International Journal of Multidisciplinary Research and Development
Online ISSN: 2349-4182, Print ISSN: 2349-5979, Impact Factor: RJIF 5.72
www.allsubjectjournal.com
Volume 3; Issue 3; March 2016; Page No. 432-434

A study on diophantine equations and their significance

Nurul Amin, Dr. VK Rathaur

Research Scholar Mathematics, Maharishi University of Information Technology, Lucknow, Uttar Pradesh, India.

Abstract

A Diophantine equation is a polynomial equation, usually in two or more unknowns such that only the integer solutions are sought or studied (an integer solution is a solution such that all the unknowns take integer values). A linear Diophantine equation is an equation between two sums of monomials of degree zero or one. An exponential Diophantine equation is one in which exponents on terms can be unknowns.

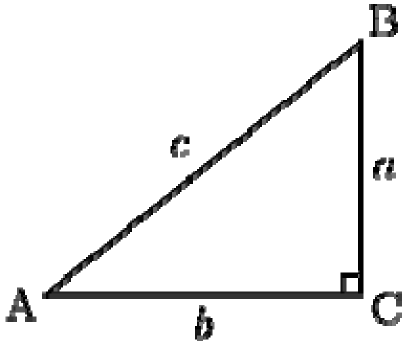
Diophantine problems have fewer equations than unknown variables and involve finding integers that work correctly for all equations. In more technical language, they define an algebraic curve, algebraic surface, or more general object, and ask about the lattice points on it.

Keywords: Diophantine equation, Analysis, Exponents

Introduction

The word Diophantine refers to the Hellenistic mathematician of the 3rd century, Diophantus of Alexandria, who made a study of such equations and was one of the first mathematicians to introduce symbolism into algebra. The mathematical study of Diophantine problems that Diophantus initiated is now called Diophantine analysis.

While individual equations present a kind of puzzle and have been considered throughout history, the formulation of general theories of Diophantine equations was an achievement of the twentieth century.



Finding all right triangles with integer side-lengths is equivalent to solving the Diophantine equation $a^2 + b^2 = c^2$.

Linear Diophantine Equations

One equation

The simplest linear Diophantine equation takes the form $ax + by = c$, where a, b and c are given integers. The solutions are described by the following theorem:

This Diophantine equation has a solution (where x and y are integers) if and only if c is a multiple of the greatest common divisor of a and b. Moreover, if (x, y) is a solution, then the other solutions have the form $(x + kv, y - ku)$, where k is an arbitrary integer, and u and v are the quotients of a and b (respectively) by the greatest common divisor of a and b.

Proof

If d is this greatest common divisor, Bézout's identity asserts the existence of integers e and f such that $ae + bf = d$. If c is a multiple of d, then $c = dh$ for some integer h, and (eh, fh) is a solution. On the other hand, for every pair of integers x and y, the greatest common divisor d of a and b divides $ax + by$.

Thus, if the equation has a solution, then c must be a multiple of d. If $a = ud$ and $b = vd$, then for every solution (x, y), we have

$a(x + kv) + b(y - ku) = ax + by + k(av - bu)$
$= ax + by + k (udv - vdu) = ax + by$,

showing that $(x + kv, y - ku)$ is another solution. Finally, given two solutions such that $ax_1 + by_1 = ax_2 + by_2 = c$, one deduces that $u(x_2 - x_1) + v(y_2 - y_1) = 0$.

As u and v are coprime, Euclid's lemma shows that there exists an integer k such that $x_2 - x_1 = kv$ and $y_2 - y_1 = -ku$. Therefore, $x_2 = x_1 + kv$ and $y_2 = y_1 - ku$, which completes the proof [1]

Chinese Remainder Theorem

The Chinese remainder theorem describes an important class of linear Diophantine systems of equations: let $n_1, \ldots, n_k$ be k pairwise coprime integers greater than one, $a_1, \ldots, a_k$ be k arbitrary integers, and N be the product $n_1 \cdots n_k$. The Chinese remainder theorem asserts that the following linear Diophantine system has exactly one solution$(x, x_1, \ldots, x_k)$ such that $0 \leq x < N$, and that the other solutions are obtained by adding to x a multiple of N:

$$\begin{aligned} x &= a_1 + n_1 x_1 \\ &\vdots \\ x &= a_k + n_k x_k \end{aligned}$$

System of Linear Diophantine Equations

More generally, every system of linear Diophantine equations may be solved by computing the Smith normal form of its matrix, in a way that is similar to the use of the reduced row echelon form to solve a system of linear equations over a field. Using matrix notation every system of linear Diophantine equations may be written

$A X = C$,

where A is an $m \times n$ matrix of integers, X is an $n \times 1$ column matrix of unknowns and C is an $m \times 1$ column matrix of integers.

The computation of the Smith normal form of A provides two unimodular matrices (that is matrices that are invertible over the integers and have ± 1 as determinant) U and V of respective dimensions $m \times m$ and $n \times n$, such that the matrix

$B = [b_{i,j}] = UAV$

is such that $b_{i,i}$ is not zero for i not greater than some integer k, and all the other entries are zero. The system to be solved may thus be rewritten as

$B (V^{-1}X) = UC$.

