APPLYING MODULAR ARITHMETIC TO DIOPHANTINE EQUATIONS

Ramy F. Taki ElDin
Physics and Engineering Mathematics Department, Faculty of Engineering, Ain Shams University, Cairo, Egypt
ramy.farouk@eng.asu.edu.eg

Received: 10/24/17, Accepted: 7/16/18, Published: 7/27/18

Abstract

In this paper, experimental results for presenting the success rates in finding integral solutions to the Diophantine equations of two variables using modular arithmetic are shown. Firstly, and for this purpose, the empirical algorithm for obtaining experimental results is presented for Diophantine equations of polynomial-type. Using modular arithmetic, the algorithm transforms the Diophantine equation to a linear recurrence relation. This defines a sequence of integers $\{\lambda_s\}_{s=1}$ and the integral solution is achieved once this sequence terminates. The algorithm could be successful in solving polynomial Diophantine equations provided that a predefined numeral system pattern to the base p (prime number) for one of the two variables exists. Secondly, without any predefined numeral system pattern, the algorithm is adopted for equations with exponential terms. Finally, and for experimental results, four strategies are proposed for the termination of the sequence $\{\lambda_s\}_s$. Success rates are compared by testing the strategies over many polynomial-type Diophantine equations. The experimental results are presented in detail and some strategies contribute to high success rates in achieving the integral solutions.

1. Introduction

Solving a Diophantine equation refers to finding an integral solution to a polynomial equation in more than one variable. Such equations have attracted researchers throughout a long history. Diophantine equations can be considered over the ring of integers $\mathbb{Z}$, the field of rational numbers $\mathbb{Q}$, or even over any finite field $\mathbb{F}_q$.

Some Diophantine equations possess infinite integral solutions, e.g., Pell's equation $x^2 - dy^2 = 1$, where d is a positive square-free integer. Others possess only a finite number of integral solutions, e.g., the Mordell curve $y^2 = x^3 + k$ contains only a finite number of integral points (X, Y). Many researchers studied Diophantine equations which have no integral solutions, e.g., the work of Lu et al. [5]. The most popular of such equations are Fermat's equation and the Mordell curve $y^2 = x^3 + k$ which have no integral solutions for $k = (4n-1)^3 - 4m^2$, where there is no prime $p \equiv 3 \pmod 4$ such that $p \,|\, m$, as proved in [1].

In this paper, Diophantine equations over $\mathbb{Z}$ that have positive integral solutions are considered. The experimental results of the success rates for solving these equations, using only modular arithmetic, are presented. In his tenth problem, Hilbert asked about the existence of an algorithm suitable for solving any Diophantine equations. In 1970, Matijasevic [7] proved the non-existence of such an algorithm. Meanwhile, researchers looked for a general algorithm for solving Diophantine equations of special forms [4]. However, in this research, we aim to test the success rate of a special algorithm in solving Diophantine equations of general form. In particular, the capability of a modular arithmetic algorithm, in solving a general form of Diophantine equations, is measured by evaluating the success rate of the algorithm in finding integral solutions. As a preparation for the experimental results, an algorithm using only simple modular arithmetic is presented. The algorithm transforms the Diophantine equation to a linear recurrence relation that generates some integer sequence $\{\lambda_s\}$. Once this sequence terminates, an integral solution is obtained and a success is recorded.

The remainder of this paper is organized as follows. In Section 2, we prove the main theorem governing the modular arithmetic algorithm proposed for experimental results. Elliptic curves are of great importance and have their applications in cryptography and integer factorization. Various applications may be found in [2, ch. 7]. Therefore, a greater attention has been given to the Diophantine equation $b_2y^2 + b_1y + b_0 = a_3x^3 + a_2x^2 + a_1x$. In Section 3, examples are used to illustrate the proof that the algorithm can succeed in obtaining an integral solution with y-coordinate, that have a known numeral system pattern to some base p.

Recently, an increasing focus on mixed polynomial-exponential Diophantine equations has been noticed [3, 6, 5]. In Section 3, and without any predefined numeral system pattern, the results are adapted with an example to find the integral solutions (X, Z) to Diophantine equations containing exponential terms: $\mathcal{A}p^{2z} + \mathcal{B}p^z + \mathcal{C} = a_3x^3 + a_2x^2 + a_1x$.

Finally, Section 4 contains our experimental results. In this section, we aim to score the success percentage of our modular arithmetic algorithm in solving Diophantine equations of the form $y^2+b_1y+b_0 = x^3$. No predefined numeral system patterns are assumed. Instead, some strategies are being suggested. Particularly, four strategies that may lead to the termination of the sequence $\{\lambda_s\}$ are proposed, tested, and their success rates are compared.

2. A Modular Arithmetic Algorithm

In this section, we consider the Diophantine equations of the form $g(y) = f(x)$, where $g(y) = \sum_{j=0}^{m} b_j y^j \in \mathbb{Z}[y]$ and $f(x) = \sum_{i=1}^{n} a_i x^i \in \mathbb{Z}[x]$. One may assume $n \geq m$ without any loss of generality. We present an empirical modular arithmetic

algorithm for obtaining positive integral solutions (X, Y) to the proposed Diophantine equations. Later on, the success rates of this algorithm are calculated.

Definition 1. For an integral solution (X, Y) to $g(y) = f(x)$ and a fixed prime number p, define

$$\ell = \left\lceil \log_p(1 + \max\{X, Y\}) \right\rceil.$$

For $s = 1, 2, \ldots, \ell$, define the unique integers $\tau_s \equiv X \pmod{p^s}$, $\gamma_s \equiv Y \pmod{p^s}$, $\alpha_s \equiv \frac{X-\tau_s}{p^s} \pmod{p}$ and $\beta_s \equiv \frac{Y-\gamma_s}{p^s} \pmod{p}$ satisfying $0 \leq \tau_s, \gamma_s < p^s$ and $0 \leq \alpha_s, \beta_s < p$.

Lemma 1. *Let $h(x) \in \mathbb{Z}[x]$ be a non-trivial polynomial with a leading coefficient not divisible by p. If $h_p(x)$ is the reduction of $h(x)$ over $\mathbb{F}_p$, then*

- *General case: If $\gcd(h_p(x), x^p - x) = 1$, then $h(\tau) \not\equiv 0 \pmod{p}$ for every $\tau \in \mathbb{Z}$.*
- *Special case: If $h(x) = 3a_3x^2 + 2a_2x + a_1$, then $h(\tau) \not\equiv 0 \pmod{p}$ for every $\tau \in \mathbb{Z}$ if and only if $\left(\frac{a_2^2 - 3a_1a_3}{p}\right) = -1$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.*

Proof. Let $\tau \in \mathbb{Z}$ and $\bar{\tau}$ be its image in $\mathbb{F}_p$. Assume $h(\tau) \equiv 0 \pmod{p}$, then $(x - \bar{\tau}) \,|\, h_p(x)$. On the other hand, from Fermat's little theorem, $\bar{\tau}^p - \bar{\tau} = 0$, so $(x - \bar{\tau}) \,|\, (x^p - x)$. Thus $h(\tau) \not\equiv 0 \pmod{p}$ since otherwise the coprimality of $h_p(x)$ and $x^p - x$ is contradicted. In fact, if $\gcd(h_p(x), x^p - x) = 1$, then $h_p(x)$ is irreducible over $\mathbb{F}_p$ or a product of irreducible factors each of degree at least 2.

Consider the special case of $h(x) = 3a_3x^2 + 2a_2x + a_1$ with $p \nmid 3a_3$. If $\left(\frac{a_2^2 - 3a_1a_3}{p}\right) \neq -1$, then there exists $\eta \in \mathbb{Z}$ such that $\eta^2 \equiv a_2^2 - 3a_1a_3 \pmod{p}$. By direct substitution, one sees that $h(\tau) \equiv 0 \pmod{p}$, for any $\tau \in \mathbb{Z}$ such that $\tau \equiv (\eta - a_2)(3a_3)^{-1} \pmod{p}$. This contradicts $h(\tau) \not\equiv 0 \pmod{p}$ for every $\tau \in \mathbb{Z}$. Conversely, if there exists $\tau \in \mathbb{Z}$ that satisfies $h(\tau) \equiv 0 \pmod{p}$ and $\left(\frac{a_2^2 - 3a_1a_3}{p}\right) = -1$, then, using $(3a_3\tau + a_2)^2 \equiv a_2^2 - 3a_1a_3 \pmod{p}$, a contradiction follows since

$$-1 = \left(\frac{a_2^2 - 3a_1a_3}{p}\right) = \left(\frac{(3a_3\tau + a_2)^2}{p}\right) = \left(\frac{3a_3\tau + a_2}{p}\right)^2 \neq -1.$$

□

Theorem 1. *Let (X, Y) be a positive integral solution to $g(y) = f(x)$. If p is a prime such that $\gcd(f_p'(x), x^p - x) = 1$, then*

$$\alpha_s \equiv (\beta_s g'(\gamma_1) + \lambda_s)(f'(\tau_1))^{-1} \pmod{p};\ s = 1, 2, \ldots, \ell, \tag{1}$$

where the integers λ_s are determined such that

$$\lambda_1 = \frac{1}{p}(g(\gamma_1) - f(\tau_1)) \quad \text{and} \quad \lambda_{s+1} = \frac{1}{p}(\lambda_s + N_s(\tau_s, \alpha_s, \gamma_s, \beta_s)), \tag{2}$$

for some integer valued function $N_s(\tau_s, \alpha_s, \beta_s, \gamma_s)$. *Moreover,* (X, Y) *is obtained once the sequence* $\{\lambda_s\}$ *terminates.*

