Diophantine Analysis and Linear Indeterminate Problems

Sandra M. Pulver

Greek mathematics is regarded worldwide for its geometric character and has gained fame in this field. However, during the late Alexandrian period, about A.D. 250, when Greek science and philosophy were on the decline as a whole, and with them mathematics, algebra began to emerge as the main topic of interest.

Not much is known about the life of Diophantus except that he died at the age of 84 and had a son who died during his middle years. This too is not certain for it was provided rather cleverly by a rhymed problem that appeared in a later collection of Greek puzzles. The known titles of the works of Diophantus are the *Arithmetics* in 13 books, the *Porisms* and a study on polygonal numbers. The *Porisms* have been lost and only part of the *Polygonal Numbers* exists. However, six or seven books of the *Arithmetics* have been preserved, and it is through them that Diophantus makes his contribution to and mark on the world of mathematics.

In the theory of Diophantine analysis, two closely related problems are treated. In the first $f(x, y, z, \ldots)$ is a given polynomial in the variables $x, y, z, \ldots$ with rational (usually integral) coefficients. The equation $f(x, y, z, \ldots) = 0$ is called a Diophantine equation when it has to be determined which rational numbers $x, y, z, \ldots$ satisfy it. Usually further restrictions are made by requiring that $x, y, z, \ldots$ be integers, and sometimes it is required that they consist of positive integers. If we have several functions $f_i(x, y, z \ldots)$, in number less than the number of variables, then the set of equations $f_i(x, y, z \ldots) = 0$ is called a Diophantine system of equations. The term Diophantine became the name for such analysis because many of the problems in the *Arithmetics* call for a solution in rational numbers. Diophantus looked for rational solutions; that is, he did not insist on having a solution in integers as is customary in most of the recent work in Diophantine analysis.

Diophantus usually dealt with problems in which one had to find a set of 2, 3 or 4 numbers such that different equations involving them in the first, second and third degrees are squares, cubes and so on. The simplest nonlinear Diophantine equation may have no solution, any finite number of an infinity of solutions. For example, $x^2 + y^2 + 1 = 0$ has no rational solution and $x^2 + y^2 - 1 = 0$ has infinite number of rational solutions but a finite number of integral ones which are trivial.

Linear indeterminate problems are ones that occur commonly in puzzles. They lead to one or more linear equations where the number of unknowns is greater than the number of equations. If there were no restraints on the kind of values the solutions could take, one could give arbitrary values to some of the variables and find the others in terms of them. Because of the nature of these problems, the solutions are limited to integers and usually positive ones so they are called linear Diophantine equations. But even with these limitations, there may be none, several or even an infinite number of solutions. Solving these equations involves a number of repeated reductions.

The first type of equation is a single linear one—$ax + by = c$—in two unknowns. The following is a trivial example: $x + 5y = 14$, which may be written $x = 14 - 5y$.

This shows that any integral value of y substituted above will give an integral value for x. If it is required to have positive solutions, then $y > 0$ and $x = 14 - 5y > 0$ and $y < {}^{14}/_{5}$. Thus $y = 1, 2$ and $x = 9, 4$, respectively.

So when one of the coefficients of x and y is one, the solution is immediate. Thus, the method for solving linear indeterminate equations is to reduce them to this simple form.

It is not certain if indeterminate problems originated within a single culture, but if they did, it seems likely that India should be considered as a source. The following appears in Mahaviracarya's *Ganita-Sara-Sangraha* which was probably composed around A.D. 850.

> In the forest 37 heaps of apples were seen by the travelers. After 17 fruits were removed the remainder was divided evenly among 79 persons. What is the share obtained by each?

If x is the number of fruits in each heap, and y the share obtained by each person, then $37x - 17 = 79y$.

Since x has the smaller coefficient, we solve for x, and by taking out the integral parts of the fractional coefficients, we obtain $x = \frac{17+79y}{37} = 2y + 1 + \frac{5y-20}{37}$.

Because x and y are integers, the quotient

$$t = \frac{5y-20}{37}$$

is integral. Now we have to find integers y and t such that $37t = 5y - 20$. This equation is of the same type as $37x - 17 = 79y$ but with smaller numbers. This equation can be further simplified because both $5y$ and 20 are divisible by 5 and $37t$ must also have this factor. Since 37 is prime to 5, t must be divisible by 5 and we write $t = 5z$ and when this is substituted in $37t = 5y - 20$ we can cancel by 5 and have the simpler equation $37z = y - 4$. This gives $y = 37z + 4$, $x = 79z + 9$ as the general solution. The problem however will only allow positive integers. So,

$37z + 4 > 0$, $79z + 9 > 0$

$z > -4/37$, $z > -9/79$.

This shows that all values $z = 0, 1, 2, \ldots$ will give positive solutions in $y = 37z + 4$ and $x = 79z + 9$. This problem illustrates the fact that even when the solutions are required to be positive, there may be an infinite number of solutions. It also shows how simplifications are available in the solution of indeterminate problems.

