

program by giving a method, called the *cakravâla* or *cyclic process*, which always succeeds in finding integers x, y, k with $x^2 - Ny^2 = k$ and $k = \pm 1, \pm 2$, or ± 4 . Admittedly, Bhâskara II did not give a proof that the cyclic process always works—this was first done by Lagrange (1768)—but in fact it does. A proof using only concepts accessible to Bhâskara II may be found in Weil (1984), p. 22. We shall merely describe the cyclic process, and one of its most spectacular successes—the solution of $x^2 - 61y^2 = 1$.

Given relatively prime a and b such that $a^2 - Nb^2 = k$, we compose the triple (a, b, k) with the triple $(m, 1, m^2 - N)$ obtained from the trivial equation

$$m^2 - N \times 1^2 = m^2 - N.$$

The result is the triple $(am + Nb, a + bm, k(m^2 - N))$, which can be scaled down to the (possibly nonintegral) triple

$$\left(\frac{am + Nb}{k}, \frac{a + bm}{k}, \frac{m^2 - N}{k} \right).$$

We now choose m so that $(a + bm)/k = b_1$ is an integer, and it turns out that $(am + Nb)/k = a_1$ and $(m^2 - N)/k = k_1$ are integers, too. If we also choose m so that $m^2 - N$ is as small as possible, we are well on the road to a triple (a_i, b_i, k_i) with $k_i = \pm 1, \pm 2$ or ± 4 .

Example. $x^2 - 61y^2 = 1$. [This is Bhâskara's example. See Colebrooke (1817), pp. 176–178.]

Solution. The equation $8^2 - 61 \times 1^2 = 3$ gives us the triple $(a, b, k) = (8, 1, 3)$. We compose $(8, 1, 3)$ with $(m, 1, m^2 - 61)$, obtaining the triple $(8m + 61, 8 + m, 3(m^2 - 61))$ and hence

$$\left(\frac{8m + 61}{3}, \frac{8 + m}{3}, \frac{m^2 - 61}{3} \right).$$

Choosing $m = 7$ (because 7^2 is the nearest square to 61 for which 3 divides $8 + m$), we get the triple $(39, 5, -4)$, so already $k = -4$. We scale down further to the triple $(39/2, 5/2, -1)$. Composing $(39/2, 5/2, -1)$ with itself gives $(1523/2, 195/2, 1)$, and composing this again with $(39/2, 5/2, -1)$ gives the integer triple $(29718, 3805, -1)$. Finally, composing the latter with itself gives the triple $(1766319049, 226153980, 1)$.

Thus the equation $x^2 - 61y^2 = 1$ has integer solution $x = 1766319049$, $y = 226153980$. \square

This amazing example was rediscovered by Fermat (1657), who posed the equation $x^2 - 61y^2 = 1$ as a challenge to his colleague Frenicle. The solution $x = 1766319049$, $y = 226153980$ is in fact the *minimal* nonzero solution of $x^2 - 61y^2 = 1$, which suggests that Pell equation has a lot of hidden complexity—one does not expect such a short question to have such a long answer. Presumably Bhâskara II and Fermat knew that the Pell equation is particularly hard for $N = 61$. Among the Pell equations for $N \leq 100$, this has one of the largest minimal solutions, and it is much larger than any for $N < 61$.

The cyclic process is a little *too* successful on $N = 61$, because it terminates before anything “cyclic” becomes apparent. In fact, the cyclic process detects the same periodicity we previously observed in the continued fraction for \sqrt{N} (Section 3.3), and the size of the minimal solution is related to the length of the period. These facts only became clear with the work of Lagrange (1768), which is based on a study of continued fractions.

EXERCISES

The surprising step in Bhaskara’s process, where choosing the integer m so that $(a + bm)/k$ is an integer also produces integers $(am + Nb)/k$ and $(m^2 - N)/k$, deserves some explanation. It depends on choosing the initial a and b so that $\gcd(a, b) = 1$ —as one normally would to make $a^2 - Nb^2 = k$ small—because there are counterexamples when $\gcd(a, b) > 1$.

