18.781 Problem Set 9 solutions

Due Monday April 22 in class. To answer any of the questions, you can quote theorems from the text.

1. Calculate the smallest positive solution of \( x^2 - 61y^2 = -1 \).

Begin with the table for calculating the continued fraction expansion of \( \sqrt{61} \) from Problem Set 8; add two columns as explained below for the convergents of the continued fraction expansion. I’ve also added a first column with the index \( i \).

Here is the table explained below:

<table>
<thead>
<tr>
<th>( i )</th>
<th>( m )</th>
<th>( q )</th>
<th>( \xi )</th>
<th>( a )</th>
<th>( h )</th>
<th>( k )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>( \sqrt{61} )</td>
<td>7</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>7</td>
<td>12</td>
<td>( 7+\sqrt{61} )/12</td>
<td>1</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>3</td>
<td>( 5+\sqrt{61} )/4</td>
<td>4</td>
<td>39</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>4</td>
<td>( 7+\sqrt{61} )/3</td>
<td>3</td>
<td>125</td>
<td>16</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>9</td>
<td>( 5+\sqrt{61} )/9</td>
<td>1</td>
<td>164</td>
<td>21</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>5</td>
<td>( 4+\sqrt{61} )/5</td>
<td>2</td>
<td>453</td>
<td>58</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>5</td>
<td>( 6+\sqrt{61} )/5</td>
<td>2</td>
<td>1070</td>
<td>137</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>9</td>
<td>( 4+\sqrt{61} )/9</td>
<td>1</td>
<td>1523</td>
<td>195</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>4</td>
<td>( 5+\sqrt{61} )/4</td>
<td>3</td>
<td>5639</td>
<td>722</td>
</tr>
<tr>
<td>9</td>
<td>7</td>
<td>3</td>
<td>( 7+\sqrt{61} )/3</td>
<td>4</td>
<td>24079</td>
<td>3083</td>
</tr>
<tr>
<td>10</td>
<td>5</td>
<td>12</td>
<td>( 5+\sqrt{61} )/12</td>
<td>1</td>
<td>29718</td>
<td>3805</td>
</tr>
<tr>
<td>11</td>
<td>7</td>
<td>1</td>
<td>7 + ( \sqrt{61} )</td>
<td>14</td>
<td>440131</td>
<td>56353</td>
</tr>
<tr>
<td>12</td>
<td>7</td>
<td>12</td>
<td>( 7+\sqrt{61} )/12</td>
<td>1</td>
<td>469849</td>
<td>60158</td>
</tr>
</tbody>
</table>

and so on; \( \sqrt{61} = \langle 7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14 \rangle \). The period \( r = 11 \) is odd, so

Theorem 7.25 in the text guarantees that the smallest positive solution of \( x^2 - 61y^2 = -1 \) is \( x = h_{11-1}, y = k_{11-1} \):

\[
(x, y) = (29718, 3805)
\]

A calculator will verify that \( x^2 = 883, 159, 524 \) and \( 61y^2 = 883, 159, 825 \), so at least this is a solution.

2. Calculate the smallest positive solution of \( x^2 - 61y^2 = 1 \).

Theorem 7.25 says that the answer is \((h_{21}, k_{21})\). One way to find these is to extend the table above for an additional nine rows. This is a painful process by hand (although easy enough on a computer). A simpler solution is to use the matrix formulas from Problem 7. I won’t repeat all the notation (what was \((P_n, Q_n)\) there is what we’re calling \((h_n, k_n)\) here) but these say that

\[
\begin{pmatrix} h_{21} \\ k_{21} \end{pmatrix} = A_0 A_1 \cdots A_{21} \\
= A_0 A_1 \cdots A_{10} A_{11} A_{12} \cdots A_{21} \\
= A_0 A_1 \cdots A_{10} A_{11} A_1 \cdots A_{10}
\]
In the last step we used the periodicity

\[ A_n = A_{n+11} \quad (n \geq 1). \]

Also

\[ A_{11} = \begin{pmatrix} 14 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 7 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix} A_0. \]

Inserting this above gives

\[ \begin{pmatrix} h_{21} \\ k_{21} \\ h_{20} \\ k_{20} \end{pmatrix} = A_0 \cdots A_{10} \begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix} A_0 \cdots A_{10}. \]

