Notes on Number Theory and Discrete Mathematics Print ISSN 1310–5132, Online ISSN 2367–8275 2025, Volume 31, Number 2, 228–235 DOI: 10.7546/nntdm.2025.31.2.228-235

Alternative solutions to the Legendre's equation

 $x^2 + ky^2 = z^2$

Kanwara Mukkhata¹ and Sompong Chuysurichay²

¹ Division of Computational Science, Faculty of Science, Prince of Songkla University 15 Kanchanavanit Rd, Hatyai, Songkhla 90110, Thailand e-mail: 6610220002@psu.ac.th

² Division of Computational Science, Faculty of Science, Prince of Songkla University 15 Kanchanavanit Rd, Hatyai, Songkhla 90110, Thailand e-mail: sompong.c@psu.ac.th

Received: 29 October 2024 Accepted: 5 May 2025 Revised: 4 May 2025 Online First: 6 May 2025

Abstract: In this paper, we aim to provide alternative solutions of the Legendre's equation $x^2 + ky^2 = z^2$, where k is a square-free positive integer. The results also lead to solutions of the well-known Pythagorean triples and Eisenstein triples.

Keywords: Diophantine equations, Pythagorean triples, Eisenstein triples. **2020 Mathematics Subject Classification:** 11D09, 11D72.

1 Introduction

Legendre's equation is the Diophantine equation

$$ax^2 + by^2 + cz^2 = 0, (1)$$

where x, y, z are integers, not all zero and a, b, c are fixed nonzero integers, not all of the same sign, and *abc* is squarefree [7]. When seeking integer solutions to (1), one often encounters constraints related to quadratic residues modulo specific integers. These constraints have led to



Copyright © 2025 by the Authors. This is an Open Access paper distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License (CC BY 4.0). https://creativecommons.org/licenses/by/4.0/

the development of numerous methods for finding integer solutions to this equation. In the case (a, b, c) = (1, 1, -1), Equation (1) simplifies to the Pythagorean equation $x^2 + y^2 = z^2$, and the solutions (x, y, z) are known as *Pythagorean triples*.

Another well-known example of integer triples are *Eisenstein triples*. Unlike Pythagorean triples, which are associated with right-angled triangles, Eisenstein triples are triples (x, y, z) of positive integers corresponding to integer-sided triangles with one angle measuring either 60 degree or 120 degree [6]. A 60-degree Eisenstein triple satisfies the equation $x^2 - xy + y^2 = z^2$, where x < z < y, which corresponds to a triangle with a 60-degree angle [6]. The equation of 60-degree Eisenstein triples can be transformed into either one of the equivalent forms $(2y - x)^2 + 3x^2 = (2z)^2$ or $(2x - y)^2 + 3y^2 = (2z)^2$, which is a special case of Legendre's equation where (a, b, c) = (1, 3, -1). We say that (x, y, z) is a 120-degree Eisenstein triples can also be transformed to either one of the equivalent equations $(2y + x)^2 + 3x^2 = (2z)^2$ or $(2x + y)^2 + 3y^2 = (2z)^2$, which is also a special case of Legendre's equation where (a, b, c) = (1, 3, -1). Several works have been done in solving special cases of (1) and related equations, see [1,2,4,5,7–9] for additional details.

The main aim of this paper is to give alternative solutions to the Diophantine equation

$$x^2 + ky^2 = z^2, (2)$$

where k is square-free and x, y, z are positive integers. It is well-known that all solutions of (2) are given by $(x, y, z) = (dx_0, dy_0, dz_0)$ where d is a positive integer and $gcd(x_0, y_0, z_0) = 1$. Hence, it suffices to find all possible solutions of (2) with gcd(x, y, z) = 1. Such a solution is called a *primitive solution*. We will prove the following theorems by using only elementary concepts from number theory. One can find similar results in [3, p. 77].

Theorem 1.1. The triple (x, y, z) is a primitive solution to the Diophantine equation (2), where k is an odd positive integer and is square-free if and only if either one of the following statements holds:

1. There are odd positive integers m and n such that

$$(x, y, z) = \left(\frac{1}{2}|\alpha m^2 - \beta n^2|, mn, \frac{1}{2}(\alpha m^2 + \beta n^2)\right),$$

where α and β are positive integers such that $\alpha\beta = k$ and $gcd(\alpha m, \beta n) = 1$.

2. There are positive integers m and n such that

$$(x, y, z) = \left(\left| \alpha m^2 - \beta n^2 \right|, 2mn, \alpha m^2 + \beta n^2 \right),$$

where α and β are positive integers such that $\alpha\beta = k$, $gcd(\alpha m, \beta n) = 1$, and $\alpha m, \beta n$ have different parity.

