5

The Pell equation

PREVIEW

The so-called *Pell equation* $x^2 - ny^2 = 1$ (wrongly attributed to Pell by Euler) is one of the oldest equations in mathematics and it is fundamental to the study of quadratic Diophantine equations. The Greeks studied the special case $x^2 - 2y^2 = 1$ because they realized that its natural number solutions throw light on the nature of $\sqrt{2}$. There is a similar connection between the natural number solutions of $x^2 - ny^2 = 1$ and $\sqrt{n}$ when n is any nonsquare natural number.

The irrationality of $\sqrt{n}$ when n is nonsquare causes strange behavior in the solutions of $x^2 - ny^2 = 1$. Nevertheless, the irrationality of $\sqrt{n}$ reflects light back on the equation: it leads to simple algebraic structure, and a simple general formula for all integer solutions of $x^2 - ny^2 = 1$ in terms of the smallest natural number solution.

But there is *no* simple formula for the smallest natural number solution and it is not trivial even to prove that it exists. In this chapter we give two proofs: the first is a relatively direct proof due to Dirichlet, based on the approximation of $\sqrt{n}$ by rational numbers. The second (in the starred sections at the end of the chapter) is based on a more general theory of quadratic forms due to Conway.

We include Conway's theory because it is a natural extension of our study of the Euclidean algorithm (particularly the results in the starred sections of Chapter 2) and because it gives a very simple explanation of *periodicity* phenomena connected with the Pell equation and $\sqrt{n}$. It also gives a highly *visual* approach to the subject, which makes the complex behavior of the Pell equation surprisingly easy to grasp.

5.1 Side and diagonal numbers

The ancient Greeks met the equation $x^2 - 2y^2 = 1$ in their efforts to understand $\sqrt{2}$, the diagonal of the unit square, which they knew to be irrational. They found a way to produce arbitrarily large solutions $(x_1, y_1), (x_2, y_2), \ldots$ of this equation, and hence fractions x_i/y_i that approximate $\sqrt{2}$ arbitrarily closely. The fractions x_i/y_i tend to $\sqrt{2}$, because if $x_i^2 - 2y_i^2 = 1$ then

$$\frac{x_i^2}{y_i^2} = 2 + \frac{1}{y_i^2} \to 2 \quad \text{as } y_i \to \infty.$$

Thus if y_i is the side of a square, x_i approximates the diagonal.

The Greeks discovered the solutions (x_i, y_i) among the "side numbers" s_i and "diagonal numbers" d_i defined by

$$\begin{aligned} d_1 &= 3, \quad s_1 = 2, \\ d_{i+1} &= d_i + 2s_i, \quad s_{i+1} = d_i + s_i. \end{aligned}$$

It follows from these equations that

$$d_1^2 - 2s_1^2 = 1, \quad d_{i+1}^2 - 2s_{i+1}^2 = -(d_i^2 - 2s_i^2).$$

Hence the odd-numbered pairs (d_1, s_1), (d_3, s_3), (d_5, s_5), … satisfy the equation $x^2 - 2y^2 = 1$ while the rest satisfy $x^2 - 2y^2 = -1$.

The first equation is an example of a *Pell equation*, the general form of which is $x^2 - ny^2 = 1$ where n is a nonsquare integer. The second is closely related to it; in fact we later look at *all* values of $x^2 - ny^2$ in order to see whether they include the value 1.

Irrational square roots

In dealing with equations $x^2 - ny^2 = 1$, where n is a nonsquare integer, we rely heavily on the irrationality of $\sqrt{n}$ proved in Section 2.5.

The upside of irrationality is that we can encode a pair of integers (a, b) by a single real number $a + b\sqrt{n}$; we say that this number has *rational part* a and *irrational part* b. Real and imaginary parts are meaningful because *if* $\sqrt{n}$ *is irrational,* $a_1, b_1, a_2, b_2 \in \mathbb{Z}$, *and*

$$a_1 + b_1\sqrt{n} = a_2 + b_2\sqrt{n},$$

then $a_1 = a_2$ *and* $b_1 = b_2$.

Suppose, on the contrary, that $b_1 \neq b_2$. Then

$$a_1 - a_2 = (b_2 - b_1)\sqrt{n},$$

and, since $b_2 - b_1 \neq 0$, we get $\sqrt{n} = \frac{a_1 - a_2}{b_2 - b_1}$. This contradicts the irrationality of $\sqrt{n}$. Hence $b_1 = b_2$, and therefore $a_1 = a_2$. □

Exercises

In the sections that follow we use numbers of the form $x_i + y_i\sqrt{n}$ to encode solution pairs of $x^2 - ny^2 = 1$. To give a taste of how this works, the following two exercises use numbers of the form $a + b\sqrt{2}$ to encode (diagonal,side) pairs.

5.1.1 Check that $(1+\sqrt{2})^2 = 3 + 2\sqrt{2}$ and that

$$(x + y\sqrt{2})(1+\sqrt{2}) = x + 2y + (x+y)\sqrt{2}.$$

5.1.2 Use induction to show from Exercise 5.1.1 that $(1+\sqrt{2})^{n+1} = d_n + s_n\sqrt{2}$.

When n is an integer square, the equation $x^2 - ny^2 = 1$ is not so interesting, so we dispose of it right now.

5.1.3 By factorizing the left-hand side of $x^2 - y^2 = 1$, show that it has only two integer solutions.

5.1.4 Show similarly that $x^2 - ny^2 = 1$ has only two integer solutions when n is a square positive integer.

5.2 The equation $x^2 - 2y^2 = 1$

It is straightforward to find all *rational* solutions of $x^2 - ny^2 = 1$ by Diophantus' method (draw the line of slope t through the rational point $(1,0)$). Thus the method of solution is completely independent of n.

It is a different matter to find even one *integer* solution of $x^2 - ny^2 = 1$ other than the obvious ones $(\pm 1, 0)$. The least positive solution $\neq (\pm 1, 0)$ depends on n in a mysterious way. However, once this least nontrivial solution is found, all other integer solutions are generated by a simple formula. We illustrate the method for the case $n = 2$.

When $x^2 - 2y^2 = 1$ the smallest integer solution $\neq (\pm 1, 0)$ can be found by trial to be $(3,2)$. Other solutions can then be found by the following *composition rule*: *if* (x_1, y_1) *and* (x_2, y_2) *are solutions of* $x^2 - 2y^2 = 1$*, then so is* (x_3, y_3)*, where* x_3 *and* y_3 *are defined by*

$$(x_1 + y_1\sqrt{2})(x_2 + y_2\sqrt{2}) = x_3 + y_3\sqrt{2}.$$

To show that this rule gives a new solution we first calculate x_3 and y_3. Expanding the left-hand side, and collecting its rational and irrational parts, we find that

$$x_3 = x_1x_2 + 2y_1y_2, \quad y_3 = x_1y_2 + y_1x_2.$$

It can then be checked by multiplication that

$$(x_1x_2 + 2y_1y_2)^2 - 2(x_1y_2 + y_1x_2)^2 = (x_1^2 - 2y_1^2)(x_2^2 - 2y_2^2) = 1 \times 1 = 1.$$

Hence $x_3^2 - 2y_3^2 = 1$, as required. □

Examples. Composing the solution $(3,2)$ with itself, we get a new solution (x_3, y_3), where

$$x_3 + y_3\sqrt{2} = (3 + 2\sqrt{2})^2 = 9 + 8 + 12\sqrt{2} = 17 + 12\sqrt{2}.$$

Equating rational and irrational parts, $x_3 = 17$, $y_3 = 12$, which is indeed another solution. If we then compose $(17,12)$ with $(3,2)$ we get

$$(17 + 12\sqrt{2})(3 + 2\sqrt{2}) = 51 + 48 + (36 + 34)\sqrt{2} = 99 + 70\sqrt{2},$$

hence another solution is $(99,70)$, and so on. By this process we can obtain infinitely many integer solutions, but it is not clear how close we are to finding all integer solutions. The situation becomes clearer when we observe that a *group structure* is present.

