Solving $Ax^2 - By^2 = N$ in integers, where $A > 0, B > 0$ and $D = AB$ is not a perfect square and $\gcd(A, B) = \gcd(A, N) = 1$.

Keith Matthews

Abstract

This generalises an earlier algorithm of the author for solving $x^2 - Dy^2 = N$.

Remark If D is a perfect square, say $D = C^2$, then the given equation is equivalent to $A^2x^2 - C^2y^2 = AN$, which is easily solved.

Equivalence classes of primitive solutions of $Ax^2 - By^2 = N$.

The identity

$$(Ax^2 - By^2)(u^2 - Dv^2) = \\ A(xu + yvB)^2 - B(uy + Avx)^2$$

shows that a solution (x, y) of $Ax^2 - By^2 = N$ and a solution (u, v) of Pell's equation $u^2 - Dv^2 = 1$, together produce a solution

$$(x', y') = (xu + yvB, uy + Avx)$$

of $Ax'^2 - By'^2 = N$. Moreover if $\gcd(x, y) = 1$, then $\gcd(x', y') = 1$.

Note that

$$Ax' + y'\sqrt{D} = (Ax + y\sqrt{D})(u + v\sqrt{D}). \qquad (1)$$

Equation (1) defines an equivalence relation on the set of all primitive solutions of $Ax^2 - By^2 = N$.

Attaching a residue class P (mod $|N|$) to each equivalence class.

If $Ax^2 - By^2 = N, \gcd(x, y) = 1 = \gcd(A, N)$, then $\gcd(y, N) = 1$.

Hence we can define $P, -|N|/2 < P \leq |N|/2$, by $x \equiv yP \pmod{|N|}$. Then

$$\begin{aligned} Ax^2 - By^2 &\equiv 0 \pmod{|N|} \\ Ay^2P^2 - By^2 &\equiv 0 \pmod{|N|} \\ AP^2 - B &\equiv 0 \pmod{|N|} \\ AP^2 &\equiv B \pmod{|N|}. \end{aligned}$$

Primitive solutions (x, y) and (x', y') are equivalent if and only if

$$\begin{aligned} Axx' - yy'B &\equiv 0 \pmod{|N|} \\ yx' - xy' &\equiv 0 \pmod{|N|}. \end{aligned}$$

Then (x, y) and (x', y') are equivalent if and only if $P \equiv P' \pmod{|N|}$.

Hence the number of equivalence classes is finite.

If (x, y) is a solution for a class C, then $(-x, y)$ is a solution for the *conjugate* class C^*.

It can happen that $C^* = C$, in which case C is called an *ambiguous* class.

The solution (x, y) in a class with least $y > 0$ is called a *fundamental* solution.

For an ambiguous class, there are either two (x, y) and $(-x, y)$ with least $y > 0$ if $x > 0$ and one if $x = 0$, namely $(0, 1)$ and we choose the one with $x \geq 0$.

Continued fractions of quadratic irrationalities.

Let $\omega = \frac{P_0+\sqrt{D}}{Q_0} = [a_0, a_1, \ldots,]$, where $Q_0 | (P_0^2 - D)$.

Then the n–th *complete quotient* $x_n = [a_n, a_{n+1}, \ldots,] = (P_n + \sqrt{D})/Q_n$.

There is a simple algorithm for calculating a_n, P_n and Q_n:

$$a_n = \left\lfloor \frac{P_n+\sqrt{D}}{Q_n} \right\rfloor, \quad (2)$$

$$P_{n+1} = a_n Q_n - P_n,$$

$$Q_{n+1} = \frac{D-P_{n+1}^2}{Q_n}.$$

We also note the following important identity

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

where $G_{n-1} = Q_0 A_{n-1} - P_0 B_{n-1}$.

With $\omega^* = \frac{P_0-\sqrt{D}}{Q_0}$, we have

$$G_{n-1}^2 - DB_{n-1}^2 = (-1)^{n+1} Q_0 Q_n.$$

Necessary conditions for solubility of $Ax^2 - By^2 = N$.

Suppose $Ax^2 - By^2 = N, \text{gcd}(x, y) = 1 = \text{gcd}(A, B) = \text{gcd}(A, N), A > 0, B > 0, y > 0$.

We have $x \equiv yP \pmod{|N|}$ and $AP^2 \equiv B \pmod{|N|}$. Also the symmetry $(x, y) \leftrightarrow (-x, y)$ allows us to assume $0 \le P \le |N|/2$.

Let $x = Py + |N|X$. Then

Substituting for $x = Py + |N|X$ in the equation $Ax^2 - By^2 = N$ gives

$A|N|X^2 + 2APXy + \frac{(AP^2-B)}{|N|}y^2 = \frac{N}{|N|}$.

