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 \(\eta\) 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 $\omega$ and $G_{n-1} = Q_0A_{n-1} - P_1B_{n-1}$, then ([2, pages 246-248])

$$(1) \quad C_n^2 - DB_{n-1}^2 = (-1)^nQ_0Q_n.$$ 

Hence if $Q_n = (-1)^nN/|N|$, 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 $\gcd(G_{n-1}, B_{n-1}) = \gcd(Q_0A_{n-1}, B_{n-1}) = \gcd(Q_0, B_{n-1})$ and equation (1) gives

$$\begin{align*}
(Q_0A_{n-1} - P_0B_{n-1})^2 - DB_{n-1}^2 &= N \\
Q_0^2A_{n-1}^2 - 2Q_0P_0A_{n-1}B_{n-1} + (P_0^2 - D)B_{n-1}^2 &= N \\
Q_0^2A_{n-1}^2 - 2P_0A_{n-1}B_{n-1} + \frac{(P_0^2 - D)}{Q_0}B_{n-1}^2 &= \frac{N}{|N|} = \pm 1.
\end{align*}$$

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 $\alpha_1$ and $\alpha_2$ to be equivalent is that

$$(2) \quad x_1x_2 - Dy_1y_2 \equiv 0 \pmod{Q_0}, \quad x_1y_2 - y_1x_2 \equiv 0 \pmod{Q_0}.$$

Each primitive solution $x + y\sqrt{D}$ determines a unique integer $P_0$ satisfying $x \equiv -P_0y \pmod{Q_0}$ 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 solvability of $x^2 - Dy^2 = N$.

**Theorem 1.** Suppose $x^2 - Dy^2 = N$ is soluble in integers $x > 0$ and $y > 0$, \( \gcd(x, y) = 1 \) and let $Q_0 = |N|$. Then $\gcd(Q_0, y) = 1$. Define $P_0$ by $x \equiv -P_0y \pmod{Q_0}$, 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 $x = Q_0X - P_0y$. Then

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

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

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 $\omega$. 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 $\omega$. 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

$$p_nS - q_nR = PS - QR = p_nq_{n-1} - p_{n-1}q_n,$$

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

$$\omega = \frac{P\zeta + R}{Q\zeta + S} = \frac{p_0\zeta + p_{n-1}}{q_0\zeta + q_{n-1}} = [a_0, a_1, \ldots, a_n, \zeta].$$

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

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

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

$$\omega = \frac{P\zeta + R}{Q\zeta + S} = \frac{p_0\zeta + p_{n-1} + kq_n}{q_0\zeta + q_{n-1} + kq_n} = \frac{p_n(\zeta + k) + p_{n-1}}{q_n(\zeta + k) + q_{n-1}},$$

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

**Proof of the Theorem.** With $Q_0 = |N|$, $x = Q_0X - P_0y$ and $x^2 - Dy^2 = N$, we have

$$P_0x + Dy \equiv -P_0^2y + Dy \equiv (-P_0^2 + D)y \equiv 0 \pmod{Q_0}.$$ \(\square\)

Hence the matrix

$$\begin{bmatrix} P & R \\ Q & S \end{bmatrix} \begin{bmatrix} X \\ y \end{bmatrix} \equiv \begin{bmatrix} \frac{P_0x + Dy}{Q_0} \\ \frac{Q_0y}{x} \end{bmatrix} \pmod{Q_0}.$$
has integer entries and determinant $\Delta = \pm 1$. For

$$\Delta = X x - \frac{y(P_0 x + Dy)}{Q_0} = \frac{(x + P_0 y)x - y(P_0 x + Dy)}{Q_0} = \frac{x^2 - Dy^2}{Q_0} = \pm 1.$$ 

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

Finally $x = Q_0 X - P_0 y = Q_0 A_{n-1} - P_0 B_n = G_{n-1}$ 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 $x \equiv -P_0 y \pmod{Q_0}$, where $P_0 \equiv \pm u_i \pmod{Q_0}$ and $x = Q_0 X - P_0 y$. Then $X/y$ will be a convergent $A_{n-1}/B_n$ of $\omega = (u_i + \sqrt{D})/Q_0$ or $\omega' = (\pm u_i + \sqrt{D})/Q_0$ and $Q_n = (-1)^n N/|N|$. $\omega'$.