5.5.1 Suppose we choose $a = 4$, $b = 2$ in $a^2 - 2b^2$, so $k = 8$. Find an m for which $(a + bm)/k$ is an integer but $(am + Nb)/k$ is not.

Supposing $\gcd(a, b) = 1$ however, we can prove that if $(a + bm)/k$ is an integer then so is $(am + Nb)/k$. It follows that $(m^2 - N)/k$ is too, thanks to the equation

$$\left(\frac{am + Nb}{k}\right)^2 - N\left(\frac{a + bm}{k}\right)^2 = \frac{m^2 - N}{k} \quad (*)$$

to which this triple corresponds. The proof that $(am + Nb)/k$ is an integer goes as follows. At the end it involves the “method of finding 1.”

5.5.2 Assuming $a + bm = kl$, substitute $kl - mb$ for one copy of a in the equation $a^2 - Nb^2 = k$, and hence show that k divides $b(am + Nb)$.

5.5.3 Substituting $kl - a$ for both copies of bm in the equation $a^2m^2 - Nb^2m^2 = km^2$, show that k divides $a^2(m^2 - N)$.

5.5.4 Deduce from Exercise 5.5.3, and the other form of equation (*),

$$(am + Nb)^2 - N(a + bm)^2 = k(m^2 - N),$$

that k^2 divides $a^2(am + Nb)^2$, so that k divides $a(am + Nb)$.

5.5.5 Deduce from Exercises 5.5.2 and 5.5.4 that k divides $(ar + bs)(am + Nb)$ for any integers r and s , and hence that k divides $am + Nb$.

5.6 Rational Triangles

After the discovery of rational right-angled triangles, and their complete description by Euclid (Section 2.8), a question one might expect to arise is: what about rational triangles in general? Of course, any three rational numbers can serve as the sides of a triangle, provided the sum of any two of them is greater than the third. Thus a “rational triangle” should be one that is rational not only in its side lengths, but also in some other quantity, such as altitude or area. Since $\text{area} = \frac{1}{2} \text{base} \times \text{altitude}$, a triangle with rational sides has rational area if and only all its altitudes are rational, so it is reasonable to define a *rational triangle* to be one with rational sides and rational area.

Many questions can be raised about rational triangles, but they rarely occur in Greek mathematics. As far as we know, the first to treat them thoroughly was Brahmagupta, in his *Brâhma-sphuṭa-siddhânta* of 628 CE. In particular, he found the following complete description of rational triangles.

Parameterization of rational triangles. *A triangle with rational sides a , b , c and rational area is of the form*

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

for some rational numbers u , v , and w .

Brahmagupta [see Colebrooke (1817), p. 306] actually has a factor $1/2$ in each of a , b , and c , but this is superfluous because, for example,

$$\frac{1}{2} \left(\frac{u^2}{v} + v \right) = \frac{(u/2)^2}{v/2} + v/2 = \frac{u_1^2}{v_1} + v_1,$$

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 $c_1 = (u^2 - v^2)/v$ and $c_2 = (u^2 - w^2)/w$.

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, which was 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 5.1). This follows from the

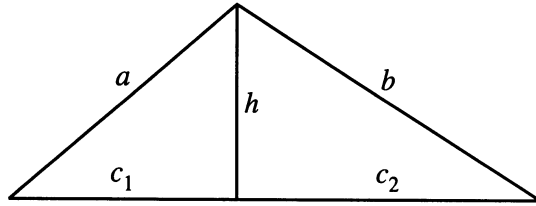


Figure 5.1: Splitting a rational triangle

Pythagorean theorem in the two right-angled triangles with sides c_1, h, a and c_2, h, b , respectively. Namely,

$$\begin{aligned} a^2 &= c_1^2 + h^2, \\ b^2 &= c_2^2 + h^2. \end{aligned}$$

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

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

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 , is 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 (Section 4.3) that any rational right-angled triangle with hypotenuse 1 has sides of the form

