where $u_1 = u/2$ and $v_1 = v/2$ are likewise rational. The formula is stated without proof, but it becomes easy to see if one rewrites a, b, c and makes the following stronger claim.

Any triangle with rational sides and rational area is of the form

$$a = \frac{u^2 + v^2}{v}, \quad b = \frac{u^2 + w^2}{w}, \quad c = \frac{u^2 - v^2}{v} + \frac{u^2 - w^2}{w}$$

for some rationals u, v, and w, with altitude $h = 2u$ splitting side c into segments $c_1 = \frac{u^2-v^2}{v}$ and $c_2 = \frac{u^2-w^2}{w}$.

The stronger claim says in particular that any rational triangle splits into two rational right-angled triangles. It follows from the parameterization of rational right-angled triangles and was presumably known to Brahmagupta.

Proof For *any* triangle with rational sides a, b, c, the altitude h splits c into rational segments c_1 and c_2 (Figure 4.3). This follows from the Pythagorean theorem in the two right-angled triangles with sides c_1, h, a and c_2, h, b respectively, namely,

$$a^2 = c_1^2 + h^2,$$
$$b^2 = c_2^2 + h^2.$$

Hence, by subtraction,

$$a^2 - b^2 = c_1^2 - c_2^2 = (c_1 - c_2)(c_1 + c_2) = (c_1 - c_2)c,$$

so

$$c_1 - c_2 = \frac{a^2 - b^2}{c}, \quad \text{which is rational.}$$

But also

$$c_1 + c_2 = c, \quad \text{which is rational,}$$

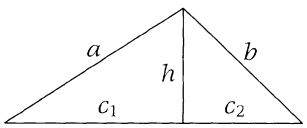

FIGURE 4.3 Splitting a rational triangle.

hence

$$c_1 = \frac{1}{2}\left(\frac{a^2 - b^2}{c} + c\right), \quad c_2 = \frac{1}{2}\left(c - \frac{a^2 - b^2}{c}\right)$$

are both rational.

Thus if the area, and hence the altitude h, are also rational, the triangle splits into two rational right-angled triangles with sides c_1, h, a and c_2, h, b.

We know from Diophantus' method (4.3) that any rational right-angled triangle with hypotenuse 1 has sides of the form

$$\frac{1 - t^2}{1 + t^2}, \quad \frac{2t}{1 + t^2}, \quad 1 \qquad \text{for some rational } t,$$

or, writing $t = v/u$,

$$\frac{u^2 - v^2}{u^2 + v^2}, \quad \frac{2uv}{u^2 + v^2}, \quad 1 \qquad \text{for some rational } u, v.$$

Thus the arbitrary rational right-angled triangle with hypotenuse 1 is a multiple (by $\frac{v}{u^2+v^2}$) of the triangle with sides

$$\frac{u^2 - v^2}{v}, \quad 2u, \quad \frac{u^2 + v^2}{v}.$$

The latter therefore represents all rational right-angled triangles with altitude $2u$, as the rational v varies. It follows that any *two* rational right-angled triangles with altitude $2u$ have sides

$$\frac{u^2 - v^2}{v}, \quad 2u, \quad \frac{u^2 + v^2}{v} \qquad \text{and} \qquad \frac{u^2 - w^2}{w}, \quad 2u, \quad \frac{u^2 + w^2}{w}$$

for some rational v and w. Putting the two together (Figure 4.4) gives an arbitrary rational triangle, and its sides and altitude are of the required form. □

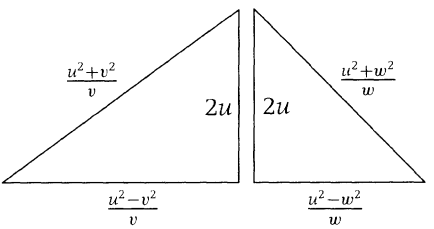

FIGURE 4.4 Assembling an arbitrary rational triangle.

Exercises

4.4.1. (Brahmagupta) Show that the triangle with sides 13, 14, 15 splits into two integer right-angled triangles.

Triangles with rational sides and rational area are sometimes called *Heronian* after the Greek mathematician Hero who lived in the first century A.D. Hero is also known for a formula giving the area of a triangle in terms of the lengths of its sides. His formula can, in fact, be derived quite easily from Brahmagupta's formulas for the sides of a rational triangle.

4.4.2. Show that for *any* triangle with sides a, b, c and altitude h on side c there *real* numbers u, v, w such that

$$a = \frac{u^2 + v^2}{v}, \quad b = \frac{u^2 + w^2}{w}, \quad c = \frac{u^2 - v^2}{v} + \frac{u^2 - w^2}{w},$$

with the side c split into parts $\frac{u^2-v^2}{v}$ and $\frac{u^2-w^2}{w}$ by the altitude $h = 2u$.

