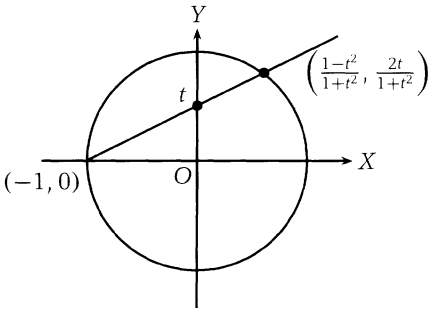

FIGURE 4.5 Projection from line to circle.

Projection from line to circle has a generalization, called *stereographic projection*, from plane to sphere. The (x, y)-plane in (x, y, z)-space is mapped to the unit sphere $x^2 + y^2 + z^2 = 1$ by projection toward the "north pole" $N = (0, 0, 1)$ (Figure 4.6). (Strictly speaking, stereographic projection goes from sphere to plane, but we are interested in both directions.)

Formulas for stereographic projection *If* $P = (u, v)$ *in the plane and* $P' = (p, q, r)$ *on the sphere correspond under stereographic projection, then*

$$u = \frac{p}{1 - r}, \qquad v = \frac{q}{1 - r}$$

and

$$p = \frac{2u}{u^2 + v^2 + 1}, \quad q = \frac{2v}{u^2 + v^2 + 1}, \quad r = \frac{u^2 + v^2 - 1}{u^2 + v^2 + 1}.$$

Proof The line through $N = (0, 0, 1)$ and $P' = (p, q, r)$ has the direction components p, q, $r - 1$, and hence parametric equations

$$x = pt, \quad y = qt, \quad z = 1 + (r - 1)t.$$

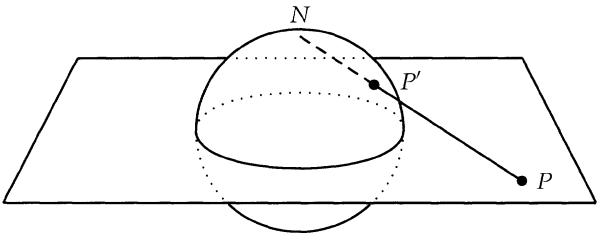

FIGURE 4.6 Projection from plane to sphere.

It meets the (x, y)-plane at P where $z = 0$, that is, where $t = \frac{1}{1-r}$, so $\frac{p}{1-r}$, $\frac{q}{1-r}$ are the coordinates u, v of P.

The line through $N = (0, 0, 1)$ and $P = (u, v)$ has direction components u, v, -1; hence parametric equations

$$x = ut, \qquad y = vt, \qquad z = 1 - t.$$

Substituting these in the equation $x^2 + y^2 + z^2 = 1$ of the sphere, we get the equation

$$u^2t^2 + v^2t^2 + (1 - t)^2 = 1$$

for the parameter value t at the intersection. This equation simplifies to

$$t^2(u^2 + v^2 + 1) - 2t = 0.$$

One solution $t = 0$ corresponds to N. P' corresponds to the other solution

$$t = \frac{2}{u^2 + v^2 + 1},$$

which gives

$$x = \frac{2u}{u^2 + v^2 + 1}, \quad y = \frac{2v}{u^2 + v^2 + 1},$$

$$z = 1 - \frac{2}{u^2 + v^2 + 1} = \frac{u^2 + v^2 - 1}{u^2 + v^2 + 1}$$

as the coordinates p, q, r of P'. □

The formulas show that p, q, and r are rational if and only if u and v are rational. Hence we have the following.

Corollary *The rational points $(p, q, r) \neq (0, 0, 1)$ on the unit sphere are*

$$p = \frac{2u}{u^2 + v^2 + 1}, \quad q = \frac{2v}{u^2 + v^2 + 1}, \quad r = \frac{u^2 + v^2 - 1}{u^2 + v^2 + 1}$$

for rational u and v.

The idea of stereographic projection applies to space of any dimension n, though naturally it is difficult to visualize when $n > 3$, and the formulas take over. However, from the two cases we know,

it is easy to see what to do next. The n-dimensional unit sphere in $(x_1, x_1, \ldots, x_n)$-space has equation

$$x_1^2 + x_2^2 + \cdots + x_n^2 = 1,$$

and its rational points $(p_1, p_2, \ldots, p_n)$ are found by connecting the "north pole" $(0, 0, \ldots, 0, 1)$ to the point $(u_1, u_2, \ldots, u_{n-1}, 0)$ for rational values of $u_1, u_2, \ldots, u_{n-1}$. The coordinates $p_1, p_2, \ldots p_n$ turn out to be

$$p_1 = \frac{2u_1}{u_1^2 + u_2^2 + \cdots + u_{n-1}^2 + 1}, \quad \cdots, \quad p_n = \frac{u_1^2 + u_2^2 + \cdots + u_{n-1}^2 - 1}{u_1^2 + u_2^2 + \cdots + u_{n-1}^2 + 1}.$$

Exercises

Each rational point $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ on the sphere $x^2 + y^2 + z^2 = 1$ corresponds to an integer quadruple (a, b, c, d) such that

$$a^2 + b^2 + c^2 = d^2,$$

so the formulas give a way to find all such quadruples.

