Solving $x^2 - Dy^2 = N$ in integers, where $D > 0$ is not a perfect square.

Keith Matthews

We describe a neglected algorithm, based on simple continued fractions, due to Lagrange, for deciding the solubility of $x^2 - Dy^2 = N$, with $\gcd(x, y) = 1$, where $D > 0$ and is not a perfect square. In the case of solubility, the fundamental solutions are also constructed.

Lagrange's well-known algorithm

In 1768, Lagrange showed that if $x^2 - Dy^2 = N$, $x > 0, y > 0, \gcd(x,y) = 1$ and $|N| < \sqrt{D}$, then x/y is a convergent A_n/B_n of the simple continued fraction of $\sqrt{D}$. For we have

$$\begin{aligned} (x + \sqrt{D}y)(x - \sqrt{D}y) &= N \\ |x - \sqrt{D}y| = \frac{|N|}{x + \sqrt{D}y} &< \frac{\sqrt{D}}{x + \sqrt{D}y}. \end{aligned}$$

Hence

$$\frac{x}{y} > \sqrt{D} \implies \left|\frac{x}{y} - \sqrt{D}\right| < \frac{1}{2y^2}$$

and

$$\frac{x}{y} < \sqrt{D} \implies \left|\frac{y}{x} - \frac{1}{\sqrt{D}}\right| < \frac{1}{2x^2}.$$

If $\sqrt{D} = [a_0, \overline{a_1, \ldots, a_l}]$, due to periodicity of $(-1)^{n+1}(A_n^2 - DB_n^2)$, for solubility, we need only check the values for the range $0 \leq n \leq \lfloor l/2 \rfloor - 1$. To find all solutions, we check the range $0 \leq n \leq l - 1$.

Example: $x^2 - 13y^2 = 3$.

$$\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}].$$

n	A_n/B_n	$A_n^2 - 13B_n^2$
0	$3/1$	-4
1	$4/1$	3
2	$7/2$	-3
3	$11/3$	4
4	$18/5$	-1

The positive solutions (x, y) are given by

$$x + y\sqrt{13} = \begin{cases} \eta^{2n}(4 + \sqrt{13}), & n \geq 0, \\ \eta^{2n+1}(7 + 2\sqrt{13}), & n \geq 0, \end{cases}$$

where $\eta = 18 + 5\sqrt{13}$.
Note: $7 + 2\sqrt{13} = -\eta(-4 + \sqrt{13})$.

Example: $x^2 - 221y^2 = 4$.

$$\sqrt{221} = [14, \overline{1, 6, 2, 6, 1, 28}].$$

n	A_n/B_n	$A_n^2 - 221B_n^2$
0	$14/1$	-25
1	$15/1$	4
2	$104/7$	-13
3	$223/15$	4
4	$1442/97$	-25
5	$1665/112$	1

The positive solutions (x, y), $\gcd(x, y) = 1$, are given by

$$x + y\sqrt{221} = \begin{cases} \eta^n(15 + \sqrt{221}), & n \geq 0, \\ \eta^n(223 + 15\sqrt{221}), & n \geq 0, \end{cases}$$

where $\eta = 1665 + 112\sqrt{221}$.
Note: (i) $x^2 - 221y^2 = -4$ has no solution in positive (x, y) with $\gcd(x, y) = 1$.
(ii) $223 + 15\sqrt{221} = -\eta(-15 + \sqrt{221})$.

In 1770, Lagrange gave a neglected algorithm for solving $x^2 - Dy^2 = N$ for arbitrary $N \neq 0$, using the continued fraction expansions of $(P \pm \sqrt{D})/|N|$, where $P^2 \equiv D \pmod{|N|}$, $-|N|/2 < P \leq |N|/2$.

The difficulty is to show that all solutions arise from the continued fractions and Lagrange's discussion of this was hard to follow.

My contribution was to give a short proof using a unimodular matrix lemma (Theorem 172 of Hardy and Wright) which gives a sufficient test for a rational to be a convergent of a simple continued fraction.

