Theorem 13-14 indicates that if the equation $x^2 - dy^2 = 1$ possesses a solution, then its positive solutions are to be found among $x = p_k$, $y = q_k$, where p_k/q_k are the convergents of $\sqrt{d}$. The period of the continued fraction expansion of $\sqrt{d}$ provides the information we need to show that $x^2 - dy^2 = 1$ actually does have a solution in integers; in fact, there are infinitely many solutions, all obtainable from the convergents of $\sqrt{d}$. Our proof relies on a lemma.

LEMMA. *Let the convergents of the continued fraction expansion of $\sqrt{d}$ be p_k/q_k. If n is the length of the period of the expansion of $\sqrt{d}$, then*

$$p_{kn-1}^2 - dq_{kn-1}^2 = (-1)^{kn} \qquad (k = 1, 2, 3, \ldots).$$

Proof: For $k \geq 1$, the continued fraction expansion of $\sqrt{d}$ can be written in the form

$$\sqrt{d} = [a_0; a_1, a_2, \ldots, a_{kn-1}, x_{kn}]$$

where

$$x_{kn} = [2a_0; \overline{a_1, \ldots, a_{n-1}, 2a_0}] = a_0 + \sqrt{d}.$$

As in the proof of Theorem 13-6, we have

$$\sqrt{d} = \frac{x_{kn}p_{kn-1} + p_{kn-2}}{x_{kn}q_{kn-1} + q_{kn-2}}.$$

Upon substituting $x_{kn} = a_0 + \sqrt{d}$ and simplifying, this reduces to

$$\sqrt{d}(a_0 q_{kn-1} + q_{kn-2} - p_{kn-1}) = a_0 p_{kn-1} + p_{kn-2} - dq_{kn-1}.$$

Because the right-hand side is rational and $\sqrt{d}$ is irrational, the foregoing relation requires that

$$a_0 q_{kn-1} + q_{kn-2} = p_{kn-1}, \qquad \text{and} \qquad a_0 p_{kn-1} + p_{kn-2} = dq_{kn-1}.$$

The effect of multiplying the first of these equations by p_{kn-1} and the second by $-q_{kn-1}$, and then adding them, is

$$p_{kn-1}^2 - dq_{kn-1}^2 = p_{kn-1}q_{kn-2} - q_{kn-1}p_{kn-2}.$$

But Theorem 13-7 informs us that $p_{kn-1}q_{kn-2} - q_{kn-1}p_{kn-2} = (-1)^{kn-2} = (-1)^{kn}$, and so

$$p_{kn-1}^2 - dq_{kn-1}^2 = (-1)^{kn},$$

which results in our lemma.

We can now describe all positive solutions of $x^2 - dy^2 = 1$, where $d > 0$ is a nonsquare integer. We state our main result as

THEOREM 13-16. *Let p_k/q_k be the convergents of the continued fraction expansion of $\sqrt{d}$ and let n be the length of the period of the expansion.*
(1) *If n is even, then all positive solutions of $x^2 - dy^2 = 1$ are given by*

$$x = p_{kn-1}, \qquad y = q_{kn-1} \qquad (k = 1, 2, 3, \ldots).$$

(2) *If n is odd, then all positive solutions of $x^2 - dy^2 = 1$ are given by*

$$x = p_{2kn-1}, \qquad y = q_{2kn-1} \qquad (k = 1, 2, 3, \ldots).$$

Proof: It has already been established that any positive solution x_0, y_0 of $x^2 - dy^2 = 1$ is of the form $x_0 = p_k$, $y_0 = q_k$ for some convergent p_k/q_k.

Taking the lemma into account, $x = p_{kn-1}$, $y = q_{kn-1}$ will furnish a solution if and only if $(-1)^{kn} = 1$. When n is even, this condition is satisfied by all integers k; when n is odd, the condition holds if and only if k is an even integer.

Example 13-7

As a first application of Theorem 13-16, we again consider the equation $x^2 - 7y^2 = 1$. Because $\sqrt{7} = [2; \overline{1, 1, 1, 4}]$, the initial twelve convergents are

$$2/1,\ 3/1,\ 5/2,\ 8/3,\ 37/14,\ 45/17,\ 82/31,\ 127/48,\ 590/223,\ 717/271,$$
$$1307/494,\ 2024/765.$$

Since the continued fraction representation of $\sqrt{7}$ has a period of length 4, the numerator and denominator of any of the convergents p_{4k-1}/q_{4k-1} form a solution of $x^2 - 7y^2 = 1$. Thus, for instance,

$$p_3/q_3 = 8/3,\ p_7/q_7 = 127/48,\ p_{11}/q_{11} = 2024/765$$

give rise to the first three positive solutions; these solutions are $x_1 = 8, y_1 = 3$; $x_2 = 127, y_2 = 48$; $x_3 = 2024, y_3 = 765$.

