The Diophantine Equation $x^2 - Dy^2 = N$, $D > 0$

Keith Matthews

Abstract. 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.

1. **Introduction**. In a memoir of 1768 (see [6, Oeuvres II, pages 377–535]), Lagrange gave a recursive method for solving $x^2 - Dy^2 = N$, with $\gcd(x, y) = 1$, where $D > 1$ and is not a perfect square, thereby reducing the problem to the case where $|N| < \sqrt{D}$, in which case the positive solutions (x, y) will be found amongst the pairs (p_n, q_n), with p_n/q_n a convergent of the simple continued fraction for $\sqrt{D}$.

It does not seem to be widely known that Lagrange also gave another algorithm in a memoir of 1770 (see [6, Oeuvres II, pages 655–726]), which may be regarded as a generalisation of the well–known method of solving Pell's equation $x^2 - Dy^2 = \pm 1$ using the simple continued fraction for $\sqrt{D}$.

In this paper, we give a version of Lagrange's second algorithm which uses only the language of simple continued fractions. Also Lagrange's proof of the necessity condition in Theorem 1 is long and not easy to follow and we have replaced it by a much simpler proof.

A. Nitaj has also given a related algorithm in his PhD. Thesis [4, pages 57–88]. His treatment of Theorem 1 requires the cases $D = 2$ or 3 and $N < 0$ to be treated separately. Also unlike our algorithm, his requires the calculation of the fundamental solution η of Pell's equation.

Lagrange's algorithm has been rediscovered by R. Mollin [2, pages 333–340]. His treatment is more complicated than ours, as it uses the language of ideals and semi–simple continued fractions, in addition to that of simple continued fractions.

2. **Constructing solutions of** $x^2 - Dy^2 = N$.

A necessary condition for the solubility of $x^2 - Dy^2 = N$, with $\gcd(x, y) = 1$, is that the congruence $u^2 \equiv D \pmod{Q_0}$ shall be soluble, where $Q_0 = |N|$.

The sufficiency part of Lagrange's algorithm was given by Perron in his introduction to a paper of Patz [5]. Perron starts with a solution P_0 of the above congruence. If $x_n = (P_n + \sqrt{D})/Q_n$ is the n–th complete convergent of the simple continued fraction for $\omega = (P_0 + \sqrt{D})/Q_0$, A_n/B_n is the n–th convergent to ω and $G_{n-1} = Q_0 A_{n-1} - P_0 B_{n-1}$, then ([2, pages 246–248])

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

Hence if $Q_n = (-1)^n N/|N|$, it follows that equation (1) gives a solution $(x, y) = (G_{n-1}, B_{n-1})$ of $x^2 - Dy^2 = N$. We also have $\gcd(x, y) = 1$.

For $\gcd(G_{n-1}, B_{n-1}) = \gcd(Q_0 A_{n-1}, B_{n-1}) = \gcd(Q_0, B_{n-1})$ and equation (1) gives

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

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

In part (a) of Theorem 2, we prove that this construction can be reversed, to provide a simple necessary condition for the solubility of $x^2 - Dy^2 = N$ where $\gcd(x, y) = 1$. (Such solutions are called *primitive.*)

In section 6, we give three numerical examples.

3. **Equivalence of solutions** (See Nagell [3, pages 204–205].)

Primitive solutions $\alpha_1 = x_1 + y_1\sqrt{D}$ and $\alpha_2 = x_2 + y_2\sqrt{D}$ of $x^2 - Dy^2 = N$ are called *equivalent* if their ratio is a solution $u + v\sqrt{D}$ of Pell's equation $u^2 - Dv^2 = 1$.

A necessary and sufficient condition for α_1 and α_2 to be equivalent is that

$$x_1x_2 - Dy_1y_2 \equiv 0 \pmod{Q_0}, \; x_1y_2 - y_1x_2 \equiv 0 \pmod{Q_0}. \tag{2}$$

Each primitive solution $x + y\sqrt{D}$ determines a unique integer P_0 satisfying $x \equiv -P_0 y \pmod{Q_0}$ and $P_0^2 \equiv D \pmod{Q_0}$, with $-Q_0/2 < P_0 \leq Q_0/2$. We say that $x + y\sqrt{D}$ belongs to P_0.

$x + \sqrt{D}$ and $-x + \sqrt{D}$ determine *conjugate* classes.

If these classes are equal, the class is called *ambiguous.*

Ambiguous classes occur precisely when $P_0 = 0$ or $Q_0/2$. Also $P_0 = 0$ if and only if $Q_0 | D$, while if Q_0 is even, $P_0 = Q_0/2$ if and only if either (a) $4|Q_0$ and $Q_0|D$ or (b) $Q_0|2D$ and D is odd.