(i) If $x \geq 0$, then

(a) X/y is a convergent A_{n-1}/B_{n-1} to $\omega = \frac{-AP+\sqrt{D}}{A|N|}$,

(b) $(x, y) = (G_{n-1}/A, B_{n-1})$,

(c) $Q_n = (-1)^n \frac{N}{|N|}$.

(ii) If $x < 0$, then

(a) X/y is a convergent A_{m-1}/B_{m-1} to $\omega^* = \frac{-AP-\sqrt{D}}{A|N|}$,

(b) $(x, y) = (G_{m-1}/A, B_{m-1})$,

(c) $Q_m = (-1)^{m+1} \frac{N}{|N|}$.

We prove (i) (a) and (ii) (a) by using the following extension of Theorem 172 in Hardy and Wright's book:

Lemma. If $\omega = \frac{U\zeta+R}{V\zeta+S}$, where $\zeta > 1$ and U, V, R, S are integers such that $V > 0, S > 0$ and $US - VR = \pm 1$, or $S = 0$ and $V = R = 1$, then U/V is a convergent to ω.

We apply the Lemma to the integer matrix

$$\begin{bmatrix} U & R \\ V & S \end{bmatrix} = \begin{bmatrix} X & \frac{-APx+By}{|N|} \\ y & Ax \end{bmatrix}.$$

The matrix has determinant

$$\begin{aligned} \Delta &= XAx - y\frac{(-APx+By)}{|N|} \\ &= \frac{Ax(x-Py)+APxy-By^2}{|N|} \\ &= \frac{Ax^2-By^2}{|N|} \\ &= \pm 1. \end{aligned}$$

Also if $\zeta = \sqrt{D}$ and $\omega = (-AP+\sqrt{D})/A|N|$, it is easy to verify that $\omega = \frac{U\zeta+R}{V\zeta+S}$ and that $S = 0$ implies $V = R = 1$.

The lemma now implies that $U/V = X/y$ is a convergent A_{n-1}/B_{n-1} to ω. Also

$$\begin{aligned} G_{n-1} &= Q_0 A_{n-1} - P_0 B_{n-1} \\ &= (A|N|)X - (-AP)y = Ax. \end{aligned}$$

Hence

$$\begin{aligned} N = Ax^2 - By^2 &= \frac{G_{n-1}^2}{A} - BB_{n-1}^2 \\ &= \frac{G_{n-1}^2 - DB_{n-1}^2}{A} \\ &= \frac{(-1)^n A|N|Q_n}{A} \\ &= (-1)^n |N| Q_n. \end{aligned}$$

Hence $Q_n = (-1)^n N/|N|$.

If $x < 0$, then $\omega^* = \frac{-X\sqrt{D}+R}{-y\sqrt{D}+x} = \frac{X\sqrt{D}-R}{y\sqrt{D}-x}$ and X/y is a convergent A_{m-1}/B_{m-1} to ω^*.

Again, $G_{m-1} = Ax$ and $Q_m = (-1)^{m+1}N/|N|$.

Refining the necessary condition for solubility

Lemma. An equivalence class of solutions contains an (x, y) with $x \geq 0$ and $y > 0$.

Proof. Let (x_0, y_0) be fundamental solution of a class C. Then if $x_0 \geq 0$ we are finished. So suppose $x_0 < 0$ and let $u + v\sqrt{D}$, $u > 0, v > 0$, be a solution of Pell's equation.

Define X and Y by

$$X + Y\sqrt{D} = (x_0 + y_0\sqrt{D})(u + v\sqrt{D}).$$

Then it can be shown that

(a) $X < 0$ and $Y < 0$ if $N > 0$,

(b) $X > 0$ and $Y > 0$ if $N < 0$.

Hence C contains a solution (X', Y') with $X' > 0$ and $Y' > 0$.

Hence a necessary condition for solubility of $Ax^2 - By^2 = N$ is that $Q_n = (-1)^n N/|N|$ holds for some n in the continued fraction for $\omega = \frac{-AP+\sqrt{D}}{A|N|}$.

Limiting the search range when testing for necessity

Let $\omega = [a_0, \ldots, a_t, \overline{a_{t+1}, \ldots, a_{t+l}}]$.

Then by periodicity of the Q_i, we can assume that $Q_n = (-1)^n N/|N|$ holds for some $n \leq t + l$ if l is even, or $n \leq t + 2l$ if l is odd.

Sufficiency.

Suppose $AP^2 \equiv B \pmod{|N|}$, $0 \le P \le |N|/2$.

