Definition: Let $d, m_0,$ and $q_0$ be integers satisfying $q_0 \mid (d - m_0^2)$, and define $\xi_0 = (m_0 + \sqrt{d})/q_0$. The Quadratic Irrational Process produces sequences of integers as follows: for $j \geq 0$, define

$$a_j = \lfloor \xi_j \rfloor, \quad m_{j+1} = a_j q_j - m_j, \quad q_{j+1} = \frac{d - m_{j+1}^2}{q_j}, \quad \xi_{j+1} = \frac{m_{j+1} + \sqrt{d}}{q_{j+1}}.$$

1. (a) Carry out the Quadratic Irrational Process for $d = 41, m_0 = 0, q_0 = 1$, through $j = 5$. Have we seen this sequence of $a_j$ before?

(b) Given the above sequence of $a_j$, calculate $h_j$ and $k_j$ through $j = 5$. For each $0 \leq j \leq 5$, calculate $h_j^2 - 41k_j^2$. Spot the pattern (you don’t have to prove it).

(c) Expand out $(h_j + k_j\sqrt{41})^2$ as one integer plus another integer times $\sqrt{41}$. Do those integers look familiar?

(d) Given integers $x, y, d,$ and $N$ such that $x^2 - dy^2 = N$, define the integers $x_\ell$ and $y_\ell$ by the identity $x_\ell + y_\ell\sqrt{d} = (x + y\sqrt{d})^\ell$. Prove that $x_\ell^2 - dy_\ell^2 = N^\ell$. Hint: consider $(x + y\sqrt{d})(x - y\sqrt{d})$.

(e) Find integers $x, y > 32$ such that $x^2 - 41y^2 = -1$. Then find integers $x, y > 2049$ such that $x^2 - 41y^2 = 1$. Using calculators is a good idea.

(a) We record our calculations (all of which use $d = 41$) in the following table:

<table>
<thead>
<tr>
<th>$j$</th>
<th>$m_j$</th>
<th>$q_j$</th>
<th>$\xi_j$</th>
<th>$a_j$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$\sqrt{41}$</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>5</td>
<td>$(6 + \sqrt{41})/5$</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>5</td>
<td>$(4 + \sqrt{41})/5$</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>1</td>
<td>$6 + \sqrt{41}$</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>5</td>
<td>$(6 + \sqrt{41})/5$</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>5</td>
<td>$(4 + \sqrt{41})/5$</td>
<td>2</td>
</tr>
</tbody>
</table>

Indeed, this sequence of $a_j$ gives the continued fraction for $\sqrt{41}$ that we saw in Friday’s class, namely the periodic continued fraction $\langle 6; 2, 2, 12 \rangle$. (Note that the table above is also periodic, since the $j = 1$ and $j = 4$ rows are identical.)

(b) This sort of calculation is familiar to us already:

<table>
<thead>
<tr>
<th>$j$</th>
<th>$a_j$</th>
<th>$h_j$</th>
<th>$k_j$</th>
<th>$h_j^2 - 41k_j^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$-2$</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$-1$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>6</td>
<td>6</td>
<td>1</td>
<td>$-5$</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>13</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>32</td>
<td>5</td>
<td>$-1$</td>
</tr>
<tr>
<td>3</td>
<td>12</td>
<td>397</td>
<td>62</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>826</td>
<td>129</td>
<td>$-5$</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>2049</td>
<td>320</td>
<td>1</td>
</tr>
</tbody>
</table>

By comparing the two tables above, we observe that $h_{j-1}^2 - 41k_{j-1}^2 = (-1)^j q_j$ for $j \geq 0$. 
(c) We have
\[(h_2 + k_2\sqrt{41})^2 = (32 + 5\sqrt{41})^2 = 32^2 + 2 \cdot 32 \cdot 5\sqrt{41} + 5^2 \cdot 41 = 2049 + 320\sqrt{41},\]
which we notice is the same as \(h_5 + k_5\sqrt{41}\).

(d) The key fact we need is that \(x_\ell\) and \(y_\ell\) also satisfy \(x_\ell - y_\ell\sqrt{41} = (x - y\sqrt{41})^\ell\): if we knew that, then
\[
x_\ell^2 - 41y_\ell^2 = (x_\ell + y_\ell\sqrt{41})(x_\ell - y_\ell\sqrt{41}) = (x + y\sqrt{41})^\ell(x - y\sqrt{41})^\ell = ((x + y\sqrt{41})(x - y\sqrt{41}))^\ell = (x^2 + dy^2)^\ell = N^\ell.
\]

There are (at least) three ways to prove that \(x_\ell - y_\ell\sqrt{41} = (x - y\sqrt{41})^\ell\):

