A Diophantine equation

Diophantus of Alexandria is thought to have lived in the third century but little of his life is known with certainty. Only six books from his thirteen-part treatise *Arithmetica* have survived. The *Arithmetica* was essentially a collection of problems having solutions in positive integers or rational numbers. Hence, today we refer to equations requiring integer solutions as Diophantine equations.

A *solution* is a pair x, y that satisfies the equation. Of concern will be whether or not solutions exist and how they might be found.

An example (II.VIII) from the *Arithmetica* is the problem of dividing a given square into two squares, for which Diophantus demonstrates how to obtain a solution in rational numbers for the given square 16:

$$4^2 = \left(\frac{16}{5}\right)^2 + \left(\frac{12}{5}\right)^2$$

This solution is not unique, as Diophantus no doubt knew. For example, it is also true that

$$4^2 = \left(\frac{96}{25}\right)^2 + \left(\frac{28}{25}\right)^2$$

and

$$4^2 = \left(\frac{84}{29}\right)^2 + \left(\frac{80}{29}\right)^2$$

Today, we would be concerned mainly with knowing how many such solutions exist and we would look for a general method to find them.

Pursuing this question further, we see that not all but still infinitely many, squares can be expressed as sums of two integer squares. For example,

$$5^2 = 3^2 + 4^2$$
$$25^2 = 9^2 + 40^2$$
$$29^2 = 19^2 + 20^2$$

and in general,

$$(m^2 + n^2)^2 = (m^2 - n^2)^2 + (2mn)^2$$

We will want to investigate precisely which squares can be expressed as sums of two integer squares.

Reading of this problem in the *Arithmetica* some 1400 years after Diophantus wrote it prompted Pierre de Fermat to claim famously that no higher power than two could be similarly decomposed into two numbers of the same power, a claim that was verified only as recently as 1994 by Andrew Wiles. Thus, Diophantus has had a lasting influence on what is now called number theory.

Equations with two unknowns of degree one

We set out the standard way of solving the linear Diophantine equation $ax + by = k$.

Existence

The equation $ax + by = k$ has infinitely many solutions when x and y are allowed to be real numbers. Thus, we have $y = -\frac{1}{b}(ax - k)$, which, of course, need not be an integer.

Given $ax + by = k$, suppose a and b have a common factor m so that $a = ma'$ and $b = mb'$. Then, $m(a'x + b'y) = k.$ The fundamental theorem of arithmetic says that an integer can be factored in essentially one way. Hence it is clear in this case that m must be a factor of k because it is a factor of $m(a'x + b'y)$.

Since any factor common to a and b must divide k, the *highest* common factor, written (a, b), of a and b divides k. Therefore, we can be sure that no solution to $ax + by = k$ exists if (a, b) does not divide k.

However, even if (a, b) divides k we still cannot be certain that there is a solution. The ancient Greeks settled this question. They demonstrated a method that always leads to a solution whenever this condition is met. First, the highest common factor (a, b) has to be expressed in a particular way. We use the Euclidean algorithm.

Euclidean algorithm

Given two numbers a and b, with $a > b$, the Euclidean algorithm begins by measuring a against the quantity b. That is,

$$a = q_1 b + r_1$$

meaning that a is equal to q_1 lots of b plus a remainder r_1 which is smaller than b. We note that any divisor of both a and b must also be a divisor of the remainder, r_1.

Next, b is measured by r_1 so that

$$b = q_2 r_1 + r_2$$

with r_2 less than r_1. Any divisor of b and r_1 is also a divisor of r_2.

Next, r_1 is measured by r_2 so that

$$r_1 = q_3 r_2 + r_3$$

with r_3 less than r_2. Any divisor of r_1 and r_2 also divides r_3.

The process continues in this way. Since the remainders are decreasing at each step, a remainder of zero must be reached in a finite number of steps. We have

$$r_{n-2} = q_n r_{n-1} + r_n$$

and finally,

$$r_{n-1} = q_{n+1} r_n.$$

As before, any divisor of r_{n-2} and r_{n-1} is also a divisor of r_n and it follows by working back through the chain of equations that

(1) any divisor of a and b must be a divisor of r_n.

On the other hand, from the final equation we see that any divisor of r_n must divide r_{n-1}. Then, because of the second last equation, we see that any divisor of r_n also divides r_{n-2} and so on. Working back through the list of equations, we find eventually that

(2) any divisor of r_n divides both a and b.

From (1) it follows that the highest common factor of a and b divides r_n and therefore, $(a, b) \leq r_n$. From (2) we conclude that r_n is a common factor of a and b so that $r_n \leq (a, b)$. Therefore, $r_n = (a, b)$.

Thus, the Euclidean algorithm always finds the greatest common divisor of two numbers.

Next, the final remainder r_n is expressed, by rearrangement, in terms of the immediately preceding remainders: $r_n = r_{n-2} - q_n r_{n-1}$. Then, since $r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$, we can use this to substitute for r_{n-1} and write

$$r_n = r_{n-2}(1 + q_n q_{n-1}) - q_n r_{n-3}.$$

The chain of substitutions continues similarly using the previous equation $r_{n-2} = r_{n-4} - q_{n-2} r_{n-3}$, and so on, until eventually we obtain r_n expressed as a linear combination of a and b. That is, we obtain an equation of the form $Aa + Bb = (a,b)$ for some constants A and B.

Solution

Comparing the result

$$Aa + Bb = (a,b)$$

obtained from the Euclidean algorithm with the Diophantine equation

$$xa + yb = k$$

and remembering that in order for a solution to the Diophantine equation to exist we require that (a,b) divides k, we can multiply $Aa + Bb = (a,b)$ by the integer $\frac{k}{(a,b)}$ to obtain

$$\frac{k}{(a,b)}Aa + \frac{k}{(a,b)}Bb = k.$$

Thus, taking $x = \frac{kA}{(a,b)}$ and $y = \frac{kB}{(a,b)}$, we have a solution.

Having found one solution, others can be found. For example, if the pair x, y satisfies the Diophantine equation, we can set $x' = x + b$ and $y' = y - a$.

Then,

$$\begin{aligned} x'a + y'b &= (x+b)a + (y-a)b \\ &= xa + ba + yb - ab \\ &= xa + yb \\ &= k \end{aligned}$$

which shows that the pair x', y' is also a solution. For a complete solution, we state with the same justification, that if integers x and y satisfy $xa + yb = k$, then the numbers

$$x' = x + (-1)^n nb, \;\; y' = y + (-1)^{n+1} na$$

also satisfy the equation for all integers n.

To find the positive solutions, we look for the cases with both $x + (-1)^n nb > 0$ and $y + (-1)^{n+1} na > 0$.