Oxford Mathematics Alphabet

UNIVERSITY OF OXFORD
Mathematical Institute

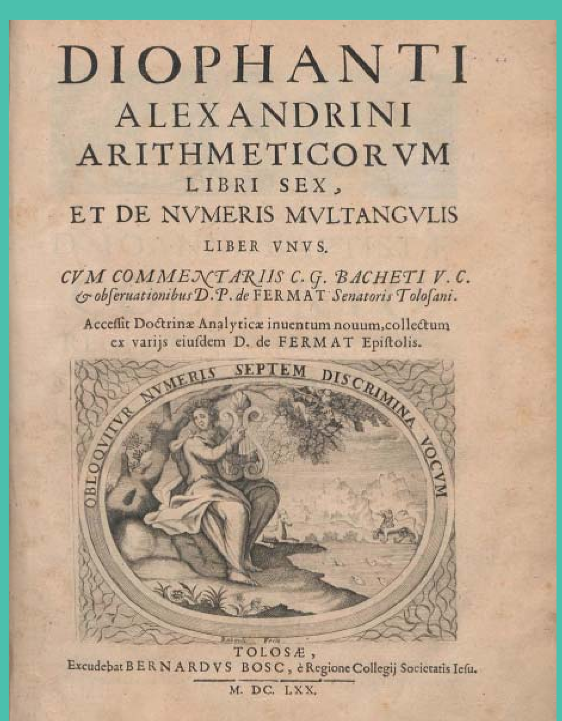
D *is for* diophantine equations

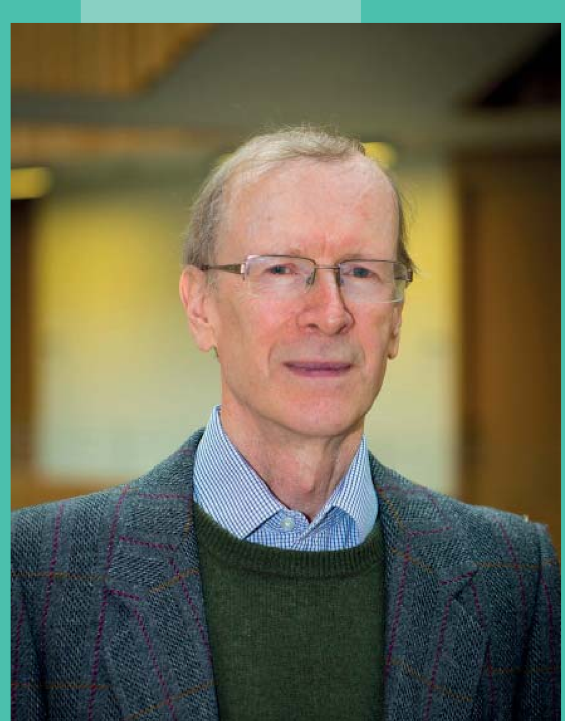
A diophantine equation is an algebraic equation, or system of equations, in several unknowns and with integer (or rational) coefficients, which one seeks to solve in integers (or rational numbers).

The most famous example of a diophantine equation appears in Fermat's Last Theorem. This is the statement, asserted by Fermat in 1637 without proof, that the diophantine equation

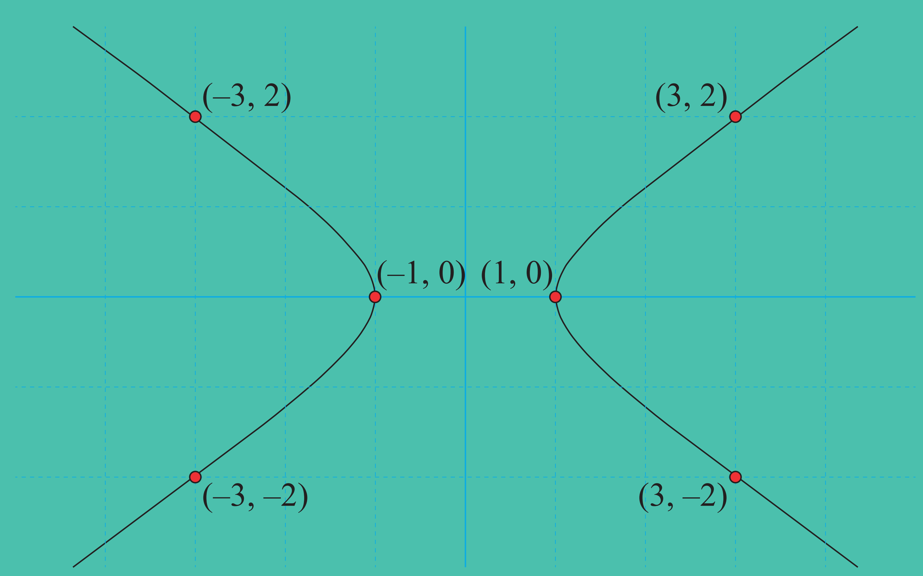
$$X^n + Y^n = Z^n$$

has no solutions in whole numbers when $n \geqslant 3$ other than the "trivial solutions" which arise when $XYZ = 0$. A proof of the theorem was finally given by Andrew Wiles in 1995.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obseruationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrinæ Analyticæ inuentum nouum, collectum ex varijs eiusdem D. de FERMAT Epistolis.
OBLOQVITVR NVMERIS SEPTEM DISCRIMINA VOCVM
TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.



The basic question one would like to answer is: does a given system of equations have solutions? And if it does have solutions, how can we find or describe them? While the Fermat equation has no (non-trivial) solutions, similar equations (for example $X^4 + 15Y^4 = Z^4$) do have non-trivial solutions.



$x^2 - 2y^2 = 1$

One could take the view that the existence of a finite number of solutions is merely accidental, and seek to decide whether a given system of equations has infinitely many solutions. For example, it is known that for any nonzero rational numbers a, b and any $n \geqslant 4$ the equation $ax^n + by^n = 1$ has only finitely many solutions.

Understanding the solutions of diophantine equations is certainly not easy. For example, consider the equation $X^5 + Y^5 = Z^5 + T^5$ to be solved in positive integers X, Y, Z, T . It has infinitely many "obvious" solutions where $\{X, Y\} = \{Z, T\}$. It is believed, but not known, that these are the only solutions. Otherwise put, it is unknown whether there is an integer that can be written as a sum of two fifth powers in two different ways. But it is known that, in a suitable sense, most of the solutions are of the obvious form.

A wide variety of methods are employed to study diophantine equations. These include algebra, especially algebraic geometry, various analytic methods (using calculus), as well as methods from mathematical logic.

Dr Jonathan Pila FRS
Reader in Mathematical Logic