Example 13-8

To find the solution of $x^2 - 13y^2 = 1$ in the smallest positive integers, we note that $\sqrt{13} = [3; \overline{1, 1, 1, 1, 6}]$ and that there is a period of length 5. The first ten convergents of $\sqrt{13}$ are

$$3/1,\ 4/1,\ 7/2,\ 11/3,\ 18/5,\ 119/33,\ 137/38,\ 256/71,\ 393/109,\ 649/180.$$

With reference to part (2) of Theorem 13-16, the least positive solution of $x^2 - 13y^2 = 1$ is obtained from the convergent $p_9/q_9 = 649/180$, the solution itself being $x_1 = 649, y_1 = 180$.

There is a quick way to generate other solutions from a single solution of Pell's equation. Before discussing this, let us define the *fundamental solution* of the equation $x^2 - dy^2 = 1$ to be its smallest positive solution. That is, it is the positive solution x_0, y_0 with the property that $x_0 < x', y_0 < y'$ for any other positive solution x', y'. Theorem 13-16 furnishes the following fact: if the length of the period of the continued fraction expansion of $\sqrt{d}$ is n, then the fundamental solution of $x^2 - dy^2 = 1$ is given by $x = p_{n-1}, y = q_{n-1}$ when n is even; and by $x_{2n-1}, y = q_{2n-1}$ when n is odd. Thus the equation $x^2 - dy^2 = 1$ can be solved in either n or $2n$ steps.

Finding the fundamental solution can be a difficult task, since the numbers in this solution can be unexpectedly large, even for comparatively small values of d. For example, the innocent-looking equation $x^2 - 991y^2 = 1$ has the smallest positive solution

$$x = 379\ 516\ 400\ 906\ 811\ 930\ 638\ 014\ 896\ 080,$$
$$y = 12\ 055\ 735\ 790\ 331\ 359\ 447\ 442\ 538\ 767.$$

The situation is even worse with $x^2 - 1000099y^2 = 1$, where the smallest positive integer x satisfying this equation has 1118 digits. Needless to say, everything is tied up with the continued fraction expansion of $\sqrt{d}$ and, in the case of $\sqrt{1000099}$, the period consists of 2174 terms.

It can also happen that the integers needed to solve $x^2 - dy^2 = 1$ are small for a given value of d and very large for the succeeding value. A striking illustration of this variation is provided by the equation $x^2 - 61y^2 = 1$, whose fundamental solution is given by

$$x = 17663319049, \qquad y = 226153980.$$

These numbers are enormous when compared with the case $d = 60$, where the solution is $x = 31, y = 4$ or with $d = 62$, where the solution is $x = 63$, $y = 8$.

With the help of the fundamental solution—which can be found by means of continued fractions or by successively substituting $y = 1, 2, 3, \ldots$ into the expression $1 + dy^2$ until it becomes a perfect square—we are able to construct all the remaining positive solutions.

THEOREM 13-17. *Let x_1, y_1 be the fundamental solution of $x^2 - dy^2 = 1$. Then every pair of integers x_n, y_n defined by the condition*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n \qquad (n = 1, 2, 3, \ldots)$$

is also a positive solution.

Proof: It is a modest exercise for the reader to check that

$$x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n.$$

Further, because x_1 and y_1 are positive, x_n and y_n are both positive integers. Bearing in mind that x_1, y_1 is a solution of $x^2 - dy^2 = 1$, we obtain

$$\begin{aligned} x_n^2 - dy_n^2 &= (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})^n(x_1 - y_1\sqrt{d})^n \\ &= (x_1^2 - dy_1^2)^n = 1^n = 1, \end{aligned}$$

and so x_n, y_n is a solution.

Let us pause for a moment to look at an example. By inspection, it is seen that $x_1 = 6, y_1 = 1$ forms the fundamental solution of $x^2 - 35y^2 = 1$. A second positive solution x_2, y_2 can be obtained from the formula

$$x_2 + y_2\sqrt{35} = (6 + \sqrt{35})^2 = 71 + 12\sqrt{35},$$

which implies that $x_2 = 71, y_2 = 12$. These integers satisfy the equation $x^2 - 35y^2 = 1$, since

$$71^2 - 35 \cdot 12^2 = 5041 - 5040 = 1.$$

A third positive solution arises from

$$\begin{aligned} x_3 + y_3\sqrt{35} &= (6 + \sqrt{35})^3 \\ &= (71 + 12\sqrt{35})(6 + \sqrt{35}) = 846 + 143\sqrt{35}. \end{aligned}$$

This gives $x_3 = 846, y_3 = 143$ and in fact

$$846^2 - 35 \cdot 143^2 = 715716 - 715715 = 1,$$

so that these values provide another solution.

Returning to the equation $x^2 - dy^2 = 1$, our final theorem tells us that any positive solution can be calculated from the formula

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n,$$

where n takes on integral values; that is, if u, v is a positive solution of $x^2 - dy^2 = 1$, then $u = x_n, v = y_n$ for a suitably chosen integer n. We state this as