There are finitely many equivalence classes and these are represented by *fundamental* solutions $x + y\sqrt{D}$, where y is positive and has least value for the class. If the class is ambiguous, we can assume that $x \geq 0$.

The equivalence class containing the fundamental solution $x_0 + y_0\sqrt{D}$ consists of the numbers $\pm(x_0 + y_0\sqrt{D})\eta^n, \; n \in \mathbb{Z}$, where $\eta = u + v\sqrt{D}$ is the fundamental solution of Pell's equation $u^2 - Dv^2 = 1$.

4. **A necessary condition for solubility of $x^2 - Dy^2 = N$.**

Theorem 1. Suppose $x^2 - Dy^2 = N$ is soluble in integers $x \geq 0$ and $y > 0$, $\gcd(x, y) = 1$ and let $Q_0 = |N|$. Then $\gcd(Q_0, y) = 1$. Define P_0 by $x \equiv -P_0 y \pmod{Q_0}$, where $D \equiv P_0^2 \pmod{Q_0}$ and $-Q_0/2 < P_0 \leq Q_0/2$.

Let $\omega = (P_0 + \sqrt{D})/Q_0$ and $x = Q_0 X - P_0 y$. Then

(i) X/y is a convergent A_{n-1}/B_{n-1} of ω;

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

We need a result which is an extension of Theorem 172 [1, pages 140—141].

Lemma. 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 to ω. Moreover if $Q \neq S > 0$, then $R/S = (p_{n-1} + kp_n)/(q_{n-1} + kq_n), k \geq 0$. 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. Hardy and Wright deal only with the case $Q > S > 0$. They write

$$\frac{P}{Q} = [a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n},$$

and assume $PS - QR = (-1)^{n-1}$. Then

$$p_n S - q_n R = PS - QR = p_n q_{n-1} - p_{n-1} q_n,$$

so $p_n(S - q_{n-1}) = q_n(R - p_{n-1})$.

Hence $q_n | (S - q_{n-1})$. Then from $q_n = Q > S > 0$ and $q_n \geq q_{n-1} > 0$, we deduce $|S - q_{n-1}| < q_n$ and hence $S - q_{n-1} = 0$. Then $S = q_{n-1}$ and $R = p_{n-1}$.

Also

$$\omega = \frac{P\zeta + R}{Q\zeta + S} = \frac{p_n\zeta + p_{n-1}}{q_n\zeta + q_{n-1}} = [a_0, a_1, \ldots, a_n, \zeta].$$

If $S = 0$ and $Q = R = 1$, then $\omega = [P, \zeta]$ and $P/Q = P/1 = p_0/q_0$.

If $Q = S$, then $Q = S = 1$ and $P - R = \pm 1$. If $P = R + 1$, then $\omega = [R, 1, \zeta]$, so $P/Q = (R + 1)/1 = p_1/q_1$. If $P = R - 1$, then $\omega = [R - 1, 1 + \zeta]$ and $P/Q = (R - 1)/1 = p_0/q_0$.

If $Q < S$, then from $q_n | (S - q_{n-1})$ and

$$S - q_{n-1} > Q - q_{n-1} = q_n - q_{n-1} \geq 0,$$

we have $S - q_{n-1} = kq_n$, where $k \geq 1$. Then

$$\omega = \frac{P\zeta + R}{Q\zeta + S} = \frac{p_n\zeta + p_{n-1} + kp_n}{q_n\zeta + q_{n-1} + kq_n} = \frac{p_n(\zeta + k) + p_{n-1}}{q_n(\zeta + k) + q_{n-1}}$$

and $\omega = [a_0, \ldots, a_n, \zeta + k]$.

Proof of the Theorem. With $Q_0 = |N|$, $x = Q_0 X - P_0 y$ and $x^2 - Dy^2 = N$, we have

$$P_0 x + Dy \equiv -P_0^2 y + Dy \equiv (-P_0^2 + D)y \equiv 0 \pmod{Q_0}.$$

Hence the matrix

$$\begin{bmatrix} P & R \\ Q & S \end{bmatrix} = \begin{bmatrix} X & \frac{P_0 x + Dy}{Q_0} \\ y & x \end{bmatrix}$$

has integer entries and determinant $\Delta = \pm 1$. For

$$\begin{aligned}\Delta &= Xx - \frac{y(P_0x + Dy)}{Q_0} \\ &= \frac{(x + P_0y)x}{Q_0} - \frac{y(P_0x + Dy)}{Q_0} \\ &= \frac{x^2 - Dy^2}{Q_0} = \pm 1.\end{aligned}$$

Also if $\zeta = \sqrt{D}$ and $\omega = (P_0 + \sqrt{D})/Q_0$, it is easy to verify that $\omega = \frac{P\zeta + R}{Q\zeta + S}$. Then the lemma implies that X/y is a convergent to ω.