Proof. From Definition 1, $\alpha_s \equiv \frac{X-\tau_s}{p^s} \pmod p$ implies that $X \equiv \tau_s + \alpha_s p^s \pmod{p^{s+1}}$. Also, $X \equiv \tau_{s+1} \pmod{p^{s+1}}$. Thus $\tau_{s+1} \equiv \tau_s + \alpha_s p^s \pmod{p^{s+1}}$. Since $0 \le \tau_{s+1} < p^{s+1}$ and $0 \le \tau_s + \alpha_s p^s < p^s + \alpha_s p^s = p^s(\alpha_s + 1) \le p^s p = p^{s+1}$, then $\tau_{s+1} = \tau_s + \alpha_s p^s$. Similarly, $\gamma_{s+1} = \gamma_s + \beta_s p^s$. Therefore

$$X = \tau_1 + \sum_{\jmath=1}^{\ell} \alpha_\jmath p^\jmath \quad = \tau_s + \alpha_s p^s + p^{s+1} \sum_{\jmath=s+1}^{\ell} \alpha_\jmath p^{\jmath-s-1} = \tau_{s+1} + p^{s+1} \sum_{\jmath=s+1}^{\ell} \alpha_\jmath p^{\jmath-s-1}$$

$$Y = \gamma_1 + \sum_{\jmath=1}^{\ell} \beta_\jmath p^\jmath \quad = \gamma_s + \beta_s p^s + p^{s+1} \sum_{\jmath=s+1}^{\ell} \beta_\jmath p^{\jmath-s-1} = \gamma_{s+1} + p^{s+1} \sum_{\jmath=s+1}^{\ell} \beta_\jmath p^{\jmath-s-1}$$

is an integral solution to $g(y) = f(x)$.

For $s = 1, 2, \ldots, \ell$, let $g(\gamma_s) - f(\tau_s) = p^s \lambda_s$ for some integer λ_s. Then

$$\begin{aligned}
p^{s+1}\lambda_{s+1} &= g(\gamma_s + \beta_s p^s) - f(\tau_s + \alpha_s p^s) \\
&= b_0 + \sum_{j=1}^{m} b_j(\gamma_s + \beta_s p^s)^j - \sum_{i=1}^{n} a_i(\tau_s + \alpha_s p^s)^i \\
&= b_0 + \sum_{j=1}^{m} b_j\Big(\gamma_s^j + \sum_{\nu=1}^{j} \big(\binom{j}{\nu}\gamma_s^{j-\nu}\beta_s^\nu p^{\nu s}\big)\Big) - \sum_{i=1}^{n} a_i\Big(\tau_s^i + \sum_{\mu=1}^{i} \big(\binom{i}{\mu}\tau_s^{i-\mu}\alpha_s^\mu p^{\mu s}\big)\Big) \\
&= g(\gamma_s) + \sum_{j=1}^{m} b_j\Big(\sum_{\nu=1}^{j} \big(\binom{j}{\nu}\gamma_s^{j-\nu}\beta_s^\nu p^{\nu s}\big)\Big) - f(\tau_s) - \sum_{i=1}^{n} a_i\Big(\sum_{\mu=1}^{i} \big(\binom{i}{\mu}\tau_s^{i-\mu}\alpha_s^\mu p^{\mu s}\big)\Big) \\
&= p^s\lambda_s + \sum_{j=1}^{m}\sum_{\nu=1}^{j} \big(b_j\binom{j}{\nu}\gamma_s^{j-\nu}\beta_s^\nu p^{\nu s}\big) - \sum_{i=1}^{n}\sum_{\mu=1}^{i} \big(a_i\binom{i}{\mu}\tau_s^{i-\mu}\alpha_s^\mu p^{\mu s}\big) \\
&= p^s\lambda_s + \sum_{\nu=1}^{m}\sum_{j=\nu}^{m} \big(b_j\binom{j}{\nu}\gamma_s^{j-\nu}\beta_s^\nu p^{\nu s}\big) - \sum_{\mu=1}^{n}\sum_{i=\mu}^{n} \big(a_i\binom{i}{\mu}\tau_s^{i-\mu}\alpha_s^\mu p^{\mu s}\big) \\
&= p^s\lambda_s + \sum_{\nu=1}^{m} \frac{\beta_s^\nu p^{\nu s}}{\nu!}\sum_{j=\nu}^{m} \big({b_j}^j P_\nu \gamma_s^{j-\nu}\big) - \sum_{\mu=1}^{n} \frac{\alpha_s^\mu p^{\mu s}}{\mu!}\sum_{i=\mu}^{n} \big({a_i}^i P_\mu \tau_s^{i-\mu}\big) \\
&= p^s\lambda_s + \sum_{\nu=1}^{m} \frac{\beta_s^\nu p^{\nu s}}{\nu!} g^{(\nu)}(\gamma_s) - \sum_{\mu=1}^{n} \frac{\alpha_s^\mu p^{\mu s}}{\mu!} f^{(\mu)}(\tau_s) \\
&= p^s\lambda_s + \beta_s p^s g'(\gamma_s) - \alpha_s p^s f'(\tau_s) + \sum_{\nu=2}^{m} \frac{\beta_s^\nu p^{\nu s}}{\nu!} g^{(\nu)}(\gamma_s) - \sum_{\mu=2}^{n} \frac{\alpha_s^\mu p^{\mu s}}{\mu!} f^{(\mu)}(\tau_s) \\
&= p^s\lambda_s + \beta_s p^s g'(\gamma_s) - \alpha_s p^s f'(\tau_s) + p^{2s}\left(\sum_{\nu=2}^{m} \frac{\beta_s^\nu p^{(\nu-2)s}}{\nu!} g^{(\nu)}(\gamma_s) - \sum_{\mu=2}^{n} \frac{\alpha_s^\mu p^{(\mu-2)s}}{\mu!} f^{(\mu)}(\tau_s)\right).
\end{aligned}$$

Dividing both sides by p^s, we get

$$\begin{aligned} p\lambda_{s+1} &= \lambda_s + \beta_s g'(\gamma_s) - \alpha_s f'(\tau_s) + p^s \left(\sum_{\nu=2}^{m} \frac{\beta_s^\nu p^{(\nu-2)s}}{\nu!} g^{(\nu)}(\gamma_s) - \sum_{\mu=2}^{n} \frac{\alpha_s^\mu p^{(\mu-2)s}}{\mu!} f^{(\mu)}(\tau_s) \right) \\ &= \lambda_s + N_s(\tau_s, \alpha_s, \gamma_s, \beta_s). \end{aligned} \tag{3}$$

Reducing Eq. (3) modulo p and using the fact that $\tau_s \equiv \tau_1 \pmod p$ and $\gamma_s \equiv \gamma_1 \pmod p$, we get

$$\alpha_s f'(\tau_1) \equiv \beta_s g'(\gamma_1) + \lambda_s \pmod p. \tag{4}$$

Using Lemma 1 with $h(x) = f'(x)$, we have $f'(\tau_1) \not\equiv 0 \pmod p$. If $X \leq Y$, it is advantageous to write Eq. (4) as

$$\alpha_s \equiv (\beta_s g'(\gamma_1) + \lambda_s)(f'(\tau_1))^{-1} \pmod p.$$

Finally, since $\ell = \left\lceil \log_p(1 + \max\{X, Y\}) \right\rceil \geq \log_p(1 + \max\{X, Y\}) \geq \log_p(1 + X) > \log_p(X)$, then $X < p^\ell$. But $\tau_\ell \equiv X \pmod{p^\ell}$ and $0 \leq \tau_\ell < p^\ell$ implies that $\tau_\ell = X$. Similarly, $\gamma_\ell = Y$. Consequently, $p^\ell \lambda_\ell = g(\gamma_\ell) - f(\tau_\ell) = g(Y) - f(X) = 0$. Thus, an integral solution $(X, Y) = (\tau_\ell, \gamma_\ell)$ is achieved if and only if $\lambda_\ell = 0$, i.e., once the sequence $\{\lambda_s\}$ terminates. □

Corollary 1. *The Diophantine equation*

$$b_2 y^2 + b_1 y + b_0 = a_3 x^3 + a_2 x^2 + a_1 x \,;\, \left(\frac{a_2^2 - 3a_1 a_3}{p} \right) = -1 \tag{5}$$

has an integral solution $(X, Y) = (\tau_\ell, \gamma_\ell)$ if and only if $\lambda_\ell = 0$, where we have, in order,

$$b_2\gamma_1^2 + b_1\gamma_1 + b_0 \equiv a_3\tau_1^3 + a_2\tau_1^2 + a_1\tau_1 \pmod p \,;\, 0 \leq \tau_1, \gamma_1 < p \tag{6}$$

$$\lambda_1 = \frac{b_2\gamma_1^2 + b_1\gamma_1 + b_0 - (a_3\tau_1^3 + a_2\tau_1^2 + a_1\tau_1)}{p} \tag{7}$$

$$\alpha_s \equiv \big(\lambda_s + \beta_s(2b_2\gamma_1 + b_1)\big)(3a_3\tau_1^2 + 2a_2\tau_1 + a_1)^{-1} \pmod p,\ 0 \leq \alpha_s < p \tag{8}$$

$$\lambda_{s+1} = \frac{\lambda_s + \beta_s(2b_2\gamma_s + b_1) + \beta_s^2 p^s b_2 - \Big(\alpha_s(3a_3\tau_s^2 + 2a_2\tau_s + a_1) + \alpha_s^2 p^s (3a_3\tau_s + a_2) + \alpha_s^3 p^{2s} a_3\Big)}{p} \tag{9}$$

$$\tau_{s+1} = \tau_s + \alpha_s p^s \tag{10}$$

$$\gamma_{s+1} = \gamma_s + \beta_s p^s. \tag{11}$$

Proof. Let (X, Y) be an integral solution to $g(y) = b_2y^2 + b_1y + b_0 = a_3x^3 + a_2x^2 + a_1x = f(x)$. From Eq. (2),

$$\lambda_1 = \frac{g(\gamma_1) - f(\tau_1)}{p} = \frac{b_2\gamma_1^2 + b_1\gamma_1 + b_0 - (a_3\tau_1^3 + a_2\tau_1^2 + a_1\tau_1)}{p} \in \mathbb{Z}.$$

Thus $p \,|\, \big(b_2\gamma_1^2 + b_1\gamma_1 + b_0 - (a_3\tau_1^3 + a_2\tau_1^2 + a_1\tau_1)\big)$ and Eq. (6) follows.