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 $\omega_i$ and $\omega'$ 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 $\omega_i$ and $\omega'$. Hence to check for solvability, we need only consider $\omega_i$.

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

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 $\omega_i$ 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 $Q_n = 1$. For if $P_n + \sqrt{D}$ is reduced, then $P_n = \sqrt{D}$ 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 $\eta_0$ 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 $G_{n+kt-1} + B_{n+kt-1}\sqrt{D} = \eta_0(G_{n-1} + B_{n-1}\sqrt{D})$. Hence $G_{n+kt-1}^2 - DB_{n+kt-1}^2 = -(G_{n-1}^2 - DB_{n-1}^2)$ if Norm$(\eta_0) = -1$.

Putting these observations together, we have the following:

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

$$\omega_i = (u_i + \sqrt{D})/Q_0 = [a_0, \ldots, a_t, a_{t+1}, \ldots, a_{t+r}].$$
(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 \( \omega_i \), 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 \( G_{n+1} + B_{n+1} \sqrt{D} \) with least \( B_{m-1} \) satisfying \( Q_m = (-1)^m N/|N| \), which arise from the continued fraction expansions of \( \omega_i \) and \( \omega_i' \), 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 \( \text{Norm}(\eta) = 1 \), one sees that to find the fundamental solution for \( x^2 - Dy^2 = N \), it suffices to examine only the cases \( Q_n = \pm 1, n \leq t + l \). However if \( \text{Norm}(\eta) = -1 \), 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 \( x \equiv \pm (-u,y) \mod{Q_0} \), while \( x^2 - Dy^2 = -N \) is soluble with \( x \equiv \pm (-u,y) \mod{Q_0} \), with \( i \neq j \). (Of course if \( |N| = p \) is prime, this cannot happen, as the congruence \( u^2 \equiv D \mod{p} \) 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 \( x^2 - 221 y^2 = -217 \), whereas \((33 - \sqrt{221})/217 \) produces the solution \(-179 + 12 \sqrt{221}\) of \( x^2 - 221 y^2 = 217 \).

6. **Example 1** (Lagrange [6, pages 719–723]). \( x^2 - 13y^2 = \pm 101 \).

   We find the solutions of \( P_0^2 \equiv 13 \mod{101} \) are \( \pm 35 \).

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

   \[
   \begin{array}{c|cccccccc}
   i & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
   \hline
   P_i & 35 & -35 & 11 & -2 & 3 & 1 & 2 & 1 & 3 \\
   Q_i & 101 & -12 & 9 & 1 & 4 & 3 & 3 & 4 & 1 \\
   A_i & 0 & 1 & 1 & 2 & 3 & 5 & 8 & 13 & 86 \\
   B_i & 1 & 2 & 3 & 5 & 8 & 13 & 21 & 34 & 225 \\
   \end{array}
   \]

   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 \( G_n = Q_n A_n - P_n B_n \), we have

   \[
   \begin{align*}
   G_2 &= 101 \cdot 1 - 35 \cdot 3 = -4, \quad x + y \sqrt{13} = -4 + 3 \sqrt{13}, \quad x^2 - 13y^2 = -101; \\
   G_7 &= 101 \cdot 13 - 35 \cdot 34 = 123, \quad x + y \sqrt{13} = 123 + 34 \sqrt{13}, \quad x^2 - 13y^2 = 101. \\
   \end{align*}
   \]