Finally $x = Q_0X - P_0y = Q_0A_{n-1} - P_0B_{n-1} = G_{n-1}$ and

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

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

Remark. The solutions u of $u^2 \equiv D \pmod{Q_0}$ come in pairs $\pm u_1, \ldots, \pm u_r$, where $0 < u_i \leq Q_0/2$, together with possibly $u_{r+1} = 0$ and $u_{r+2} = Q_0/2$. Hence we can state the following:

Corollary. Suppose $x^2 - Dy^2 = N$ is soluble, with $x \geq 0$ and $y > 0$, $\gcd(x, y) = 1$ and $Q_0 = |N|$. Let $x \equiv -P_0y \pmod{Q_0}$, where $P_0 \equiv \pm u_i \pmod{Q_0}$ and $x = Q_0X - P_0y$. Then X/y will be a convergent A_{n-1}/B_{n-1} of $\omega_i = (u_i + \sqrt{D})/Q_0$ or $\omega_i' = (-u_i + \sqrt{D})/Q_0$ and $Q_n = (-1)^n N/|N|$.

5. **An algorithm for solving $x^2 - Dy^2 = N$.** In view of the Corollary, we know that the primitive solutions to $x^2 - Dy^2 = N$ with $y > 0$ will be found by considering the continued fraction expansions of both ω_i and ω' for $1 \leq i \leq r + 2$.

One can show that each equivalence class contains solutions (x, y) with $x \geq 0$ and $y > 0$, so the necessary condition $Q_n = (-1)^n N/|N|$ shall occur for some n holds for both ω_i and ω_i'. Hence to check for solubility, we need only consider ω_i.

Suppose that $\omega_i = (u_i + \sqrt{D})/Q_0 = [a_0, \ldots, a_t, \overline{a_{t+1}, \ldots, a_{t+l}}]$.

If $x^2 - Dy^2 = N$ is soluble with $x \geq 0$ and $y > 0$, there are infinitely many such solutions and hence $Q_n = \pm 1$ holds for ω_i for some $n > t + l$ and hence, by periodicity, also in the range $t + 1 \leq n \leq t + l$. Any such n must have $Q_n = 1$, as $(P_n + \sqrt{D})/Q_n$ is reduced for n in this range and so $Q_n > 0$. Moreover if l is even, the condition $Q_n = (-1)^n N/|N|$ is also preserved.

Moreover there can be at most one n in the range $t+1 \leq n \leq t+l$ for which $Qn = 1$. For if $P_n + \sqrt{D}$ is reduced, then $P_n = \lfloor \sqrt{D} \rfloor$ and hence two such occurrences of $Q_n = 1$ within a period would give a smaller period.

We also remark that l is odd, if and only if the fundamental solution η_0 of the Pell equation $x^2 - Dy^2 = \pm 1$ has norm equal to -1. Consequently a solution of $x^2 - Dy^2 = N$ gives rise to a solution of $x^2 - Dy^2 = -N$; indeed we see that if $t + 1 \leq n \leq t + l$ and $k \geq 1$, then $G_{n+kl-1} + B_{n+kl-1}\sqrt{D} = \eta_0^k (G_{n-1} + B_{n-1}\sqrt{D})$. Hence $G_{n+l-1}^2 - DB_{n+l-1}^2 = -(G_{n-1}^2 - DB_{n-1}^2)$ if $\mathrm{Norm}(\eta_0) = -1$.

Putting these observations together, we have the following:

Theorem 2. For $1 \leq i \leq r + 2$, let

$$\omega_i = (u_i + \sqrt{D})/Q_0 = [a_0, \ldots, a_t, \overline{a_{t+1}, \ldots, a_{t+l}}].$$

(a) Then a necessary condition for $x^2 - Dy^2 = N$, $\gcd(x, y) = 1$, to be soluble is that for some i in $i = 1, \ldots, r + 2$, we have $Q_n = 1$ for some n in $t + 1 \leq n \leq t + l$, where if l is even, then $(-1)^n N/|N| = 1$.

(b) Conversely, suppose for ω_i, we have $Q_n = 1$ for some n with $t + 1 \leq n \leq t + l$. Then

(i) If l is even and $(-1)^n N/|N| = 1$, then $x^2 - Dy^2 = N$ is soluble with solution $G_{n-1} + B_{n-1}\sqrt{D}$.