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

or, writing $t = v/u$,

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

Thus the arbitrary rational right-angled triangle with hypotenuse 1 is a multiple [by $v/(u^2 + v^2)$] 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. And it follows that any *two* rational

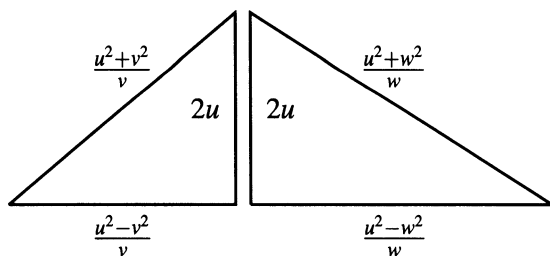


Figure 5.2: Assembling an arbitrary rational triangle

right-angled triangles with altitude $2u$ have sides

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

for some rational v and w . Putting the two together (Figure 5.2) gives an arbitrary rational triangle, and its sides and altitude are of the required form. \square

Exercises

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

5.6.2 Show that for *any* triangle with sides a, b, c and altitude h on side c there are *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 $(u^2 - v^2)/v$ and $(u^2 - w^2)/w$ by the altitude $h = 2u$.

5.6.3 Define the *semiperimeter* of the triangle with sides a, b , and c to be $s = (a + b + c)/2$. Then, with the notation of Exercise 5.6.2, show that

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

5.6.4 Deduce from Exercise 5.6.3 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 . (This formula for area in terms of a, b , and c is named after the Greek mathematician Hero, or Heron, who lived in the first century CE.)

5.7 Biographical Notes: Brahmagupta and Bhâskara

Brahmagupta was born in 598 CE, the son of Jiṣṇagupta, and lived until at least 665. His book the *Brâhma-sphuṭa-siddhânta* describes him as the teacher from Bhillamâla, which is a town now known as Bhinmal in the Indian state of Gujarat. Very little is known for certain about his life except that he was prominent in astronomy as well as mathematics.

Apart from the mathematical contributions described above, he is known for introducing a general solution formula for the quadratic equation (see Section 6.3), and a remarkable formula for the area of a cyclic quadrilateral. The latter states that if a quadrilateral has sides a, b, c , and d , semiperimeter s , and all vertices on a circle, then its area is $\sqrt{(s-a)(s-b)(s-c)(s-d)}$. Notice that this generalizes the Heron formula mentioned in Exercise 5.6.4.

Brahmagupta's parameterization of rational triangles leads naturally to other rationality questions, about triangles and other figures. The most famous of these is probably: is there a *rational box*? That is, is there a solid with rational rectangular faces whose body diagonal and the three face diagonals are all rational? According to Dickson (1920), p. 497, a mathematician named Paul Halcke found a box with rational sides and face diagonals in 1719. Its sides are 44, 240, and 117. However, the body diagonal of this box is irrational, and it is still not known whether a rational box exists, despite the efforts of many mathematicians, including Euler and Mordell.

Bhāskara II was born in 1114 or 1115 and died around 1185. He was the son of Maheśvara, from the city of Bījāpur. A great admirer of Brahmagupta, Bhāskara became the greatest mathematician and astronomer in twelfth-century India, serving as head of the observatory at Ujjain. His most famous work, the *Līlāvātī*, is said to be named after his daughter, to console her for an astrological forecast that went wrong.

The story goes that Bhāskara used his astronomical knowledge (which in those days included astrological “knowledge”) to choose the most propitious date and time for his daughter's wedding. As the time approached, one of her pearls fell into the water clock as she leaned over it, stopping the outflow of water. Before anyone noticed, however, the crucial time passed, and the wedding had to be called off. The hapless Līlāvātī never married, and now she is remembered only through the book that bears her name.