11.2 Problems

1. Show that if x,y,z is a Pythagorean triple and n is an integer $n > 2$, then $x^n + y^n \neq z^n$.
2. Show that Fermat's last theorem is a consequence of Theorem 11.2, and the assertion that $x^p + y^p = z^p$ has no solutions in nonzero integers when p is an odd prime.
3. Using Fermat's little theorem, show that if p is prime and
   a) if $x^{p-1} + y^{p-1} = z^{p-1}$, then $p \mid xyz$.
   b) if $x^p + y^p = z^p$, then $p \mid (x+y-z)$.
4. Show that the diophantine equation $x^4-y^4 = z^2$ has no solutions in nonzero integers using the method of infinite descent.
5. Using problem 4, show that the area of a right triangle with integer sides is never a perfect square.
6. Show that the diophantine equation $x^4 + 4y^4 = z^2$ has no solutions in nonzero integers.
7. Show that the diophantine equation $x^t - 8y^4 = z^2$ has no solutions in nonzero integers.
8. Show that the diophantine equation $x^4 + 3y^4 = z^4$ has infinitely many solutions.
9. Show that in a Pythagorean triple there is at most one perfect square.
10. Show that the diophantine equation $x^2 + y^2 = z^3$ has infinitely many integer solutions by showing that for each positive integer k the integers $x = 3k^2-1, y = k(k^2-3), z = k^2 + 1$ form a solution.

11.2 Computer Projects

1. Write a computer program to search for solutions of diophantine equations such as $x^n + y^n = z^n$.

11.3 Pell's Equation

In this section, we study diophantine equations of the form

$$x^2 - dy^2 = n \ , \tag{11.2}$$

where d and n are fixed integers. When $d < 0$ and $n < 0$, there are no solutions of (11.2). When $d < 0$ and $n > 0$, there can be at most a finite

number of solutions, since the equation $x^2 - dy^2 = n$ implies that $|x| \leqslant \sqrt{n}$ and $|y| \leqslant \sqrt{n/|d|}$. Also, note that when d is a perfect square, say $d = D^2$, then

$$x^2 - dy^2 = x^2 - D^2y = (x+Dy)(x-Dy) = n .$$

Hence, any solution of (11.2), when d is a perfect square, corresponds to a simultaneous solution of the equations

$$\begin{aligned} x + Dy &= a \\ x - Dy &= b , \end{aligned}$$

where a and b are integers such that $n = ab$. In this case, there are only a finite number of solutions, since there is at most one solution in integers of these two equations for each factorization $n = ab$.

For the rest of this section, we are interested in the diophantine equation $x^2 - dy^2 = n$, where d and n are integers and d is a positive integer which is not a perfect square. As the following theorem shows, the simple continued fraction of $\sqrt{d}$ is very useful for the study of this equation.

Theorem 11.3. Let d and n be integers such that $d > 0$, d is not a perfect square, and $|n| < \sqrt{d}$. If $x^2 - dy^2 = n$, then x/y is a convergent of the simple continued fraction of $\sqrt{d}$.

Proof. First consider the case where $n > 0$. Since $x^2 - dy^2 = n$, we see that

$$(x+y\sqrt{d})(x-y\sqrt{d}) = n . \tag{11.3}$$

From (11.3), we see that $x - y\sqrt{d} > 0$, so that $x > y\sqrt{d}$. Consequently,

$$\frac{x}{y} - \sqrt{d} > 0 ,$$

and since $0 < n < \sqrt{d}$, we see that

$$\begin{aligned} \frac{x}{y} - \sqrt{d} &= \frac{(x-\sqrt{d}y)}{y} \\ &= \frac{x^2-dy^2}{y(x + y\sqrt{d})} \end{aligned}$$

$$< \frac{n}{y(2y\sqrt{d})}$$
$$< \frac{\sqrt{d}}{2y^2\sqrt{d}}$$
$$= \frac{1}{2y^2}.$$

Since $0 < \frac{x}{y} - \sqrt{d} < \frac{1}{2y^2}$, Theorem 10.18 tells us that x/y must be a convergent of the simple continued fraction of $\sqrt{d}$.