4.6.1. Find formulas that give all such quadruples (a, b, c, d).

4.6.2. Do your formulas give the quadruples $(1, 2, 2, 3)$ and $(1, 4, 8, 9)$?

The projection of the plane onto the sphere minus N generalizes to any surface given by a quadratic equation in x, y, z.

4.6.3. Find a rational point T on the surface $2x^2 + 3y^2 + 4z^2 = 5$, and hence find formulas for all its rational points $\neq T$.

4.6.4.* If S is a surface given by a quadratic equation with rational coefficients, show that the rational points on S (if any) may be obtained by projecting from any rational point T off the (x, y)-plane to the rational points on the (x, y)-plane.

Thus, as with curves, a quadratic surface with rational coefficients has either no rational points or infinitely many.

4.6.5.* Show that the sphere $x^2 + y^2 + z^2 = 7$ has no rational points. (*Hint*: Consider remainders on division by 8.)

4.7* The Area of Rational Right Triangles

In this section we return to the interpretation of a rational Pythagorean triple (a, b, c) as a right-angled triangle with rational sides a, b, c: we shall call it the *rational right triangle* (a, b, c). Geometry suggests some interesting questions about such a triangle (a, b, c). For example, what can we say about its area? Diophantus answered many questions of this type in Book VI of his *Arithmetica*. He found triangles (a, b, c) whose area $ab/2$ is a square $\pm$ a given number, a square $\pm$ the sum of the perpendiculars, a square minus the hypotenuse, and a square minus the perimeter. However, the possibility of the area being *exactly* a square is ignored!

The first to ask whether there is such a triangle was Fibonacci, who raised the question in his *Liber Quadratorum* (book of squares) in 1225. (Strictly speaking, he asked an equivalent question; see Sigler (1987) p. 84.) In 1640 Fermat proved that the answer is no. His proof is a spectacular application of infinite descent to Pythagorean triples, and several variations of it exist. The following version is based on Young (1992). It assumes the formula for primitive Pythagorean triples from the exercises to Section 4.2.

Fermat's theorem on rational right triangles *The area of a rational right triangle is not a square.*

Proof Given any rational right triangle, we can take its sides to be integers with no common prime divisor, by multiplying through by a common denominator and canceling any common prime factors. This process multiplies its area by a square (because the base and height are both multiplied by the same factor), so if there is a rational right triangle with square area, there is a primitive Pythagorean triple (a, b, c) with $ab/2$ a square. The strategy of the proof is to look for a smaller triangle with the same property.

The formula for primitive Pythagorean triples gives natural numbers u and v such that

$$a = 2uv, \quad b = u^2 - v^2, \quad c = u^2 + v^2,$$

where $\gcd(u, v) = 1$ and one of u, v is even, the other odd. It follows that the area of triangle (a, b, c) is

$$\frac{ab}{2} = uv(u^2 - v^2) = uv(u - v)(u + v).$$

The factors u, v, $u - v$, $u + v$ have no common prime divisor, as one checks by comparing them in pairs. A common prime divisor of u and $u - v$ also divides their difference, v, and we know that u and v have no such divisor. Similarly, the pairs u, $u + v$ and v, $u - v$ and v, $u + v$ each have no common prime divisor. Finally, a common prime divisor of $u - v$ and $u + v$ divides their sum $2u$ and their difference $2v$. Because one of u, v is even and the other is odd, $u - v$ is odd and hence 2 is *not* a divisor of $u - v$, $2u$ and $2v$. Any common prime divisor must then divide u and v, and hence it does not exist.