Exercises

Another way to arrive at the composition rule is to use the irrational factorization

$$x^2 - 2y^2 = (x - y\sqrt{2})(x + y\sqrt{2}). \qquad (*)$$

We suppose that $1 = x_1^2 - 2y_1^2$ and $1 = x_2^2 - 2y_2^2$, so that

$$1 = 1 \times 1 = (x_1^2 - 2y_1^2)(x_2^2 - 2y_2^2). \qquad (**)$$

5.2.1 Apply the factorization (*) to each factor on the right-hand side of (**), then combine the factors in a different way to show that

$$\begin{aligned} 1 = {} & [x_1x_2 + 2y_1y_2 - (x_1y_2 + y_1x_2)\sqrt{2}] \\ & \times [x_1x_2 + 2y_1y_2 + (x_1y_2 + y_1x_2)\sqrt{2}]. \end{aligned}$$

5.2.2 Deduce from Exercise 5.2.1 that $x_3^2 - 2y_3^2 = 1$, where

$$x_3 = x_1x_2 + 2y_1y_2 \quad \text{and} \quad y_3 = x_1y_2 + y_1x_2.$$

In Section 5.4 we generalize this method to find a composition rule for solutions of $x^2 - ny^2 = 1$.

5.3 The group of solutions

Not only do solutions (x_1, y_1) and (x_2, y_2) of $x^2 - 2y^2 = 1$ have a "product" $(x_1x_2 + 2y_1y_2, x_1y_2 + y_1x_2)$, corresponding to the product of numbers

$$(x_1 + y_1\sqrt{2})(x_2 + y_2\sqrt{2}),$$

the numbers $x + y\sqrt{n}$ such that $x^2 - ny^2 = 1$ include $1 = 1 + 0\sqrt{n}$ and the multiplicative inverse $x - y\sqrt{2}$ of the number $x + y\sqrt{2}$:

$$(x + y\sqrt{2})(x - y\sqrt{2}) = x^2 - 2y^2 = 1$$

since $x^2 - 2y^2 = 1$ by the assumption that (x, y) is a solution.

Thus the solutions (x, y) form a *group*, with the same structure as the set of numbers $x + y\sqrt{2}$, where x, y are integers such that $x^2 - 2y^2 = 1$. To understand this group we first focus on the subgroup of *positive* numbers $x + y\sqrt{2}$ where $x^2 - 2y^2 = 1$.

Structure of positive solutions. *The group of positive $x + y\sqrt{2}$, where (x, y) is an integer solution of $x^2 - 2y^2 = 1$, is the infinite cyclic group of powers of $3 + 2\sqrt{2}$.*

To see why, apply the log function to all the positive numbers $x + y\sqrt{2}$ where x, y are integers such that $x^2 - 2y^2 = 1$. Since $\log(ab) = \log a + \log b$, the resulting numbers $\log(x + y\sqrt{2})$ then form a group under $+$.

This group has a least positive element, $\log(3 + 2\sqrt{2})$, because

- $3 + 2\sqrt{2}$ is the least $x + y\sqrt{2}$ corresponding to solutions (x, y) with $x, y > 0$,
- solutions $(x, -y)$ with $y > 0$ are inverses of solutions (x, y) with $x, y > 0$. Hence the corresponding $x - y\sqrt{2}$ are < 1, and their logs are < 0.

But any such group of numbers consists of the integer multiples of its least positive element m: if any element k lies between multiples of m,

$$mn < k < m(n + 1),$$

we also have $k - mn$ in the group, and the size of this element,

$$0 < k - mn < |m|,$$

contradicts the minimality of m. □

Thus all solutions (x,y) of $x^2-2y^2=1$ for which $x+y\sqrt{2}>0$ correspond to powers of $3+2\sqrt{2}$. Now for *any* solution (x,y) either $x+y\sqrt{2}$ or $-x-y\sqrt{2}$ is >0. Hence the remaining solutions (x,y) are just the negatives of those obtained from the powers of $3+2\sqrt{2}$.

Exercises

Suppose we define integer pairs (u_k,v_k) by the equation

$$u_k+v_k\sqrt{2}=(3+2\sqrt{2})^k \quad \text{for all integers } k.$$

Then what we have just proved is that the pairs (u_k,v_k) are all the integer solutions (x,y) of $x^2-2y^2=1$ with x positive. It is now quite easy to express u_k and v_k as explicit functions of k, though (not surprisingly) these functions involve $\sqrt{2}$.

5.3.1 Given that $(3+2\sqrt{2})^k=u_k+v_k\sqrt{2}$, what is $(3-2\sqrt{2})^k$?

5.3.2 Deduce from Exercise 5.3.1 that

$$u_k=\frac{1}{2}\left[(3+2\sqrt{2})^k+(3-2\sqrt{2})^k\right], \quad v_k=\frac{1}{2\sqrt{2}}\left[(3+2\sqrt{2})^k-(3-2\sqrt{2})^k\right].$$

5.3.3 Deduce from Exercise 5.3.2 that $u_k=$ nearest integer to $(3+2\sqrt{2})^k/2$. And $v_k=$?

5.4 The general Pell equation and $\mathbb{Z}[\sqrt{n}]$

If n is a nonsquare integer we define

$$\mathbb{Z}[\sqrt{n}]=\{x+y\sqrt{n}:x,y\in\mathbb{Z}\}.$$

Just as we used the numbers $x+y\sqrt{2}$ to study $x^2-2y^2=1$ we use the numbers $x+y\sqrt{n}$ to study $x^2-ny^2=1$.

In fact, x^2-ny^2 is what we call the *norm* of $x+y\sqrt{n}$ in $\mathbb{Z}[\sqrt{n}]$, the product of $x+y\sqrt{n}$ by its *conjugate* $x-y\sqrt{n}$:

$$\text{norm}(x+y\sqrt{n})=(x-y\sqrt{n})(x+y\sqrt{n})=x^2-ny^2.$$

Thus finding solutions of the Pell equation is the same as finding elements of $\mathbb{Z}[\sqrt{n}]$ with norm 1.

The advantage of searching in $\mathbb{Z}[\sqrt{n}]$, rather than among pairs (x,y) of integers, is that we can use algebra on numbers in $\mathbb{Z}[\sqrt{n}]$.

Brahmagupta composition rule. *If (x_1, y_1) and (x_2, y_2) are both solutions of the Pell equation $x^2 - ny^2 = 1$, then so is*

$$(x_3, y_3) = (x_1x_2 + ny_1y_2, x_1y_2 + y_1x_2).$$

This generalizes the "composition" rule used for $n = 2$ in Section 5.2 and it may be proved as follows, using factorization in $\mathbb{Z}[\sqrt{n}]$.

Since (x_1, y_1) and (x_2, y_2) are solutions,

$$x_1^2 - ny_1^2 = 1 = x_2^2 - ny_2^2.$$

Therefore

$$\begin{aligned}
1 &= (x_1^2 - ny_1^2)(x_2^2 - ny_2^2) \\
&= (x_1 - y_1\sqrt{n})(x_1 + y_1\sqrt{n}) \times (x_2 - y_2\sqrt{n})(x_2 + y_2\sqrt{n}) \\
&= (x_1 - y_1\sqrt{n})(x_2 - y_2\sqrt{n}) \times (x_1 + y_1\sqrt{n})(x_2 + y_2\sqrt{n}) \\
&= [x_1x_2 + ny_1y_2 - (x_1y_2 + y_1x_2)\sqrt{n}] \times [x_1x_2 + ny_1y_2 + (x_1y_2 + y_1x_2)\sqrt{n}] \\
&= (x_1x_2 + ny_1y_2)^2 - n(x_1y_2 + y_1x_2)^2 \\
&= x_3^2 - ny_3^2
\end{aligned}$$

□

This "composition" of solutions to form a new solution was discovered by the Indian mathematician Brahmagupta around 600 CE (but without using $\sqrt{n}$).