Formal differentiation yields $f'(x) = 3a_3x^2 + 2a_2x + a_1$, $f''(x) = 6a_3x + 2a_2$, $f'''(x) = 6a_3$, $g'(y) = 2b_2y + b_1$ and $g''(y) = 2b_2$. From Lemma 1, $\big(\frac{a_2^2 - 3a_1a_3}{p}\big) = -1$ implies that $3a_3\tau_1^2 + 2a_2\tau_1 + a_1 \not\equiv 0 \pmod{p}$. Hence, Eq. (8) results from Eq. (1).

In this case, Eq. (3) becomes

$$\begin{aligned}\lambda_{s+1} &= \frac{\lambda_s + \big(\beta_s g'(\gamma_s) + \frac{p^s\beta_s^2}{2} g''(\gamma_s)\big) - \big(\alpha_s f'(\tau_s) + \frac{p^s\alpha_s^2}{2} f''(\tau_s) + \frac{p^{2s}\alpha_s^3}{6} f'''(\tau_s)\big)}{p} \\ &= \frac{\big(\lambda_s + \beta_s(2b_2\gamma_s + b_1) + \beta_s^2 p^s b_2 - (\alpha_s(3a_3\tau_s^2 + 2a_2\tau_s + a_1) + \alpha_s^2 p^s(3a_3\tau_s + a_2) + \alpha_s^3 p^{2s} a_3)\big)}{p}.\end{aligned}$$

□

As already shown above, Corollary 1 defines an appropriate algorithm to determine an integral solution to Eq. (5), equivalently $\lambda_\ell = 0$, once the integers β_s, for $1 \le s \le \ell - 1$, are predefined. In fact, if we propose an integral solution with y-coordinate possessing a known numeral system pattern to the base p, then the numbers β_s can be easily determined from this pattern. This is shown in Lemma 2 below.

3. Diophantine Equations with Exponential Terms

In this section, the algorithm defined by Corollary 1 is adapted to Diophantine equations with exponential terms. Firstly, such equations are transformed to the form (5) with a predefined numeral system pattern to the base p for Y. Secondly, the algorithm defined by Corollary 1 is properly applied.

Lemma 2. *An integral solution (X, Y) to Eq. (5) with $X \le Y = \frac{a(p^t-1)}{(p-1)}$, for an integer a such that $0 \le a < p$ and an unknown positive integer t, is achieved once $\lambda_t = 0$. Moreover, $\gamma_1 = \beta_s = a$ for $1 \le s < t$.*

Proof. Assume an integral solution with $X \le Y = \frac{a(p^t-1)}{(p-1)}$, then

$$\begin{aligned}\ell &= \big\lceil \log_p(1 + \max\{X, Y\}) \big\rceil = \big\lceil \log_p(1 + Y) \big\rceil = \left\lceil \log_p(1 + \frac{a(p^t - 1)}{(p-1)}) \right\rceil \\ &\le \left\lceil \log_p(1 + \frac{(p-1)(p^t-1)}{(p-1)}) \right\rceil = \big\lceil \log_p(p^t) \big\rceil = t.\end{aligned}$$

Moreover, since $\gamma_\ell \equiv Y \pmod{p^\ell} \equiv \frac{a(p^t-1)}{(p-1)} \pmod{p^\ell} \equiv \sum_{\jmath=0}^{t-1} ap^\jmath \pmod{p^\ell} \equiv \sum_{\jmath=0}^{\ell-1} ap^\jmath \pmod{p^\ell}$ and $0 \le \gamma_\ell, \sum_{\jmath=0}^{\ell-1} ap^\jmath < p^\ell$, then $\gamma_\ell = \sum_{\jmath=0}^{\ell-1} ap^\jmath$.

Assume $\ell \leq t-1$. From Corollary 1 and using $0 = \lambda_\ell = g(\gamma_\ell) - f(\tau_\ell)$, we get the following contradiction

$$Y = \gamma_\ell = \sum_{\jmath=0}^{\ell-1} ap^\jmath \leq \sum_{\jmath=0}^{t-2} ap^\jmath < ap^{t-1} + \sum_{\jmath=0}^{t-2} ap^\jmath = \sum_{\jmath=0}^{t-1} ap^\jmath = \frac{a(p^t-1)}{(p-1)} = Y.$$

Thus $\ell = t$ and the integral solution is achieved once $\lambda_\ell = \lambda_t = 0$.

For $1 \leq s < t$, from Definition 1, since $\gamma_s \equiv Y \equiv \frac{a(p^t-1)}{(p-1)} \equiv \frac{a(p^s-1)}{(p-1)} \pmod{p^s}$ and $1 \leq \gamma_s < p^s$, then $\gamma_s = \frac{a(p^s-1)}{(p-1)}$. Thus $\gamma_1 = a$. Also, since $\beta_s \equiv \frac{\frac{a(p^t-1)}{(p-1)} - \gamma_s}{p^s} \equiv \frac{\frac{a(p^t-1)}{(p-1)} - \frac{a(p^s-1)}{(p-1)}}{p^s} \equiv \frac{a(p^{t-1}+p^{t-2}+\cdots+p^s)}{p^s} \equiv a(p^{t-s-1} + \cdots + p + 1) \equiv a \pmod{p}$ and $1 \leq a, \beta_s < p$, then $\beta_s = a$. □

Example 1. Consider an integral solution to the equation

$$y^2 - 1230000y + 494359 = x^3 - 456000x^2 - 654000x$$

with a y-coordinate of the form $\frac{7^t-1}{2}$. From Lemma 1, $f'(\tau_1) \not\equiv 0 \pmod{p}$ since

$$\left(\frac{(456000)^2 + 3(654000)}{7}\right) = \left(\frac{(6)^2 + 3(4)}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

However, it is enough to check that $f'(\tau_1) \not\equiv 0 \pmod{7}$, where $0 \leq \tau_1 < 7$ is chosen to satisfy Eq. (6). Since $Y = \frac{7^t-1}{2} = 3\sum_{\jmath=0}^{t-1} 7^\jmath$, then $a = \gamma_1 = \beta_s = 3$ and Eq. (6) reduces to

$$\tau_1^3 + \tau_1^2 + 3\tau_1 \equiv 1 \pmod{7}.$$

It is easily seen that $\tau_1 = 4$ and $f'(4) \equiv 3 \not\equiv 0 \pmod{7}$. From Eq. (7), $\lambda_1 = 959472$. Now, equations (8), (9), (10) and (11) are

$$\alpha_s \equiv (5\lambda_s + 6\beta_s) \pmod{7}$$

$$\lambda_{s+1} = \frac{\lambda_s + \beta_s(2\gamma_s - 1230000) + \beta_s^2 7^s - \left(\alpha_s(3\tau_s^2 - 912000\tau_s - 654000) + \alpha_s^2 7^s(3\tau_s - 456000) + \alpha_s^3 7^{2s}\right)}{7}$$

$$\tau_{s+1} = \tau_s + \alpha_s 7^s$$

$$\gamma_{s+1} = \gamma_s + \beta_s 7^s.$$

Calculations are summarized in Table 1. From Lemma 2, the integral solution is $(\tau_{11}, \gamma_{11}) = (1169620, 988663371)$ since $\lambda_{11} = 0$.

Theorem 2. *An integral solution to*

$$\mathcal{A}p^{2z} + \mathcal{B}p^z + \mathcal{C} = a_3x^3 + a_2x^2 + a_1x\,;\ \left(\frac{a_2^2 - 3a_1a_3}{p}\right) = -1 \tag{12}$$

is $(X, Z) = (\tau_Z, Z)$. *It is obtained once* $\lambda_Z = 0$ *using Eqs.* (7), (8), (9), (10) *and* (11) *with* $b_2 = \mathcal{A}$, $b_1 = 2\mathcal{A} + \mathcal{B}$, $b_0 = \mathcal{A} + \mathcal{B} + \mathcal{C}$, $\gamma_1 = \beta_s = p-1$ *for* $1 \leq s < Z$ *and* τ_1 *is such that* $a_3\tau_1^3 + a_2\tau_1^2 + a_1\tau_1 \equiv \mathcal{C}$ *(mod* p*).*

s	γ_s	τ_s	λ_s	β_s	α_s	s	γ_s	τ_s	λ_s	β_s	α_s
1	3	4	959472	3	5	7	411771	346077	15986158669	3	1
2	24	39	14081584	3	6	8	2882400	1169620	-169343996841	3	0
3	171	333	147336541	3	0	9	20176803	1169620	-24182644176	3	0
4	1200	333	20521522	3	4	10	141237624	1169620	-3386012985	3	0
5	8403	9937	2620471545	3	6	11	**988663371**	**1169620**	0		
6	58824	110779	36010090404	3	2						

Table 1: Calculations for finding an integral solution to $y^2 - 1230000y + 494359 = x^3 - 456000x^2 - 654000x$.

