107.15 Fruit diophantine equation

Introduction

A popular problem making the rounds in social media (stated as a problem about distribution of fruits) is the possibility of finding positive integer solutions in x, y, z of the equation that appears in the statement below. In this short note, we prove:

Theorem 1

The equation

$$y^2 - xyz + z^2 = x^3 - 5$$

has no integer solutions.

Note that the special case asserting that $y^2 = x^3 - 5$ has no integer solutions is already of interest.

The problem originated from the question "What is the smallest unsolved diophantine equation?" that was posed by user Zidane in MathOverflow [1]. In this question, the notion of size of a polynomial is the following one:

for $P(x_1, \ldots, x_d) = \sum_{i_1,\ldots,i_d} a_{i_1,\ldots,i_d} x_1^{i_1} \ldots x_d^{i_d} \in \mathbb{Z}[x_1, \ldots, x_d]$, define

$$|P|(x_1, \ldots, x_d) = \sum_{i_1,\ldots,i_d} |a_{i_1,\ldots,i_d}| x_1^{i_1} \ldots x_d^{i_d}.$$

Then, the size $h(P)$ of P is defined as $|P|(2, \ldots, 2)$. Bogdan Grechuk [2] considered the first part of the problem: " for which smallest P does one not know if there exists an integral solution of $P(\mathbf{x}) = 0$?"

The first non-trivial example of such a polynomial P was obtained in the case when $h(P) = 22$ and, that corresponded to the equation $x^2 + y^2 - z^2 = xyz - 2$. Will Sawin showed that this equation has no non-trivial solution. The next 'unknown' diophantine equation that appeared on the scene was $y(x^3 - y) = z^2 + 2$ with $h(P) = 26$, and this was solved later by the user Servaes. Finally for $h(P) = 29$, Grechuk asked for possible solutions for the two Diophantine equations $y(x^2 + 2) = 2zx + 2z^2 + 1$ (which he himself solved later) and $y^2 - xyz + z^2 = x^3 - 5$. The last equation gained quite a bit of popularity in the social media thanks to the blog 'theHigherGeometer', where David Roberts posed this problem as a 'fruit equation' [3]. This is what we solve here.

Proof of Theorem 1

Fix a prospective candidate $x = k$ that gives an integral solution. Then we are looking for an integral solution of the equation

$$y^2 - kyz + z^2 = k^3 - 5. \tag{1}$$

We divide the proof into two cases.

Case 1: k is even

Then (1) becomes

$$\left(y - \frac{kz}{2}\right)^2 - \left(\frac{k^2}{4} - 1\right)z^2 = k^3 - 5.$$

Rewriting in terms of $d = \frac{1}{2}k$ and $u = y - \frac{1}{2}kz$, this becomes the Pell's equation

$$u^2 - (d^2 - 1)z^2 = 8d^3 - 5. \tag{2}$$

If d is odd, then $d^2 - 1$ is a multiple of 8 and hence, the left-hand side and right-hand side of (2) are respectively congruent modulo 8 to a perfect square and -5; this is impossible.

If d is even, the left and right side of (2) are congruent modulo 4 to $u^2 + z^2$ and -5 respectively; once again this is impossible.

We conclude that there is no solution of (1) with even k.

Case 2: k is odd.

Viewing (1) modulo 2, we obtain

$$y^2 + yz + z^2 = 0 \qquad (\mathrm{mod}\, 2).$$

This implies $y \equiv z \equiv 0 \,(\mathrm{mod}\, 2)$. This implies that left side of (1) is congruent to 0 modulo 4. As a consequence, we obtain $k^3 - 5 \equiv 0 \,(\mathrm{mod}\, 4)$ or equivalently $k \equiv 1 \,(\mathrm{mod}\, 4)$. Rewriting (1) as

$$\left(y - \frac{kz}{2}\right)^2 - (k^2 - 4)\frac{z^2}{4} = k^3 - 5.$$

and substituting $z = 2v$ and $u = y - vk$, (1) becomes the Pell's equation

$$u^2 - (k^2 - 4)v^2 = k^3 - 5. \tag{3}$$

We need to find integral solutions of the Brahmagupta-Pell equation $u^2 - (k^2 - 4)v^2 = k^3 - 5$, for integers $k \equiv 1 \,(\mathrm{mod}\, 4)$. We divide the proof again into some cases.

Case 2a: $k \equiv 1 \,(\mathrm{mod}\, 12)$

In this case, $3 \mid (k + 2)$ and $k^3 \equiv 1 \,(\mathrm{mod}\, 3)$. Modulo 3, (3) gives us $u^2 \equiv 2 \,(\mathrm{mod}\, 3)$. As a consequence, we see there is no solution in this case.

Case 2b: $k \equiv 9 \,(\mathrm{mod}\, 12)$

Note that in this case we have $k - 2 \equiv 7 \,(\mathrm{mod}\, 12)$, hence $6 \nmid (k - 2)$.

First observe that if all the prime divisors of $k - 2$ are congruent to ± 1 modulo 12, then $k - 2$ is congruent to ± 1 modulo 12, which contradicts the fact that $k - 2 \equiv 7 \,(\mathrm{mod}\, 12)$. Thus there exists a prime p such that $p \equiv 5$ or $7 \,(\mathrm{mod}\, 12)$ and p divides $k - 2$. This implies $k \equiv 2 \,(\mathrm{mod}\, p)$, hence $k^3 \equiv 8 \,(\mathrm{mod}\, p)$. Modulo p, (3) gives us

$$u^2 \equiv 3 \pmod{p}.$$

By quadratic reciprocity, this equation has no solution as 3 is a square modulo p if, and only if, $p \equiv \pm 1 \pmod{12}$.