We also have an identity solution $(1, 0)$ and an inverse $(x, -y)$ of each solution (x, y), hence the solutions form a group, as we saw previously in the special case $n = 2$. As in that case, we can prove that all solutions come from powers of the smallest positive solution.

Example. Solutions of $x^2 - 3y^2 = 1$.

We find by trial that the smallest positive solution is $(2, 1)$. Composing $(2, 1)$ with itself we get the solutions

$$\begin{aligned}
(2 \times 2 + 3 \times 1 \times 1, 2 \times 1 + 1 \times 2) &= (7, 4), \\
(2 \times 7 + 3 \times 1 \times 4, 2 \times 4 + 1 \times 7) &= (26, 15),
\end{aligned}$$

and so on. These solutions correspond to the powers of $2 + \sqrt{3}$.

The calculation used to prove the Brahmagupta composition rule actually shows a more general property, which holds not only with integer

coefficients x, y but also with *rational* coefficients, that is, quotients of integers. We use the symbol $\mathbb{Q}$ ("quotients") for the rational numbers and make the natural generalization of $\mathbb{Z}[\sqrt{n}]$ to

$$\mathbb{Q}[\sqrt{n}] = \{x + y\sqrt{n} : x, y \in \mathbb{Q}\}.$$

This set of numbers is the set of quotients of elements of $\mathbb{Z}[n]$ and it is a number *field*, that is, closed under $+$, $-$, $\times$, and $\div$ (by nonzero members). The closure properties are easily checked by calculation (exercises).

We extend the definition of norm to $\mathbb{Q}[\sqrt{n}]$ by the same formula

$$\text{norm}(x + y\sqrt{n}) = x^2 - ny^2.$$

This formula remains meaningful because each element of $\mathbb{Q}[\sqrt{n}]$ is uniquely expressible as $x + y\sqrt{n}$ with $x, y \in \mathbb{Q}$, by the argument of Section 5.1.

Multiplicative property of the norm. *For any α and β in $\mathbb{Q}[\sqrt{n}]$*

$$\text{norm}(\alpha)\text{norm}(\beta) = \text{norm}(\alpha\beta).$$

Proof. Let $\alpha = x_1 + y_1\sqrt{n}$ and $\beta = x_2 + y_2\sqrt{n}$. Then

$$\begin{aligned}\text{norm}(\alpha)\text{norm}(\beta) &= (x_1^2 - ny_1^2)(x_2^2 - ny_2^2) \\ &= (x_1x_2 + ny_1y_2)^2 - n(x_1y_2 + y_1x_2)^2 \\ &\qquad \text{by the calculation above} \\ &= \text{norm}(\alpha\beta).\end{aligned}$$

□

Exercises

5.4.1 Show that $+$, $-$, and $\times$ of numbers in $\mathbb{Q}[n]$ are themselves numbers in $\mathbb{Q}[n]$.

5.4.2 Show that $1/(x + y\sqrt{n})$ for $x, y \in \mathbb{Q}$ (not both zero) is of the form $x' + y'\sqrt{n}$ for $x', y' \in \mathbb{Q}$. Deduce that $\mathbb{Q}[n]$ is closed under $\div$ by nonzero members.

The multiplicative property of the norm can be restated as follows.

5.4.3 If (x_1, y_1) satisfies $x^2 - ny^2 = k_1$ and (x_2, y_2) satisfies $x^2 - ny^2 = k_2$, show that $(x_1x_2 + ny_1y_2, x_1y_2 + y_1x_2)$ satisfies $x^2 - ny^2 = k_1k_2$.

Brahmagupta used this fact to solve $x^2 - ny^2 = 1$ via easier equations $x^2 - ny^2 = k$. His method is most convenient when there is an obvious solution of $x^2 - ny^2 = -1$.

5.4.4 Find a nontrivial solution of $x^2 - 17y^2 = -1$ by inspection, and use it to find a nontrivial solution of $x^2 - 17y^2 = 1$.

5.4.5 Similarly find a nontrivial solution of $x^2 - 37y^2 = 1$.

5.5 The pigeonhole argument

The smallest nontrivial solution of $x^2 - ny^2 = 1$ is not always so easy to find as for $n = 2$ and $n = 3$. For example, the smallest nontrivial solution of $x^2 - 61y^2 = 1$ is

$$(x, y) = (1766319049, 226153980)!$$

This amazing example was discovered by Bhaskara II in 12th century India and rediscovered by Fermat.

The smallest nontrivial solution appears so unpredictably that its existence is not clear in general. However, Lagrange proved in 1768 that *if n is any nonsquare positive integer, the Pell equation $x^2 - ny^2 = 1$ has an integer solution $\neq (\pm 1, 0)$.*

An interesting new proof of this was given by Dirichlet around 1840. He used what is now called the "pigeonhole principle": if more than k pigeons go into k boxes then at least one box contains at least two pigeons (finite version); if infinitely many pigeons go into k boxes, then at least one box contains infinitely many pigeons (infinite version).

Dirichlet's argument can be subdivided into the following steps. First, a theorem on the approximation of irrational numbers:

Dirichlet's approximation theorem. *For any irrational $\sqrt{n}$ and integer $B > 0$ there are integers a, b with $0 < b < B$ and*

$$|a - b\sqrt{n}| < \frac{1}{B}.$$

Proof. For any integer $B > 0$ consider the $B - 1$ numbers $\sqrt{n}$, $2\sqrt{n}$ …, $(B-1)\sqrt{n}$. For each multiplier k choose the integer A_k such that

$$0 < A_k - k\sqrt{n} < 1.$$

Since $\sqrt{n}$ is irrational, the $B - 1$ numbers $A_k - k\sqrt{n}$ are strictly between 0 and 1 and they are all different for the same reason (by the result of Section 5.1). Thus we have $B + 1$ different numbers

$$0, \qquad A_1 - \sqrt{n}, \quad A_2 - 2\sqrt{n}, \quad \ldots, \quad A_{B-1} - (B-1)\sqrt{n}, \quad 1$$

in the interval from 0 to 1.

If we then divide this interval into B subintervals of length $1/B$, it follows by the finite pigeonhole principle that at least one subinterval contains

two of the numbers. The difference between these two numbers, which is of the form $a - b\sqrt{n}$ for some integers a and b, is therefore irrational and such that

$$|a - b\sqrt{n}| < \frac{1}{B}.$$

Also, $b < B$ because b is the difference of two positive integers less than B. □

The next few steps are short and directed towards applications of the infinite pigeonhole principle.

1. Since Dirichlet's approximation theorem holds for all $B > 0$, we can make $1/B$ arbitrarily small, thus forcing the choice of new values of a and b. Thus *there are infinitely many integer pairs* (a,b) *with* $|a - b\sqrt{n}| < 1/B$. Since $0 < b < B$, we have

$$|a - b\sqrt{n}| < \frac{1}{b}.$$

2. It follows from step 1 that

$$|a + b\sqrt{n}| \leq |a - b\sqrt{n}| + |2b\sqrt{n}| \leq |3b\sqrt{n}|,$$

and therefore

$$|a^2 - nb^2| \leq \frac{1}{b} \cdot 3b\sqrt{n} = 3\sqrt{n}.$$

Hence *there are infinitely many* $a - b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ *with norm of size* $\leq 3\sqrt{n}$.