Proof. We have (X, Z) is an integral solution to Eq. (12) if and only if $\mathcal{A}p^{2Z} + \mathcal{B}p^Z + \mathcal{C} = a_3X^3 + a_2X^2 + a_1X$. The latter is true if and only if $\mathcal{A}(p^Z - 1)^2 + (2\mathcal{A} + \mathcal{B})(p^Z - 1) + \mathcal{A} + \mathcal{B} + \mathcal{C} = a_3X^3 + a_2X^2 + a_1X$. Equivalently, (X, Y) is an integral solution to Eq. (5) with $Y = p^Z - 1 = (p-1)\sum_{j=0}^{Z-1} p^j$. From Lemma 2 and Corollary 1, this solution is achieved once $\lambda_\ell = \lambda_Z = 0$. Hence, $X = \tau_\ell = \tau_Z$.

Comparing Y with the form in Lemma 2, we deduce that $\gamma_1 = \beta_s = p - 1$ for $s = 1, 2, \ldots, Z-1$. Finally, Eq. (6) with $\gamma_1 = p-1$ reduces to $a_3\tau_1^3 + a_2\tau_1^2 + a_1\tau_1 \equiv \mathcal{C} \pmod{p}$. □

Remark 1.

1. The condition $\left(\frac{a_2^2 - 3a_1a_3}{p}\right) = -1$ in Corollary 1 and Theorem 2 is sufficient but not necessary for $f'(\tau_1) \not\equiv 0 \pmod{p}$, where τ_1 is a solution to Eq. (6).

2. The equations can be modified to find an integral solution (X, Z) to $\mathcal{A}n^{2z} + \mathcal{B}n^z + \mathcal{C} = a_3x^3 + a_2x^2 + a_1x$, where n is any positive integer. In particular, (X, Z) is an integral solution if and only if (X, Y) is an integral solution to Eq. (5), with $b_2 = \mathcal{A}$, $b_1 = 2\mathcal{A} + \mathcal{B}$, $b_0 = \mathcal{A} + \mathcal{B} + \mathcal{C}$ and
$$Y = n^Z - 1 = (n-1)\sum_{j=0}^{Z-1} n^j.$$
Equations (7), (9), (10) and (11) are to be modified by replacing p by n. Moreover, calculations in Eqs. (6) and (8) are carried over the ring $\mathbb{Z}/n\mathbb{Z}$. Once $\lambda_\ell = 0$, the integral solution is $X = \tau_\ell$ and $Z = \ell$.

3. Using Theorem 1, Theorem 2 may be generalized to Diophantine equations of the form $g(p^z) = f(x)$.

Example 2. Consider an integral solution to the equation
$$11^{2z} - 1598326 = x^3 + 2x^2 - 1304290x.$$
Equivalently, from Theorem 2, the algorithm of Corollary 1 is applied to $y^2 + 2y - 1598325 = x^3 + 2x^2 - 1304290x$ with $Y = 11^Z - 1$. Calculations are summarized in Table 2. Since $\lambda_{10} = 0$, an integral solution is $X = \tau_{10} = 8762295$ and $Z = \ell = 10$.

s	γ_s	τ_s	λ_s	β_s	α_s	s	γ_s	τ_s	λ_s	β_s	α_s
1	10	3	210420	10	7	6	1771560	1676051	-2657697847388	10	4
2	120	80	844915	10	2	7	19487170	8762295	-34522692656760	10	0
3	1330	322	290429	10	5	8	214358880	8762295	-3138214017840	10	0
4	14640	6977	-22567766	10	4	9	2357947690	8762295	-282953722920	10	0
5	161050	65541	-1747499718	10	10	10	**25937424600**	**8762295**	0		

Table 2: Calculations for finding an integral solution to $11^{2z} - 1598326 = x^3 + 2x^2 - 1304290x$.

4. Four Strategies and Experimental Results

As mentioned above, no general algorithm is suitable for solving all Diophantine equations. However, in Corollary 1, we showed a modular arithmetic algorithm that succeeded with all Diophantine equations (5) that have a predefined numeral system pattern for Y. Also, by Theorem 2, the algorithm succeeded in solving all mixed polynomial-exponential Diophantine equations (12). As we mentioned earlier, our aim is to test a special algorithm by applying it on general form Diophantine equations. Hence, the polynomial-type Diophantine equations (5) should be considered without any known numeral system pattern. However, to achieve an integral solution, some data seem to be missing. The missing data can be dealt with in a variety of methods that lead to comparing success rates on a sample of Diophantine equations.

An integral solution to Eq. (5) is achieved once $\lambda_\ell = 0$, where the sequence $\{\lambda_s\}$ is determined by Eqs. (7) and (9). However, the termination of the sequence depends on the choices of β_s and α_s, for $1 \leq s < \ell$. Moreover, Eq. (8) is a linear relation between β_s and α_s. Therefore, the missing data for achieving an integral solution can be handled by suggesting some strategies. A good strategy is the one that predicts the values of β_s and α_s, with respecting Eq. (8), so that the sequence $\{\lambda_s\}$ terminates.

Since we are proposing a comparison for success rates, some strategies that may lead to an integral solution to Eq. (5) are suggested. In fact, many strategies may be planned for the goal of $\lambda_\ell = 0$. However, for comparison purposes, we propose only four strategies that may suit some special Diophantine equations in the form of (5). Furthermore, the success percentages of these strategies, in achieving an integral solution, are computed and compared.

Strategies are suggested for Diophantine equations (5) satisfying the following conditions:

1. $b_2, b_1, a_3, a_2, a_1 \geq 0$.
2. b_1 is odd.
3. X is even if a_1 is odd.

4. X is odd if $a_3 + a_1$ is odd.

With these conditions and for $p = 2$, Eq. (8) has the form

$$\alpha_s + \beta_s \equiv \lambda_s \pmod 2 \,;\, \alpha_s, \beta_s \in \{0, 1\}. \tag{13}$$

Moreover, equations (7) and (9), used in determining the sequence $\{\lambda_s\}_{s=1}^{\ell}$, have the following forms:

$$\lambda_1 = \frac{\gamma_1(b_2 + b_1) + b_0 - \tau_1(a_3 + a_2 + a_1)}{2}$$

$$\lambda_{s+1} = \frac{\lambda_s + \beta_s\big(b_2(2\gamma_s + 2^s) + b_1\big) - \alpha_s\big(a_3(3\tau_s^2 + 3\tau_s 2^s + 2^{2s}) + a_2(2\tau_s + 2^s) + a_1\big)}{2}.$$

From Corollary 1, (τ_ℓ, γ_ℓ) is an integral solution if and only if $\lambda_\ell = 0$. For this goal, some strategies may be designed depending on the sign and magnitude of λ_s of the current step and previous steps as well. However, we propose strategies depending only on the sign of the current step λ_s as follows:

- **Strategy 1:**
  - If $\lambda_s > 0$, set $\beta_s = 0$ and evaluate α_s using Eq. (13).
  - If $\lambda_s < 0$, set $\beta_s = 1$ and evaluate α_s using Eq. (13).
- **Strategy 2:**
  - If $\lambda_s > 0$, set $\alpha_s = 1$ and evaluate β_s using Eq. (13).
  - If $\lambda_s < 0$, set $\alpha_s = 0$ and evaluate β_s using Eq. (13).
- **Strategy 3:**
  - If $\lambda_s > 0$, set $\beta_s = 0$ and evaluate α_s using Eq. (13).
  - If $\lambda_s < 0$, set $\alpha_s = 0$ and evaluate β_s using Eq. (13).
- **Strategy 4:**
  - If $\lambda_s > 0$, set $\alpha_s = 1$ and evaluate β_s using Eq. (13).
  - If $\lambda_s < 0$, set $\beta_s = 1$ and evaluate α_s using Eq. (13).

Example 3. Consider an integral solution to $y^2 + y + 1981675 = x^3 + 2x$. Clearly, the x-coordinate should be odd, i.e., $X \equiv \tau_1 \equiv 1 \pmod 2$. If a solution is intended with odd y-coordinate, i.e., $Y \equiv \gamma_1 \equiv 1 \pmod 2$, Strategy 2 leads to the integral solution $(2175, 101425)$. Calculations are summarized in Table 3, where $\lambda_{17} = 0$ is observed and the integral solution is deduced immediately.

s	γ_s	τ_s	λ_s	β_s	α_s	s	γ_s	τ_s	λ_s	β_s	α_s
1	1	1	990837	0	1	10	49	127	-63	1	0
2	1	3	495411	0	1	11	1073	127	530	1	1
3	1	7	247665	0	1	12	3121	2175	-2509128	0	0
4	1	15	123642	1	1	13	3121	2175	-1254564	0	0
5	17	31	61004	1	1	14	3121	2175	-627282	0	0
6	49	63	27093	0	1	15	3121	2175	-313641	1	0
7	49	127	-504	0	0	16	35889	2175	-137315	1	0
8	49	127	-252	0	0	17	**101425**	**2175**	0		
9	49	127	-126	0	0						

Table 3: Calculations for finding an integral solution to $y^2 + y + 1981675 = x^3 + 2x$ using Strategy 2.

Over a sample of Diophantine equations, we aim to compare the success percentage of each strategy in obtaining integral solutions. Recently, Diophantine equations with integral solutions of less than 10 digits are not of any interest, as these kinds of equations can be solved, almost immediately, with a trivial brute force search. However, for comparison purposes, the chosen random sample of Diophantine equations does not need to have large integral solutions. The random sample consists of some Diophantine equations of the form $y^2 + b_1 y + b_0 = x^3$ that have integral solutions with odd X, $b_1 = 1, 3, 5$ and $|b_0| < 10000$. Precisely, the sample consists of all the Diophantine equations that have been solved successfully through at least one of the four strategies. The coefficients b_1 and b_0 of each equation are listed in Table 4. Moreover, the integral solution and the effective strategies are recorded next to each equation.