Thus a square area $ab/2 = uv(u - v)(u + v)$ has factors u, v, $u - v$, and $u + v$, which are themselves squares, by unique prime factorization. It follows that $u^2 - v^2 = (u - v)(u + v)$ is a product of squares, hence also a square, say w^2. This gives us

$$u^2 - v^2 = w^2, \quad \text{or} \quad v^2 + w^2 = u^2,$$

so (v, w, u) is a *second Pythagorean triple*. We already know $\gcd(u, v) = 1$, so the new triple is primitive, hence there are natural numbers u_1 and v_1 with

$$v = 2u_1v_1, \quad w = u_1^2 - v_1^2, \quad u = u_1^2 + v_1^2.$$

(We know that v is the even member $2u_1v_1$ because $w^2 = u^2 - v^2$ is odd, hence w is the odd member.)

Because $u = u_1^2 + v_1^2$ is a square, say w_1^2, we have a *third Pythagorean triple* (u_1, v_1, w_1). The area of the corresponding right triangle is $u_1v_1/2 = v/4$, which is a square (because v is a square, as we found in the previous paragraph). Thus we have found another triangle with the same property as the first.

The third triangle still has natural number sides and natural number area, but its area $v/4$ is less than the area $uv(u-v)(u+v)$ of the first triangle. Therefore, if there is a rational right triangle with square area, we can make an infinite descent, which is impossible. □

Fermat drew some conclusions from this argument, which are as remarkable as the theorem itself.

Corollaries

1. *There are no natural numbers a, b, c such that $a^4 - b^4 = c^2$.*
2. *There are no natural numbers x, y, z such that $x^4 + y^4 = z^4$.*

Proof 1. For any natural numbers a, b, and c, consider the triangle with sides

$$a^4 - b^4, \quad 2a^2b^2, \quad a^4 + b^4.$$

This is a right-angled triangle because

$$(a^4 - b^4)^2 + (2a^2b^2)^2 = (a^4 + b^4)^2.$$

But if $a^4 - b^4 = c^2$, its area $(a^4 - b^4)a^2b^2$ is the square $a^2b^2c^2$, which contradicts the theorem. Hence $a^4 - b^4 = c^2$ is impossible for natural numbers a, b, and c.

2. If $x^4 + y^4 = z^4$ for natural numbers x, y, and z then

$$z^4 - y^4 = x^4 = (x^2)^2,$$

which is a special case of the equation proved impossible in part 1. Hence there are no such natural numbers x, y, and z. □

Fermat also proved the impossibility of the equation $a^4 + b^4 = c^2$ in the natural numbers. A proof is outlined in the exercises.

Exercises

The structure of the proof of Fermat's theorem on rational right triangles can be presented quite concisely if the checks on divisibility are left to the reader. It goes as follows:

(a, b, c) a primitive Pythagorean triple with $ab/2$ a square

$\Rightarrow a = 2uv, \quad b = u^2 - v^2, \quad c = u^2 + v^2$ with $uv(u^2 - v^2)$ a square, for some natural numbers u and v

$\Rightarrow u, v, u - v, u + v$ are squares

$\Rightarrow u^2 - v^2 = (u - v)(u + v) = w^2$ for some natural number w

$\Rightarrow (v, w, u)$ a primitive Pythagorean triple

$\Rightarrow v = 2u_1v_1, \quad w = u_1^2 - v_1^2, \quad u = u_1^2 + v_1^2,$
for some natural numbers u_1 and v_1
$\Rightarrow u_1^2 + v_1^2$ is a square, say w_1^2, because u is a square
$\Rightarrow (u_1, v_1, w_1)$ a Pythagorean triple, with $u_1v_1/2 = v/4$ a square
$\Rightarrow$ infinite descent, because $v/4 < ab/2 = uv(u^2 - v^2)$

The impossibility of $a^4 + b^4 = c^2$ is usually proved with the help of a formula for Pythagorean triples, but this step can be bypassed. The following proof from Cassels (1991) uses more basic facts about remainders on division by 2 and 4, together with unique prime factorization. It begins by assuming that a, b, and c have no common prime divisor, and $a^4 + b^4 = c^2$. Then it follows that c is odd, and so is one of the others, say b, by the argument preceding Exercise 4.2.1.

4.7.1. Check the details in the following proof:

$a^4 + b^4 = c^2$, with no common prime divisor of a, b, c and a even
$\Rightarrow (c + b^2)(c - b^2) = a^4$
$\Rightarrow c + b^2 = 8u^4$ and $c - b^2 = 2v^4$
or $c + b^2 = 2u^4$ and $c - b^2 = 8v^4$
$\Rightarrow b^2 = 4u^4 - v^4$ (impossible, considering remainders on division by 4)
or $b^2 = u^4 - 4v^4$
$\Rightarrow (u^2 + b)(u^2 - b) = 4v^4$
$\Rightarrow u^2 + b = 2r^4$ and $u^2 - b = 2s^4$
$\Rightarrow u^2 = r^4 + s^4$
$\Rightarrow$ infinite descent