When $n < 0$, we divide both sides of $x^2 - dy^2 = n$ by $-d$, to obtain

$$y^2 - (\frac{1}{d})x^2 = -\frac{n}{d}.$$

By a similar argument to that given when $n > 0$, we see that y/x is a convergent of the simple continued fraction expansion of $1/\sqrt{d}$. Therefore, from problem 7 of Section 10.3, we know that $x/y = 1/(y/x)$ must be a convergent of the simple continued fraction of $\sqrt{d} = 1/(1/\sqrt{d})$. □

We have shown that solutions of the diophantine equation $x^2 - dy^2 = n$, where $|n| < \sqrt{d}$, are given by the convergents of the simple continued fraction expansion of $\sqrt{d}$. The next theorem will help us use these convergents to find solutions of this diophantine equation.

Theorem 11.4. Let d be a positive integer that is not a perfect square. Define $\alpha_k = (P_k + \sqrt{d})/Q_k$, $a_k = [\alpha_k]$, $P_{k+1} = a_kQ_k - P_k$, and $Q_{k+1} = (d - P_{k+1}^2)/Q_k$, for $k = 0,1,2,...$ where $\alpha_0 = \sqrt{d}$. Furthermore, let p_k/q_k denote the kth convergent of the simple continued fraction expansion of $\sqrt{d}$. Then

$$p_k^2 - dq_k^2 = (-1)^{k-1}Q_{k+1}.$$

Before we prove Theorem 11.4, we prove a useful lemma.

Lemma 11.4. Let $r + s\sqrt{d} = t + u\sqrt{d}$ where r, s, t, and u are rational numbers and d is a positive integer that is not a perfect square. Then $r = t$ and $s = u$.

Proof. Since $r + s\sqrt{d} = t + u\sqrt{d}$, we see that if $s \neq u$ then

$$\sqrt{d} = \frac{r-t}{u-s}.$$

By Theorem 10.1, $(r-t)/(u-s)$ is rational, and by Theorem 10.2 $\sqrt{d}$ is irrational. Hence, $s = u$, and consequently $r = t$. □

We can now prove Theorem 11.4.

Proof. Since $\sqrt{d} = \alpha_0 = [a_0;a_1, a_2,...,a_k, \alpha_{k+1}]$, Theorem 10.9 tells us that

$$\sqrt{d} = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}}.$$

Since $\alpha_{k+1} = (P_{k+1} + \sqrt{d})/Q_{k+1}$ we have

$$\sqrt{d} = \frac{(P_{k+1} + \sqrt{d})p_k + Q_{k+1}p_{k-1}}{(P_{k+1} + \sqrt{d})q_k + Q_{k+1}q_{k-1}}.$$

Therefore, we see that

$$dq_k + (P_{k+1}q_k + Q_{k+1}q_{k-1})\sqrt{d} = (P_{k+1}p_k + Q_{k+1}p_{k-1}) + p_k\sqrt{d}.$$

From Lemma 11.4, we find that $dq_k = P_{k+1}p_k + Q_{k+1}p_{k-1}$ and $P_{k+1}q_k + Q_{k+1}q_{k-1} = p_k$. When we multiply the first of these two equations by q_k and the second by p_k, subtract the first from the second, and then simplify, we obtain

$$p_k^2 - dq_k^2 = (p_kq_{k-1} - p_{k-1}q_k)Q_{k+1} = (-1)^{k-1}Q_{k+1},$$

where we have used Theorem 10.10 to complete the proof. □

The special case of the diophantine equation $x^2 - dy^2 = n$ with $n = 1$ is called *Pell's equation.* We will use Theorems 11.3 and 11.4 to find all solutions of Pell's equation and the related equation $x^2 - dy^2 = -1$.