(ii) If l is odd, then $G_{n-1} + B_{n-1}\sqrt{D}$ is a solution of $x^2 - Dy^2 = (-1)^n|N|$, while $G_{n+l-1} + B_{n+l-1}\sqrt{D}$ will be a solution of $x^2 - Dy^2 = (-1)^{n+1}|N|$.

(iii) At least one of the $G_{m-1} + B_{m-1}\sqrt{D}$ with least B_{m-1} satisfying $Q_m = (-1)^m N/|N|$, which arise from the continued fraction expansions of ω_i and ω_i', will be a fundamental solution of $x^2 - Dy^2 = N$.

Remarks. 1. Unlike the case of Pell's equation, $Q_n = \pm 1$ can also occur for $n < t + 1$ and can contribute to a fundamental solution. If Norm $(\eta) = 1$, one sees that to find the fundamental solution for $x^2 - Dy^2 = N$, it suffices to examine only the cases $Q_n = \pm 1, n <= t + l$. However if Norm $(\eta) = -1$, one may have to examine the range $t + l + 1 \leq n \leq t + 2l$ as well.

2. It can happen that l is even and that $x^2 - Dy^2 = N$ is soluble with $x \equiv \pm(-u_i y) \pmod{Q_0}$, while $x^2 - Dy^2 = -N$ is soluble with $x \equiv \pm(-u_j y) \pmod{Q_0}$, with $i \neq j$. (Of course if $|N| = p$ is prime, this cannot happen, as the congruence $u^2 \equiv D \pmod{p}$ has two solutions if p does not divide D and one solution if p divides D.)

An example of this is $D = 221, N = 217$ (see Example 2 later). Then $u_1 = 2, u_2 = 33$. Also $l = 6$ and $(2 + \sqrt{221})/217$ produces the solution $-2 + \sqrt{221}$ of $x^2 - 221y^2 = -217$, whereas $(33 - \sqrt{221})/217$ produces the solution $-179 + 12\sqrt{221}$ of $x^2 - 221y^2 = 217$.

6. **Example 1** (Lagrange [6, pages 719–723]). $x^2 - 13y^2 = \pm 101$.
We find the solutions of $P_0^2 \equiv 13 \pmod{101}$ are ± 35.

(a) $\frac{35+\sqrt{13}}{101} = [0, 2, 1, 1, \overline{1, 1, 1, 1, 6}]$.

i	0	1	2	3	4	5	6	7	8
P_i	35	−35	11	−2	3	1	2	1	3
Q_i	101	−12	9	**1**	4	3	3	4	**1**
A_i	0	1	1	2	3	5	8	13	86
B_i	1	2	3	5	8	13	21	34	225

We observe that $Q_3 = Q_8 = 1$. The period length is odd, so both the equations $x^2 - 13y^2 = \pm 101$ are soluble. With $G_n = Q_0 A_n - P_0 B_n$, we have
$G_2 = 101 \cdot 1 - 35 \cdot 3 = -4$. $x + y\sqrt{13} = -4 + 3\sqrt{13}$, $x^2 - 13y^2 = -101$;
$G_7 = 101 \cdot 13 - 35 \cdot 34 = 123$. $x + y\sqrt{13} = 123 + 34\sqrt{13}$, $x^2 - 13y^2 = 101$.

(b) $\frac{-35+\sqrt{13}}{101} = [-1, 1, 2, 4, \overline{1, 1, 1, 1, 6}]$.

i	0	1	2	3	4	5	6	7	8
P_i	−35	−66	23	1	3	1	2	1	3
Q_i	101	−43	12	**1**	4	3	3	4	**1**
A_i	−1	0	−1	−4	−5	−9	−14	−23	−152
B_i	1	1	3	13	16	29	45	74	489

We observe that $Q_3 = Q_8 = 1$. Hence
$G_2 = 101 \cdot (-1) - (-35) \cdot 3 = 4$. $x + y\sqrt{13} = 4 + 3\sqrt{13}$, $x^2 - 13y^2 = -101$;
$G_7 = 101 \cdot (-23) - (-35) \cdot 74 = 267$. $x + y\sqrt{13} = 267 + 74\sqrt{13}$, $x^2 - 13y^2 = 101$.

Hence $-4 + 3\sqrt{13}$ and $123 + 34\sqrt{13}$ are fundamental solutions for the equations $x^2 - 13y^2 = -101$ and $x^2 - 13y^2 = 101$ respectively.