4.4.3. Define the *semiperimeter* s of the triangle with sides a, b, and c to be $(a + b + c)/2$. Then, with the notation of Exercise 4.4.2, show that

$$s(s-a)(s-b)(s-c) = u^2(v+w)^2\left(\frac{u^2}{vw} - 1\right)^2.$$

4.4.4. Deduce from Exercise 4.4.3 that

$$\sqrt{s(s-a)(s-b)(s-c)} = u\left(\frac{u^2 - v^2}{v} + \frac{u^2 - w^2}{w}\right)$$

is the area of the triangle with sides a, b and c.

Area $= \sqrt{s(s-a)(s-b)(s-c)}$ is Hero's formula. It defies the Greek geometric tradition by multiplying four lengths—something usually rejected as physically meaningless. Brahmagupta probably was aware of this formula, because he stated a generalization of it: the area of a *cyclic quadrilateral* (a four-sided polygon with its vertices on a circle) is $\sqrt{(s-a)(s-b)(s-c)(s-d)}$, where a, b, c, d are the sides of the quadrilateral and s is half its perimeter.

4.5 Rational Points on Quadratic Curves

The method for finding rational Pythagorean triples can also be used to find rational points on other quadratic curves. If we know one rational point P, then any other rational point Q will give a line PQ with rational slope, hence all rational points occur on lines through P with rational slope. Conversely, a line with rational slope, through one rational point, will meet the curve in a second rational point, *provided the coefficients in the equation of the curve are all rational.*

To see that rational coefficients are needed, consider the curve $y = \sqrt{2}x^2$. This has one rational point $(0, 0)$, and the line $y = x$ through this point has slope 1. But the line meets the curve again where $x = \sqrt{2}x^2$, that is, at the irrational point $x = 1/\sqrt{2}$.

To see what happens when the coefficients are rational, consider the curve $x^2 + 3y^2 = 1$. This has an obvious rational point $(-1, 0)$, and if we take the line $y = t(x + 1)$ through this point with rational slope t, its intersections with the curve are found by substituting $t(x + 1)$ for y in the equation for the curve. This gives the quadratic equation in x,

$$x^2 + 3t^2(x + 1)^2 - 1 = 0.$$

which we will *not* attempt to solve this time (though it is not hard). Instead, bear in mind that $x = -1$ is a solution of this equation, and hence $x + 1$ is a factor of the left-hand side. If we expand the left-hand side, we shall find a rational coefficient k of x^2 (built from the rational t by $+$, $-$, and $\times$), and therefore

$$x^2 + 3t^2(x + 1)^2 - 1 = k(x + 1)(x - u)$$

where $x = u$ is the other solution of the equation. It follows, by comparing coefficients on the two sides, that ku is the negative of the constant term on the left-hand side. This constant term is also rational, because it is built from the rational t by $+$, $-$ and $\times$. Thus the x coefficient u of the second point of intersection is rational, and hence so is the y coefficient, because $y = t(x + 1)$.

Similar reasoning applies to any quadratic equation with rational coefficients, hence we have the following.

Description of the rational points on a quadratic curve *If a curve $\mathcal{K}$ is given by a quadratic equation with rational coefficients, then the rational points on $\mathcal{K}$ consist of*

1. *Any single rational point P on $\mathcal{K}$.*
2. *The points where lines through P with rational slope meet $\mathcal{K}$.*

It is not claimed that a curve with rational coefficients has *any* rational points. However, if it has one, it has infinitely many, because there are infinitely many lines of rational slope through any point P.

Example *The curve $x^2 + y^2 = 3$ has no rational points.*

First note that any rational point (x, y) has $x = u/w$, $y = v/w$ for some integers u, v, and w (with w the common denominator of x and y). It follows, multiplying through by w^2, that a rational point on $x^2 + y^2 = 3$ gives integers satisfying

$$u^2 + v^2 = 3w^2.$$

We can assume that u, v, w have no common divisor > 1, so they are not all even. Then at least one of u and v is odd, because if u, v are even so is $u^2 + v^2 = 3w^2$, and $3w^2$ is even only if w is even. However ...

1. If u, v are both odd then u^2, v^2 both leave remainder 1 on division by 4, hence u^2+v^2 leaves remainder 2 (compare with the exercises to Section 4.2). But $3w^2$ leaves remainder 3 (if w is odd) or 0 (if w is even).
2. If one of u, v is odd and the other even, then $u^2 + v^2$ leaves remainder 1 on division by 4, which again is not the remainder left by $3w^2$.

