (QX+Py)^2+(QX+Py-y)y\\ &= (-B_{s-1})^2+(-B_{s-1}-(B_s-B_{s-1}))(B_s-B_{s-1})\\ &= B_{s-1}^2+B_{s-1}B_s-B_s^2\\ &= -\frac{1}{4}((2B_s-B_{s-1})^2-5B_{s-1}^2). \qquad (3.7)\end{aligned}$$

However

$$B_s = a_sB_{s-1}+B_{s-2} \geq 2B_{s-1} > \left(\frac{1+\sqrt{5}}{2}\right)B_{s-1}$$

so

$$2B_s-B_{s-1} > \sqrt{5}B_{s-1}$$

and hence

$$(2B_s-B_{s-1})^2-5B_{s-1}^2>0.$$

Then equation (3.7) gives $Q<0$. □

4. The main result

Theorem 1. *Suppose*

$$ax^2+bxy+cy^2=N, \qquad (4.1)$$

where $N\neq 0$, $\gcd(x,y)=1=\gcd(a,N)$ *and* $y>0$ *and* $D=b^2-4ac>0$ *is not a perfect square.*

Let θ *satisfy* $x\equiv y\theta \pmod{|N|}$, $0\leq\theta<|N|$. *Then*

$$a\theta^2+b\theta+c\equiv 0 \pmod{|N|}.$$

Let $x=y\theta+|N|X$, $n=2a\theta+b$, $Q=a|N|$, $\omega=\frac{-n+\sqrt{D}}{2Q}$ *and* $\omega^*=\frac{-n-\sqrt{D}}{2Q}$.

Also let $n=2P$ *or* $2P+1$, *according as* b *is even or odd. Then*

(i) *if* $QX+Py>0$, X/y *is a convergent to* ω;

(ii) *Suppose* $QX+Py\leq 0$. *Then*

(a) *If $D \neq 5$, or $D = 5$ and $-(QX+Py) \geq y$, then X/y is a convergent to ω^*.*

(b) *If $D = 5$ and $y > -(QX+Py) \geq 0$, then*

$$\frac{X}{y} = \frac{A_r - A_{r-1}}{B_r - B_{r-1}} = \frac{A'_s - A'_{s-1}}{B'_s - B'_{s-1}}$$

which is not a convergent to ω or ω^*.
Also $aN < 0$.

Conversely,

(a) *if X/y is a convergent A_{i-1}/B_{i-1} to ω (resp. ω^*) and $Q_i = (-1)^i 2N/|N|$ (resp. $(-1)^{i+1}2N/|N|$), or*

(b) *if $D = 5, aN < 0$ and $\frac{X}{y} = \frac{A_r - A_{r-1}}{B_r - B_{r-1}}$, where r is defined earlier,*

then (x, y), with $x = y\theta + |N|X$, will be a solution to (4.1), possibly imprimitive.

Proof. Suppose

$$ax^2 + bxy + cy^2 = N,$$

where $\gcd(x, y) = 1 = \gcd(a, N)$ and $y > 0$. Then clearly $\gcd(y, |N|) = 1$. Let $x \equiv y\theta \pmod{|N|}$ and

$$x = y\theta + |N|X. \tag{4.2}$$

Then

$$a\theta^2y^2 + b(y\theta)y + cy^2 \equiv 0 \pmod{|N|}$$

$$a\theta^2 + b\theta + c \equiv 0 \pmod{|N|} \tag{4.3}$$

$$4a^2\theta^2 + 4ab\theta + 4ac \equiv 0 \pmod{4|N|} \tag{4.4}$$

$$(2a\theta + b)^2 \equiv b^2 - 4ac \pmod{4|N|},$$

$$\text{or } n^2 \equiv D \pmod{4|N|}. \tag{4.5}$$

Also

$$a(y\theta + |N|X)^2 + b(y\theta + |N|X)y + cy^2 = N$$

$$|N|^2aX^2 + (2a\theta + b)|N|Xy + (a\theta^2 + b\theta + c)y^2 = N$$

$$QX^2 + nXy + Ry^2 = \frac{N}{|N|}, \tag{4.6}$$

where $Q = a|N|$, $R = (a\theta^2 + b\theta + c)/|N|$ and $n^2 - 4QR = D$.