Theorem 1.2. The triple (x, y, z) is a primitive solution to the Diophantine equation (2), where k is an even positive integer and is square-free if and only if there are positive integers α, β, m , and n such that

$$(x, y, z) = \left(\left| \alpha m^2 - \beta n^2 \right|, 2mn, \alpha m^2 + \beta n^2 \right),$$

where $\alpha\beta = k$, $gcd(\alpha m, \beta n) = 1$, and $\alpha m, \beta n$ have different parity.

2 Alternative characterization

In this section, we give elementary proofs of Theorem 1.1 and Theorem 1.2. Let us start with the following lemma.

Lemma 2.1. Let a, b, and c be positive integers where b is square-free. If $a^2 \mid bc^2$, then $a \mid c$.

Proof. Suppose that $a^2 | bc^2$. Since the result is obvious for b = 1, we assume that b > 1. The fundamental theorem of arithmetic implies that there are distinct prime numbers p_1, p_2, \ldots, p_n such that $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}, b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, and $c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$ where $\alpha_i \ge 0, \beta_i \in \{0, 1\}$ and $\gamma_i \ge 0$ for all $i = 1, 2, \ldots, n$. Then $2\alpha_i \le \beta_i + 2\gamma_i$ for all $i = 1, 2, \ldots, n$.

We consider two cases.

- Case 1: $\beta_i = 0$. Then $2\alpha_i \leq 2\gamma_i$ and so $\alpha_i \leq \gamma_i$ for all i = 1, 2, ..., n.
- Case 2: $\beta_i = 1$. Then $2\alpha_i \le 1 + 2\gamma_i$. Since $2\alpha_i$ is even and $1 + 2\gamma_i$ is odd, $2\alpha_i \le 2\gamma_i$ and hence $\alpha_i \le \gamma_i$ for all i = 1, 2, ..., n.

This implies $\alpha_i \leq \gamma_i$ for all i = 1, 2, ..., n. Therefore, $a \mid c$.

Proof of Theorem 1.1. Let (x, y, z) be a primitive solution to the Diophantine equation (2) where k is odd and square-free. We consider two cases.

• Case 1: y is odd.

Then z - x is odd. Suppose that $z = x + n^2\beta$, where n and β are odd positive integers, and β is square-free. Putting z in (2) and simplifying, we have

$$ky^2 = n^2\beta(2x + n^2\beta). \tag{3}$$

From (3), we have $n^2 \mid ky^2$. By Lemma 2.1, $n \mid y$. Suppose that y = nl for some odd $l \in \mathbb{N}$. Putting y in (3), we have

$$kl^2 = \beta(2x + n^2\beta). \tag{4}$$

Dividing (4) by $gcd(k, \beta)$ on both sides, we get

$$\frac{kl^2}{\gcd(k,\beta)} = \frac{\beta}{\gcd(k,\beta)}(2x+n^2\beta).$$
(5)

From (5), we must have $\frac{\beta}{\gcd(k,\beta)} \mid l^2$, since $\frac{k}{\gcd(k,\beta)}$ and $\frac{\beta}{\gcd(k,\beta)}$ are relatively prime. Since $\frac{\beta}{\gcd(k,\beta)}$ is square-free, $\frac{\beta}{\gcd(k,\beta)} \mid l$. Let $l = \frac{\beta m}{\gcd(k,\beta)}$ for some odd $m \in \mathbb{N}$. Putting l in (4) and simplifying, we get

$$x = \frac{\beta}{\gcd(k,\beta)} \left[\frac{km^2}{2\gcd(k,\beta)} - \frac{\gcd(k,\beta)n^2}{2} \right].$$

We also have

$$y = nl = \frac{\beta}{\gcd(k,\beta)}(mn).$$

Then we finally get

$$z = x + \beta n^2 = \frac{\beta}{\gcd(k,\beta)} \left[\frac{km^2}{2\gcd(k,\beta)} + \frac{\gcd(k,\beta)n^2}{2} \right]$$

Since k and β are relatively prime and gcd(x, y, z) = 1, we must have $\frac{\beta}{gcd(k, \beta)} = 1$. This means $\beta = gcd(k, \beta)$ and hence $\beta \mid k$. Let $\alpha = \frac{k}{\beta}$. Then $\alpha\beta = k$ and

$$(x, y, z) = \left(\frac{1}{2}(\alpha m^2 - \beta n^2), mn, \frac{1}{2}(\alpha m^2 + \beta n^2)\right).$$