Thus, in all cases an integer solution of $u^2 + v^2 = 3w^2$ gives a contradiction, hence there is no rational point on $x^2 + y^2 = 3$. □

Probably the first result of this type was discovered by Diophantus, who stated that $x^2+y^2 = 15$ has no rational solution (*Arithmetica* Book VI, Problem 14; see Heath (1910), p.237). The argument for $x^2 + y^2 = 15$ is virtually the same as the argument for $x^2 + y^2 = 3$, because $15w^2$ leaves the same remainder on division by 4 as $3w^2$ does.

These examples remind us that questions about rational numbers are basically questions about integers, and sometimes we have to go back to the integers to answer them. Nevertheless, rational points on curves are generally easier to find than integer points. This is already clear for the line $ax+by=c$ with integer coefficients, where integer points exist only when $\gcd(a,b)$ divides c, and finding them amounts to finding the gcd (see Section 1.5). Rational points always exist, and we can find them simply by solving for $y=(c-ax)/b$ and letting x run through the rationals. (Or, if $b=0$, solve for x in terms of y.) Deeper problems occur with the quadratic curves $x^2-dy^2=1$. Their rational points are no harder to find than rational points on the unit circle, but finding integer points is an entirely different matter (see Chapters 8 and 9).

Exercises

The curves $x^2-dy^2=1$ for $d>0$ are called *hyperbolas* and some of their geometric properties will be studied in Chapters 8 and 9. The geometry has some bearing on the behavior of integer points, as we shall see in Chapter 9, but algebra also plays an important role, as we shall see in Chapter 8. For the moment, we shall investigate these curves as best we can with our current tools.

4.5.1. Show that the hyperbola $x^2-dy^2=1$ approaches arbitrarily close to the lines $x=\pm\sqrt{d}y$, and hence sketch the curve.

4.5.2. Show that the rational points other than $(-1,0)$ on $x^2-dy^2=1$ are given by the formulas

$$x=\frac{1+dt^2}{1-dt^2}, \qquad y=\frac{2t}{1-dt^2}.$$

You will probably find that these formulas are no help in finding integer points on $x^2-dy^2=1$, other than the obvious ones $(-1,0)$ and $(1,0)$. In fact, the integer points depend mysteriously on the value of d, which we assume to be a natural number from now on.

4.5.3. By factorizing the left-hand side, show that there are no integer points on the hyperbola $x^2-y^2=1$, other than the obvious ones.

4.5.4. Find a nonobvious integer point on each of the hyperbolas $x^2 - 2y^2 = 1$, $x^2 - 3y^2 = 1$, and $x^2 - 5y^2 = 1$. What happens on $x^2 - 4y^2 = 1$?

One expects that rational points on curves with irrational coefficients are not so interesting, because they presumably occur only "by accident." But if so, it is still worth making this presumption more precise. In fact they *are* accidental, in the sense that there are only finitely many rational points on each curve with irrational coefficients. We shall confine attention to quadratic curves and assume further that their equations are of the form $ax^2 + by^2 = c$ with c rational. (This can always be arranged by shift of origin and rotation of axes, as we shall see in Chapter 8.)

4.5.5. Suppose that $\mathcal{K}$ is a curve given by $ax^2 + by^2 = c$, and that $\mathcal{K}$ has infinitely many rational points. Deduce that the coefficients a, b satisfy infinitely many equations of the form

$$Aa + Bb = c, \quad \text{for rational numbers } A, B.$$

4.5.6. Deduce from Exercise 4.5.5 that $\mathcal{K}$ has rational coefficients.

Even when a quadratic curve $\mathcal{K}$ has only finitely many rational points, the idea of considering the line of slope t through a point on $\mathcal{K}$ is fruitful, because it shows that x and y can always be expressed as rational *functions* of t. (Recall from the comment after Exercise 4.3.2 that a rational function of t is built from t and constants by rational operations. The constants need not be rational.)

4.5.7. If $\mathcal{K}$ is the curve $ax^2 + bxy + cy^2 + dx + ey + f = 0$, and (r, s) is any point on $\mathcal{K}$, use the line through (r, s) with slope t to find parametric equations for $\mathcal{K}$, $x = u(t)$, $y = v(t)$, where $u(t)$ and $v(t)$ are rational functions of t.

4.6* Rational Points on the Sphere

The geometric construction used in Section 4.2 to find rational points on the circle can be viewed as *projection* of the y-axis onto the circle minus the point $(-1, 0)$. In fact, it is precisely the point $y = t$ that is projected to the point $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ (Figure 4.5).