Diophantine Equations

Tucson Math Circle

Gaurish Korpal

https://gkorpal.github.io/

November 21, 2019

"There is no algorithm which, for a given arbitrary Diophantine equation, would tell whether the equation has a solution or not."
— Yuri Matiyasevich, *Hilbert's tenth problem: What can we do with Diophantine equations?, 1996.*

1 Bézout's identity

Theorem 1. *Let a and b be nonzero integers, and let $d = \gcd(a, b)$. The equation $ax + by = d$ always has a solution (x_1, y_1) in integers, and this solution can be found by the Euclidean algorithm. Then every solution to the equation can be obtained by substituting integers k into the formula*

$$\left(x_1 + \frac{b}{d}\cdot k,\ y_1 - \frac{a}{d}\cdot k\right)$$

For a proof of this theorem, refer [Silverman, Chapter 5 and 6].

Exercise 1. Find all the integer solutions (if they exist) of the following equations:

1. $127x + 52y = 1$
2. $127x - 52y + 1 = 0$
3. $127x - 52y = 2$
4. $1313x + 182y = 13$
5. $1313x + 182y - 1 = 0$
6. $1313x - 182y = 117$

One can also solve such equations using continued fractions, see [Gelfond, §2].

2 Pythagorean triple

Theorem 2. *Let a be a nonzero integer. The equation $ax^2 + y^2 = z^2$ has infinitely many primitive solutions. That is, there exits infinitely many triples (x_1, y_1, z_1) such that x_1, y_1 and z_1 have no common factors and satisfy $ax_1^2 + y_1^2 = z_1^2$.*

For a proof of this theorem, refer [Davenport, §VII.2] or [Gelfond, §3].

Exercise 2. Find all the non-zero integer solutions (if they exist) of the following equations:

1. $x^2 + y^2 = z^2$
2. $x^2 - y^2 = z^2$
3. $x^2 + 2y^2 = z^2$
4. $x^2 + y^2 = 2z^2$
5. $x^2 + 3y^2 = z^2$
6. $x^2 + y^2 = 3z^2$

One can also solve such equations using co-ordinate geometry, see [Silverman, Chapter 2 and 3]. The general case $ax^2 + by^2 = cz^2$ is much more difficult to tackle, see [Davenport, §VII.3].

3 Cattle Problem of Archimedes

Theorem 3. *Let D be a positive integer that is not a perfect square. Then equation $x^2 - Dy^2 = 1$ always has solutions in positive integers. If (x_1, y_1) is the solution with smallest x_1, then every solution (x_k, y_k) can be obtained by taking powers*

$$x_k + \sqrt{D}y_k = (x_1 + \sqrt{D}y_1)^k \quad \textit{for } k = 1, 2, 3, \ldots$$

For a proof of this theorem, refer [Silverman, Chapter 34].

Exercise 3. Find all the positive integer solutions (if they exist) of the following equations:

1. $x^2 - y^2 = 1$
2. $x^2 - 2y^2 = 1$
3. $x^2 - 3y^2 = 1$
4. $x^2 - 4y^2 = 1$
5. $x^2 - 63y^2 = 1$
6. $x^2 - 64y^2 = 1$

One can also solve such equations using continued fractions, see [Davenport, §IV.11] and [Gelfond, §4 and 5].

4 Congruent number problem

A congruent number is a positive integer that is the area of a right triangle with three rational number sides.

Theorem 4. *A square-free positive integer n is a congruent number if and only if the equation $y^2 = x^3 - n^2x$ has infinitely many rational solutions.*

For more details, see [Chahal]. Nobody knows how to determine if n is a congruent number.

Exercise 4. Find all the rational solutions (if they exist) of the following equations

1. $y^2 = x^3 - x$ (Fermat, 1640)
2. $y^2 = x^3 - 25x$ (Fibonacci)
3. $y^2 = x^3 - 36x$ (Hint: $5^2 = 3^2 + 4^2$)
4. $y^2 = x^3 - 157^2x$ (Don Zagier)

For a discussion about similar equations, see [Davenport, §VII.4 and 5].

References

[Gelfond] A. O. Gelfond. “Solving Equations in Integers” (Little Mathematics Library). Mir Publishers, 1981. (*Translated from Russian to English by O. B. Sheinin*). `https://archive.org/details/SolvingEquationsInIntegerslittleMathematicsLibrary`

[Davenport] H. Davenport. “The Higher Arithmetic: An Introduction to the Theory of Numbers” (8th edition). Cambridge University Press, 2012. `https://doi.org/10.1017/CBO9780511818097`

[Silverman] Joseph H. Silverman. “A Friendly Introduction to Number Theory” (4th edition). Pearson, 2012. `https://www.math.brown.edu/~jhs/frint.html`

[Chahal] J. S. Chahal. *Congruent Numbers and Elliptic Curves.* American Mathematical Monthly, Vol. 113, No. 4 (Apr. 2006), pp. 308-317 (10 pages). `https://www.jstor.org/stable/27641916`

Further Reading

1. T. Andreescu, D. Andrica, and I. Cucurezeanu. “An Introduction to Diophantine Equations: A Problem-Based Approach.” Birkhäuser Basel, 2010. `https://doi.org/10.1007/978-0-8176-4549-6`

2. W. Sierpińksi. “Elementary Theory of Numbers” (North-Holland Mathematical Library, Volume 31). PWN-Polish Scientific Publishers, 1988.

3. I. Niven, H. S. Zuckerman, and H. L. Montgomery. “An Introduction to the Theory of Numbers.” (5th edition), John Wiley & Sons, 1991.