Calling y_i the entries of $V^{-1}X$ and d_i those of $D = UC$, this leads to the system

$b_{i,i}\, y_i = d_i$ for $1 \leq i \leq k$,

$0\, y_i = d_i$ for $k < i \leq n$.

This system is equivalent to the given one in the following sense: A column matrix of integers x is a solution of the given system if and only if $x = Vy$ for some column matrix of integers y such that $By = D$ [2].

It follows that the system has a solution if and only if $b_{i,i}$ divides d_i for $i \leq k$ and $d_i = 0$ for $i > k$. If this condition is fulfilled, the solutions of the given system are

$$V \begin{bmatrix} \frac{d_1}{b_{1,1}} \\ \vdots \\ \frac{d_k}{b_{k,k}} \\ h_{k+1} \\ \vdots \\ h_n \end{bmatrix},$$

Where $h_{k+1} \ldots h_n$ are arbitrary integers.

Hermite normal form may also be used for solving systems of linear Diophantine equations. However, Hermite normal form does not directly provide the solutions; to get the solutions from the Hermite normal form, one has to successively solve several linear equations.

Nevertheless, Richard Zippel wrote that the Smith normal form "is somewhat more than is actually needed to solve linear diophantine equations. Instead of reducing the equation to diagonal form, we only need to make it triangular, which is called the Hermite normal form. The Hermite normal form is substantially easier to compute than the Smith normal form."

Integer linear programming amounts to finding some integer solutions (optimal in some sense) of linear systems that include also inequations. Thus systems of linear Diophantine equations are basic in this context, and textbooks on integer programming usually have a treatment of systems of linear Diophantine equations [3].

Diophantine Geometry

Diophantine geometry, which is the application of techniques from algebraic geometry in this field, has continued to grow as a result; since treating arbitrary equations is a dead end, attention turns to equations that also have a geometric meaning. The central idea of Diophantine geometry is that of a rational point, namely a solution to a polynomial equation or a system of polynomial equations, which is a vector in a prescribed field K, when K is not algebraically closed.

Modern Research

One of the few general approaches is through the Hasse principle. Infinite descent is the traditional method, and has been pushed a long way.

The depth of the study of general Diophantine equations is shown by the characterization of Diophantine sets as equivalently described as recursively enumerable. In other words, the general problem of Diophantine analysis is blessed or cursed with universality, and in any case is not something that will be solved except by re-expressing it in other terms.

The field of Diophantine approximation deals with the cases of Diophantine inequalities. Here variables are still supposed to be integral, but some coefficients may be irrational numbers, and the equality sign is replaced by upper and lower bounds [4].

The most celebrated single question in the field, the conjecture known as Fermat's Last Theorem, was solved by Andrew Wiles but using tools from algebraic geometry developed during the last century rather than within number theory where the conjecture was originally formulated. Other major results, such as Faltings' theorem, have disposed of old conjectures.

Infinite Diophantine Equations

An example of an infinite diophantine equation is:

$n = a^2 + 2b^2 + 3c^2 + 4d^2 + 5e^2 + \ldots$,

Which can be expressed as "How many ways can a given integer n be written as the sum of a square plus twice a square plus thrice a square and so on?" The number of ways this can be done for each n forms an integer sequence. Infinite Diophantine equations are related to theta functions and infinite dimensional lattices. This equation always has a solution for any positive n. Compare this to:

$n = a^2 + 4b^2 + 9c^2 + 16d^2 + 25e^2 + \ldots$,

Which does not always have a solution for positive n.

Exponential Diophantine Equations

If a Diophantine equation has as an additional variable or variables occurring as exponents, it is an exponential Diophantine equation. Examples include the Ramanujan–Nagell equation, $2^n - 7 = x^2$, and the equation of the Fermat-Catalan conjecture and Beal's conjecture, $a^m + b^n = c^k$ with inequality restrictions on the exponents. A general theory for such equations is not available; particular cases such as Catalan's conjecture have been tackled. However, the majority are solved via ad hoc methods such as Stormer's theorem or even trial and error.

References

1. Mordell LJ. Diophantine equations. Pure and Applied Mathematics 30. Academic Press, 2012. ISBN 0-12-506250-8. Zbl 0188.34503.
2. Schmidt, Wolfgang M. Diophantine approximations and Diophantine equations. Lecture Notes in Mathematics 1467. Berlin: Springer-Verlag, 2012. ISBN 3-540-54058-X.Zbl 0754.11020.
3. Shorey TN, Tijdeman R. Exponential Diophantine equations. Cambridge Tracts in Mathematics 87. Cambridge University Press, 2011. ISBN 0-521-26826-5.Zbl 0606.10011.
4. Smart Nigel P. The algorithmic resolution of Diophantine equations. London Mathematical Society Student Texts 41. Cambridge University Press, 2008. ISBN 0-521-64156-X. Zbl 0907.11001.
5. Stillwell John. Mathematics and its History (Second ed.). Springer Science and Business Media Inc, 2004. ISBN 0-387-95336-1.