In Section 4.3 it was pointed out that the formula for rational Pythagorean triples gives us functions that rationalize the irrational function $\sqrt{1 - x^2}$. For example, if we substitute $x = \frac{1-t^2}{1+t^2}$ we find $\sqrt{1 - x^2} = \frac{2t}{1+t^2}$. Fermat's results about fourth powers can be similarly used to prove that the functions $\sqrt{1 - x^4}$ and $\sqrt{1 + x^4}$ can *not* be rationalized. In the latter case, for example, the idea is to suppose that there is some rational function $x(t)$ such that $\sqrt{1 + x(t)^4}$ is a rational function $y(t)$ and derive a contradiction. A rational function is a quotient of polynomials, so we are

supposing that there are polynomials $p(t)$, $q(t)$, $r(t)$, $s(t)$ such that

$$\sqrt{1 + \frac{p(t)^4}{q(t)^4}} = \frac{r(t)}{s(t)},$$

or equivalently,

$$s(t)^4 \left(q(t)^4 + p(t)^4\right) = q(t)^4 r(t)^2 s(t)^2.$$

This yields polynomials $a(t) = s(t)q(t)$, $b(t) = s(t)p(t)$, and $c(t) = q(t)^2 r(t)s(t)$ with

$$a(t)^4 + b(t)^4 = c(t)^2,$$

which is the same as the Fermat equation, but with polynomials in place of the natural numbers a, b, and c. It can be proved impossible by imitating the argument given earlier because polynomials behave a lot like natural numbers. The degree of a polynomial serves as measure of its size, which can be used in proofs by induction (or descent).

4.7.2.* Show that polynomials have the following *division property*. If $a(t)$ and $b(t)$ are polynomials and $b(t)$ has degree > 0, then

$$a(t) = q(t)b(t) + r(t)$$

for some polynomials $q(t)$ and $r(t)$, with $r(t)$ of smaller degree than $b(t)$.

The theory of divisibility and factorization now unfolds for polynomials just as it did for natural numbers in Sections 1.5 and 1.6. The polynomials analogous to primes are called *irreducibles*.

4.7.3.* Check that there is a Euclidean algorithm for polynomials, an irreducible divisor property, and unique factorization into irreducibles (up to the order of factors and constant multiples of factors).

4.7.4.* Deduce from Exercise 4.7.3* that if the product of relatively prime polynomials is a square, then each factor is itself a square.

We can now imitate the argument of Exercise 4.7.1 with polynomials in place of natural numbers, but it is *easier* because polynomials need not have rational coefficients. If $p(t)$ and $q(t)$ are relatively prime polynomials and $p(t)q(t)$ is a square, we can conclude not only that $p(t) = u(t)^2$ and $q(t) = v(t)^2$, but also that $p(t) = 2U(t)^2$ and $q(t) = 2V(t)^2$, for the polynomials $U = u/\sqrt{2}$ and $V = v/\sqrt{2}$. This means it is no longer necessary to worry about the coefficients 2, 4, and 8.

4.7.5.* By imitating the argument in Exercise 4.7.1, show that there are no polynomials $a(t)$, $b(t)$, $c(t)$ of degree > 0 such that

$$a(t)^4 + b(t)^4 = c(t)^2.$$

4.8 Discussion

Diophantus and His Legacy

The last peak in classical Greek mathematics was reached by Diophantus of Alexandria, sometime between 150 A.D. and 300 A.D. The surviving parts of his work, the *Arithmetica*, seem at first quite elementary, a random collection of solved problems about numbers. There are no general theorems, and there is no apparent "depth," because later results do not depend on earlier ones, as they do in Euclid's *Elements*. However, this apparent simplicity is deceptive. The problems of Diophantus effectively illustrate general theorems, and some of them were deep enough to inspire Fermat and Euler, the greatest number theorists of the 17th and 18th centuries. Euler wrote:

> Diophantus himself, it is true, gives only the most special solutions of all the questions which he treats, and he is generally content with indicating numbers which furnish one single solution. But it must not be supposed that his method is restricted to these very special solutions. In his time the use of letters to denote undetermined numbers was not yet established, and consequently the more general solutions which we are enabled to give by means of such notation could not be expected from him. Nevertheless, the actual methods which he uses for solving any of his problems are as general as those which are in use today; nay, we are obliged to admit that there is hardly any method yet invented in this kind of analysis of which there are not sufficiently distinct traces to be discovered in Diophantus. (Euler *Opera Omnia* 1, II, p.429–430, translated by Heath (1910) p. 56)