A NOTE ON THE DIOPHANTINE EQUATION $\mathbf{lx^3 - kx^2 + kx - l = y^2}$: THE CASES $\mathbf{k = 3l \pm 1}$

Konstantine Zelator

Abstract. In this work, we investigate the Diophantine equation $lx^3 - kx^2 + kx - l = y^2$ where k and l are positive integers. The two results are Theorems 1.1 and 1.2. The first theorem states that if $k = 3l-1$ and $l = \rho^2$, the above equation has a unique integer solution, namely $(x, y) = (1, 0)$. The second theorem says that if $k = 3l + 1$ and $l \equiv 0, 1, 4, 5, 7 \pmod 8$ the above equation also has a unique solution, the pair $(x, y) = (1, 0)$.

1. Introduction. The motivating problem behind this work is the following problem. Find all integer solutions of the Diophantine equation $x^3 - 2x^2 + 2x - 1 = y^2$. In other words, we are looking for the pairs (x, y) in $\mathbb{Z} \times \mathbb{Z}$, which satisfy the preceding equation. As it turns out, this problem has a unique solution, namely the pair $(x, y) = (1, 0)$. This equation is a special case of the two-variable Diophantine equation which we will study in this article, (with $l = 1, k = 2$):

$$lx^3 - kx^2 + kx - l = y^2, \tag{1.1}$$

where l and k are positive integers. It is worth mentioning that Diophantine equations of the form $ay^2 = f(x)$, where a is a nonzero integer and f is a cubic polynomial with integer coefficients, and also equations like $ay^3 = g(x)$ where g is a quadratic polynomial with integer coefficients, when studied from the point of view of finding rational solutions, lead to the theory of rational points on elliptic curves, as such plane curves are known. Rational points on elliptic curves is a subject well beyond the scope of this paper. When it comes to finding the integer solutions to such equations, the situation is quite different, the same kind of unified theory does not really exist. In [1], one can find historical information on such Diophantine equations. The main results of this article are the following theorems.

Theorem 1.1. Let l, k be positive integers which satisfy the conditions $k = 3l - 1$ and $l = \rho^2$ for some positive integer ρ. Then the Diophantine equation

$$lx^3 - kx^2 + kx - l = y^2,$$

has a unique solution, the pair $(x, y) = (1, 0)$.

Theorem 1.2. Let l, k be positive integers such that $k = 3l + 1$ and $l \equiv 0, 1, 4, 5 \text{ or } 7 \pmod 8$. Then the Diophantine equation,

$$lx^3 - kx^2 + kx - l = y^2,$$

has a unique solution, the pair $(x, y) = (1, 0)$.

The organization of this paper is as follows. In Section 2 we prove a lemma and a proposition. Lemma 2.1 is used in the proof of Proposition 2.2, which in turn is used to establish the two theorems. The proofs of the two theorems are found in Section 3.

2. A Lemma, A Proposition, and Their Proofs.

Note. The author of this work wishes to extend his gratitude to the referee for the valuable suggestions and comments. Because of these comments and meticulous work on the part of the referee, the original more complicated structure of this paper has been significantly simplified.

Lemma 2.1. If l, k are positive integers such that either $k = 3l - 1$; or $k = 3l + 1$ and $l \neq 2$, then the quadratic equation $lx^2 + (l - k)x + l = 0$ has no integer roots.

Proof. We introduce a new variable t: $t = x - 1$; $t + 1 = x$. Then, the said quadratic equation takes the form $l \cdot (t + 1)^2 + (l - k)(t + 1) + l = 0$; or equivalently

$$lt^2 + (3l - k)t + 3l - k = 0. \tag{2.1}$$

Accordingly,

$$\begin{cases} lt^2 + t + 1 = 0, & \text{if } k = 3l - 1 \\ lt^2 - t - 1 = 0, & \text{if } k = 3l + 1. \end{cases} \tag{2.2}$$

If the quadratic equation in the hypothesis of Lemma 2.1 has an integer root, then so must one of the equations in (2.2). Hence, if r is such an integer root of the first equation in (2.2), then $r(lr + 1) = -1$; while if r is an integer root of the second equation in (2.2), then $r(lr - 1) = 1$. In either case, r must be a divisor of 1, and so $r = 1$ or -1.

If $r = 1$ is a root of the first equation in (2.2) we obtain

$$l = -2. \tag{2.3}$$

If $r = -1$ is a root of the first equation in (2.2), then

$$l = 0. \tag{2.4}$$

If $r = 1$ is a root of the second equation in (2.2) we have

$$l = 2. \tag{2.5}$$

Finally, if $r = -1$ is a root of the second equation in (2.2), then

$$l = 0. \tag{2.6}$$

It is clear that in all cases (2.3)–(2.6) the hypothesis on l is violated; namely that $l \neq 2$ and l being a positive integer.

The next proposition will be used in the proof of the main result.

Proposition 2.2. Let k and l be positive integers. Consider the equation

$$lx^3 - kx^2 + kx - l = y^2. \tag{2.7}$$

(1) Equation (2.7) has no integer solutions (x, y) with $x \leq 0$.
(2) The pair $(x, y) = (1, 0)$ is a solution to equation (2.7).
(3) If $k = 3l - 1$, then equation (2.7) has a solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ with $x > 1$ if and only if $x = a^2 + 1$, $y = \pm ab$ for some positive integers a and b satisfying the condition $la^4 + a^2 + 1 = b^2$.
(4) If $k = 3l+1$ and $l \neq 2$, then equation (2.7) has a solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ with $x > 1$ if and only if $x = a^2 + 1$, $y = \pm ab$ for some positive integers a and b satisfying the condition $la^4 - a^2 - 1 = b^2$.