Often the number of equations is one less than the number of unknowns. The procedure is to eliminate some of the unknowns until one winds up with a single equation with two unknowns which is the case above.

In medieval times, problems of this kind were called "problems coeci" probably referring to the fact that they related to scenarios in which people paid bills, as in the following problem from Christoff Rudolff in 1526.

At an inn, a party of 20 persons pay a bill for 20 groschen. The party consists of men (x), and women (y) and maidens (z), each man paying 3, each woman 2 and each maiden ½ groschen. How was the party composed? The equations are $x + y + z = 20$, $3x + 2y + z/2 = 20$. We double the second equation and subtract the first from it to obtain $5x + 3y = 20$ or $3y = 20 - 5x$. Once again we simplify (by substituting $y = 5u$) to obtain:

$3u = 4 - x$

$x = 4 - 3u$, $y = 5u$, $z = 16 - 2u$.

For a positive solution

$x = 4 - 3u > 0$, $u < 4/3$

$y = 5u > 0$, $u > 0$

$z = 16 - 2u > 0$, $u < 8$.

This provides a unique solution in which $u = 1$ and $x = 1$, $y = 5$ and $z = 14$.

Then there are those problems in which the number of unknowns is at least two greater than the number of equations. In this case also, one can eliminate some of the unknowns and end up with a single equation with several unknowns. For example, there may be two equations and four unknowns and one of them may be eliminated to obtain a single equation with three unknowns. However, in the case of one equation with three unknowns, the general solution will contain two parameters instead of one as in the previous problems.

Diophantus worked extensively with the Pythagorean theorem trying to find right triangles with integral sides. However, one doesn't have to be restricted to integers because if any rational solution had been found, the three numbers could be written with a common denominator

$$a = \frac{a_i}{m},\ b = \frac{b_i}{m},\ c = \frac{c_i}{m}$$

and $a_i^2 + b_i^2 = c_i^2$ would be an integral solution.

It is enough to find primitive integral solutions of the Pythagorean equation. (Primitive solutions are those in which there is no factor, d, common to a, b and c because if there were, then the equation could be canceled by d^2.) In order for a primitive solution to exist, any two of the numbers a, b and c must be relatively prime. If a and b had a common factor x, both sides of the Pythagorean equation would be divisible by x^2. But then c is divisible by x which contradicts the assumption that the solution was primitive.

It will be determined that in a primitive solution a, b and c, the numbers a and b can't both be odd. This is so because of the following theorem:

> The square of a number is either divisible by 4 or leaves a remainder of 1 when divided by 4.

This is proven by the fact that every number is of the form $2n$ or $2n + 1$ and when they are squared, the results are $4n^2$ and $4n^2 + 4n + 1$. If a and b were both odd, both sides of the Pythagorean equation, $a^2 + b^2 = c^2$ would leave the remainder 2 when divided by 4 which contradicts the theorem.

Now, a will be even and b and c are odd since there are no common factors. Then the equation is $a^2 = c^2 - b^2 = (c + b)(c - b)$. Both sides are divisible by 4 since a is of the form $2n$ and when one divides by this factor, one gets

$$\frac{a^2}{2} = \left(\frac{c+b}{2}\right) \times \left(\frac{c-b}{2}\right)$$

The two factors on the right are relatively prime because any common factor, d, would divide their sum and difference. But since

$$\frac{c+b}{2} + \frac{c-b}{2} = c \qquad \frac{c+b}{2} - \frac{c-b}{2} = b$$

and b and c are relatively prime, d must equal 1.

When the two numbers on the right in

$$\frac{a^2}{2} = \left(\frac{c+b}{2}\right) \times \left(\frac{c-b}{2}\right)$$

are relatively prime, their prime factorizations are different and their products can't be a square unless each of them is a square. So,

$$\frac{c+b}{2} = u^2 \quad \frac{c+b}{2} = v^2$$

and by substituting above in we get

$$\frac{a^2}{2} = \left(\frac{c+b}{2}\right) \times \left(\frac{c-b}{2}\right)$$

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

To verify that this is a primitive solution, we see that any common factor of b and c has to divide their sum and difference. However, $c + b = 2u^2$, $c - b = 2v^2$ and since u and v are relatively prime, 2 is the only common factor which is eliminated when one of the numbers is odd and the other even.

Bibliography

Carmichael, R. C. *Diophantine Analysis*. New York: John Wiley & Sons, 1915.

Dudley, U. *Elementary Number Theory*. San Francisco, Calif.: W. H. Freeman, 1978.

Gardener, M. *Wheels, Life and Other Mathematical Amusements*. New York: W. H. Freeman, 1983.

Heath, Sir T. *A History of Greek Mathematics*. New York: Dover, 1981.

Ore, O. *Number Theory and Its History*. New York: Dover, 1948.

In the equations $a + b + c = d + e + f = g + h + i$, is it possible to substitute the natural numbers 1, 2, 3, . . . , 8, 9 in the place of the variables?