Since x must be positive, we may choose $x = \frac{1}{2} |\alpha m^2 - \beta n^2|$ to ensure non-negativity regardless of the sign of $\alpha m^2 - \beta n^2$. We also note that $|\alpha m^2 - \beta n^2| \ge 2$ since α and β are odd and square-free, as well as m and n are odd. Next, let $d = \gcd(\alpha m, \beta n)$. Suppose d > 1 and let p be a prime divisor of d. Then $p \mid \alpha m$ and $p \mid \beta n$. Note that p is odd since k, m and n are odd. This implies $p \mid x$ and $p \mid z$. Since $\gcd(x, y, z) = 1, p \nmid y$. This means that $p \nmid m$ and $p \nmid n$. Thus $p \mid \alpha$ and $p \mid \beta$, contradicting the fact that k is square-free. Hence $\gcd(\alpha m, \beta n) = 1$. In conclusion, we get

$$(x, y, z) = \left(\frac{1}{2}|\alpha m^2 - \beta n^2|, mn, \frac{1}{2}(\alpha m^2 + \beta n^2)\right),$$

where $\alpha\beta = k$ and $gcd(\alpha m, \beta n) = 1$.

Conversely, suppose that $(x, y, z) = (\frac{1}{2}|\alpha m^2 - \beta n^2|, mn, \frac{1}{2}(\alpha m^2 + \beta n^2))$, where m and n are odd positive integers such that $gcd(\alpha m, \beta n) = 1$. It is clear that (x, y, z) defined above is a solution to (2) and $gcd(\alpha m^2, \beta n^2) = 1$. Let d = gcd(x, y, z) and suppose that d > 1. Let p be a prime divisor of d. Then p divides $\frac{1}{2}(\alpha m^2 - \beta^2)$ and $\frac{1}{2}(\alpha m^2 + \beta n^2)$. This implies that p must divide $gcd(\alpha m^2, \beta n^2) = 1$, a contradiction. Therefore, (x, y, z) is a primitive solution of (2).

• Case 2: y is even.

Let $y = 2y_1$ for some $y_1 \in \mathbb{N}$. Then z - x is even, so we write $\frac{z - x}{2} = n^2 \beta$ where $\beta, n \in \mathbb{N}$ and β is square-free. Thus $z = x + 2n^2\beta$. Putting y and z in (2), we have

$$ky_1^2 = n^2\beta(x+n^2\beta).$$
(6)

From (6), we have $n^2 \mid ky_1^2$. Since k is square-free, Lemma 2.1 implies that $n \mid y_1$. Let $y_1 = ln$ for some $l \in \mathbb{N}$. Putting y_1 in (6) and simplifying, we get

$$kl^2 = \beta(x + n^2\beta). \tag{7}$$

Dividing (7) on both sides by $gcd(k, \beta)$, we get

$$\frac{kl^2}{\gcd(k,\beta)} = \frac{\beta}{\gcd(k,\beta)}(x+n^2\beta).$$
(8)

From (8), we have $\frac{\beta}{\gcd(k,\beta)} \mid \frac{kl^2}{\gcd(k,\beta)}$. Then we get $\frac{\beta}{\gcd(k,\beta)} \mid l^2$, because $\frac{k}{\gcd(k,\beta)}$ and $\frac{\beta}{\gcd(k,\beta)}$ are relatively prime. Since $\frac{\beta}{\gcd(k,\beta)}$ is square-free, we must have that $\frac{\beta}{\gcd(k,\beta)} \mid l$. Let $l = \frac{\beta m}{\gcd(k,\beta)}$ for some $m \in \mathbb{N}$. Putting l in (7) and solving for x, we get

$$x = \frac{\beta}{\gcd(k,\beta)} \left[\frac{km^2}{\gcd(k,\beta)} - \gcd(k,\beta)n^2 \right].$$

We also have

$$y = 2y_1 = 2(ln) = \frac{\beta}{\gcd(k,\beta)}(2mn)$$

and

$$z = x + 2n^2\beta = \frac{\beta}{\gcd(k,\beta)} \left[\frac{km^2}{\gcd(k,\beta)} + \gcd(k,\beta)n^2\right]$$

Since gcd(x, y, z) = 1, we must have $\frac{\beta}{gcd(k,\beta)} = 1$. This means that $\beta = gcd(k,\beta)$ and hence $\beta \mid k$. Let $\alpha = \frac{k}{\beta}$. Then $\alpha\beta = k$ and $(x, y, z) = (\alpha m^2 - \beta n^2, 2mn, \alpha m^2 + \beta n^2)$.