In Table 5, we evaluate the ratios of the number of equations solved successfully by each strategy compared to the total number of tested equations, for $b_1 = 1, 3$ and 5. It was observed that strategies 1, 2, 3 and 4 succeeded to solve 32.5%, 65%, 55% and 39% of the listed equations, respectively.

b_1	b_0	(X, Y)	**Strg**	b_1	b_0	(X, Y)	**Strg**	b_1	b_0	(X, Y)	**Strg**
1	-9899	(1,99)	2,3	3	-9897	(1,98)	2,3	5	-9905	(19,127)	1,4
1	-9701	(1,98)	2,3	3	-9699	(1,97)	2,3	5	-9893	(1,97)	2,3
1	-9505	(1,97)	2,3	3	-9651	(19,127)	1,4	5	-9695	(1,96)	2,3
1	-9397	(19,127)	1,4	3	-9503	(1,96)	2,3	5	-9647	(19,126)	1,4
1	-9311	(1,96)	2,3	3	-9395	(19,126)	1,4	5	-9499	(1,95)	2,3
1	-9143	(19,126)	1,4	3	-9309	(1,95)	2,3	5	-9305	(1,94)	2,3
1	-9119	(1,95)	2,3	3	-9117	(1,94)	2,3	5	-9113	(1,93)	2,3
1	-8929	(1,94)	2,3	3	-8927	(1,93)	2,3	5	-8923	(1,92)	2,3
1	-8741	(1,93)	2,3	3	-8739	(1,92)	2,3	5	-8735	(1,91)	2,3
1	-8555	(1,92)	2,3	3	-8553	(1,91)	2,3	5	-8549	(1,90)	2,3
1	-8371	(1,91)	2,3	3	-8369	(1,90)	2,3	5	-8365	(1,89)	2,3
1	-8189	(1,90)	2,3	3	-8187	(1,89)	2,3	5	-8183	(1,88)	2,3
1	-8009	(1,89)	2,3	3	-8007	(1,88)	2,3	5	-8003	(1,87)	2,3
1	-7831	(1,88)	2,3	3	-7829	(1,87)	2,3	5	-7825	(1,86)	2,3
1	-7655	(1,87)	2,3	3	-7653	(1,86)	2,3	5	-7649	(1,85)	2,3
1	-7481	(1,86)	2,3	3	-7479	(1,85)	2,3	5	-7503	(21,127)	1,4
1	-7309	(1,85)	2,3	3	-7307	(1,84)	2,3	5	-7475	(1,84)	2,3
1	-7139	(1,84)	2,3	3	-7249	(21,127)	1,4	5	-7303	(1,83)	2,3

Table 4 – *Continued on next page*

Continued from previous page

b_1	b_0	(X,Y)	**Strg**	b_1	b_0	(X,Y)	**Strg**	b_1	b_0	(X,Y)	**Strg**
1	-6995	(21,127)	1,4	3	-7137	(1,83)	2,3	5	-7245	(21,126)	1,4
1	-6971	(1,83)	2,3	3	-6993	(21,126)	1,4	5	-7133	(1,82)	2,3
1	-6805	(1,82)	2,3	3	-6969	(1,82)	2,3	5	-6981	(39,255)	1,4
1	-6741	(21,126)	1,4	3	-6803	(1,81)	2,3	5	-6965	(1,81)	2,3
1	-6641	(1,81)	2,3	3	-6639	(1,80)	2,3	5	-6799	(1,80)	2,3
1	-6479	(1,80)	2,3	3	-6477	(1,79)	2,3	5	-6635	(1,79)	2,3
1	-6319	(1,79)	2,3	3	-6471	(39,255)	1,4	5	-6473	(1,78)	2,3
1	-6161	(1,78)	2,3	3	-6317	(1,78)	2,3	5	-6467	(39,254)	1,4
1	-6005	(1,77)	2,3	3	-6159	(1,77)	2,3	5	-6313	(1,77)	2,3
1	-5961	(39,255)	1,4	3	-6003	(1,76)	2,3	5	-6155	(1,76)	2,3
1	-5851	(1,76)	2,3	3	-5959	(39,254)	1,4	5	-5999	(1,75)	2,3
1	-5699	(1,75)	2,3	3	-5849	(1,75)	2,3	5	-5845	(1,74)	2,3
1	-5549	(1,74)	2,3	3	-5697	(1,74)	2,3	5	-5693	(1,73)	2,3
1	-5451	(39,254)	1,4	3	-5547	(1,73)	2,3	5	-5543	(1,72)	2,3
1	-5401	(1,73)	2,3	3	-5399	(1,72)	2,3	5	-5395	(1,71)	2,3
1	-5255	(1,72)	2,3	3	-5253	(1,71)	2,3	5	-5249	(1,70)	2,3
1	-5111	(1,71)	2,3	3	-5109	(1,70)	2,3	5	-5105	(1,69)	2,3
1	-4969	(1,70)	2,3	3	-4967	(1,69)	2,3	5	-4963	(1,68)	2,3
1	-4829	(1,69)	2,3	3	-4827	(1,68)	2,3	5	-4823	(1,67)	2,3
1	-4691	(1,68)	2,3	3	-4689	(1,67)	2,3	5	-4685	(1,66)	2,3
1	-4555	(1,67)	2,3	3	-4553	(1,66)	2,3	5	-4597	(23,127)	1,4
1	-4421	(1,66)	2,3	3	-4419	(1,65)	2,3	5	-4549	(1,65)	2,3
1	-4289	(1,65)	2,3	3	-4343	(23,127)	1,4	5	-4415	(1,64)	2,3
1	-4159	(1,64)	2,3	3	-4287	(1,64)	2,3	5	-4339	(23,126)	1,4
1	-4089	(23,127)	1,4	3	-4157	(1,63)	1,2,3,4	5	-4283	(1,63)	1,2,3,4
1	-4031	(1,63)	1,2,3,4	3	-4131	(3,63)	1,4	5	-4257	(3,63)	1,4
1	-4005	(3,63)	1,4	3	-4087	(23,126)	1,4	5	-4159	(5,63)	1,4
1	-3907	(5,63)	1,4	3	-4033	(5,63)	1,4	5	-4153	(1,62)	1,2,3,4
1	-3905	(1,62)	1,2,3,4	3	-4029	(1,62)	1,2,3,4	5	-4127	(3,62)	1,4
1	-3879	(3,62)	1,4	3	-4003	(3,62)	1,4	5	-4029	(5,62)	1,4
1	-3835	(23,126)	1,4	3	-3905	(5,62)	1,4	5	-4025	(1,61)	2,3
1	-3781	(5,62)	1,4	3	-3903	(1,61)	2,3	5	-3941	(7,63)	1,4
1	-3781	(1,61)	2,3	3	-3815	(7,63)	1,4	5	-3899	(1,60)	2,3
1	-3689	(7,63)	1,4	3	-3779	(1,60)	2,3	5	-3811	(7,62)	1,4
1	-3659	(1,60)	2,3	3	-3687	(7,62)	1,4	5	-3775	(1,59)	2,3
1	-3563	(7,62)	1,4	3	-3657	(1,59)	2,3	5	-3653	(1,58)	2,3
1	-3539	(1,59)	2,3	3	-3537	(1,58)	2,3	5	-3555	(9,63)	1,4
1	-3421	(1,58)	2,3	3	-3429	(9,63)	1,4	5	-3533	(1,57)	2,3
1	-3305	(1,57)	2,3	3	-3419	(1,57)	2,3	5	-3425	(9,62)	1,4
1	-3303	(9,63)	1,4	3	-3303	(1,56)	2,3	5	-3415	(1,56)	2,3
1	-3191	(1,56)	2,3	3	-3301	(9,62)	1,4	5	-3299	(1,55)	2,3
1	-3177	(9,62)	1,4	3	-3189	(1,55)	2,3	5	-3185	(1,54)	2,3
1	-3079	(1,55)	2,3	3	-3077	(1,54)	2,3	5	-3073	(1,53)	2,3
1	-2969	(1,54)	2,3	3	-2967	(1,53)	2,3	5	-2963	(1,52)	2,3
1	-2861	(1,53)	2,3	3	-2859	(1,52)	2,3	5	-2953	(11,63)	1,4
1	-2755	(1,52)	2,3	3	-2827	(11,63)	1,4	5	-2855	(1,51)	2,3
1	-2701	(11,63)	1,4	3	-2753	(1,51)	2,3	5	-2823	(11,62)	1,4
1	-2651	(1,51)	2,3	3	-2699	(11,62)	1,4	5	-2749	(1,50)	2,3
1	-2575	(11,62)	1,4	3	-2649	(1,50)	2,3	5	-2645	(1,49)	2,3
1	-2549	(1,50)	2,3	3	-2547	(1,49)	2,3	5	-2543	(1,48)	2,3
1	-2449	(1,49)	2,3	3	-2447	(1,48)	2,3	5	-2443	(1,47)	2,3
1	-2351	(1,48)	2,3	3	-2349	(1,47)	2,3	5	-2345	(1,46)	2,3
1	-2255	(1,47)	2,3	3	-2253	(1,46)	2,3	5	-2249	(1,45)	2,3
1	-2161	(1,46)	2,3	3	-2159	(1,45)	2,3	5	-2155	(1,44)	2,3
1	-2069	(1,45)	2,3	3	-2067	(1,44)	2,3	5	-2087	(13,63)	1,4
1	-1979	(1,44)	2,3	3	-1977	(1,43)	2,3	5	-2063	(1,43)	2,3
1	-1891	(1,43)	2,3	3	-1961	(13,63)	1,4	5	-1973	(1,42)	2,3
1	-1835	(13,63)	1,4	3	-1889	(1,42)	2,3	5	-1957	(13,62)	1,4
1	-1805	(1,42)	2,3	3	-1833	(13,62)	1,4	5	-1885	(1,41)	2,3
1	-1721	(1,41)	2,3	3	-1803	(1,41)	2,3	5	-1799	(1,40)	2,3
1	-1709	(13,62)	1,4	3	-1719	(1,40)	2,3	5	-1715	(1,39)	2,3
1	-1639	(1,40)	2,3	3	-1637	(1,39)	2,3	5	-1633	(1,38)	2,3
1	-1559	(1,39)	2,3	3	-1557	(1,38)	2,3	5	-1553	(1,37)	2,3
1	-1481	(1,38)	2,3	3	-1479	(1,37)	2,3	5	-1475	(1,36)	2,3
1	-1405	(1,37)	2,3	3	-1403	(1,36)	2,3	5	-1399	(1,35)	2,3
1	-1331	(1,36)	2,3	3	-1329	(1,35)	2,3	5	-1325	(1,34)	2,3
1	-1259	(1,35)	2,3	3	-1257	(1,34)	2,3	5	-1253	(1,33)	2,3
1	-1189	(1,34)	2,3	3	-1187	(1,33)	2,3	5	-1183	(1,32)	2,3
1	-1121	(1,33)	2,3	3	-1119	(1,32)	2,3	5	-1139	(25,127)	1,4
1	-1055	(1,32)	2,3	3	-1053	(1,31)	1,2,3,4	5	-1115	(1,31)	1,2,3,4
1	-991	(1,31)	1,2,3,4	3	-1027	(3,31)	1,4	5	-1089	(3,31)	1,4
1	-965	(3,31)	1,4	3	-989	(1,30)	1,2,3,4	5	-1049	(1,30)	1,2,3,4
1	-929	(1,30)	1,2,3,4	3	-963	(3,30)	1,4	5	-1023	(3,30)	1,4
1	-903	(3,30)	1,4	3	-929	(5,31)	1,4	5	-991	(5,31)	1,4
1	-869	(1,29)	2,3	3	-927	(1,29)	2,3	5	-985	(1,29)	2,3
1	-867	(5,31)	1,4	3	-885	(25,127)	1,4	5	-925	(5,30)	1,4
1	-811	(1,28)	2,3	3	-867	(1,28)	2,3	5	-923	(1,28)	2,3
1	-805	(5,30)	1,4	3	-865	(5,30)	1,4	5	-909	(15,63)	1,4
1	-755	(1,27)	2,3	3	-809	(1,27)	2,3	5	-881	(25,126)	1,4
1	-735	(33,191)	2	3	-783	(15,63)	1,4	5	-863	(1,27)	2,3
1	-701	(1,26)	2,3	3	-753	(1,26)	2,3	5	-805	(1,26)	2,3
1	-657	(15,63)	1,4	3	-733	(33,190)	2	5	-779	(15,62)	1,4
1	-649	(7,31)	1,4	3	-711	(7,31)	1,4	5	-773	(7,31)	1,4
1	-649	(1,25)	2,3	3	-699	(1,25)	2,3	5	-749	(1,25)	2,3