Pell's equation

The special case $N = 1$ is known as *Pell's equation*. If $\eta_0 = x_0 + y_0\sqrt{D}$ denotes the fundamental solution of $x^2 - Dy^2 = 1$, ie, the solution with least positive x and y, then the general solution is given by

$$x + y\sqrt{D} = \pm\eta_0^n, n \in \mathbb{Z}.$$

We can calculate (x_0, y_0) by expanding $\sqrt{D}$ as a periodic continued fraction:

$$\sqrt{D} = [a_0, \overline{a_1, \ldots, a_l}].$$

Then

$$x_0/y_0 = \begin{cases} \frac{A_{l-1}}{B_{l-1}}, & \text{if } l \text{ is even} \\ \frac{A_{2l-1}}{B_{2l-1}}, & \text{if } l \text{ is odd,} \end{cases}$$

Equivalence classes of primitive solutions of $x^2 - Dy^2 = N$.

The identity

$$(x^2 - Dy^2)(u^2 - Dv^2) = (xu + yvD)^2 - D(uy + vx)^2$$

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

$$(x', y') = (xu + yvD, uy + vx)$$

of $x'^2 - Dy'^2 = N$.
Note that the equation

$$x' + y'\sqrt{D} = (x + y\sqrt{D})(u + v\sqrt{D})$$

defines an equivalence relation on the set of all primitive solutions of $x^2 - Dy^2 = N$.

Associating a congruence class mod $|N|$ to each equivalence class

If $x^2 - Dy^2 = N$ with $\gcd(x, y) = 1$, then $\gcd(y, N) = 1$.

We define P by $x \equiv yP \pmod{|N|}$. Then

$$\begin{aligned}
x^2 - Dy^2 &\equiv 0 \pmod{|N|} \\
y^2P^2 - Dy^2 &\equiv 0 \pmod{|N|} \\
P^2 - D &\equiv 0 \pmod{|N|} \\
P^2 &\equiv D \pmod{|N|}.
\end{aligned}$$

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

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

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.

A class is ambiguous if and only if $P \equiv 0$ or $|N|/2 \pmod{|N|}$.

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 $x \geq 0$.

.

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 $x^2 - Dy^2 = N$

Suppose $x^2 - Dy^2 = N, \gcd(x, y) = 1, y > 0$.

Let $x \equiv yP \pmod{|N|}$. Then by dealing with the conjugate class instead, if necessary, we can assume $0 \leq P \leq |N|/2$. Also $P^2 \equiv D \pmod{|N|}$.

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

Lagrange substituted for $x = Py + |N|X$ in the equation $x^2 - Dy^2 = N$ to get

$|N|X^2 + 2PXy + \frac{(P^2-D)}{|N|}y^2 = \frac{N}{|N|}$.

He then appealed to a result on a general homogeneous equation $f(X, y) = 1$ and deduced that X/y is a convergent to a root of equation $f(X, y) = 0$.

Our main result is:

(i) If $x \geq 0$, then X/y is a convergent A_{n-1}/B_{n-1} to $\omega = \frac{-P+\sqrt{D}}{|N|}$, $x = G_{n-1} = PB_{n-1} + |N|A_{n-1}$ and $Q_n = (-1)^n \frac{N}{|N|}$.

(ii) If $x <= 0$, then X/y is a convergent A_{m-1}/B_{m-1} to $\omega^* = \frac{-P-\sqrt{D}}{|N|} = \frac{P+\sqrt{D}}{-|N}$, $x = -G_{m-1} = PB_{m-1} + |N|A_{m-1}$ and $Q_m = (-1)^{m+1} \frac{N}{|N|}$.

We prove (i) and (ii) 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 matrix

$$\begin{bmatrix} U & R \\ V & S \end{bmatrix} = \begin{bmatrix} X & \frac{-Px+Dy}{|N|} \\ y & x \end{bmatrix}.$$

The matrix has integer entries. For

$x \equiv yP \pmod{|N|}$ and $P^2 \equiv D \pmod{|N|}$.

Hence

$$\begin{aligned} -Px + Dy &\equiv -P^2y + Dy \pmod{|N|} \\ &\equiv (D - P^2)y \equiv 0 \pmod{|N|}. \end{aligned}$$

The matrix $\begin{bmatrix} X & \frac{-Px+Dy}{|N|} \\ y & x \end{bmatrix}$ has determinant

$$\begin{aligned} \Delta &= Xx - \frac{y(-Px+Dy)}{|N|} \\ &= \frac{(x-Py)x - y(-Px+Dy)}{|N|} \\ &= \frac{x^2 - Dy^2}{|N|} = \frac{N}{|N|} = \pm 1. \end{aligned}$$