3. By the infinite pigeonhole principle we obtain in turn

   - infinitely many $a - b\sqrt{n}$ with the same norm, N say,
   - infinitely many of these with a in the same congruence class, mod N,
   - infinitely many of these with b in the same congruence class, mod N.

4. From step 3 we get two positive numbers, $a_1 - b_1\sqrt{n}$ and $a_2 - b_2\sqrt{n}$, with

   - the same norm N,

- $a_1 \equiv a_2 \pmod N$,
- $b_1 \equiv b_2 \pmod N$.

The final step uses the quotient $a - b\sqrt{n}$ of the two numbers just found. Its norm $a^2 - nb^2$ is clearly 1 by the multiplicative property of norm. It is not so clear that a and b are integers, but this now follows from the congruence conditions in step 4.

Nontrivial solution of the Pell equation. *When n is a nonsquare positive integer, the equation $x^2 - ny^2 = 1$ has an integer solution $(a,b) \neq (\pm 1, 0)$.*

Proof. Consider the quotient $a - b\sqrt{n}$ of the two numbers $a_1 - b_1\sqrt{n}$ and $a_2 - b_2\sqrt{n}$ found in step 4. We have

$$\begin{aligned} a - b\sqrt{n} = \frac{a_1 - b_1\sqrt{n}}{a_2 - b_2\sqrt{n}} &= \frac{(a_1 - b_1\sqrt{n})(a_2 + b_2\sqrt{n})}{a_2^2 - nb_2^2} \\ &= \frac{a_1a_2 - nb_1b_2}{N} + \frac{a_1b_2 - b_1a_2}{N}\sqrt{n}, \end{aligned}$$

where $N = a_2^2 - nb_2^2$ is the common norm of $a_1 - b_1\sqrt{n}$ and $a_2 - b_2\sqrt{n}$. Since the latter numbers have equal norms, their quotient $a - b\sqrt{n}$ has norm 1 by the multiplicative property of norm (Section 5.4).

Since $a_1 - b_1\sqrt{n}$ and $a_2 - b_2\sqrt{n}$ are unequal and positive, their quotient $a - b\sqrt{n} \neq \pm 1$. It remains to show that a and b are integers. This amounts to showing that N divides $a_1a_2 - nb_1b_2$ and $a_1b_2 - b_1a_2$, or that

$$a_1a_2 - nb_1b_2 \equiv a_1b_2 - b_1a_2 \equiv 0 \pmod N.$$

The first congruence follows from the fact that $a_1^2 - nb_1^2 = N$, which implies

$$0 \equiv a_1^2 - nb_1^2 \equiv a_1a_1 - nb_1b_1 \equiv a_1a_2 - nb_1b_2 \pmod N,$$

replacing a_1 and b_1 by their respective congruent values $a_1 \equiv a_2 \pmod N$ and $b_1 \equiv b_2 \pmod N$ found in step 4.

The second congruence follows from $a_1 \equiv a_2 \pmod N$ and $b_2 \equiv b_1 \pmod N$ by multiplying to obtain $a_1b_2 \equiv b_1a_2 \pmod N$, in other words, $a_1b_2 - b_1a_2 \equiv 0 \pmod N$. □

5.6 *Quadratic forms

Dirichlet's pigeonhole argument is one of the neatest ways to prove the existence of nontrivial solutions of the Pell equation and it contains ideas that can be applied in other situations. Nevertheless, it is not obviously relevant to other quadratic Diophantine equations, so there is reason give a second proof: one that draws on a general theory of quadratic forms.

A *binary quadratic form* $Ax^2+Bxy+Cy^2$, where $A,B,C \in \mathbb{Z}$, can be viewed as an integer-valued function of integer pairs, or *vectors* (x,y). Many classical questions in number theory are concerned with the values of quadratic forms. For example, the Pell equation asks whether 1 is a value of the form x^2-ny^2, when n is a nonsquare natural number. To approach such questions we use two elementary properties of quadratic forms that can be confirmed by simple algebra.

Properties of quadratic forms. *If* $f(x,y)=Ax^2+Bxy+Cy^2$ *and* $\mathbf{v}=(x,y)$ *then*

1. $f(k\mathbf{v})=k^2f(\mathbf{v})$,
2. $f(\mathbf{v}_1+\mathbf{v}_2)+f(\mathbf{v}_1-\mathbf{v}_2)=2[f(\mathbf{v}_1)+f(\mathbf{v}_2)]$

Proof. 1. If $\mathbf{v}=(x,y)$ then $k\mathbf{v}=(kx,ky)$. Hence

$$f(k\mathbf{v})=A(kx)^2+B(kx)(ky)+C(ky)^2=k^2(Ax^2+Bxy+Cy^2)=k^2f(\mathbf{v}).$$

2. If $\mathbf{v}_1=(x_1,y_1)$ and $\mathbf{v}_2=(x_2,y_2)$ then

$$f(\mathbf{v}_1)=Ax_1^2+Bx_1y_1+Cy_1^2 \quad \text{and} \quad f(\mathbf{v}_2)=Ax_2^2+Bx_2y_2+Cy_2^2.$$

Also

$$\begin{aligned}
f(\mathbf{v}_1+\mathbf{v}_2) &= A(x_1+x_2)^2+B(x_1+x_2)(y_1+y_2)+C(y_1+y_2)^2\\
&= Ax_1^2+Ax_2^2+Bx_1y_1+Bx_2y_2+Cy_1^2+Cy_2^2\\
&\quad +2Ax_1x_2+Bx_2y_1+Bx_1y_2+2Cy_1y_2,\\
f(\mathbf{v}_1-\mathbf{v}_2) &= A(x_1-x_2)^2+B(x_1-x_2)(y_1-y_2)+C(y_1-y_2)^2\\
&= Ax_1^2+Ax_2^2+Bx_1y_1+Bx_2y_2+Cy_1^2+Cy_2^2\\
&\quad -2Ax_1x_2-Bx_2y_1-Bx_1y_2-2Cy_1y_2.
\end{aligned}$$

Hence

$$\begin{aligned} f(\mathbf{v}_1+\mathbf{v}_2)+f(\mathbf{v}_1-\mathbf{v}_2) &= 2Ax_1^2+2Bx_1y_1+2Cy_1^2+2Ax_2^2+2Bx_2y_2+2Cy_2^2 \\ &= 2\,[f(\mathbf{v}_1)+f(\mathbf{v}_2)] \end{aligned}$$ □

A simple consequence of Property 1 is that $f(-\mathbf{v}) = f(\mathbf{v})$, so a quadratic form makes no distinction between a vector $\mathbf{v}$ and its negative. Property 1 also says that $f(k\mathbf{v})$ is a multiple of $f(\mathbf{v})$; in particular $f(\mathbf{v})$ is *prime* (or 1) only for vectors $\mathbf{v} = (x,y)$ that are not integer multiples of other integer vectors, that is, for (x,y) with relatively prime x and y. We call these *primitive vectors*.

In Section 2.8 we found a map of all the primitive vectors with positive x and y. We also found that the latter vectors are generated from $\mathbf{i} = (1,0)$ and $\mathbf{j} = (0,1)$ by the processes $(\mathbf{v}_1,\mathbf{v}_2) \mapsto (\mathbf{v}_1+\mathbf{v}_2,\mathbf{v}_2)$ and $(\mathbf{v}_1,\mathbf{v}_2) \mapsto (\mathbf{v}_1,\mathbf{v}_1+\mathbf{v}_2)$. In the next section we see that vectors with x and y of opposite sign are similarly generated from $(0,-1)$ and $(1,0)$. Then Property 2 shows that there is a simple relation between the values of f at successive stages in these processes. This leads to a "map" of the values of f.