Table 4 – *Continued on next page*

Continued from previous page

b_1	b_0	(X,Y)	**Strg**	b_1	b_0	(X,Y)	**Strg**	b_1	b_0	(X,Y)	**Strg**
1	-631	(25,127)	1,4	3	-655	(15,62)	1,4	5	-729	(33,189)	2
1	-599	(1,24)	2,3	3	-647	(7,30)	1,4	5	-707	(7,30)	1,4
1	-587	(7,30)	1,4	3	-647	(1,24)	2,3	5	-695	(1,24)	2,3
1	-551	(1,23)	2,3	3	-629	(25,126)	1,4	5	-643	(1,23)	2,3
1	-531	(15,62)	1,4	3	-597	(1,23)	2,3	5	-593	(1,22)	2,3
1	-505	(1,22)	2,3	3	-549	(1,22)	2,3	5	-545	(1,21)	2,3
1	-461	(1,21)	2,3	3	-503	(1,21)	2,3	5	-499	(1,20)	2,3
1	-419	(1,20)	2,3	3	-459	(1,20)	2,3	5	-455	(1,19)	2,3
1	-379	(1,19)	2,3	3	-417	(1,19)	2,3	5	-413	(1,18)	2,3
1	-377	(25,126)	1,4	3	-377	(1,18)	2,3	5	-387	(9,31)	1,4
1	-353	(33,190)	2	3	-351	(33,189)	2	5	-373	(1,17)	2,3
1	-341	(1,18)	2,3	3	-339	(1,17)	2,3	5	-347	(33,188)	2
1	-305	(1,17)	2,3	3	-325	(9,31)	1,4	5	-335	(1,16)	2,3
1	-271	(1,16)	2,3	3	-303	(1,16)	2,3	5	-321	(9,30)	1,4
1	-263	(9,31)	1,4	3	-269	(1,15)	1,2,3,4	5	-299	(1,15)	1,2,3,4
1	-239	(1,15)	1,2,3,4	3	-261	(9,30)	1,4	5	-273	(3,15)	1,4
1	-213	(3,15)	1,4	3	-243	(3,15)	1,4	5	-265	(1,14)	1,2,3,4
1	-209	(1,14)	1,2,3,4	3	-237	(1,14)	1,2,3,4	5	-239	(3,14)	1,4
1	-201	(9,30)	1,4	3	-211	(3,14)	1,4	5	-233	(1,13)	2,3
1	-183	(3,14)	1,4	3	-207	(1,13)	2,3	5	-203	(1,12)	2,3
1	-181	(35,207)	1	3	-179	(35,206)	1	5	-191	(37,223)	1,4
1	-181	(1,13)	2,3	3	-179	(1,12)	2,3	5	-175	(5,15)	1,4
1	-155	(1,12)	2,3	3	-153	(1,11)	2,3	5	-175	(1,11)	2,3
1	-131	(1,11)	2,3	3	-145	(5,15)	1,4	5	-149	(1,10)	2,3
1	-115	(5,15)	1,4	3	-129	(1,10)	2,3	5	-141	(5,14)	1,4
1	-109	(1,10)	2,3	3	-113	(5,14)	1,4	5	-125	(1,9)	2,3
1	-89	(1,9)	2,3	3	-107	(1,9)	2,3	5	-103	(1,8)	2,3
1	-85	(5,14)	1,4	3	-87	(1,8)	2,3	5	-83	(1,7)	1,2,3,4
1	-71	(1,8)	2,3	3	-69	(1,7)	1,2,3,4	5	-65	(1,6)	1,2,3,4
1	-55	(1,7)	1,2,3,4	3	-53	(1,6)	1,2,3,4	5	-57	(3,7)	1,4
1	-41	(1,6)	1,2,3,4	3	-43	(3,7)	1,4	5	-49	(1,5)	2,3
1	-29	(3,7)	1,4	3	-39	(1,5)	2,3	5	-39	(3,6)	1,4
1	-29	(1,5)	2,3	3	-27	(3,6)	1,4	5	-35	(1,4)	2,3
1	-19	(1,4)	2,3	3	-27	(1,4)	2,3	5	-23	(1,3)	1,2,3,4
1	-15	(3,6)	1,4	3	-17	(1,3)	1,2,3,4	5	-13	(1,2)	1,2,3,4
1	-11	(1,3)	1,2,3,4	3	-9	(1,2)	1,2,3,4	5	-5	(1,1)	1,2,3,4
1	-7	(5,11)	1,2,3,4	3	-5	(5,10)	1,2,3,4	5	-1	(5,9)	1,3
1	-5	(1,2)	1,2,3,4	3	-3	(1,1)	1,2,3,4	5	1	(1,0)	1,2,3,4
1	-1	(1,1)	1,2,3,4	3	1	(1,0)	1,2,3,4	5	3	(3,3)	2,4
1	1	(1,0)	1,2,3,4	3	9	(3,3)	2,4	5	13	(3,2)	2,4
1	7	(3,4)	1,2,3,4	3	17	(5,9)	1,3	5	21	(5,8)	1,3
1	15	(3,3)	2,4	3	17	(3,2)	2,4	5	21	(3,1)	1,2,3,4
1	21	(3,2)	2,4	3	23	(3,1)	1,2,3,4	5	27	(3,0)	1,2,3,4
1	25	(3,1)	1,2,3,4	3	27	(3,0)	1,2,3,4	5	33	(39,241)	2
1	27	(3,0)	1,2,3,4	3	29	(39,242)	2	5	43	(7,15)	2,4
1	27	(39,243)	2	3	37	(5,8)	1,3	5	77	(7,14)	2,4
1	35	(5,9)	1,3	3	39	(7,16)	2,3	5	77	(11,33)	3
1	37	(7,17)	2,3	3	71	(15,56)	1,4	5	109	(7,13)	2,4
1	53	(5,8)	1,3	3	73	(7,15)	2,4	5	119	(5,1)	1,3
1	69	(15,57)	1,4	3	105	(7,14)	2,4	5	125	(5,0)	1,3
1	71	(7,16)	2,3	3	121	(5,1)	1,3	5	139	(7,12)	2,4
1	103	(7,15)	2,4	3	125	(5,0)	1,3	5	147	(11,32)	3
1	123	(5,1)	1,3	3	135	(7,13)	2,4	5	147	(137,1601)	3
1	125	(5,0)	1,3	3	143	(11,33)	3	5	167	(7,11)	2,4
1	133	(7,14)	2,4	3	163	(7,12)	2,4	5	183	(23,107)	2,4
1	161	(7,13)	2,4	3	179	(23,108)	2,4	5	193	(7,10)	2,4
1	177	(23,109)	2,4	3	189	(7,11)	2,4	5	217	(7,9)	1,2,3,4
1	183	(15,56)	1,4	3	211	(11,32)	3	5	239	(7,8)	1,2,3,4
1	183	(135,1568)	3	3	213	(7,10)	2,4	5	259	(7,7)	2,4
1	187	(7,12)	2,4	3	235	(7,9)	1,2,3,4	5	277	(7,6)	2,4
1	209	(11,33)	3	3	255	(7,8)	1,2,3,4	5	293	(7,5)	2,4
1	211	(7,11)	2,4	3	273	(7,7)	2,4	5	301	(15,53)	2,4
1	233	(7,10)	2,4	3	289	(7,6)	2,4	5	307	(7,4)	2,4
1	253	(7,9)	1,2,3,4	3	297	(15,54)	2,4	5	319	(7,3)	2,4
1	271	(7,8)	1,2,3,4	3	303	(7,5)	2,4	5	329	(7,2)	2,4
1	275	(11,32)	3	3	315	(7,4)	2,4	5	337	(7,1)	1,2,3,4
1	287	(7,7)	2,4	3	325	(7,3)	2,4	5	343	(7,0)	1,2,3,4
1	295	(15,55)	2,4	3	333	(7,2)	2,4	5	355	(9,17)	1,3
1	301	(7,6)	2,4	3	339	(7,1)	1,2,3,4	5	363	(17,65)	3
1	313	(7,5)	2,4	3	343	(7,0)	1,2,3,4	5	393	(9,16)	1,3
1	323	(7,4)	2,4	3	389	(9,17)	1,3	5	411	(15,52)	2,4
1	331	(7,3)	2,4	3	407	(15,53)	2,4	5	497	(17,64)	3
1	337	(7,2)	2,4	3	425	(9,16)	1,3	5	519	(15,51)	2,4
1	341	(7,1)	1,2,3,4	3	493	(17,65)	3	5	553	(63,497)	1,4
1	343	(7,0)	1,2,3,4	3	515	(15,52)	2,4	5	625	(15,50)	2,4
1	405	(15,54)	2,4	3	549	(63,498)	4	5	723	(9,1)	1,3
1	423	(9,17)	1,3	3	621	(15,51)	2,4	5	729	(9,0)	1,3
1	457	(9,16)	1,3	3	625	(17,64)	3	5	729	(15,49)	1,2,3,4
1	513	(15,53)	2,4	3	725	(9,1)	1,3	5	831	(15,48)	1,2,3,4
1	547	(63,499)	4	3	725	(15,50)	2,4	5	931	(15,47)	2
1	619	(15,52)	2,4	3	729	(9,0)	1,3	5	943	(79,699)	2
1	623	(17,65)	3	3	827	(15,49)	1,2,3,4	5	943	(13,33)	3
1	723	(15,51)	2,4	3	927	(15,48)	1,2,3,4	5	957	(11,17)	1,3
1	727	(9,1)	1,3	3	939	(79,700)	2	5	995	(11,16)	1,3