We have a formula for \( A_0 \cdots A_{10} \) from the table in \#1; inserting it gives

\[ \begin{pmatrix} h_{21} \\ k_{21} \\ h_{20} \\ k_{20} \end{pmatrix} = \begin{pmatrix} 29718 & 24079 \\ 3805 & 3083 \end{pmatrix} \begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 29718 & 24079 \\ 3805 & 3083 \end{pmatrix} \]
\[ = \begin{pmatrix} 29718 \cdot 29718 + 24079 \cdot 24079 \\ 3805 \cdot 3805 + 3083 \cdot 3083 \end{pmatrix} \begin{pmatrix} 29718 & 24079 \\ 3805 & 3083 \end{pmatrix} \]
\[ = \begin{pmatrix} 29718 \cdot 61 \cdot 3805 \\ 3805 \cdot 29718 \end{pmatrix} \begin{pmatrix} 29718 & 24079 \\ 3805 & 3083 \end{pmatrix} \]
\[ = \begin{pmatrix} 1766319049 \\ 226153980 \end{pmatrix} h_{20}. \]

I didn’t do the calculations of the last two entries because we don’t need them. So the smallest positive solution we are looking for is

\[ x = 1766319049, \quad y = 226153980 \]
\[ x^2 = 3119882982860264401, \quad 61y^2 = 3119882982860264400. \]

There is another, even easier, way to get this. An easy generalization of Theorem 7.26 says that if \((x_1, y_1)\) is the smallest positive solution of \(x^2 - dy^2 = -1\), then all positive solutions of \(x^2 - dy^2 = (-1)^n\) are the integers defined by

\[ x_n + y_n \sqrt{d} = (x_1 + y_1 \sqrt{d})^n. \]

In particular, the smallest solution with +1 comes from \(n = 2\):

\[ x = x_1^2 + 61y_1^2, \quad y = 2x_1y_1. \]

That’s evidently what the matrix calculation gave (at least after I inserted the factorization of 232105 before the last step).

This is all still accessible to hand calculation. For a more serious Pell’s equation, and really big numbers, you might Google Archimedes’ cattle problem.

3. A Pythagorean triple consists of three positive integers \(x\), \(y\), and \(z\) satisfying \(x^2 + y^2 = z^2\). If \(a > b\) are positive integers, then

\[ (a^2 - b^2, 2ab, a^2 + b^2), \quad (2ab, a^2 - b^2, a^2 + b^2) \]
are both Pythagorean triples. A Pythagorean triple is called *primitive* if \(x, y,\) and \(z\) are relatively prime. We are going to prove in class that any primitive Pythagorean triple is given by one of the formulas (PT).

a) **Find a non-primitive Pythagorean triple given by one of the formulas (PT).**

Taking \(a = 3, b = 1\) leads to the non-primitive triple \((8, 6, 10)\).

b) **Find necessary and sufficient conditions on the integers \(a > b > 0\) so that the triples (PT) are primitive.** You should explain as completely as you can why your conditions are necessary (that is, why (PT) is *not* primitive when they fail) and why they are sufficient (that is, why (PT) *is* primitive when they hold). (Hint: one of the conditions is that \(a\) and \(b\) are relatively prime.)

The requirements are

\[
a \text{ and } b \text{ are relatively prime}
\]

and

\[
a \text{ and } b \text{ have different parity (one even and one odd)}.
\]

If \(a\) and \(b\) have the common factor \(d\), then \(x, y,\) and \(z\) have the common factor \(d^2\), so the triple is *not* primitive. That’s why the first condition is necessary. If \(a\) and \(b\) are both odd, then \(a^2\) and \(b^2\) are both odd, so \(a^2 - b^2\) and \(a^2 + b^2\) must be even. Therefore \(x, y,\) and \(z\) have the common factor 2, and the triple is *not* primitive. If \(a\) and \(b\) are both even, then they are not relatively prime, and we already know that the triple is not primitive.