Equivalent forms

Another view of a quadratic form f, related to the one described above, surveys all *equivalent* forms $f^*(x,y) = f(px+qy, rx+sy)$, obtained by replacing the row vector $(x\ \ y)$ by

$$(px+qy\ \ rx+sy) = (x\ \ y)\begin{pmatrix} p & r \\ q & s \end{pmatrix} = (x\ \ y)M,$$

where the matrix M and its inverse M^{-1} both have integer entries. When M satisfies these conditions, the pairs $(px+qy, rx+sy)$ run through the set $\mathbb{Z}^2$ of all integer pairs when (x,y) does. Indeed, if (x',y') is any integer pair, we have

$$(x'\ \ y') = (x\ \ y)M \Leftrightarrow (x\ \ y) = (x'\ \ y')M^{-1}.$$

Thus equivalent forms have the same set of values. Examples are x^2+y^2 and $x^2+2xy+2y^2$, the latter obtained from x^2+y^2 when (x,y) is replaced by $(x+y,y)$.

When M and M^{-1} both have integer entries, then $\det M$ and $\det M^{-1}$ are both integers. Since

$$MM^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

it follows by taking the determinant of both sides that

$$\det M \cdot \det M^{-1} = 1$$

(due to the multiplicative property: $\det(M_1 M_2) = \det M_1 \cdot \det M_2$). The only possible values for $\det M$ and $\det M^{-1}$ are therefore ± 1. Thus the condition for a matrix M to define an equivalence of quadratic forms is that M have integer entries and that $\det M = ps - qr = \pm 1$. Such a matrix is called *unimodular*.

Now an arbitrary quadratic form can be expressed as a matrix product,

$$Ax^2 + Bxy + Cy^2 = (x \;\; y) \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}. \qquad (*)$$

So it follows from what we have just seen that any equivalent form is obtained by replacing

$$\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \quad \text{by} \quad M \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} M^{-1},$$

where M is unimodular. This is so because the new matrix effects the replacement of $(x \;\; y)$ by $(x \;\; y)M$.

Formula (*) reveals an *invariant* of the form $Ax^2 + Bxy + Cy^2$ under equivalence, namely the determinant $AC - B^2/4$ of its matrix. Indeed, the determinant of any equivalent,

$$\det \; M \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} M^{-1},$$

is equal (again by the multiplicative property of determinants) to

$$\begin{aligned} \det M \det \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \det M^{-1} &= (\pm 1)^2 \det \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \\ &= \det \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}, \end{aligned}$$

since $\det M = \det M^{-1} = \pm 1$ by hypothesis. Thus *all equivalents of the form $Ax^2 + Bxy + Cy^2$ have the same determinant*.

Exercises

Although equivalent forms have the same determinant, the converse is not always true. It so happens that the form x^2+y^2 is equivalent to all other forms with determinant 1, but x^2+5y^2 is *not* equivalent to all other forms with determinant 5.

5.6.1 Show that $13x^2+16xy+5y^2$ has determinant 1, and that it is equivalent to x^2+y^2 via the matrix $M=\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$.

5.6.2 Show that $2x^2+2xy+3y^2$ has the same determinant as x^2+5y^2, but that it is not equivalent to x^2+5y^2, by showing that x^2+5y^2 does not take the value 7.

5.6.3 More generally, show that x^2+5y^2 takes no values $\equiv 3$ or 7 (mod 20), by working out the possible values of x^2+5y^2 (mod 20).

5.7 *The map of primitive vectors

In Section 2.8 we described a partition of the plane (a "map") into regions labelled by $(1,0)$, $(0,1)$ and all the primitive vectors (a,b) of natural numbers. Figure 5.1 (right half) shows this map again, rotated through 90°, together with a near mirror image of it (left half) in which the second coordinate of each pair has a negative sign.

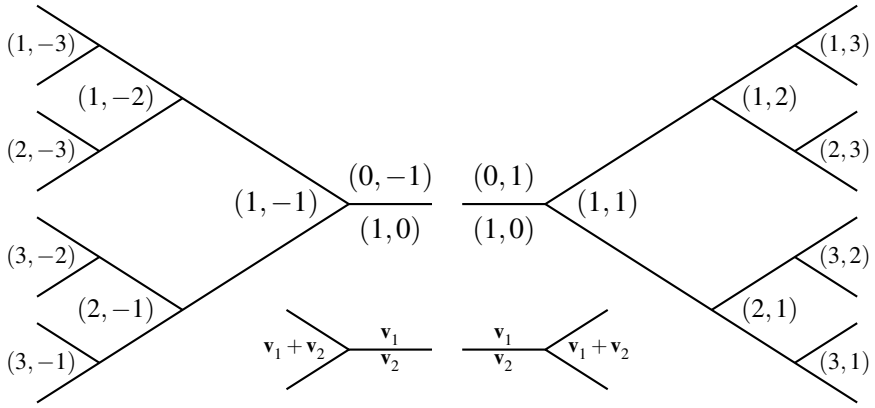

Figure 5.1: Two partial maps of primitive vectors

Also in the right half of the figure we have the schematic vector sum rule that generates all the labels from $(1,0)$ and $(0,1)$, and in the left half the mirror image rule that obviously applies there.

We put these two maps side by side because we want to join them together, but we seem prevented from doing so by the incompatible labels, $(0,1)$ and $(0,-1)$, in the upper central region. The conflict can be resolved by giving each label a $\pm$ sign. This yields Figure 5.2, which we call the (complete) *map of primitive vectors*, for the obvious reason that it contains every primitive vector. The $\pm$ labelling fuses the two vector sum rules into the single *vector difference/sum rule* shown at the bottom of the Figure.

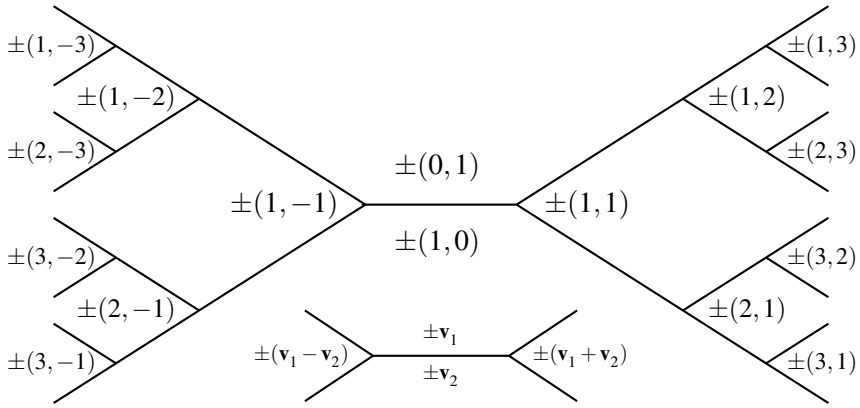

Figure 5.2: The complete map of primitive vectors

This rule needs some clarification because of the ambiguous signs. In a $\pm$ pair of vectors, say $\pm(1,2)$, we are free to choose either $(1,2)$ or $-(1,2)$ as $\mathbf{v}_1$. Likewise for the pair, say $\pm(2,3)$, labelling a region below an edge of region $\pm\mathbf{v}_1$: we can choose either $(2,3)$ or $-(2,3)$ to be $\mathbf{v}_2$. The vector difference/sum rule says that, *for some choice of* $\mathbf{v}_1$ *and* $\mathbf{v}_2$, the region between $\mathbf{v}_1$ and $\mathbf{v}_2$ at the left end of their common edge is labelled $\pm(\mathbf{v}_1-\mathbf{v}_2)$ and the region at the right end is labelled $\pm(\mathbf{v}_1+\mathbf{v}_2)$. In this example the regions are as in Figure 5.3.