Theorem 11.5. Let d be a positive integer that is not a perfect square. Let p_k/q_k denote the kth convergent of the simple continued fraction of $\sqrt{d}$, $k = 1,2,3,...$ and let n be the period length of this continued fraction. Then, when n is even, the positive solutions of the diophantine equation $x^2 - dy^2 = 1$ are $x = p_{jn-1}$, $y = q_{jn-1}$, $j = 1,2,3,...$, and the diophantine equation $x^2 - dy^2 = -1$ has no solutions. When n is odd, the positive solutions of $x^2 - dy^2 = 1$ are $x = p_{2jn-1}, y = q_{2jn-1}$, $j = 1,2,3,...$ and the solutions of $x^2 - dy^2 = -1$ are $x = p_{(2j-1)n-1}, y = q_{(2j-1)n-1}$, $j = 1,2,3,...$.

Proof. Theorem 11.3 tells us that if x_0,y_0 is a positive solution of $x^2 - dy^2 = \pm 1$, then $x_0 = p_k$, $y_0 = q_k$ where p_k/q_k is a convergent of the simple continued fraction of $\sqrt{d}$. On the other hand, from Theorem 11.4 we know that

$$p_k^2 - dq_k^2 = (-1)^{k-1}Q_{k+1},$$

where Q_{k+1} is as defined in the statement of Theorem 11.4.

Because the period of the continued expansion of $\sqrt{d}$ is n, we know that $Q_{jn} = Q_0 = 1$ for $j = 1,2,3,...$, (since $\sqrt{d} = \dfrac{P_0 + \sqrt{d}}{Q_0}$). Hence,

$$p_{jn-1}^2 - d\ q_{jn-1}^2 = (-1)^{jn}Q_{nj} = (-1)^{jn}.$$

This equation shows that when n is even p_{jn-1}, q_{jn-1} is a solution of $x^2 - dy^2 = 1$ for $j = 1,2,3,...$, and when n is odd, p_{2jn-1}, q_{2jn-1} is a solution of $x^2 - dy^2 = 1$ and $p_{2(j-1)n-1}, q_{2(j-1)n-1}$ is a solution of $x^2 - dy^2 = -1$ for $j = 1,2,3,...$.

To show that the diophantine equations $x^2 - dy^2 = 1$ and $x^2 - dy^2 = -1$ have no solutions other than those already found, we will show that $Q_{k+1} = 1$ implies that $n|k$ and that $Q_j \neq -1$ for $j = 1,2,3...$.

We first note that if $Q_{k+1} = 1$, then

$$\alpha_{k+1} = P_{k+1} + \sqrt{d}.$$

Since $\alpha_{k+1} = [a_{k+1};a_{k+2},...]$, the continued fraction expansion of α_{k+1} is purely periodic. Hence, Theorem 10.20 tells us that $-1 < \alpha_{k+1} = P_{k+1} - \sqrt{d} < 0$. This implies that $P_{k+1} = [\sqrt{d}]$, so that $\alpha_k = \alpha_0$, and $n|k$.

To see that $Q_j \neq -1$ for $j = 1,2,3,...$, note that $Q_j = -1$ implies that $\alpha_j = -P_j - \sqrt{d}$. Since α_j has a purely periodic simple continued fraction expansion, we know that

$$-1 < \alpha_j' = -P_j + \sqrt{d} < 0$$

and

$$\alpha_j = -P_j - \sqrt{d} > 1.$$

From the first of these inequalities, we see that $P_j > -\sqrt{d}$ and, from the second, we see that $P_j < -1-\sqrt{d}$. Since these two inequalities for p_j are contradictory, we see that $Q_j \neq -1$.

Since we have found all solutions of $x^2-dy^2 = 1$ and $x^2-dy^2 = -1$, where x and y are positive integers, we have completed the proof. □

We illustrate the use of Theorem 11.5 with the following examples.

Example. Since the simple continued fraction of $\sqrt{13}$ is $[3;\overline{1,1,1,1,6}]$ the

positive solutions of the diophantine equation $x^2 - 13y^2 = 1$ are p_{10j-1}, q_{10j-1}, $j = 1,2,3,...$ where p_{10j-1}/q_{10j-1} is the $(10j-1)$th convergent of the simple continued fraction expansion of $\sqrt{13}$. The least positive solution is $p_9 = 649$, $q_9 = 180$. The positive solutions of the diophantine equation $x^2 - 13y^2 = -1$ are $p_{10j-6}, q_{10j-6}, j = 1,2,3,...$; the least positive solution is $p_4 = 18, q_4 = 5$.