Table 4 – *Continued on next page*

Continued from previous page

b_1	b_0	(X,Y)	**Strg**	b_1	b_0	(X,Y)	**Strg**	b_1	b_0	(X,Y)	**Strg**
1	729	(9,0)	1,3	3	991	(11,17)	1,3	5	1013	(13,32)	3
1	753	(17,64)	3	3	1009	(13,33)	3	5	1029	(15,46)	2
1	825	(15,50)	2,4	3	1025	(15,47)	2	5	1125	(15,45)	2
1	925	(15,49)	1,2,3,4	3	1027	(11,16)	1,3	5	1219	(15,44)	2
1	937	(79,701)	2	3	1077	(13,32)	3	5	1311	(15,43)	2
1	1023	(15,48)	1,2,3,4	3	1121	(15,46)	2	5	1325	(11,1)	1,3
1	1025	(11,17)	1,3	3	1215	(15,45)	2	5	1331	(11,0)	1,3
1	1059	(11,16)	1,3	3	1307	(15,44)	2	5	1401	(15,42)	2
1	1075	(13,33)	3	3	1327	(11,1)	1,3	5	1489	(15,41)	2
1	1119	(15,47)	2	3	1331	(11,0)	1,3	5	1551	(63,496)	1,4
1	1141	(13,32)	3	3	1397	(15,43)	2	5	1575	(15,40)	2
1	1213	(15,46)	2	3	1485	(15,42)	2	5	1587	(41,257)	3
1	1305	(15,45)	2	3	1547	(63,497)	1,4	5	1589	(77,672)	3
1	1329	(11,1)	1,3	3	1571	(15,41)	2	5	1659	(15,39)	2
1	1331	(11,0)	1,3	3	1585	(77,673)	3	5	1741	(15,38)	2
1	1395	(15,44)	2	3	1655	(15,40)	2	5	1821	(15,37)	2
1	1483	(15,43)	2	3	1737	(15,39)	2	5	1823	(13,17)	1,3
1	1545	(63,498)	4	3	1817	(15,38)	2	5	1861	(13,16)	1,3
1	1569	(15,42)	2	3	1857	(13,17)	1,3	5	1899	(15,36)	2
1	1653	(15,41)	2	3	1893	(13,16)	1,3	5	1975	(15,35)	2
1	1735	(15,40)	2	3	1895	(15,37)	2	5	2049	(15,34)	2
1	1815	(15,39)	2	3	1971	(15,36)	2	5	2105	(41,256)	3
1	1891	(13,17)	1,3	3	2045	(15,35)	2	5	2121	(15,33)	2,3
1	1893	(15,38)	2	3	2101	(41,257)	3	5	2191	(13,1)	1,3
1	1925	(13,16)	1,3	3	2117	(15,34)	2	5	2191	(15,32)	2,3
1	1969	(15,37)	2	3	2187	(15,33)	2,3	5	2197	(13,0)	1,3
1	2043	(15,36)	2	3	2193	(13,1)	1,3	5	2259	(15,31)	2,4
1	2115	(15,35)	2	3	2197	(13,0)	1,3	5	2273	(23,97)	1,3
1	2185	(15,34)	2	3	2255	(15,32)	2,3	5	2309	(19,65)	3
1	2195	(13,1)	1,3	3	2321	(15,31)	2,4	5	2325	(15,30)	2,4
1	2197	(13,0)	1,3	3	2341	(79,699)	2	5	2345	(79,698)	2
1	2253	(15,33)	2,3	3	2385	(15,30)	2,4	5	2389	(15,29)	2,4
1	2319	(15,32)	2,3	3	2439	(19,65)	3	5	2397	(27,129)	3
1	2339	(79,700)	2	3	2447	(15,29)	2,4	5	2443	(19,64)	3
1	2383	(15,31)	2,4	3	2467	(23,97)	1,3	5	2451	(15,28)	2,4
1	2445	(15,30)	2,4	3	2507	(15,28)	2,4	5	2471	(23,96)	1,3
1	2505	(15,29)	2,4	3	2543	(63,496)	1,4	5	2511	(15,27)	2,4
1	2541	(63,497)	1,4	3	2565	(15,27)	2,4	5	2569	(15,26)	2,4
1	2563	(15,28)	2,4	3	2571	(19,64)	3	5	2625	(15,25)	2,4
1	2569	(19,65)	3	3	2617	(41,256)	3	5	2659	(27,128)	3
1	2615	(41,257)	3	3	2621	(15,26)	2,4	5	2679	(15,24)	2,4
1	2619	(15,27)	2,4	3	2655	(27,129)	3	5	2731	(15,23)	2,4
1	2661	(23,97)	1,3	3	2663	(23,96)	1,3	5	2781	(15,22)	2,4
1	2673	(15,26)	2,4	3	2675	(15,25)	2,4	5	2829	(15,21)	2,4
1	2699	(19,64)	3	3	2727	(15,24)	2,4	5	2875	(15,20)	2,4
1	2725	(15,25)	2,4	3	2777	(15,23)	2,4	5	2919	(15,19)	2,4
1	2775	(15,24)	2,4	3	2825	(15,22)	2,4	5	2961	(15,18)	2,4
1	2823	(15,23)	2,4	3	2871	(15,21)	2,4	5	3001	(15,17)	1,2,3,4
1	2855	(23,96)	1,3	3	2915	(15,20)	2,4	5	3023	(47,315)	2
1	2869	(15,22)	2,4	3	2915	(27,128)	3	5	3039	(15,16)	1,2,3,4
1	2913	(15,21)	2,4	3	2957	(15,19)	2,4	5	3075	(15,15)	2,4
1	2913	(27,129)	3	3	2997	(15,18)	2,4	5	3109	(15,14)	2,4
1	2955	(15,20)	2,4	3	3019	(47,316)	2	5	3141	(15,13)	2,4
1	2995	(15,19)	2,4	3	3035	(15,17)	1,2,3,4	5	3171	(15,12)	2,4
1	3017	(47,317)	2	3	3071	(15,16)	1,2,3,4	5	3199	(15,11)	2,4
1	3033	(15,18)	2,4	3	3105	(15,15)	2,4	5	3225	(15,10)	2,4
1	3069	(15,17)	1,2,3,4	3	3137	(15,14)	2,4	5	3249	(15,9)	2,4
1	3103	(15,16)	1,2,3,4	3	3139	(539,12512)	3	5	3271	(15,8)	2,4
1	3129	(41,256)	3	3	3167	(15,13)	2,4	5	3291	(15,7)	2,4
1	3135	(15,15)	2,4	3	3195	(15,12)	2,4	5	3309	(15,6)	2,4
1	3137	(539,12513)	3	3	3221	(15,11)	2,4	5	3325	(15,5)	2,4
1	3165	(15,14)	2,4	3	3245	(15,10)	2,4	5	3339	(15,4)	2,4
1	3171	(27,128)	3	3	3267	(15,9)	2,4	5	3351	(15,3)	2,4
1	3193	(15,13)	2,4	3	3287	(15,8)	2,4	5	3361	(15,2)	2,4
1	3219	(15,12)	2,4	3	3305	(15,7)	2,4	5	3369	(15,1)	1,2,3,4
1	3243	(15,11)	2,4	3	3321	(15,6)	2,4	5	3375	(15,0)	1,2,3,4
1	3265	(15,10)	2,4	3	3335	(15,5)	2,4	5	3391	(31,160)	2,3
1	3285	(15,9)	2,4	3	3347	(15,4)	2,4	5	3541	(63,494)	4
1	3303	(15,8)	2,4	3	3357	(15,3)	2,4	5	3659	(17,33)	1,3
1	3319	(15,7)	2,4	3	3365	(15,2)	2,4	5	3715	(31,159)	2
1	3333	(15,6)	2,4	3	3371	(15,1)	1,2,3,4	5	3729	(17,32)	1,3
1	3345	(15,5)	2,4	3	3375	(15,0)	1,2,3,4	5	4037	(31,158)	2
1	3355	(15,4)	2,4	3	3387	(31,161)	2,3	5	4269	(255,4069)	4
1	3363	(15,3)	2,4	3	3537	(63,495)	4	5	4357	(31,157)	2
1	3369	(15,2)	2,4	3	3711	(31,160)	2,3	5	4533	(63,493)	4
1	3373	(15,1)	1,2,3,4	3	3725	(17,33)	1,3	5	4661	(35,193)	1,3
1	3375	(15,0)	1,2,3,4	3	3793	(17,32)	1,3	5	4675	(31,156)	2
1	3385	(31,162)	2	3	4033	(31,159)	2	5	4711	(21,65)	3
1	3535	(63,496)	4	3	4265	(255,4070)	4	5	4845	(21,64)	3
1	3709	(31,161)	2,3	3	4353	(31,158)	2	5	4907	(17,1)	1,3
1	3791	(17,33)	1,3	3	4529	(63,494)	4	5	4913	(17,0)	1,3
1	3857	(17,32)	1,3	3	4671	(31,157)	2	5	4991	(31,155)	2
1	4031	(31,160)	2,3	3	4841	(21,65)	3	5	5051	(35,192)	1,3
1	4263	(255,4071)	4	3	4909	(17,1)	1,3	5	5305	(31,154)	2