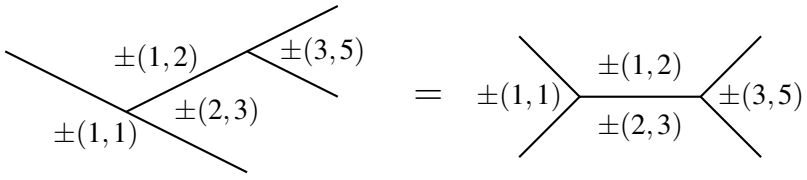

Figure 5.3: Regions above, below, and at the ends of an edge

Figure 5.3 shows how lines may be deformed to conform with the schematic diagram for the difference/sum rule—in particular the edge common to regions $\pm(1,2)$ and $\pm(2,3)$ is not really horizontal—within bounds that preserve the meanings of "above", "below", "right end", and "left end" for the edge common to the regions $\pm(1,2)$ and $\pm(2,3)$. Here the choice

$$\mathbf{v}_1 = (1,2),\ \mathbf{v}_2 = (2,3) \quad \text{gives} \quad \mathbf{v}_1 + \mathbf{v}_2 = (3,5),\ \mathbf{v}_1 - \mathbf{v}_2 = -(1,1),$$

so at the right end $\pm(3,5) = \pm(\mathbf{v}_1 + \mathbf{v}_2)$ and at the left end $\pm(1,1) = \pm(\mathbf{v}_1 - \mathbf{v}_2)$, as required.

It follows from the vector sum rules in the separate left and right maps in Figure 5.1 that the vector difference/sum rule holds in the complete map. This is proved by a finite number of simple checks, similar to the example above but more general. The details are left to the exercises.

The sign ambiguity $\pm(x,y)$ has no effect on the value of a quadratic form because

$$Ax^2 + Bxy + Cy^2 = A(-x)^2 + B(-x)(-y) + C(-y)^2.$$

Hence the map of primitive vectors gives an *unambiguous map of all values of the quadratic form* $f(x,y) = Ax^2 + Bxy + Cy^2$ *for relatively prime* x *and* y, obtained by entering each value $f(a,b)$ in the region $\pm(a,b)$. Moreover, it is possible to see some pattern in this map, thanks to the parallel between the vector difference/sum rule and Property 2 of quadratic forms proved in the previous section. We show this in the next section, assisted by the invariance of the determinant $AC - B^2/4$ under change of variables. The complete map also displays such changes, as we are about to see.

The tree of integral bases

In Section 5.6 we defined forms f, f^* to be *equivalent* if $f^*(x,y)$ results from $f(x,y)$ by replacing the vector (x,y) by a vector $(px+qy, rx+sy)$, which is equivalent to it in the sense that $(px+qy, rx+sy)$ runs through $\mathbb{Z}^2$ when (x,y) does. Since

$$(x,y) = x(1,0) + y(0,1) \quad \text{and} \quad (px+qy, rx+sy) = x(p,r) + y(q,s),$$

this amounts to replacing the vectors $(1,0)$ and $(0,1)$ by the new vectors (p,r) and (q,s). We call the pair of vectors $(1,0)$ and $(0,1)$ an *integral basis of* $\mathbb{Z}^2$ because any integer vector (x,y) is a linear combination of them with integer coefficients, namely $x(1,0) + y(0,1)$.

Equivalence says that the replacement $M : (x,y) \mapsto (px+qy, rx+sy)$ is invertible, so the inverse matrix M^{-1} has integer coefficients and the new vectors also form an integral basis. Thus the criterion for a pair of vectors (p,r) and (q,s) to form an integral basis is the criterion derived in Section 5.6 for M and M^{-1} to be integral, namely $ps - qr = \pm 1$.

Now in Section 2.7 we showed that, if (p,r) and (q,s) are labels on two regions with a common edge in the map of relatively prime pairs, then

$$ps - rq = \pm 1.$$

It is easily seen that this property extends to the complete map of Figure 5.2. Thus *each edge in the map of primitive vectors represents an integral basis of* $\mathbb{Z}^2$, namely the pair of labels on the regions that meet along the edge. The $\pm$ signs on the labels give four different bases, but they are essentially the same. Since the edges of the map form a tree, and each edge is associated in this way with an integral basis (up to sign), we call the edge complex of the map of primitive vectors the *tree of integral bases.*

As the name suggests, the tree represents *all* integral bases. We do not need this fact. However, it is easy to prove using the vector difference/sum rule to implement a kind of Euclidean algorithm (see exercises).

Exercises

To prove that the vector difference/sum rule holds in the complete map of primitive vectors we check that it holds in the middle and in "general position" on the right and left.

5.7.1 Verify that the difference/sum rule holds in the middle of the map (Figure 5.4) by choosing $\mathbf{v}_1 = (0,1)$ and $\mathbf{v}_2 = (1,0)$.

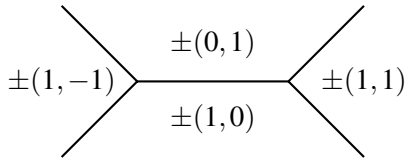

Figure 5.4: The middle of the complete map

5.7.2 Figure 5.5 shows one "general position" on the right side of the complete map. By choosing $\mathbf{v}_1 = \mathbf{u}_1$ and $\mathbf{v}_2 = \mathbf{u}_1 + \mathbf{u}_2$, verify that the difference/sum holds here.

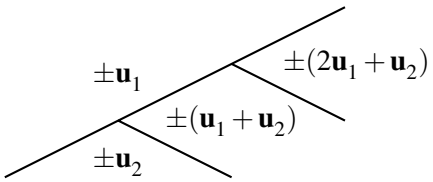

Figure 5.5: One "general position" on the right

5.7.3 Work out which other general positions occur on the right and on the left and verify that the difference/sum rule holds for each of them.

5.7.4 The "vector sum/difference rule" shown in Figure 5.6 is also valid. Why?

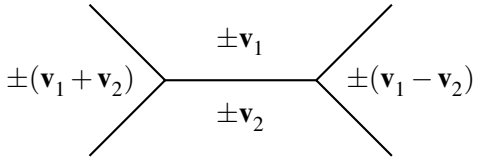

Figure 5.6: The sum/difference rule

To prove that the tree in the complete map represents all integral bases we use the difference/sum and sum/difference rules to trace a path from a given basis $\{(p,r),(q,s)\}$ back to $\{(1,0),(0,1)\}$. Exercise 5.7.5 is an example, and Exercises 5.7.6–5.7.8 show why such a path can always be found.

5.7.5 By repeatedly subtracting the "smaller" vector from the "larger", reduce the pair $\{(35,3),(23,2)\}$ to the pair $\{(1,0),(11,1)\}$. The latter pair is represented in the tree (why?), hence so is the former (why?).

5.7.6 Show that if

$$(p',r') = (p+q,r+s), \quad (q',s') = (q,s)$$

or

$$(p',r') = (p,r), \quad (q',s') = (p+q,r+s)$$

then $ps-qr = \pm 1 \Leftrightarrow p's'-q'r' = \pm 1$.

5.7.7 By repeatedly adding or subtracting one vector from the other, show that any pair $\{(p,r),(q,s)\}$ with $pr-qs = \pm 1$ reduces to a pair of the form $\{(p',0),(q',s')\}$. (*Hint*: $\gcd(r,s) = 1$. Why?) Deduce from Exercise 5.7.6 that $p' = \pm 1$, $q' = \pm 1$.