Since x must be positive, we may choose $x = |\alpha m^2 - \beta n^2|$ to ensure non-negativity regardless of the sign of $\alpha m^2 - \beta n^2$. We also note that $|\alpha m^2 - \beta n^2| \ge 1$ since α and β are square-free. Next, let $d = \gcd(\alpha m, \beta n)$. Suppose that d > 1 and let p be a prime divisor of d. Then $p \mid \alpha m^2$ and $p \mid \beta n^2$. This implies that $p \mid x$ and $p \mid z$. Since $\gcd(x, y, z) = 1$, $p \nmid y$. This means that $p \nmid m$ and $p \nmid n$. Thus $p \mid \alpha$ and $p \mid \beta$, contradicting the fact that k is square-free. Hence $\gcd(\alpha m, \beta n) = 1$.

Next, suppose that αm and βn have the same parity. Since $\alpha m^2 - \alpha m = \alpha m(m-1)$ is even, αm^2 and αm have the same parity. Likewise, βn^2 and βn have the same parity. Thus αm^2 and βn^2 have the same parity. This forces x and z to be even. Thus $gcd(x, y, z) \ge 2$, which is a contradiction. Therefore, αm and βn have different parity.

In summary, we have

$$(x, y, z) = (|\alpha m^2 - \beta n^2|, 2mn, \alpha m^2 + \beta n^2)$$

where $\alpha\beta = k$, $gcd(\alpha m, \beta n) = 1$, and $\alpha m, \beta n$ have different parity.

Conversely, one can show that (x, y, z) defined above is a primitive solution to (2) by mimicking the proof of Case 1.

Proof of Theorem 1.2. Let (x, y, z) be a primitive solution to (2) where k is even and square-free. Then $k \equiv 2 \pmod{4}$. If y is odd, then $y^2 \equiv 1 \pmod{4}$. This implies that $z^2 \equiv 2 \text{ or } 3 \pmod{4}$, which is impossible. Hence y is even. Thus the result follows Case 2 of Theorem 1.1.

3 Applications

This section is devoted to applications of Theorem 1.1 to the well-known Pythagorean triples and Eisenstein triples.

Corollary 3.1. [3, Theorem 2.2.1] *The primitive solutions to the Pythagorean triple* $x^2 + y^2 = z^2$ *with y even are given by*

$$(x, y, z) = (m^2 - n^2, 2mn, m^2 + n^2),$$

where m and n are positive integers with different parity such that m > n and gcd(m, n) = 1.

Proof. This is a direct consequence of Theorem 1.1 for k = 1.

Next, we apply the same theorem to get alternative solutions of the 60-degree Eisenstein triples. It is well-known that if (x, y, z) is a primitive 60-degree Eisenstein triple, then so is (y - x, y, z) [6]. Here, we give an alternative proof of the following result as a corollary of Theorem 1.1.

Corollary 3.2. [6, Theorem 13] The positive integers x, y and z form a pair of primitive 60-degree Eisenstein triple (x, y, z) and (y - x, y, z) with x + y + z not a multiple of 3 if and only if there exist relatively prime positive integers m and n such that m > n, $m \not\equiv n \pmod{3}$, and

$$(x, y, z) = (n^{2} + 2mn, m^{2} + 2mn, m^{2} + mn + n^{2}).$$

Proof. Let x < z < y be a primitive solution to the equation

$$x^2 - xy + y^2 = z^2 \tag{1}$$

with $x + y + z \not\equiv 0 \pmod{3}$. Then x and y must have different parity. We assume without loss of generality that x is odd. Multiplying by 4 on both sides of (1) and simplifying, we get

$$(2y - x)^2 + 3x^2 = (2z)^2.$$
 (2)

Note that gcd(2y - x, x, 2z) = 1. Theorem 1.1 implies that

$$(2y - x, x, 2z) = \left(\frac{1}{2}(a^2 - 3b^2), ab, \frac{1}{2}(a^2 + 3b^2)\right)$$

for some odd positive integers a, b where $a > \sqrt{3}b$. Thus

$$(x, y, z) = \left(ab, \frac{1}{4}(a+3b)(a-b), \frac{1}{4}(a^2+3b^2)\right).$$

Choose $m = \frac{a-b}{2}$ and n = b. Then m and n are positive integers. Moreover, we have

$$(x, y, z) = (n^{2} + 2mn, m^{2} + 2mn, m^{2} + mn + n^{2}),$$

as required. We also note that m > n since x < y and gcd(m, n) = 1 since gcd(x, y, z) = 1. Finally, we note that if $m \equiv n \pmod{3}$, then $x + y + z = 2m^2 + 5mn + 2n^2 \equiv 0 \pmod{3}$. Thus $m \not\equiv n \pmod{3}$. The converse is clear.