Case 2c: $k \equiv 5 \pmod{12}$

In this case, we have $3 \mid (k - 2)$. Modulo 3, (3) gives us

$$u^2 \equiv 0 \pmod{3}.$$

Writing $u = 3w$ and $k = 12r + 5$, (3) becomes

$$3w^2 - (4r + 1)(12r + 7)v^2 = 2^6.3^2r^3 + 2^4.3^2.5r^2 + 2^2.3.5^2r + 40. \qquad (4)$$

Modulo 3, (4) gives us

$$-(r + 1)v^2 \equiv 1 \pmod{3}.$$

The above equation implies $r \equiv 1 \pmod{3}$, say $r = 3s + 1$. Then, $k = 36s + 17$; so, $k - 2 = 3(12s + 5)$. If all the prime divisors of $12s + 5 = \frac{1}{3}(k - 2)$ are congruent to ± 1 modulo 12, then $\frac{1}{3}(k - 2)$ is congruent to ± 1 modulo 12, which contradicts the fact that $\frac{1}{3}(k - 2) \equiv 5 \pmod{12}$. Thus there exists a prime p such that $p \equiv 5$ or $7 \pmod{12}$ and p divides $k - 2$. This implies $k \equiv 2 \pmod{p}$.

Modulo p, (3) gives us $u^2 \equiv 3 \pmod{p}$. By quadratic reciprocity, this equation has no solution.

We make some comments which may be of interest to readers familiar with the basics of the theory of elliptic curves. Briefly speaking, elliptic curves over $\mathbb{Q}$ are cubic equations of the form $y^2 + axy = x^3 + bx + c$ where a, b, c are rational numbers and the discriminant of the cubic on the right is not zero. The set of points $(x, y) \in \mathbb{Q}^2$ that are solutions of the above equation possess a composition that equips it with the structure of an abelian group. The so-called Mordell-Weil theorem asserts that this group of rational solutions is a finitely generated abelian group (more generally, one considers number fields and not just $\mathbb{Q}$; the case of $\mathbb{Q}$ was treated by Mordell earlier). This group of rational points is usually called the Mordell-Weil group of the elliptic curve over $\mathbb{Q}$. It is a subtle point to decide whether a given elliptic curve can have rational points but no integral points because the latter may not form a group.

The main result, Theorem 1, can be rephrased as a statement that certain elliptic curves have no integer points:

For any integer k, the elliptic curve E_k given by the Weierstrass equation $y^2 - kxy = x^3 - (k^2 + 5)$ has no integral points.

Remarks

For $|k| \leqslant 5$, the above assertion on elliptic curves can also be verified

using LMFDB [4]. We note that $E_k \cong E_{-k}$ over $\mathbb{Q}$ given by $(x, y) \to (x, -y)$. We also remark that even when E_k does not have integral solutions, it may have rational solutions; that is, it need not have trivial Mordell-Weil group.

For example, using LMFDB [4] we see that E_1 has Mordell-Weil group isomorphic to $\mathbb{Z}$ generated by $\left(\frac{101}{16}, \frac{-821}{64}\right)$. In other words, the fruit equation $y^2 - xyz + z^2 = x^3 - 5$ has the rational solution $\left(\frac{101}{16}, \frac{-821}{64}, 1\right)$.

On the other hand E_0, E_2, E_3, E_4 have trivial Mordell-Weil group.

The curve E_5 has minimal Weirstrass equation $y^2 + xy = x^3 - 13x - 13$ obtained via the change of variables $(x, y) \to (x + 2, 2x - y - 1)$. Using LMFDB [4] we see that this elliptic curve $y^2 + xy = x^3 - 13x - 13$ has Mordell-Weil group isomorphic to $\mathbb{Z}$ generated by $\left(\frac{-71}{64}, \frac{593}{512}\right)$, which gives us a rational point (of infinite order) $\left(\frac{-199}{64}, \frac{-4289}{512}\right)$ for $y^2 - 5xy = x^3 - 30$.

Acknowledgments

We are grateful to Aditya Karnataki for sharing this problem on social media; this brought it to our attention. We would also like to thank Bogdan Grechuk for bringing up all these interesting diophantine equations through his investigations. Last but not least, we are indebted to the referee for suggesting a number of amendments of a linguistic nature as well as for pointing out that it is better to mention elliptic curves in a gentler manner.

References

1. https://mathoverflow.net/q/316708/
2. Bogdan Grechuk, Diophantine equations: a systematic approach, arXiv preprint, arXiv:2108.08705 [math.GM], https://arxiv.org/abs/2108.08705
3. https://thehighergeometer.wordpress.com/2021/07/27/diophantine-fruit/
4. The L-functions and Modular Forms Database, http://www.lmfdb.org/

DIPRAMIT MAJUMDAR
Department of Mathematics,
Indian Institute of Technology Madras,
IIT P.O. Chennai 600036, India
e-mail: *dipramit@gmail.com*
B. SURY
Stat-Math Unit, Indian Statistical Institute,
8th Mile Mysore Road, Bangalore 560059, India
e-mail: *surybang@gmail.com*