5.7.8 Deduce that $\{(p',0),(q',s')\}$ in Exercise 5.7.7 is represented by an edge in the tree, and hence so is $\{(p,r),(q,s)\}$.

5.8 *Periodicity in the map of $x^2 - ny^2$

In the previous section we briefly mentioned how a *map of any quadratic form* f may be superimposed on the map of primitive vectors by marking the region $\pm\mathbf{v}$ with the value $f(\mathbf{v}) = f(-\mathbf{v})$. We now investigate maps of quadratic forms in more depth and, to get an idea of what to expect, we first present the map of $x^2 - 3y^2$ in Figure 5.7. Only the right half is shown, because the left half is its mirror image. The values are marked as numbers in circles.

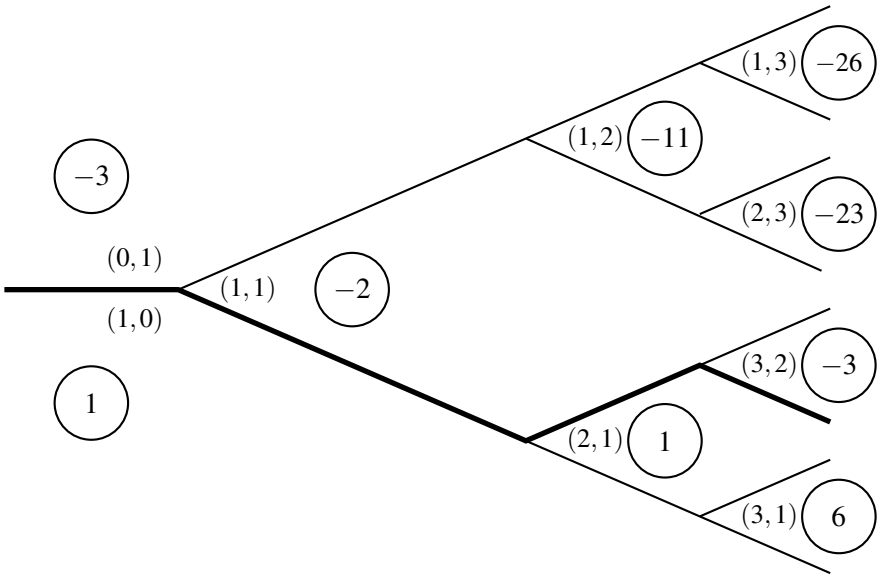

Figure 5.7: The map of $x^2 - 3y^2$

In this map there seems to be a single dividing line between positive and negative values of $x^2 - 3y^2$. Conway calls this line the *river*, and we have drawn it heavily in Figure 5.7. On either side of the river the values of $x^2 - 3y^2$ appear to increase in absolute value as one moves away from it (which is why one expects there to be only one river). And, rather unexpectedly, the values *along* the river seem to be *periodic*: in successive regions "above" the river the values are $-3, -2, -3, -2, \ldots$ and below each pair of successive regions with values -3, -2 there is a single region with value 1. Figure 5.8 confirms the pattern a bit further.

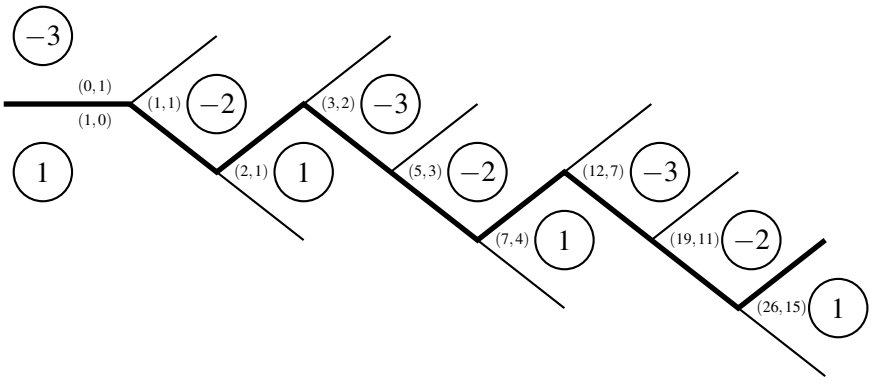

Figure 5.8: The river for $x^2 - 3y^2$

If this pattern continues indefinitely, then we can generate the sequence of positive solutions of the Pell equation $x^2 - 3y^2 = 1$, namely $(2,1)$, $(7,4)$, $(26,15),\ldots$, by applying the vector addition rule for the map of primitive vectors to locate the successive regions with value 1 (see exercises).

The example of $x^2 - 3y^2$ is a good example of what happens with any *indefinite* quadratic form, that is, one that takes both positive and negative values but not the value zero. With the help of the following proposition we can show that any indefinite quadratic form has a unique "river", with periodic behavior.

Arithmetic progression rule. *If L, U, D, R (for "left", "up", "down", "right") are the values of a quadratic form f around an edge as shown in Figure 5.9 then*

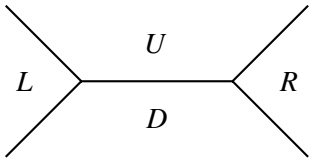

Figure 5.9: Values in regions around an edge

1. *L, $U+D$, R is an arithmetic progression.*
2. *If (p,r) and (q,s) respectively are the regions above and below the edge, then the common difference in this progression is the coefficient of xy in the quadratic form $f(px+qy, rx+sy)$.*

Proof. The difference/sum rule in the map of primitive vectors (Section 5.7) implies that

$$L = f(\mathbf{v}_1 - \mathbf{v}_2), \quad U = f(\mathbf{v}_1), \quad D = f(\mathbf{v}_2), \quad R = f(\mathbf{v}_1 + \mathbf{v}_2),$$

where $\mathbf{v}_1$ and $\mathbf{v}_2$ are the regions above and below the middle edge. It then follows from Property 2 of quadratic forms (Section 5.6) that

$$L + R = 2(U + D), \quad \text{or} \quad (U + D) - L = R - (U + D),$$

and this says that L, $U + D$, R is an arithmetic progression.

Recall from Section 5.7 that if the basis $\mathbf{i} = (1,0)$, $\mathbf{j} = (0,1)$ of $\mathbb{Z}^2$ is replaced by the basis $\mathbf{v}_1 = (p,r)$, $\mathbf{v}_2 = (q,s)$, then the form $f(x,y)$ is replaced by the equivalent form $f^*(x,y) = f(px + qy, rx + sy) = Ax^2 + Bxy + Cy^2$ say. Also, the values of f at $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_1 + \mathbf{v}_2$ and $\mathbf{v}_1 - \mathbf{v}_2$ are the same as the values f^* at $\mathbf{i}$, $\mathbf{j}$, $\mathbf{i} + \mathbf{j}$ and $\mathbf{i} - \mathbf{j}$, namely A, C, $A + B + C$ and $A - B + C$ respectively.

Thus the common difference, $(U + D) - L$, of the arithmetic progression is $A + C - (A - B + C) = B$, as claimed. □

Part 1 of the arithmetic progression rule is enough to show:

Uniqueness of the river. *For any form $x^2 - ny^2$, where n is a nonsquare natural number, there is a unique edge path in the map of primitive vectors that separates regions of positive value from regions of negative value.*

Proof. Such a form is never zero, because $x^2 - ny^2 = 0$ implies $n = x^2/y^2$ is a square; and $x^2 - ny^2$ certainly takes both positive and negative values. Consider a place on its map where a region of value $L < 0$ meets two regions with values $U, D > 0$ as in Figure 5.9. (If the region with value L is actually on the right, it is still true that L, $U + D$, R is an arithmetic progression.)

Then Part 1 implies that $R - (U + D) = (U + D) - L > U + D$, hence $R > \max(U, D)$. Thus moving one edge away from the border between positive and negative values leads to a region of greater positive value.