**Proof 1:** We have
\[
x_\ell + y_\ell\sqrt{41} = (x + y\sqrt{41})^\ell
\]
\[
= \sum_{i=0}^{\ell} \binom{\ell}{i} (y\sqrt{41})^i x^{\ell-i}
\]
\[
= \sum_{0 \leq i \leq \ell, \ i \ even} \binom{\ell}{i} (y\sqrt{41})^i x^{\ell-i} + \sum_{0 \leq i \leq \ell, \ i \ odd} \binom{\ell}{i} (y\sqrt{41})^i x^{\ell-i}
\]
\[
= \sum_{0 \leq i \leq \ell, \ i \ even} \binom{\ell}{i} y^{i/2} 41^{1/2}x^{\ell-i} + \sqrt{41} \sum_{0 \leq i \leq \ell, \ i \ even} \binom{\ell}{i} y^i 41^{(\ell-1)/2}x^{\ell-i},
\]

since both sums are manifestly integers, the first sum equals \(x_\ell\) and the second equals \(y_\ell\). On the other hand,

\[
(x - y\sqrt{41})^\ell = \sum_{i=0}^{\ell} \binom{\ell}{i} (-y\sqrt{41})^i x^{\ell-i}
\]
\[
= \sum_{0 \leq i \leq \ell, \ i \ even} \binom{\ell}{i} (-y\sqrt{41})^i x^{\ell-i} + \sum_{0 \leq i \leq \ell, \ i \ odd} \binom{\ell}{i} (-y\sqrt{41})^i x^{\ell-i}
\]
\[
= \sum_{0 \leq i \leq \ell, \ i \ even} \binom{\ell}{i} y^{i/2} 41^{1/2}x^{\ell-i} - \sqrt{41} \sum_{0 \leq i \leq \ell, \ i \ even} \binom{\ell}{i} y^i 41^{(\ell-1)/2}x^{\ell-i}
\]
\[
= x_\ell - y_\ell\sqrt{41},
\]
since the two resulting sums are exactly the same as before.

**Proof 2:** We proceed by induction on \(\ell\); the base case is trivial because \(x_1 = x\) and \(y_1 = y\).

Note that
\[
x_{\ell+1} + y_{\ell+1}\sqrt{41} = (x + y\sqrt{41})^{\ell+1} = (x + y\sqrt{41})^\ell(x - y\sqrt{41}) = (x_\ell + y_\ell\sqrt{41})(x + y\sqrt{41})
\]
\[
= (x_\ell x + 41y_\ell y) + (x_\ell y + y_\ell x)\sqrt{41},
\]
and so \( x_{\ell+1} = x_{\ell}x + 41y_{\ell}y \) and \( y_{\ell+1} = x_{\ell}y + y_{\ell}x \). On the other hand, under the induction hypothesis that \( x_{\ell} - y_{\ell}\sqrt{41} = (x - y\sqrt{41})^\ell \), we have

\[
(x - y\sqrt{41})^{\ell+1} = (x - y\sqrt{41})^\ell (x - y\sqrt{41}) = (x_{\ell} - y_{\ell}\sqrt{41})(x - y\sqrt{41})
\]

\[
= (x_{\ell}x + 41y_{\ell}y) - (x_{\ell}y + y_{\ell}x)\sqrt{41} = x_{\ell+1} - y_{\ell+1}\sqrt{41}
\]
as desired.

**Proof 3:** Let \( f(t) \in \mathbb{Q}[t] \) be irreducible, and let \( \alpha \) and \( \beta \) be any two roots of \( f \). Then Galois theory tells us that there exists a field isomorphism from \( \mathbb{Q}(\alpha) \) to \( \mathbb{Q}(\beta) \) that sends \( \alpha \) to \( \beta \). In particular, if \( g(t) \in \mathbb{Q}[t] \) is any polynomial, so that \( g(\alpha) = \sum_{i=0}^{\ell} r_i \alpha^i \) for some rational numbers \( r_i \), then \( g(\beta) = \sum_{i=0}^{\ell} r_i \beta^i \) for the same rational numbers. Our desired identity is the special case where \( f(t) = t^2 - 41 \), \( \alpha = \sqrt{41} \), \( \beta = -\sqrt{41} \), and \( g(t) = (x + yt)^\ell \).

(e) We define \( x = 32 \) and \( y = 5 \), so that \( x^2 - 41y^2 = -1 \). By part (d), if we define \( x_{\ell} \) and \( y_{\ell} \) by \( x_{\ell} + y_{\ell}\sqrt{41} = (x + y\sqrt{41})^\ell \), we then have \( x_{\ell}^2 - 41y_{\ell}^2 = (-1)^\ell \). Indeed, we saw the case \( \ell = 2 \) in part (c). Taking \( \ell = 3 \) and \( \ell = 4 \):

\[
(32 + 5\sqrt{41})^3 = 32^3 + 3 \cdot 32^2 \cdot 5\sqrt{41} + 3 \cdot 32 \cdot (5\sqrt{41})^2 + (5\sqrt{41})^3
\]

\[
= 32768 + 15360\sqrt{41} + 98400 + 5125\sqrt{41}
\]

\[
= 131168 + 20485\sqrt{41}
\]

\[
(32 + 5\sqrt{41})^4 = 32^4 + 4 \cdot 32^3 \cdot 5\sqrt{41} + 6 \cdot 32^2 \cdot (5\sqrt{41})^2 + 4 \cdot 32 \cdot (5\sqrt{41})^3 + (5\sqrt{41})^4
\]

\[
= 1050625 + 656000\sqrt{41} + 6297600 + 655360\sqrt{41} + 1048576
\]

\[
= 8396801 + 1311360\sqrt{41};
\]

and indeed \( 131168^2 - 41 \cdot 20485^2 = -1 \) and \( 8396801^2 - 41 \cdot 1311360^2 = 1 \).