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

   \[
   \begin{array}{c|cccccccc}
   i & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
   \hline
   P_i & -35 & -66 & 23 & 1 & 3 & 1 & 2 & 1 & 3 \\
   Q_i & 101 & -43 & 12 & 1 & 4 & 3 & 3 & 4 & 1 \\
   A_i & -1 & 0 & -1 & -4 & -5 & -9 & -14 & -23 & -152 \\
   B_i & 1 & 1 & 3 & 13 & 16 & 29 & 45 & 74 & 489 \\
   \end{array}
   \]
We observe that $Q_3 = Q_8 = 1$. Hence

$G_2 = 101 \cdot (-1) - (35) \cdot 3 = 4 \cdot x + y\sqrt{13} = 4 + 3\sqrt{13}, x^2 - 13y^2 = -101$;

$G_7 = 101 \cdot (-23) - (35) \cdot 74 = 267 \cdot x + y\sqrt{13} = 267 + 74\sqrt{13}, x^2 - 13y^2 = 101$.

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 $P_0^2 \equiv 221 \ (\mod 217)$ are $\pm 2$ and $\pm 33$.

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

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_1$</td>
<td>2</td>
<td>-2</td>
<td>14</td>
<td>11</td>
<td>13</td>
<td>13</td>
<td>11</td>
<td>14</td>
</tr>
<tr>
<td>$Q_1$</td>
<td>217</td>
<td>1</td>
<td>25</td>
<td>4</td>
<td>13</td>
<td>4</td>
<td>25</td>
<td>1</td>
</tr>
<tr>
<td>$A_1$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>7</td>
<td>15</td>
<td>97</td>
<td>112</td>
<td>3233</td>
</tr>
<tr>
<td>$B_1$</td>
<td>1</td>
<td>12</td>
<td>13</td>
<td>90</td>
<td>193</td>
<td>1248</td>
<td>1441</td>
<td>41596</td>
</tr>
</tbody>
</table>

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.

$G_0 = 217 \cdot 0 - 2 \cdot 1 = -2 \cdot x + y\sqrt{221} = -2 + \sqrt{221}, x^2 - 221y^2 = -217$.

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

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

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_1$</td>
<td>33</td>
<td>-33</td>
<td>17</td>
<td>0</td>
<td>13</td>
<td>11</td>
<td>14</td>
<td>14</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>$Q_1$</td>
<td>217</td>
<td>-4</td>
<td>17</td>
<td>13</td>
<td>4</td>
<td>25</td>
<td>1</td>
<td>25</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>$A_1$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>13</td>
<td>15</td>
<td>433</td>
<td>448</td>
<td>3121</td>
<td>6690</td>
</tr>
<tr>
<td>$B_1$</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>9</td>
<td>59</td>
<td>68</td>
<td>1963</td>
<td>2031</td>
<td>14149</td>
<td>30329</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_1$</td>
<td>-33</td>
<td>-184</td>
<td>29</td>
<td>11</td>
<td>14</td>
<td>14</td>
<td>11</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>$Q_1$</td>
<td>217</td>
<td>-155</td>
<td>4</td>
<td>25</td>
<td>1</td>
<td>25</td>
<td>4</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>$A_1$</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
<td>-29</td>
<td>-30</td>
<td>-209</td>
<td>-448</td>
<td>-2897</td>
</tr>
<tr>
<td>$B_1$</td>
<td>1</td>
<td>1</td>
<td>11</td>
<td>12</td>
<td>347</td>
<td>359</td>
<td>2501</td>
<td>5361</td>
<td>34667</td>
</tr>
</tbody>
</table>

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 $\pm 33$. However $(33 + \sqrt{79})/101 = [0, 2, 2, 3, 5, 1, 1, 1]$ and from the table

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_i$</td>
<td>33</td>
<td>-33</td>
<td>13</td>
<td>5</td>
<td>7</td>
<td>8</td>
<td>7</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>$Q_i$</td>
<td>101</td>
<td>-10</td>
<td>9</td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>10</td>
<td>7</td>
<td>9</td>
</tr>
</tbody>
</table>

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


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