The conclusions of the theorem then follow from Lemma 3, applied to the equation $Q'X^2 + n'Xy + R'y^2 = 1$, where $Q' = \epsilon Q, n' = \epsilon n, R' = \epsilon R$ and $\epsilon = |N|/N$. □

5. The algorithm

Let $\Delta = D/4$ if b is even and let the i–th complete convergent to ω or ω^* be denoted by $(P_i+\sqrt{\Delta})/Q_i$ or $(P_i+\sqrt{D})/Q_i$, according as b is even or odd.

If equation (4.1) is soluble with $x \equiv y\theta \pmod{|N|}$, $y>0$, there will be infinitely many solutions because of equations (2.2). It follows that if ω and ω^* are not purely periodic, we need only examine the first period $m \le i \le m+l$ of the continued fractions for ω and ω^* to determine solubility of (4.1). For, with ω (resp. ω^*) being $(-P\pm\sqrt{\Delta})/Q$ (resp. $(-(2P+1)\pm\sqrt{D})/2Q$), the equation $Q_i=\pm 1$ (resp. ± 2) will hold for infinitely many i by periodicity and so there will be at least one such i in the range $m \le i \le m+l$. Any such i must have $Q_i = 1$ (resp. 2), as $(P_i+\sqrt{\Delta})/Q_i$ (resp. $(P_i+\sqrt{D})/Q_i$) is reduced for i in this range and so $Q_i>0$. Moreover if l is even, the sign of $(-1)^i N/|N|$ is preserved from one period to the next. If l is odd, then the first or second period will produce a solution. If ω or ω^* is purely periodic, we must examine Q_2, which corresponds to the third period.

Moreover there can be at most one i in a period for which $Q_i=1$ (resp. 2). For if $P_i+\sqrt{\Delta}$ (resp. $(P_i+\sqrt{D})/2$ is reduced, then $P_i=\lfloor\sqrt{\Delta}\rfloor$ (resp. $P_i = 2\lfloor(\sqrt{D}-1)/2\rfloor+1$) and hence two such occurrences of $Q_i=1$ (resp. 2) within a period would give a smaller period.

Hence we have the following algorithm essentially due to Lagrange, apart from stage 1:

1. If $\gcd(a,N)>1$, find a unimodular transformation of the given quadratic form into one in which $\gcd(a,N)=1$. (See the last paragraph of the Introduction.)

2. Find all solutions θ of the congruence (4.3) in the range $0\le\theta<|N|$. (This can be done as follows:

First solve $t^2 \equiv b^2-4ac \pmod{4|N|}$, $-|N|<t\le|N|$. (If there are no solutions t, then there is no primitive solution of (4.1) corresponding to t.)

Then solve $a\theta \equiv \frac{t-b}{2} \pmod{|N|}$, $0\le\theta<|N|$.)

For each θ, let $n=2a\theta+b$, $P=\lfloor n/2\rfloor$ and $Q=a|N|$.

3. For each of the numbers $\omega=\frac{-P+\sqrt{\Delta}}{Q}$ (resp. $\frac{-(2P+1)+\sqrt{D}}{2Q}$), test the first period to see if $Q_i=1$ (resp. 2) occurs. If l is even, test additionally for $1=(-1)^iN/|N|$ (resp. $2=(-1)^iN/|N|$) to hold.

Similarly for each of the numbers $\omega^*=\frac{-P-\sqrt{\Delta}}{Q}$ (resp. $\frac{-(2P+1)-\sqrt{D}}{2Q}$), with i replaced by $i+1$.

If $D=5$, test additionally to see if $aN<0$ holds.

4. For each θ and corresponding ω for which test 3 succeeds, find the least i for which the condition $Q_i=(-1)^iN/|N|$ (resp. $Q_i=(-1)^i2N/|N|$)

holds. If l is even, this will occur in or before the first period, while if l is odd, this will occur in or before the second period. Similarly for ω^*.

For the corresponding convergent A_{i-1}/B_{i-1} to ω or ω^*, write $X = A_{i-1}$, $y = B_{i-1}$. If $D = 5$ and $aN < 0$, in relation to ω, write $X = A_r - A_{r-1}, y = B_r - B_{r-1}$. Then $x = y\theta + |N|X$ produces a solution of (4.1) with $x \equiv y\theta \pmod{|N|}$.

Choose the solution (x, y) with lesser of the y values.

The algorithm will produce a solution (x, y) from each class, with the additional feature that the least positive y is chosen, if the quadratic form satisfies $\gcd(a, N) = 1$.