(i) Let $\omega = \frac{-AP+\sqrt{D}}{A|N|}$ and suppose $Q_n = (-1)^n N/|N|$ for some minimal $n \ge 1$. Then

$$\begin{aligned} G_{n-1} &= Q_0 A_{n-1} - P_0 B_{n-1} \\ &= A|N|A_{n-1} + APB_{n-1} \\ &= A(|N|A_{n-1} + PB_{n-1}). \end{aligned}$$

Also

$$\begin{aligned} G_{n-1}^2 - DB_{n-1}^2 &= (-1)^n Q_0 Q_n \\ &= (-1)^n (A|N|)(-1)^n N/|N| \\ &= AN. \end{aligned}$$

Hence $A(G_{n-1}/A)^2 - BB_{n-1}^2 = N$ and the equation $Ax^2 - By^2 = N$ has the solution $(|N|A_{n-1} + PB_{n-1}, B_{n-1})$.

Similarly (ii): with $\omega^* = \frac{-AP-\sqrt{D}}{A|N|}$ and $Q_m = (-1)^{m+1}N/|N|$ for some minimal $m \geq 1$, the equation $Ax^2 - By^2 = N$ has the solution $(|N|A_{m-1} + PB_{m-1}, B_{m-1})$.

Then the solution (x, y) in (i) and (ii) with smaller y, will be the fundamental solution for the class P.

Primitivity of solutions

The fact that gcd $(G_{n-1}/A, B_{n-1}) = 1$ if $Q_n = \pm 1$, follows from the next result.

Theorem. Let $Ax^2 - By^2 = N, AP^2 \equiv B \pmod{Q}$ and $x \equiv Py \pmod{Q}$, where $Q = |N|$. Then gcd$(x, y) = 1$.

Proof. (Inspired by Peter Hackman's.)

$$\begin{aligned} APx - By &\equiv (AP^2 - B)y \equiv 0 \pmod{Q} \\ \text{so } APx - By &= aQ. \quad (1) \\ \text{Also } -Py + x &= bQ. \quad (2) \end{aligned}$$

Then adding y times (1) and Ax times (2) gives:

$$(ay + bxA)Q = -By^2 + Ax^2 = N.$$

Hence $ay + bxA = N/Q = \pm 1$ and gcd$(x, y) = 1$.

An example: $4x^2 - 7y^2 = -111$.

The solutions of $4P^2 \equiv 7 \pmod{111}$ satisfying $0 \le P \le 55$ are $P = 14$ and $P = 23$.

(a) $P = 14$:

(i) $\omega = \frac{-AP+\sqrt{D}}{A|N|} = \frac{-56+\sqrt{28}}{444} =$
$[-1, 1, 7, 1, \overline{3, 10, 3, 2}]$ and
$Q_5 = 1 = (-1)^5 N/|N|$, $A_4/B_4 = -4/35$.

Then
$G_4/A = |N|A_4 + PB_4 = 111 * -4 + 14 * 35 = 46$
and $(G_4/A, B_4) = (46, 35)$ is a solution.

(ii) $\omega^* = \frac{-AP-\sqrt{D}}{A|N|} = \frac{-56-\sqrt{28}}{444} =$
$[-1, 1, 6, 4, \overline{10, 3, , 2, 3}]$ and
$Q_4 = 1 = (-1)^{(4+1)} N/|N|$, $A_3/B_3 = -4/29$.

Then
$G_3/A = |N|A_3 + PB_3 = 111 * -4 + 14 * 29 = -38$
and $(G_3/A, B_3) = (-38, 29)$ is a solution.
Hence $(-38, 29)$ is the fundamental solution for class $P = 14$.

(b) $P = 23$:

(i) $\omega = \frac{-AP+\sqrt{D}}{A|N|} = \frac{-92+\sqrt{28}}{444} =$
$[-1, 1, 4, 8, \overline{3, 2, 3, 10}]$ and
$Q_3 = 1 = (-1)^3 N/|N|$, $A_2/B_2 = -1/5$.

Then
$G_2/A = |N|A_2 + PB_2 = 111 * -1 + 23 * 5 = 4$
and $(G_2/A, B_2) = (4, 5)$ is a solution.

(ii) $\omega^* = \frac{-AP-\sqrt{D}}{A|N|} = \frac{-92-\sqrt{28}}{444} =$
$[-1, 1, 3, 1, 1, \overline{3, 2, 3, 10}]$ and
$Q_4 = 1 = (-1)^{(4+1)} N/|N|$, $A_3/B_3 = -1/5$.

Then
$G_3/A = |N|A_3 + PB_3 = 111 * -1 + 23 * 5 = 4$
and $(G_3/A, B_3) = (4, 5)$ is a solution. Hence
$(4, 5)$ is the fundamental solution for class
$P = 23$.

Now the fundamental solution of $x^2 - 28y^2 = 1$ is $\eta = 127 + 24\sqrt{28}$.

Hence the complete solution for $4x^2 - 7y^2 = -111$ is given by

$x + y\sqrt{28} = \pm\eta^n(\pm 38 + 29\sqrt{28})$ and $\pm\eta^n(\pm 4 + 5\sqrt{28}), n \in \mathbb{Z}$.

13th September 2007