Notes on Diophantine Equations

David K. Zhang

Last modified May 24, 2022

A ***Diophantine equation*** is a polynomial equation with integer coefficients, in any number of variables, for which we seek integer solutions. For example, the Diophantine equation

$$x^2 + y^2 = z^2 \qquad\qquad x, y, z \in \mathbb{Z}$$

defines the set of Pythagorean triples $(x, y, z) \in \mathbb{Z}^3$. Every Diophantine equation can be written in the form

$$P(x_1, \ldots, x_n) = 0 \qquad\qquad x_1, \ldots, x_n \in \mathbb{Z}$$

for some polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$. For example, the preceding Diophantine equation can be represented by the polynomial $P(x, y, z) = x^2 + y^2 - z^2$. In this article, we will freely identify Diophantine equations and polynomials with integer coefficients.

- Any Diophantine equation of the form

  $$x_1 + Q(x_2, \ldots, x_n) = 0$$

  can be trivially solved by assigning arbitrary integer values to $x_2, \ldots, x_n$ and taking $x_1 = -Q(x_2, \ldots, x_n)$.

  More generally, we say that a variable x_1 ***occurs linearly*** in a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$ if P can be written in the form

  $$P(x_1, \ldots, x_n) = ax_1x_2^{j_2} \cdots x_k^{j_k} + Q(x_{k+1}, \ldots, x_n)$$

  for some polynomial $Q \in \mathbb{Z}[x_{k+1}, \ldots, x_n]$. The corresponding Diophantine equation

  $$ax_1x_2^{j_2} \cdots x_k^{j_k} + Q(x_{k+1}, \ldots, x_n) = 0$$

  can be solved by assigning $x_2 = \cdots = x_k = 1$ and checking whether it is possible for $Q(x_{k+1}, \ldots, x_n)$ to be a multiple of a, which can be tested in finite time by computing $Q(x_{k+1}, \ldots, x_n)$ modulo a for all values of $x_{k+1}, \ldots, x_n \in \{0, \ldots, a-1\}$. This observation allows us to exclude all Diophantine equations that contain a linear variable.

- If a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$ has no roots in $\mathbb{R}^n$, then it obviously cannot have any roots in $\mathbb{Z}^n$. This condition can be checked in finite time[1] using the algorithms of real algebraic geometry, such as cylindrical algebraic decomposition.

[1] The computational complexity of the cylindrical algebraic decomposition algorithm is doubly-exponential in the number of variables in the polynomial under consideration.

More generally, if the set of roots of P in $\mathbb{R}^n$ is bounded, then there are only finitely many points of $\mathbb{Z}^n$ that we need to check in order to determine whether P has an integer-valued root. The boundedness of this set can be checked by performing quantifier elimination on the following formula:

$$\forall t \in \mathbb{R}\ \exists x_1, \ldots, x_n \in \mathbb{R} : P(x_1, \ldots, x_n) = 0 \wedge x_1^2 + \cdots + x_n^2 \geq t$$

This observation allows us to exclude all Diophantine equations whose set of real-valued solutions is empty or bounded.

Lemma: Let $n \in \mathbb{Z}$. If p is an odd prime factor of $n^2 + 1$, then $p \equiv 1 \pmod 4$.

Proof: Let p be an odd prime. If $p \mid (n^2 + 1)$, then $n^2 \equiv -1 \pmod p$, which shows that -1 is a quadratic residue modulo p. Using the properties of the Legendre symbol, it follows that

$$1 = \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

which shows that $(p-1)/2$ is an even number. **QED**

Theorem: The Diophantine equation

$$x^2y + y^2 + z^2 + 1 = 0$$

has no integer-valued solutions.

Proof: We proceed by contradiction. Using the substitution $y \mapsto -y$, we can rewrite this equation as

$$y(x^2 - y) = z^2 + 1.$$

In other words, this equation expresses $z^2 + 1$ as a product of two integers whose sum is a perfect square. Observe that both of the factors, y and $x^2 - y$, must be positive.

Recall that every perfect square is congruent to 0 or 1 modulo 4. Hence, the right-hand side of this equation is congruent to 1 or 2 modulo 4. There are two ways to express each of these quantities as a product modulo 4:

$$1 \times 1 \equiv 3 \times 3 \equiv 1 \pmod 4 \qquad\qquad 1 \times 2 \equiv 3 \times 2 \equiv 2 \pmod 4$$

Thus, the two factors on the left-hand side must be congruent to $(1,1)$, $(3,3)$, $(1,2)$, or $(2,3)$ modulo 4. The first three options are impossible because their sum modulo 4 is not 0 or 1. The preceding lemma implies that the final option is impossible, since no odd prime factor of $z^2 + 1$ (and hence, by induction, no odd factor of $z^2 + 1$) can be congruent to 3 modulo 4. **QED**

Theorem: The Diophantine equation

$$x^2y + 3y + z^2 + 1 = 0$$

has no integer-valued solutions.

Proof: Substitute $y \mapsto -y$ to obtain the equation $y(x^2 + 3) = z^2 + 1$. Working modulo 4, the right-hand side is either 1 or 2, while $x^2 + 3$ is either 0 or 3. Observe that $x^2 + 3 \equiv 0$ is impossible because it would force the right-hand side to be 0, and $x^2 + 3 \equiv 3$ is impossible by the preceding lemma. **QED**