6. Examples

Example 1 (Gauss, Article 205). [3, p 189]

$$42x^2 + 62xy + 21y^2 = 585. \tag{6.1}$$

As gcd (42, 585) = 3 = gcd (21, 585), we make a suitable transformation

$$x = -x' + y', y = 2x' - y',$$

which gives

$$42x^2 + 62xy + 21y^2 = 2x'^2 + 18x'y' + y'^2.$$

The latter form has $\Delta = 79$ and $\gcd(2, 585) = 1$.

We list the roots of $2\theta^2 + 18\theta + 1 \equiv 0 \pmod{585}$ and corresponding values $P = 2\theta + 9$:

θ	34	47	74	164	412	502	529	542
P	77	103	157	337	833	1013	1067	1093

We find that only $P = 157$ and 1013 give solutions of equation (6.1):

(i) $\omega = (-157 + \sqrt{79})/1170$ gives $Q_3 = 1$, $A_2/B_2 = -1/7$.

Then $y' = 7$ and $x' = 7 \cdot 74 - 585 \cdot 1 = -67$. Hence $(x, y) = (74, -141)$ is a solution of (6.1).

$\omega^* = (-157 - \sqrt{79})/1170$ also gives the solution $(74, -141)$.

(ii) $\omega = (-1013 + \sqrt{79})/1170$ gives $Q_2 = 1$, $A_1/B_1 = -6/7$. Then $y' = 7$ and $x' = 7 \cdot 502 - 585 \cdot 6 = 4$. Hence $(x, y) = (3, 1)$ is a solution of (6.1).

$\omega^* = (-1013 - \sqrt{79})/1170$ also gives the solution $(3, 1)$.

In fact Gauss gave solutions $(83, -87)$ and $(3, 1)$. In the notation of (2.2), the solutions $(x, y) = (83, -87)$ and $(x', y') = (74, -141)$ are related by the solution $(u, v) = (-80, 9)$ of the Pell equation $x^2 - 79y^2 = 1$.

Summarising:

$42x^2 + 62xy + 21y^2 = 585$	
Solution	$n \pmod{1170}$
$(74, -141)$	314
$(3, 1)$	-314

Example 2. $3x^2 - 3xy - 2y^2 = 202$.

Here $D = 33$.

The solutions of $3\theta^2 - 3\theta - 2 \equiv 0 \pmod{202}$ are $39, 63, 140, 164$, with corresponding n values $231, 375, 837, 981$.

(i) $\theta = 39$, $\omega = (-231 + \sqrt{33})/1212$, $Q_3 = -2, A_2/B_2 = -1/5$.
Then $x = y\theta + |N|X = 5 \cdot 39 + 202 \cdot (-1) = -7$ and $(x, y) = (-7, 5)$.
$\omega^* = (-231 - \sqrt{33})/1212$ produces the same solution.

(ii) $\theta = 63$, $\omega = (-375 + \sqrt{33})/1212$, $Q_6 = 2, A_5/B_5 = -7/23$.
Then $x = 23 \cdot 63 + 202 \cdot (-7) = 35$ and $(x, y) = (35, 23)$.
$\omega^* = (-375 - \sqrt{33})/1212$ gives $Q_5 = 2, A_4/B_4 = -11/35$.
Then $x = 35 \cdot 63 + 202 \cdot (-11) = -17$ and we get the equivalent solution $(-17, 35)$.

(iii) $\theta = 140$, $\omega = (-837 + \sqrt{33})/1212$, $Q_4 = 2, A_3/B_3 = -24/35$.
Then $x = 35 \cdot 140 + 202 \cdot (-24) = 52$ and $(x, y) = (52, 35)$.
$\omega^* = (-837 - \sqrt{33})/1212$ gives $Q_5 = 2, A_4/B_4 = -16/23$.
Then $x = 23 \cdot 140 + 202 \cdot (-16) = -12$ and we get the equivalent solution $(-12, 23)$.

(iv) $\theta = 164$, $\omega = (-981 + \sqrt{33})/1212$, $Q_2 = 2, A_1/B_1 = -4/5$.
Then $x = 5 \cdot 164 + 202 \cdot (-4) = 12$ and $(x, y) = (12, 5)$.
$\omega^* = (-981 - \sqrt{33})/1212$ produces the same solution.

