Diophantine Equation

Nguyễn Quản Bá Hồng[*]

Ngày 28 tháng 11 năm 2022

Abstract

A set of problems of Diophantine equations.

Contents

1 Wikipedia/Diophantine Equation

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

"In mathematics, a *Diophantine equation* is a polynomial equation, usually involving 2 or more unknowns, s.t. the only solutions of interest are the integer ones. A *linear Diophantine equation* equates to a constant the sum of 2 or more monomials, each of degree 1. An *exponential Diophantine equation* is one in which unknowns can appear in exponents.

Diophantine problems have fewer equations than unknowns & involve finding integers that solve simultaneously all equations. As such systems of equations define algebraic curves, algebraic surfaces, or, more generally, algebraic sets, their study is a part of algebraic geometry that is called *Diophantine geometry*.

The word *Diophantine* refers to the Hellenistic mathematician of the 3rd century, Diophantus of Alexandria, who made a study of such equations & was 1 of the 1st 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 & have been considered throughout history, the formulation of general theories of Diophantine equations (beyond the case of linear & quadratic equations) was an achievement of the 20th century." – Wikipedia/Diophantine equation

1.1 Examples of Diophantine Equation

"In the following Diophantine equations, w, x, y, z are the unknowns & the other letters are given constants: • $ax+by = c$: a linear Diophantine equation. • $w^3+x^3 = y^3+z^3$: The smallest nontrivial solution in positive integers is $12^3+1^3 = 9^3+10^3 = 1729$. It was famously given as an evident property of 1729, a taxicab number (also named Hardy–Ramanujan number) by Ramanujan to Hardy while meeting in 1917. There are infinitely many nontrivial solutions. • For $n = 2$, there are infinitely many solutions (x, y, z): the Pythagorean triples. For larger integer values of n, Fermat's Last Theorem (initially claimed in 1637 by Fermat & proved by Andrew Wiles in 1995) states there are no positive integer solutions (x, y, z). • $x^2 - ny^2 = \pm 1$: This is Pell's equation, which is named after the English mathematician John Pell. It was studied by Brahmagupta in the

[*]Independent Researcher, Ben Tre City, Vietnam
e-mail: nguyenquanbahong@gmail.com; website: https://nqbh.github.io.

7th century, as well as by Fermat in the 17th century. • $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$: The Erdős–Strauss conjecture states that, for every positive integer $n \geq 2$, there exists a solution in x, y, z, all as positive integers. Although not usually stated in polynomial form, this example is equivalent to the polynomial equation $4xyz = yzn + xzn + xyn = n(xy + yz + zx)$. • $x^4 + y^4 + z^4 = w^4$: Conjectured incorrectly by Euler to have no nontrivial solutions. Proved by Elkies to have infinitely many nontrivial solutions, with a computer search by Frye determining the smallest nontrivial solution, $95800^4 + 217519^4 + 414560^4 = 422481^4$." – Wikipedia/Diophantine equation/example

1.2 Linear Diophantine Equations

1.2.1 1 equation

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

Theorem 1.1. *This Diophantine equation has a solution (where $x, y \in \mathbb{Z}$) if & only if c is a multiple of the greatest common divisor of a & 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, & u, v are the quotients of a, b (respectively) by the greatest common divisor of a & b.*

Chứng minh. If d is this greatest common divisor, Bézout's identity asserts the existence of integers e & f s.t. $ae+bf = d$. If c is a multiple of d, then $c = dh$ for some integer h, & (eh, fh) is a solution. On the other hand, for every pair of integers x & y, the greatest common divisor d of a & b divides $ax+by$. Thus, if the equation has a solution, then c must be a multiple of d. If $a = ud$ & $b = vd$, 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 2 solutions s.t. $ax_1 + by_1 = ax_2 + by_2 = c$, one deduces that $u(x_2 - x_1) + v(y_2 - y_1) = 0$. As u & v are coprime, Euclid's lemma shows that v divides $x_2 - x_1$, & thus that there exists an integer k s.t. $x_2 - x_1 = kv$ & $y_2 - y_1 = -ku$. Therefore, $x_2 = x_1 + kv$ & $y_2 = y_1 - ku$, which completes the proof." – Wikipedia/Diophantine equation/example/1 equation □

1.2.2 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 1, $a_1, \ldots, a_k$ be k arbitrary integers, & N be the product $n_1, \ldots, n_k$. The Chinese remainder theorem asserts that the following linear Diophantine system has exactly 1 solution $(x, x_1, \ldots, x_k)$ s.t. $0 \leq x < N$, & that the other solutions are obtained by adding to x a multiple of N: $x = a_i + n_i x_i$, $i = 1, \ldots, k$." – Wikipedia/Diophantine equation/example/Chinese remainder theorem

1.2.3 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 $AX = C$, where A is an $m \times n$ matrix of integers, X is an $n \times 1$ column matrix of unknowns & C is an $m \times 1$ column matrix of integers.

The computation of the Smith normal form of A provides 2 unimodular matrices (that is matrices that are invertible over the integers & have ± 1 as determinant) U & V of respective dimensions $m \times m$ & $n \times n$, s.t. the matrix $B = [b_{ij}] = UAV$ is s.t. $b_{ii} \neq 0$ for $i \leq k$ for some integer k, & 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 $V^{-1}X$ & d_i those of $D = UC$, this leads to the system $b_{ii}y_i = d_i$ for $1 \leq i \leq k$, $0y_i = d_i$ 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 iff $x = Vy$ for some column matrix of integers y s.t. $By = D$. It follows that the system has a solution iff b_{ii} divides d_i for $i \leq k$ & $d_i = 0$ for $i > k$. If this condition is fulfilled, the solutions of the given system as $V\left[\frac{d_1}{b_{11}}, \ldots, \frac{d_k}{b_{kk}}, h_{k+1}, \ldots, h_n\right]^\top$, where $h_{k+1}, \ldots, h_n$ are arbitrary integers.

Hermit 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 sole 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, & textbooks on integer programming usually have a treatment of systems of linear Diophantine equations." – Wikipedia/Diophantine equation/example/system of linear Diophantine equations

1.3 Homogeneous Equations

1.4 Diophantine Analysis

1.5 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, $2^n - 7 = x^2$, & the equation of the Fermat–Catalan conjecture & 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 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 Størmer's theorem or even trial & error." – Wikipedia/Diophantine equation/exponential Diophantine equations

2 Phương Pháp Xét Tính Chia Hết

Bài toán 2.1 (Bình, 2021, Thí dụ 1, p. 6)**.** *Giải phương trình nghiệm nguyên* $3x + 17y = 159$.

Bài toán 2.2 (Bình, 2021, Thí dụ 2, p. 6)**.** *Tìm nghiệm nguyên của phương trình* $xy - x - y = 2$.

Bài toán 2.3 (Bình, 2021, Thí dụ 3, p. 7)**.** *Tìm nghiệm nguyên của phương trình* $2xy - x + y = 3$.

Tài liệu

Bình, Vũ Hữu (2021). *Phương Trình Nghiệm Nguyên & Kinh Nghiệm Giải.* Nhà Xuất Bản Giáo Dục Việt Nam, p. 224.