More generally, if $D > \max(U, L)$ then $R > D$ by a similar application of Part 1, so it follows that values of regions *continually increase* as we move further from the negative region. Similarly, values on the negative side continually decrease as we move further from the boundary path between positive and negative regions. Hence there is only one edge path separating the positive- from negative-valued regions. □

We need Part 2 of the arithmetic progression rule to prove the more difficult periodicity property, which guarantees the existence of nontrivial solutions of the Pell equation.

Periodicity of the river. *When n is a nonsquare natural number, the pattern of values along the sides of the river for $x^2 - ny^2$ is periodic.*

Proof. It will suffice to prove that regions sharing edges with the river are bounded in absolute value. Indeed, if that is so, the values L, U and D in Figure 5.9 around some edge in the river will recur; hence so will the value R (being determined by L, U and D according to the arithmetic progression rule), whose region also shares an edge with the river, and so on.

As we saw in the proof of Part 2, the values U and D equal C and A, where $Ax^2 + Bxy + Cy^2$ is a quadratic form f^* equivalent to $f(x,y) = x^2 - ny^2$. But we know from Section 5.6 that the determinant $AC - B^2/4$ is the same for all equivalents f^* of f. Here C and A, being the values of regions on opposite sides of the river, have opposite signs. Hence

$$|AC - B^2/4| = |A||C| + B^2/4$$

Since $AC - B^2/4$ is constant, it follows that $|A|$ and $|C|$—the absolute values of D and U—are bounded as required. □

Exercises

The "Pell quadratic forms" $x^2 - ny^2$ are by no means the only indefinite forms. Another interesting example is $x^2 + xy - y^2$, which is related to the *golden ratio* $\frac{1+\sqrt{5}}{2}$ and the Fibonacci sequence $1, 1, 2, 3, 5, 8, 13, \ldots$.

5.8.1 Show that $x^2 + xy - y^2 = \left(x + y\frac{1+\sqrt{5}}{2}\right)\left(x + y\frac{1-\sqrt{5}}{2}\right)$ and deduce from this that the form $x^2 + xy - y^2$ is indefinite.

5.8.2 Construct enough of the river for $x^2 + xy - y^2$ to show that its period looks like Figure 5.10.

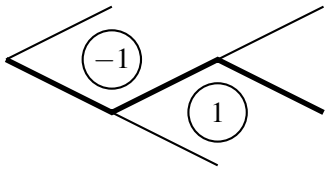

Figure 5.10: The period of $x^2 + xy - y^2$

5.8.3 Show that the positive labels (x_i, y_i) alternately below and above the river (in the regions marked alternately 1 and -1) satisfy

$$(x_1, y_1) = (1,1), \quad (x_{i-1}, y_{i-1}) + (x_i, y_i) = (x_{i+1}, y_{i+1}).$$

5.8.4 Deduce from Exercise 5.8.3 that the natural number pairs satisfying the equation $x^2 + xy - y^2 = 1$ are (F_{2n+1}, F_{2n+2}) for $n = 0, 1, 2, 3, \ldots$, where $F_1 = F_2 = 1$ and $F_i + F_{i-1} = F_{i+1}$ (the Fibonacci sequence).

Periodicity in the shape of the river leads naturally to recurrence relations between the vectors labelling riverside regions. The Fibonacci relation arising from $x^2 + xy - y^2$ is the simplest example of such a recurrence relation. Another is the relation for $x^2 - 3y^2$, whose river was constructed above.

5.8.5 Use two successive periods in the river for $x^2 - 3y^2$ to show that the non-negative solutions (x_i, y_i) of $x^2 - 3y^2 = 1$ satisfy

$$(x_0, y_0) = (1,0), \quad (x_{i+1}, y_{i+1}) = 4(x_i, y_i) - (x_{i-1}, y_{i-1}).$$

The river also shows why certain equations do *not* have solutions.

5.8.6 Explain why the equation $x^2 - 3y^2 = -1$ has no integer solution.

5.9 Discussion

The Pell equation $x^2 - ny^2 = 1$ is one of the oldest and most important quadratic Diophantine equations. Probably its only rival is the Pythagorean equation $x^2 + y^2 = z^2$. The Pell equation also dates back to the time of the Pythagoreans (around 500 BCE), who studied the special case $x^2 - 2y^2 = 1$ in connection with the $\sqrt{2}$, as mentioned in Section 5.1.

Another famous Pell equation is due to Archimedes. His "cattle problem" leads to the Pell equation $x^2 - 4729494y^2 = 1$, the least nontrivial solution of which has an x with 206545 digits! This solution was surely not known to Archimedes, though perhaps he knew that Pell equations could have remarkably large solutions. For an excellent discussion of the cattle problem, and the computational issues it raises, see Lenstra (2002).

The Pell equation was rediscovered in India, where mathematicians were also fascinated by short questions with long answers. Around 600 CE, Brahmagupta discovered the formula for composing solutions we used in Section 5.4. He used a generalization of it to find the minimal solution $(1151, 120)$ of $x^2 - 92y^2 = 1$ (saying that "a person solving this equation within a year is a mathematician"). In 1150 CE Bhaskara II extended Brahmagupta's idea to a method that solves all Pell equations, illustrating it with

the well chosen example $x^2 - 61y^2 = 1$. He found its minimal solution, (1766319049,226153980), which is by far the largest minimal solution of any Pell equation $x^2 - ny^2 = 1$ with $n \leq 61$.

In Europe nothing was known of the Indian discoveries, but the Pell equation resurfaced in the 17th century when Fermat independently discovered how to solve it. He did not reveal his method, but he evidently knew what he was doing, because he too picked $x^2 - 61y^2 = 1$ as a challenge to other mathematicians. He also posed the even more formidable equation $x^2 - 109y^2 = 1$, the minimal solution of which is

$$(158070671986249, 15140424455100).$$

His English rivals Wallis and Brouncker rose to the challenge with a method that solves the Pell equation, not unlike the method of Bhaskara II (see Weil (1984), p. 94). In the 18th century these methods morphed into the simpler and more elegant *continued fraction algorithm*, which can be viewed as the Euclidean algorithm applied to the pair $(\sqrt{n}, 1)$.

All of these methods are based on the *observation of periodicity* in certain computations. It is likely that the ancient Greeks observed periodicity in the Euclidean algorithm, because simple geometric arguments show its periodicity on pairs such as $(\sqrt{2}, 1)$ and $(\sqrt{3}, 1)$ (see, for example, Stillwell (1998), p. 268, or Artmann (1999), p. 242). However, while many could *use* periodicity to solve instances of the Pell equation, the first to *prove* that periodicity always occurs was Lagrange (1768). He thereby showed that the continued fraction method always works. He underlined the importance of this result by showing that solving the Pell equation leads to the solution of *all* quadratic Diophantine equations in two variables.

Conway's visual approach, expounded in Sections 5.6–5.8, is certainly related to the old approaches to the Pell equation. But it is essentially simpler in that *it replaces a process (the Euclidean algorithm) by a picture (the map of primitive vectors)*. I have attempted to make this as clear as possible by deriving the map of primitive vectors and its properties directly from properties of the Euclidean algorithm, before imprinting the values of a quadratic form on it. (Conway assumes the simplest properties of the map, or sketches topological proofs, and proves others with the help of quadratic forms.) For further insights obtainable from Conway's approach, see the book Conway (1997) or his related video $ax^2 + hxy + by^2$ available from the American Mathematical Society.

Springer

http://www.springer.com/978-0-387-95587-2

Elements of Number Theory

Stillwell, J.
2003, XII, 256 p., Hardcover
ISBN: 978-0-387-95587-2