Also if $\zeta = \sqrt{D}$ and $\omega = (-P + \sqrt{D})/|N|$, it is easy to verify that

$$\omega = \frac{U\zeta + R}{V\zeta + S}.$$

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

$G_{n-1} = Q_0 A_{n-1} - P_0 B_{n-1} = |N|X + Py = x$. Hence

$N = x^2 - Dy^2 = G_{n-1}^2 - DB_{n-1}^2 = (-1)^n |N| Q_n$,

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

There is a similar proof for (ii) by considering the matrix

$$\begin{bmatrix} X & \frac{Px-Dy}{|N|} \\ y & -x \end{bmatrix}.$$

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 $x^2 - Dy^2 = N$ is that $Q_n = (-1)^n N/|N|$ holds for some n in the continued fraction for $\omega = \frac{-P+\sqrt{D}}{|N|}$.

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 $P^2 \equiv D \pmod{|N|}$, $0 \leq P \leq |N|/2$ and that

$\omega = \frac{-P+\sqrt{D}}{|N|} = [a_0, \ldots, a_t, \overline{a_{t+1}, \ldots, a_{t+l}}]$.

(i) Suppose $Q_n = (-1)^n N/|N|$ for some n in $1 \leq n \leq t+l$ if l is even, or $1 \leq n \leq t+2l$ if l is odd.

Then with $G_{n-1} = |N|A_{n-1} + PB_{n-1}$, the equation $x^2 - Dy^2 = N$ has the solution (G_{n-1}, B_{n-1}).

(ii) Also let $\omega^* = \frac{-P-\sqrt{D}}{|N|} = [b_0, \ldots, b_s, \overline{b_{s+1}, \ldots, b_{s+l}}]$ and suppose $Q_m = (-1)^{m+1} N/|N|$ for some m in $1 \leq m \leq s+l$ if l is even, or $1 \leq m \leq s+2l$ if l is odd. Then $x^2 - Dy^2 = N$ also has the solution (G_{m-1}, B_{m-1}).

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

Primitivity of solutions

For $\omega = (-P + \sqrt{D})/|N|$,

$\gcd(G_{n-1}, B_{n-1}) = 1$ if $Q_n = -1)^n N/|N|$. For

$$\begin{aligned}\gcd(G_{n-1}, B_{n-1}) &= \gcd(Q_0 A_{n-1} - P_0 B_{n-1}, B_{n-1}) \\ &= \gcd(Q_0 A_{n-1}, B_{n-1}) \\ &= \gcd(Q_0, B_{n-1}).\end{aligned}$$

Also

$$\begin{aligned}(Q_0 A_{n-1} - P_0 B_{n-1})^2 - DB_{n-1}^2 &= N \\ Q_0^2 A_{n-1}^2 - 2Q_0 P_0 A_{n-1} B_{n-1} + (P_0^2 - D) B_{n-1}^2 &= N \\ Q_0 A_{n-1}^2 - 2P_0 A_{n-1} B_{n-1} + \frac{(P_0^2 - D)}{Q_0} B_{n-1}^2 &= N/|N| = \pm 1.\end{aligned}$$

Hence $\gcd(Q_0, B_{n-1}) = 1$.

An example: $x^2 - 221y^2 = 217$ and -217

We find the solutions of $P^2 \equiv 221 \pmod{217}$ satisfying $0 \le P \le 103$ are $P = 2$ and $P = 33$.

(a) $\frac{-2+\sqrt{221}}{217} = [0, 16, \overline{1, 6, 2, 6, 1, 28}]$.

i	0	1	2	3	4	5	6	7
P_i	-2	2	14	11	13	13	11	14
Q_i	217	**1**	25	4	13	4	25	**1**
A_i	0	1	1	7	15	97	112	3233
B_i	1	16	17	118	253	1636	1889	54528

The period length is 6 and $Q_1 = 1 = (-1)^1(-217)/|-217|$.

Hence $(G_0, B_0) = (2, 1)$ is a solution of $x^2 - 221y^2 = -217$ and this is clearly a fundamental one, so there is no need to examine the continued fraction expansion of $\frac{-2-\sqrt{221}}{217}$.