Summarising:

$3x^2 - 3xy - 2y^2 = 202$	
Solution	$n \pmod{404}$
$(35, 23)$	29
$(-12, 23)$	-29
$(12, 5)$	231
$(-7, 5)$	-231

There are 4 equivalence classes of solutions.

Example 3. $f(x, y) = 19x^2 - 85xy + 95y^2 = -671$.

Here $D = 5$.

The solutions of $19\theta^2 - 85\theta + 95 \equiv 0 \pmod{671}$ are $443, 454, 504, 515$, with corresponding n values $16749, 17167, 19067, 19485$.

The exceptional solutions give the solutions with smallest y:

(i) $\theta = 443$: $\omega = (-16749 + \sqrt{5})/25498 = [-1, 2, 1, 10, 1, 1, 2, \overline{1}]$,
$Q_7 = 2, A_5/B_5 = -44/67$. Also $A_6/B_6 = -111/169$.

Exceptional solution:
$(X, y) = (A_6 - A_5, B_6 - B_5) = (-67, 102)$, $(x, y) = (229, 102)$.
$\omega^* = [-1, 2, 1, 10, 3, \overline{1}]$ gives $Q_6 = 2$ and correspondingly $(x, y) = (301, 137)$.

(ii) $\theta = 454$: $\omega = (-17167 + \sqrt{5})/25498 = [-1, 3, 16, 1, 2, \overline{1}]$,
$Q_5 = 2, A_3/B_3 = -35/52$. Also $A_4/B_4 = -103/153$.
Exceptional solution:
$(X, y) = (A_4 - A_3, B_4 - B_3) = (-68, 101)$, $(x, y) = (226, 101)$.
$\omega^* = [-1, 3, 16, 3, \overline{1}]$ gives $Q_4 = 2$ and correspondingly $(x, y) = (329, 150)$.

(iii) $\theta = 504$: $\omega = (-19067 + \sqrt{5})/25498 = [-1, 3, 1, 26, 2, \overline{1}]$,
$Q_5 = 2, A_3/B_3 = -80/107$ and $A_4/B_4 = -163/218$.
Exceptional solution:
$(X, y) = (A_4 - A_3, B_4 - B_3) = (-83, 111)$, $(x, y) = (251, 111)$.
$\omega^* = [-1, 3, 1, 28, \overline{1}]$ gives $Q_4 = 2$ and correspondingly $(x, y) = (254, 115)$.

(iv) $\theta = 515$: $\omega = (-19485 + \sqrt{5})/25498 = [-1, 4, 4, 5, 2, \overline{1}]$,
$Q_5 = 2, A_3/B_3 = -68/89$. Also $A_4/B_4 = -149/195$.
Exceptional solution:
$(X, y) = (A_4 - A_3, B_4 - B_3) = (-81, 106)$, $(x, y) = (239, 106)$.
$\omega^* = [-1, 4, 4, 7, \overline{1}]$ gives $Q_4 = 2$ and correspondingly $(x, y) = (271, 123)$.

Summarising:

$19x^2 - 85xy + 95y^2 = -671.$	
Solution	$n \pmod{1342}$
$(226, 101)$	279
$(251, 111)$	-279
$(239, 106)$	645
$(229, 102)$	-645

There are 4 equivalence classes of solutions.

7. Appendix

Lemma 4. *Let*

$$\omega = \frac{-(2P+1) + \sqrt{5}}{2Q} = [a_0, \dots, a_r, \overline{1}],$$

$$\omega^* = \frac{-(2P+1) - \sqrt{5}}{2Q} = [b_0, \dots, b_s, \overline{1}],$$

where $a_r > 1$ if $r > 0$ and $b_s > 1$ if $s > 0$. Then $r - 1 \equiv s \pmod{2}$ and

$$A_r - A_{r-1} = A'_s - A'_{s-1} \text{ and } B_r - B_{r-1} = B'_s - B'_{s-1}.$$

Proof. We have

$$\omega = \frac{-P + \alpha^{-1}}{Q} = \frac{A_r\alpha + A_{r-1}}{B_r\alpha + B_{r-1}}$$

and hence

$$(7.1) \qquad QA_r = -PB_r + B_{r-1}$$

$$(7.2) \qquad -QA_{r-1} = -B_r + (P+1)B_{r-1}.$$

Then (7.1) gives

$$(7.3) \qquad B_{r-1} = PB_r + QA_r,$$

and (7.2) and (7.3) give

$$\begin{aligned} -QA_{r-1} &= -B_r + (P+1)(PB_r + QA_r) \\ &= -B_r + P(P+1)B_r + Q(P+1)A_r \\ &= QRB_r + Q(P+1)A_r. \end{aligned}$$