We have $\eta = 649 + 180\sqrt{13}$, so the complete solution of $x^2 - 13y^2 = -101$ is given by $x + y\sqrt{13} = \pm\eta^n(\pm 4 + 3\sqrt{13}), n \in \mathbb{Z}$, while the complete solution of $x^2 - 13y^2 = 101$ is given by $x + y\sqrt{13} = \pm\eta^n(\pm 123 + 34\sqrt{13}), n \in \mathbb{Z}$.

Example 2. $x^2 - 221y^2 = \pm 217$.

We find the solutions of $P_0^2 \equiv 221 \pmod{217}$ are ± 2 and ± 33.

(a) $\frac{2+\sqrt{221}}{217} = [0, 12, \overline{1, 6, 2, 6, 1, 28}]$.

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	12	13	90	193	1248	1441	41596

We observe that $Q_1 = Q_7 = 1$. The period length is even and $(-1)^7 = -1$. Hence the equation $x^2 - 221y^2 = -217$ is soluble.
$G_0 = 217 \cdot 0 - 2 \cdot 1 = -2$. $x + y\sqrt{221} = -2 + \sqrt{221}$, $x^2 - 221y^2 = -217$.

There is no need to expand $\frac{-2+\sqrt{221}}{217}$, as $-2 + \sqrt{221}$ is a fundamental solution.

(b) $\frac{33+\sqrt{221}}{217} = [0, 4, 1, 1, \overline{6, 1, 28, 1, 6, 2}]$.

i	0	1	2	3	4	5	6	7	8	9
P_i	33	-33	17	0	13	11	14	14	11	13
Q_i	217	-4	17	13	4	25	**1**	25	4	13
A_i	0	1	1	2	13	15	433	448	3121	6690
B_i	1	4	5	9	59	68	1963	2031	14149	30329

We observe that $Q_6 = 1$. The period length is even and $(-1)^6 = 1$. Hence the equation $x^2 - 221y^2 = 217$ is soluble.
$G_5 = 217 \cdot 15 - 33 \cdot 68 = 1011$. $x + y\sqrt{221} = 1011 + 68\sqrt{221}$, $x^2 - 221y^2 = 217$.

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

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 $Q_4 = 1$. The period length is even and $(-1)^4 = 1$. Hence the equation $x^2 - 221y^2 = 217$ is soluble. We have
$G_3 = 217 \cdot (-1) - (-33) \cdot 12 = 179$. $x + y\sqrt{221} = 179 + 12\sqrt{221}$, $x^2 - 221y^2 = 217$.

It follows from (b) and (c) that $179 + 12\sqrt{221}$ is a fundamental solution.

We have $\eta = 1665 + 112\sqrt{221}$, so the complete solution of $x^2 - 221y^2 = -217$ is given by $x + y\sqrt{221} = \pm\eta^n(\pm 2 + \sqrt{221}), n \in \mathbb{Z}$, while the complete solution of $x^2 - 221y^2 = 217$ is given by $x + y\sqrt{221} = \pm\eta^n(\pm 179 + 12\sqrt{221}), n \in \mathbb{Z}$.

Example 3. (Lagrange [6, pages 723–725]) $x^2 - 79y^2 = \pm 101$. We find the solutions of $P_0^2 \equiv 79 \pmod{101}$ are ± 33. However $(33 + \sqrt{79})/101 = [0, 2, 2, \overline{2, 3, 5, 1, 1, 1}]$ and from the table

i	0	1	2	3	4	5	6	7	8
P_i	33	−33	13	5	7	8	7	3	4
Q_i	101	−10	9	6	5	3	10	7	9

we see that the condition $Q_n = 1$ does not hold for $3 \le n \le 8$.

Hence the equations $x^2 - 79y^2 = \pm 101$ are not soluble.

The calculations were carried out with the author's number theory program CALC and bc program `surd`.

References

[1] G.H. Hardy and E.M. Wright, *An Introduction to Theory of Numbers*, Oxford University Press 1962.
[2] R.A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, NY 1998.
[3] T. Nagell, *Introduction to Number Theory*, Chelsea Publishing Company, NY 1981.
[4] A. Nitaj, *Conséquences et aspects expérimentaux des conjectures abc et de Szpiro*, Thèse, Caen 1994.
[5] W. Patz, *Über die Gleichung* $X^2 - DY^2 = \pm c \cdot (2^{31} - 1)$, Bayer. Akad. Wiss. Math–Natur. Kl. S.–B (1948) 21–30.
[6] J.-A. Serret (Ed), *Oeuvres de Lagrange, I–XIV*, Gauthiers–Villars, Paris 1877.

Keith Matthews
Department of Mathematics
University of Queensland
Brisbane
Australia 4072
e–mail: krm@maths.uq.edu.au