(b) $\frac{-33+\sqrt{221}}{217} = [-1, 1, 10, \overline{1, 28, 1, 6, 2, 6}]$.

i	0	1	2	3	4	5	6	7	8
P_i	-33	-184	29	11	14	14	11	13	13
Q_i	217	-155	4	25	**1**	25	4	13	4
A_i	-1	0	-1	-1	-29	-30	-209	-448	-2897
B_i	1	1	11	12	347	359	2501	5361	34667

We observe that $Q_4 = 1 = (-1)^4 \cdot 217/|217|$ and the period length is 6. Hence $(G_3, B_3) = (179, 12)$ is a solution of $x^2 - 221y^2 = 217$.

c) $\frac{-33-\sqrt{221}}{217} = [-1, 1, 3, 1, 1, \overline{6, 1, 28, 1, 6, 2}]$.

i	0	1	2	3	4	5	6	7
P_i	33	184	-29	17	0	13	11	14
Q_i	-217	155	-4	17	13	4	25	**1**
A_i	-1	0	-1	-1	-2	-13	-15	-433
B_i	1	1	4	5	9	59	68	1963

i	8	9	10
P_i	14	11	13
Q_i	25	4	13
A_i	-448	-3121	-6690
B_i	2031	14149	30329

We observe that $Q_7 = 1 = (-1)^8 \cdot 217/|217|$. Hence $(-G_6, B_6) = (1011, 68)$ is a solution of $x^2 - 221y^2 = 217$.

It follows from (b) and (c) that $(179, 12)$ is a fundamental solution.

Here $\eta_0 = 1665 + 112\sqrt{221}$ is the fundamental solution of Pell's equation. Then the complete solution of $x^2 - 221y^2 = -217$ is given by

$$x + y\sqrt{221} = \pm(\pm 2 + \sqrt{221})\eta_0^n, n \in \mathbb{Z}.$$

The complete solution of $x^2 - 221y^2 = 217$ is given by

$$x + y\sqrt{221} = \pm(\pm 179 + 12\sqrt{221})\eta_0^n, n \in \mathbb{Z}.$$

Lagrange also discussed the general equation $ax^2 + bxy + cy^2 = N$, where $D = b^2 - 4ac > 0$ is not a perfect square and $\gcd(a, N) = 1$.

The continued fraction approach goes through with suitable modifications.

However an exceptional case, not noted by Lagrange, arises when $D = 5$ and $aN < 0$, in which there is a solution not arising directly from convergents.

This was pointed out by Serret in 1877 and dealt with in 1986 by M. Pavone.

An example is $x^2 - xy - y^2 = -1$, where the solution $(0, 1)$ is such an exception.

We use 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.

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 $Q < S$.

Theorem. Suppose

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

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 A_{i-1}/B_{i-1} to ω and $Q_i = (-1)^i 2N/|N|$.

(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 A_{i-1}/B_{i-1} to ω^* and $Q_i = (-1)^{i+1} 2N/|N|$.

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

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

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

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

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^*.

The assumption that $\gcd(a, N) = 1$ involves no loss of generality. For as pointed out by Gauss in his Disquisitiones, if $\gcd(a, b, c) = 1$, 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.

Example: Solving $x^2 - py^2 = -\left(\frac{2}{p}\right)\frac{p-1}{2}$, $p = 4n+3$

Let p be a prime of the form $4n+3$. Then it is classical that the equation $x^2 - py^2 = 2\left(\frac{2}{p}\right)$ has a solution in integers.

So with $\omega_1 = (1+\sqrt{p})/2 = [\lambda, \overline{a_1, \ldots, a_{L-1}, 2\lambda+1}]$, there is exactly one n, $1 \le n \le L$ satisfying $Q_n(-1)^n = \left(\frac{2}{p}\right)$. ($Q_n = 1$ and L is even and $n = L/2$.)

Now in solving the given equation, notice that $P = 1$ is a solution of $P^2 \equiv p \pmod{(p-1)/2}$.

So with $\omega_2 = (-1+\sqrt{p})/((p-1)/2)$, the first complete quotient is in fact ω_1.

It follows that the corresponding Q_{n+1} is the old Q_n and so now $Q_n(-1)^{n+1} = -\left(\frac{2}{p}\right)$. hence there is a solution of $x^2 - py^2 = -\left(\frac{2}{p}\right)\frac{p-1}{2}$.

John Robertson (September 2004) has produced the following short proof of the previous result.

Assume $X^2 - pY^2 = 2\left(\frac{2}{p}\right), p = 4n + 3.$

Make the integer transformation

$x = (pY - X)/2, y = (X - Y)/2.$

Then $x^2 - py^2 = -\left(\frac{2}{p}\right)(p - 1)/2.$