Hence

$$(7.4) \qquad -A_{r-1} = RB_r + (P+1)A_r.$$

Also (7.2) and (7.3) imply

$$(7.5) \qquad -A_r = PA_{r-1} + RB_{r-1}.$$

Now let $X = A_r - A_{r-1}$, $y = B_r - B_{r-1}$.
Hence

$$\begin{aligned} QX^2 + (2P+1)Xy + Ry^2 &= X(QX + Py) + y((P+1)X + Ry) \\ &= (A_r - A_{r-1})(2B_{r-1} - B_r) \\ &\qquad + (B_r - B_{r-1})(A_r - 2A_{r-1}) \\ &= A_rB_{r-1} - A_{r-1}B_r = (-1)^{r-1}. \end{aligned}$$

Now $y = B_r - B_{r-1} \geq B_r - 2B_{r-1} = -(QX + Py) \geq 0$.
Similarly with

$$\omega^* = \frac{-P - \alpha}{Q} = \frac{A'_s\alpha + A'_{s-1}}{B'_s\alpha + B'_{s-1}}$$

and with $X = A'_s - A'_{s-1}, y = B'_s - B'_{s-1}$, we find

$$\begin{aligned} QX + Py &= -B'_{s-1} \\ (P+1)X + Ry &= A'_{s-1}, \end{aligned}$$

and

$$QX^2 + (2P+1)Xy + Ry^2 = (-1)^s.$$

Also

$$y = B'_s\alpha - B'_{s-1} \geq B'_{s-1} = -(QX + Py) \geq 0.$$

It follows from cases (ii) and (iii)(c) in the proof of Lemma 3, that

$$(-1)^{r-1}Q < 0, \ (-1)^s Q < 0$$

and

$$A_r - A_{r-1} = A'_s - A'_{s-1} \text{ and } B_r - B_{r-1} = B'_s - B'_{s-1}.$$

□

Acknowledgement

The author is grateful to John Robertson for improving the presentation of the paper.

The algorithm has been implemented in the author's number theory calculator program CALC, available at `http://www.maths.uq.edu.au/~krm/`

References

[1] G. CORNACCHIA, *Su di un metodo per la risoluzione in numeri interi dell' equazione* $\sum_{h=0}^{n} C_h x^{n-h} = P$. Giornale di Matematiche di Battaglini **46** (1908), 33–90.
[2] A. FAISANT, *L'equation diophantienne du second degré*. Hermann, Paris, 1991.
[3] C. F. GAUSS, *Disquisitiones Arithmeticae*. Yale University Press, New Haven, 1966.
[4] G. H. HARDY, E. M. WRIGHT, *An Introduction to Theory of Numbers*, Oxford University Press, 1962.
[5] L. K. HUA, *Introduction to Number Theory*. Springer, Berlin, 1982.
[6] G. B. MATHEWS, *Theory of numbers*, 2nd ed. Chelsea Publishing Co., New York, 1961.
[7] K. R. MATTHEWS, *The Diophantine equation* $x^2 - Dy^2 = N, D > 0$. Exposition. Math. **18** (2000), 323–331.
[8] R. A. MOLLIN, *Fundamental Number Theory with Applications*. CRC Press, New York, 1998.
[9] A. NITAJ, *Conséquences et aspects expérimentaux des conjectures abc et de Szpiro*. Thèse, Caen, 1994.
[10] M. PAVONE, *A Remark on a Theorem of Serret*. J. Number Theory **23** (1986), 268–278.
[11] J. A. SERRET (Ed.), *Oeuvres de Lagrange, I–XIV*, Gauthiers–Villars, Paris, 1877.
[12] J. A. SERRET, *Cours d'algèbre supérieure*, Vol. I, 4th ed. Gauthiers–Villars, Paris, 1877.
[13] T. SKOLEM, *Diophantische Gleichungen*, Chelsea Publishing Co., New York, 1950.

Keith MATTHEWS
Department of Mathematics
University of Queensland
4072 Brisbane, Australia
E-mail : `krm@maths.uq.edu.au`