Proof. Statements (1) and (2) follow simply by inspection.

(3) First we prove the sufficiency case. Assume that a and b are positive integers satisfying the condition $la^4 + a^2 + 1 = b^2$. A substitution shows that the two pairs $(x, y) = (a^2 + 1, \ \pm ab)$ are solutions to the equation (2.7). The calculations are straightforward and are left to the reader. Next, we prove the necessity. Suppose that (x, y) is an integral solution of equation (2.7) with $x > 1$. It follows that

$$(x - 1)(lx^2 + (l - k)x + l) = y^2. \tag{2.8}$$

Note that $y \neq 0$. For if $y = 0$, then since $x > 1$, (2.8) would imply $lx^2 + (l - k)x + l = 0$, which is impossible by Lemma 2.1. Therefore, $x > 1$ and $y \neq 0$; $x > 1$ and $y^2 > 0$ in (2.8) which implies $lx^2 + (l - k)x + l > 0$. Let d be the greatest common divisor of the two factors on the left hand side of equation (2.8). Then $x - 1 = dq$ for some positive integer q. We have $lx^2 + (l - k)x + l = l(dq + 1)^2 + (l - k)(dq + 1) + l$, which implies that

$$lx^2 + (l - k)x + 1 = d(lq^2 + 2lq + q(l - k)) + 3l - k. \tag{2.9}$$

Since d is a divisor of the left hand side of (2.9), it follows that d must be a divisor of $3l - k = 1$. Hence, $d = 1$. Therefore, the two factors on the left hand side are relatively prime. Hence, we conclude that the two factors must be perfect squares. This implies that $x - 1 = a^2$ and $lx^2 + (l - k)x + l = b^2$ for some positive integers a and b. It follows, based on equation (2.8), that $y = \pm ab$ and $x = a^2 + 1$. Also, $lx^2 + (l - k)x + l = l(a^2 + 1)^2 + (l - k)(a^2 + 1) + l = b^2$ and hence, $la^4 + a^2 + 1 = b^2$, since $k = 3l - 1$.

(4) We go back to equation (2.8). Suppose that (x, y) is an integral solution of (2.8) with $x > 1$. We have $(x-1)(lx^2 + (l-k)x + l) = y^2$, and with $k = 3l + 1$ and $l \neq 2$. Again, as we showed in the proof of part (3) there is no integer solution with $x > 1$ and $y = 0$. For this would imply that $lx^2 + (l-k)x + l = 0$ has an integer root, which is ruled out by Lemma 2.1. Thus, $x > 1$ and $y^2 > 0$ in (2.8) which implies $lx^2 + (l-k)x + l > 0$. The rest of the proof is nearly identical to that of part (3), so we leave the calculations to the interested reader. We only note that in the proof of part (4) we have instead $3l - k = -1$; and the condition $la^4 - a^2 - 1 = b^2$.

3. Proofs of the Two Theorems.

Proof of Theorem 1.1. By Proposition 2.2, we know that the given equation has no integer solutions with $x \leq 0$ and that $(x, y) = (1, 0)$ is a solution. To conclude the proof we must show that it has no solutions with $x > 1$. If it did have a solution (x, y) with $x > 1$ then according to Proposition 2.2, we would have that $x = a^2 + 1$ and $y = \pm ab$ for some positive integers a and b satisfying the condition $la^4 + a^2 + 1 = b^2$. However, $la^4 + a^2 + 1 = b^2$ is impossible. Indeed, $l = \rho^2$; ρ a natural number and consequently

$$(\rho a^2)^2 < \rho^2 a^4 + \rho a^2 + 1 < (\rho a^2 + 1)^2,$$

clearly showing the positive integer $\rho^2 a^4 + \rho a^2 + 1$ lies between two consecutive integer squares; and hence, itself cannot be an integral or perfect square.

Proof of Theorem 1.2. If the equation had an integer solution (x, y) with $x > 1$ then by Proposition 2.2, we must have that $x = a^2 + 1$ and $y = \pm ab$ for some positive integers $a,\ b$ satisfying the condition $la^4 - a^2 - 1 = b^2$. This condition implies that a must be an odd integer. If a were even then obviously $b^2 \equiv 3 \pmod 4$, which is impossible since the square of an integer is congruent to 0 or 1 mod 4. Thus, a is odd which in turn implies that $a^2 \equiv 1 \pmod 8$ and so $a^2 \equiv 1 \equiv a^4 \pmod 8$. Thus, $la^4 - a^2 - 1 = b^2$ implies that $l \equiv 2 + b^2 \pmod 8$. However, $b^2 \equiv 0, 1, 4 \pmod 8$. Therefore, $l \equiv 2, 3, 6 \pmod 8$, contrary to the hypothesis that $l \equiv 0, 1, 4, 5, 7 \pmod 8$. It is now clear that equation (1.1) cannot have an integer solution with $x > 1$.

Reference

1. L. E. Dickson, *History of the Theory of Numbers*, Vol. II, AMS Chelsea Publishing, Providence, Rhode Island, 1992.

Mathematics Subject Classification (2000): 11Dxx

Konstantine Zelator
Dept. of Math and Computer Science
Rhode Island College
600 Mount Pleasant Avenue
Providence, RI 02908
email: kzelator@ric.edu