Example. Since the continued fraction of $\sqrt{14}$ is $[3;\overline{1,2,1,6}]$, the positive solutions of $x^2 - 14y^2 = 1$ are p_{4j-1}, q_{4j-1}, $j = 1,2,3,...$ where p_{4j-1}/q_{4j-1} is the jth convergent of the simple continued fraction expansion of $\sqrt{14}$. The least positive solution is $p_3 = 15$, $q_3 = 4$. The diophantine equation $x^2 - 14y^2 = -1$ has no solutions, since the period length of the simple continued fraction expansion of $\sqrt{14}$ is even.

We conclude this section with the following theorem that shows how to find all the positive solutions of Pell's equation $x^2 - dy^2 = 1$ from the least positive solution, without finding subsequent convergents of the continued fraction expansion of $\sqrt{d}$.

Theorem 11.6. Let x_1, y_1 be the least positive solution of the diophantine equation $x^2 - dy^2 = 1$, where d is a positive integer that is not a perfect square. Then all positive solutions x_k, y_k are given by

$$x_k + y_k\sqrt{d} = (x_1 + y_1\sqrt{d})^k$$

for $k = 1,2,3,...$. (Note that x_k and y_k are determined by the use of Lemma 11.4).

Proof. We need to show that x_k, y_k is a solution for $k = 1,2,3,...$ and that every solution is of this form.

To show that x_k, y_k is a solution, first note that by taking conjugates, it follows that $x_k - y_k\sqrt{d} = (x_1 - y_1\sqrt{d})^k$, because from Lemma 10.4, the conjugate of a power is the power of the conjugate. Now, note that

$$\begin{aligned} x_k^2 - dy_k^2 &= (x_k + y_k\sqrt{d})(x_k - y_k\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})^k (x_1 - y_1\sqrt{d})^k \\ &= (x_1^2 - dy_1^2)^k \\ &= 1. \end{aligned}$$

Hence x_k, y_k is a solution for $k = 1,2,3,...$.

To show that every positive solution is equal to x_k, y_k for some positive integer k, assume that X, Y is a positive solution different from x_k, y_k for $k = 1,2,3,...$. Then there is an integer n such that

$$(x_1 + y_1\sqrt{d})^n < X + Y\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1}.$$

When we multiply this inequality by $(x_1 + y_1\sqrt{d})^{-n}$, we obtain

$$1 < (x_1 - y_1\sqrt{d})^n(X + Y\sqrt{d}) < x_1 + y_1\sqrt{d},$$

since $x_1^2 - dy_1^2 = 1$ implies that $x_1 - y_1\sqrt{d} = (x_1 + y_1\sqrt{d})^{-1}$.

Now let

$$s + t\sqrt{d} = (x_1 - y_1\sqrt{d})^n(X + Y\sqrt{d}),$$

and note that

$$\begin{aligned} s^2 - dt^2 &= (s - t\sqrt{d})(s + t\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})^n(X - Y\sqrt{d})(x_1 - y_1\sqrt{d})^n(X + Y\sqrt{d}) \\ &= (x_1^2 - dy_1^2)^n(X^2 - dY^2) \\ &= 1. \end{aligned}$$

We see that s,t is a solution of $x^2 - dy^2 = 1$, and furthermore, we know that $1 < s + t\sqrt{d} < x_1 + y_1\sqrt{d}$. Moreover, since we know that $s + t\sqrt{d} > 1$, we see that $0 < (s + t\sqrt{d})^{-1} < 1$. Hence

$$s = \frac{1}{2}[(s + t\sqrt{d}) + (s - t\sqrt{d})] > 0$$

and

$$t = \frac{1}{2\sqrt{d}}[(s + t\sqrt{d}) - (s - t\sqrt{d})] > 0.$$

This means that s,t is a positive solution, so that $s \geqslant x_1$, and $t \geqslant y_1$, by the choice of x_1,y_1 as the smallest positive solution. But this contradicts the inequality $s + t\sqrt{d} < x_1 + y_1\sqrt{d}$. Therefore X,Y must be x_k,y_k for some choice of k. □

To illustrate the use of Theorem 11.6, we have the following example.