Conversely, suppose these two requirements are satisfied; we want to know that the triple is primitive. Suppose that \(x\) and \(y\) have a common prime factor \(p\). This means that \(a^2 - b^2 = (a + b)(a - b)\) and \(2ab\) have the common factor \(p\). Since \(a\) and \(b\) have opposite parity, \(x\) is odd, so \(p\) must be odd. Therefore \(p\) is a factor either of \(a\) or of \(b\), and also either of \(a + b\) or \(a - b\). This is four cases. For example if \(p\) is a factor of \(a\) and of \(a + b\), then it must also be a factor of \(b\), contradicting our hypothesis that \(a\) and \(b\) are relatively prime. The other three cases are identical, all leading to contradictions; so the conclusion is that \(x\) and \(y\) cannot have a common prime factor, as we wished to show.

c) **Find an example of a non-primitive Pythagorean triple that is *not* given by one of the formulas (PT).**

I’m not sure of the best systematic way to proceed. The smallest non-primitive triple is \((6, 8, 10)\). This is given by the second formula in (PT) with \(a = 3, b = 1\). The next is \((9, 12, 15)\). If this is to be given by either formula (PT) it must be the first, since the second formula would say that 9 was even. So we want to see whether there exist \(a > b > 0\) with

\[
a^2 - b^2 = 9, \quad ab = 6.
\]

The only solutions to the second equation are \(a = 6, b = 1\) and \(a = 3, b = 2\). Neither of these satisfies the first. The conclusion is that \((9, 12, 15)\) is *not* given by a formula (PT).
d) There is a function \( F : \mathbb{R}^2 \to \mathbb{R}^3 \),
\[
F(\alpha, \beta) = (\alpha^2 - \beta^2, 2\alpha\beta, \alpha^2 + \beta^2).
\]

Give the simplest and most complete description you can of the image of \( F \). (Hint: the image of \( F \) is a “parametric surface.” Another example of a parametric surface is
\[
G(\theta, \phi) = (\cos \theta \sin \phi, \sin \theta \sin \phi, \cos \phi),
\]
spherical coordinates. An answer for \( G \) might be, “the image of \( G \) is the unit sphere \( x^2 + y^2 + z^2 = 1 \).”

The image in \( \mathbb{R}^3 \) is the half cone
\[
x^2 + y^2 = z^2, \quad z \geq 0.
\]

That \( F(\alpha, \beta) \) belongs to this half cone is very easy: \( z \) is a sum of squares, so must be nonnegative, and verifying the cone equation is easy algebra. Seeing that the image is the entire half cone requires a bit of thought. One possibility is to identify \( \mathbb{R}^2 \) with the complex numbers \( \mathbb{C} \) in the usual way; then
\[
F : \mathbb{C} \to \mathbb{C} \times \mathbb{R}, \quad F(w) = (w^2, |w|^2).
\]

In these coordinates the equation of the cone is
\[
\{(u, t) \in \mathbb{C} \times \mathbb{R} \mid t = \pm|u|\}.
\]

Now it’s more or less clear that the map \( F \) is two-to-one from \( \mathbb{C} \) to the positive cone: the preimage of \((u, |u|)\) consists of the two square roots of the complex number \( u \). (Well, if \( u = 0 \) there is only one square root.)

**********************************************************************************

Summary of the method from the text and class for calculating the continued fraction expansion of \((m_0 + \sqrt{d})/q_0\) and the convergents
\[
\langle a_0, \ldots, a_i \rangle = \frac{h_i}{k_i}:
\]
make a table with rows numbered \( i = 0, 1, 2, \ldots \), and six columns of data: \( m_i, q_i, \xi_i = (m_i + \sqrt{d})/q_i, a_i = \lfloor \xi_i \rfloor, h_i, \) and \( k_i \). Calculate row \( i + 1 \) from row \( i \) by the formulas
\[
m_{i+1} = q_i a_i - m_i, \quad q_{i+1} = (d - m_{i+1}^2)/q_i.
\]
This works as long as \( m_0 \) is an integer, \( d \) is a positive integer non-square, and \( q_0 \) is a divisor of \( d - m_0^2 \).

For the convergents: \( h_i = a_i h_{i-1} + h_{i-2}, k_i = a_i k_{i-1} + k_{i-2} \). These formulas get started with \( h_{-2} = 0, h_{-1} = 1, k_{-2} = 1, k_{-1} = 0 \).