Table 4 – *Continued on next page*

Continued from previous page

b_1	b_0	(X,Y)	**Strg**	b_1	b_0	(X,Y)	**Strg**	b_1	b_0	(X,Y)	**Strg**
1	4351	(31,159)	2	3	4913	(17,0)	1,3	5	5523	(63,492)	4
1	4527	(63,495)	4	3	4973	(21,64)	3	5	5605	(19,33)	1,3
1	4669	(31,158)	2	3	4987	(31,156)	2	5	5617	(31,153)	2
1	4911	(17,1)	1,3	3	5047	(35,193)	1,3	5	5675	(19,32)	1,3
1	4913	(17,0)	1,3	3	5301	(31,155)	2	5	5727	(287,4859)	2
1	4971	(21,65)	3	3	5435	(35,192)	1,3	5	5731	(25,97)	1,3
1	4985	(31,157)	2	3	5519	(63,493)	4	5	5927	(31,152)	2
1	5101	(21,64)	3	3	5613	(31,154)	2	5	5929	(25,96)	1,3
1	5299	(31,156)	2	3	5671	(19,33)	1,3	5	6235	(31,151)	2
1	5433	(35,193)	1,3	3	5723	(287,4860)	2	5	6511	(63,491)	4
1	5517	(63,494)	4	3	5739	(19,32)	1,3	5	6541	(31,150)	2
1	5611	(31,155)	2	3	5923	(31,153)	2	5	6845	(31,149)	2
1	5721	(287,4861)	2	3	5925	(25,97)	1,3	5	6853	(19,1)	1,3
1	5737	(19,33)	1,3	3	6121	(25,96)	1,3	5	6859	(19,0)	1,3
1	5803	(19,32)	1,3	3	6231	(31,152)	2	5	7103	(29,129)	3
1	5819	(35,192)	1,3	3	6507	(63,492)	4	5	7147	(31,148)	2
1	5921	(31,154)	2	3	6537	(31,151)	2	5	7365	(29,128)	3
1	6119	(25,97)	1,3	3	6841	(31,150)	2	5	7447	(31,147)	2
1	6229	(31,153)	2	3	6855	(19,1)	1,3	5	7497	(63,490)	4
1	6313	(25,96)	1,3	3	6859	(19,0)	1,3	5	7593	(153,1888)	1,3
1	6505	(63,493)	4	3	7143	(31,149)	2	5	7617	(23,65)	3
1	6535	(31,152)	2	3	7361	(29,129)	3	5	7745	(31,146)	2
1	6839	(31,151)	2	3	7443	(31,148)	2	5	7751	(23,64)	3
1	6857	(19,1)	1,3	3	7493	(63,491)	4	5	7789	(75,641)	3
1	6859	(19,0)	1,3	3	7589	(153,1889)	1,3	5	8007	(21,33)	1,3
1	7141	(31,150)	2	3	7621	(29,128)	3	5	8041	(31,145)	2
1	7441	(31,149)	2	3	7741	(31,147)	2	5	8077	(21,32)	1,3
1	7491	(63,492)	4	3	7747	(23,65)	3	5	8335	(31,144)	2
1	7619	(29,129)	3	3	7879	(23,64)	3	5	8481	(63,489)	4
1	7739	(31,148)	2	3	8037	(31,146)	2	5	8627	(31,143)	2
1	7877	(29,128)	3	3	8073	(21,33)	1,3	5	8891	(65,513)	3
1	7877	(23,65)	3	3	8141	(21,32)	1,3	5	8917	(31,142)	2
1	8007	(23,64)	3	3	8331	(31,145)	2	5	9075	(75,640)	3
1	8035	(31,147)	2	3	8477	(63,490)	4	5	9205	(31,141)	2
1	8139	(21,33)	1,3	3	8623	(31,144)	2	5	9255	(21,1)	1,3
1	8205	(21,32)	1,3	3	8913	(31,143)	2	5	9261	(21,0)	1,3
1	8329	(31,146)	2	3	9071	(75,641)	3	5	9463	(63,488)	4
1	8475	(63,491)	4	3	9201	(31,142)	2	5	9491	(31,140)	2
1	8621	(31,145)	2	3	9257	(21,1)	1,3	5	9775	(31,139)	2
1	8911	(31,144)	2	3	9261	(21,0)	1,3	5	9789	(27,97)	1,3
1	9199	(31,143)	2	3	9459	(63,489)	4	5	9921	(65,512)	3
1	9259	(21,1)	1,3	3	9487	(31,141)	2	5	9987	(27,96)	1,3
1	9261	(21,0)	1,3	3	9771	(31,140)	2				
1	9457	(63,490)	4	3	9917	(65,513)	3				
1	9485	(31,142)	2	3	9983	(27,97)	1,3				
1	9769	(31,141)	2								

Table 4: Successful strategies in solving $y^2 + b_1 y + b_0 = x^3$ with odd X.

	Strategy 1	**Strategy 2**	**Strategy 3**	**Strategy 4**
$b_1 = 1$	102/316	210/316	174/316	126/316
$b_1 = 3$	103/315	206/315	175/315	123/315
$b_1 = 5$	102/312	202/312	174/312	120/312

Table 5: Strategies success ratios for different b_1 values.

5. Conclusion

A modular arithmetic algorithm is used to test the success rates of different strategies in solving polynomial-type Diophantine equations. We have proved the success of the algorithm in solving:

- Diophantine equations of the form $b_2y^2 + b_1y + b_0 = a_3x^3 + a_2x^2 + a_1x$ with y-coordinate having a known numeral system pattern to the base p.
- Diophantine equations of the form $\mathcal{A}p^{2z} + \mathcal{B}p^z + \mathcal{C} = a_3x^3 + a_2x^2 + a_2x$.

As an integral solution is achieved once the sequence $\{\lambda_s\}$ terminates, this suggests that many strategies may lead to a terminated sequence. Four strategies are proposed and their success rates are compared over a sample of Diophantine equations. For simplicity, the proposed strategies rely only on the sign of λ_s for the current step. Some strategies yield a fairly good success rate. For instance, Strategy 2 succeeded in solving almost 65% of the Diophantine equations listed in Table 4.

For future research and better results, other strategies, depending on the signs and magnitudes of the numbers λ_s of the current step and previous ones, may be suggested and their success rates would be examined and compared.

Acknowledgement. The author is very grateful to the anonymous reviewers and the Managing Editor, Professor Bruce Landman, for their detailed comments that have improved the quality of this paper.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

[2] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer, New York, 2001.

[3] L. Hajdu and I. Pink, On the Diophantine equation $1 + 2^a + x^b = y^n$, *J. Number Theory* **143** (2014), 1-13.

[4] C. Hering, On the Diophantine equations $ax^2 + bx + c = c_0c_1^{y_1} \cdots c_r^{y_r}$, *Appl. Algebra Engrg. Comm. Comput.* **7** (1996), 251-262.

[5] Y. Lu and X. Li, A note on the equation $x^y + y^z = z^x$, *J. Inequal. Appl.* (2014), 2014:170.

[6] F. Lucaa and G. Soydan, On the Diophantine equation $2^m + nx^2 = y^n$, *J. Number Theory* **132** (2012), 2604-2609.

[7] Yu. V. Matiyasevich, What can and cannot be done with Diophantine problems, *Proc. Steklov Inst. Math.* **275** (2011), 118-132.