Example. From a previous example we know that the least positive solution of the diophantine equation $x^2 - 13y^2 = 1$ is $x_1 = 649$, $y_1 = 180$. Hence, all positive solutions are given by x_k, y_k where

$$x_k + y_k\sqrt{13} = (649 + 180\sqrt{13})^k .$$

For instance, we have

$$x_2 + y_2\sqrt{13} = 842361 + 233640\sqrt{13}$$

Hence $x_2 = 842361$, $y_2 = 233640$ is the least positive solution of $x^2 - 13y^2 = 1$, other than $x_1 = 649$, $y_1 = 180$.

11.3 Problems

1. Find all the solutions of each of the following diophantine equations
   a) $x^2 + 3y^2 = 4$
   b) $x^2 + 5y^2 = 7$
   c) $2x^2 + 7y^2 = 30$.
2. Find all the solutions of each of the following diophantine equations
   a) $x^2 - y^2 = 8$
   b) $x^2 - 4y^2 = 40$
   c) $4x^2 - 9y^2 = 100$.
3. For which of the following values of n does the diophantine equation $x^2 - 31y^2 = n$ have a solution

   a) 1 d) −3
   b) −1 e) 4
   c) 2 f) −5?

4. Find the least positive solution of the diophantine equations
   a) $x^2 - 29y^2 = -1$
   b) $x^2 - 29y^2 = 1$.
5. Find the three smallest positive solutions of the diophantine equation $x^2 - 37y^2 = 1$.
6. For each of the following values of d determine whether the diophantine equation $x^2 - dy^2 = -1$ has solutions

   a) 2 e) 17
   b) 3 f) 31
   c) 6 g) 41
   d) 13 h) 50.

7. The least positive solution of the diophantine equation $x^2 - 61y^2 = 1$ is $x_1 = 1766319049$, $y_1 = 226153980$. Find the least positive solution other than x_1, y_1.

8. Show that if p_k/q_k is a convergent of the simple continued fraction expansion of $\sqrt{d}$ then $|p_k^2 - dq_k^2| < 1 + 2\sqrt{d}$.

9. Show that if d is a positive integer divisible by a prime of the form $4k + 3$, then the diophantine equation $x^2 - dy^2 = -1$ has no solutions.

10. Let d and n be positive integers.

    a) Show that if r,s is a solution of the diophantine equation $x^2 - dy^2 = 1$ and X,Y is a solution of the diophantine equation $x^2 - dy^2 = n$ then $Xr \pm dYs$, $Xs \pm Yr$ is also a solution of $x^2 - dy^2 = n$.

    b) Show that the diophantine equation $x^2 - dy^2 = n$ either has no solutions, or infinitely many solutions.

11. Find those right triangles having legs with lengths that are consecutive integers. (Hint: use Theorem 11.1 to write the lengths of the legs as $x = s^2 - t^2$ and $y = 2st$, where s and t are positive integers such that $(s,t) = 1$, $s > t$ and s and t have opposite parity. Then $x - y = \pm 1$ implies that $(s - t)^2 - 2t^2 = \pm 1$.)

12. Show that each of the following diophantine equations has no solutions

    a) $x^4 - 2y^4 = 1$ b) $x^4 - 2y^2 = -1$.

11.3 Computer Projects

Write programs to do the following:

1. Find those integers n with $|n| < \sqrt{d}$ such that the diophantine equation $x^2 - dy^2 = n$ has no solutions.

2. Find the least positive solutions of the diophantine equations $x^2 - dy^2 = 1$ and $x^2 - dy^2 = -1$.

3. Find the solutions of Pell's equation from the least positive solution (see Theorem 11.6).