60-degree Eisenstein triples actually represent integer triangles (a triangle all of whose side lengths are positive integers) with one angle measures 60° . They also lead to another class of integer triangles with one angle measures 120° . The characterization of primitive 120-degree Eisenstein triples is similar to that of 60-degree Eisenstein triples. We state without proof the following corollary.

Corollary 3.3. [3, p. 93] The triple (x, y, z) is a primitive solution to the 120-degree Eisenstein triple where x < y < z and x + y + z is not a multiple of 3 if and only if there exist relatively prime positive integers m and n such that m > n, $m \not\equiv n \pmod{3}$, and

$$(x, y, z) = (m^2 - n^2, 2mn + n^2, m^2 + mn + n^2).$$

The following tables present primitive solutions of Legendre's equation $x^2 + ky^2 = z^2$ where k = 2, 15, and 30 with restricted range $1 \le m \le 4$ and $1 \le n \le 4$.

k	α	β	m	n	x	$egin{array}{c} y \end{array}$	\boldsymbol{z}
2	1	2	1	1	1	2	3
			1	2	7	4	9
			1	3	17	6	19
			1	4	31	8	33
			3	1	7	6	11
			3	2	1	12	17
			3	4	23	24	41
				1			
$egin{array}{c} k \end{array}$	α	β	m	\boldsymbol{n}	\boldsymbol{x}	\boldsymbol{y}	z
15	1	15	1	1	7	1	8
			1	2	59	4	61
			1	3	67	3	68
			1	4	239	8	241
			2	1	11	4	19
			2	3	131	12	139
			4	1	1	8	31
			4	3	119	24	151
15	3	5	1	1	1	1	4
			1	2	17	4	23
			1	4	77	8	83
			2	1	7	4	17
			3	1	11	3	16
			3	2	7	12	47
			3	4	53	24	107
			4	1	43	8	53

k	α	β	m	\boldsymbol{n}	x	$oldsymbol{y}$	\boldsymbol{z}
30	1	30	1	1	29	2	31
			1	2	119	4	121
			1	3	269	6	271
			1	4	479	8	481
30	2	15	1	1	13	2	17
			1	3	133	6	137
			2	1	7	4	23
			2	3	127	12	143
			4	1	17	8	47
			4	3	103	24	167
30	3	10	1	1	7	2	13
			1	2	37	4	43
			1	4	157	8	163
			3	1	17	6	37
			3	2	13	12	67
			3	4	133	24	187
30	5	6	1	1	1	2	11
			1	2	19	4	29
			1	3	49	6	59
			1	4	91	8	101

Acknowledgements

The first author is grateful to the Development and Promotion of Science and Technology Talent Project (DPST) scholarship. The authors would also like to thank the anonymous referees for their valuable comments and suggestions, which have greatly improved the quality of this paper.

References

- [1] Abdelalim, S., & Dyani, H. (2014). The solution of the Diophantine equation $x^2 + 3y^2 = z^2$. International Journal of Algebra, 8(15), 729–732.
- [2] Amato, R. (2017). A characterization of Pythagorean triples. *JP Journal of Algebra, Number Theory and Applications*, 39(2), 221–230.
- [3] Andreescu, T., Andrica, D., & Cucurezeanu, I. (2010). *An Introduction to Diophantine Equations: A Problem-Based Approach*. Birkhäuser, New York.
- [4] Cotronei, A. (2019). A characterization of Eisenstein triples. International Journal of Mathematics and Computer Science, 14(3), 583–590.
- [5] Dubner, H., & Forbes, T. (2001). Prime Pythagorean triangles. *Journal of Integer Sequences*, 4(2), Article 01.2.3.
- [6] Gordon, R. A. (2012). Properties of Eisenstein triples. *Mathematics Magazine*, 85(1), 12–25.
- [7] Hudson, R. H., & Williams, K. S. (1983). On Legendre's equation $ax^2 + by^2 + cz^2 = 0$. Journal of Number Theory, 16(1), 100–105.
- [8] Mangalaeng, A. H. (2022). The primitive-solutions of Diohantine equation $x^2 + pqy^2 = z^2$, for primes p, q. Jurnal Matematika, Statistika dan Komputasi, 18(2), 308–314.
- [9] Tang, Q. (2021). On the Diophantine equation $z^2 = f(x)^2 \pm f(x)f(y) + f(y)^2$. Notes on Number Theory and Discrete Mathematics, 27(2), 88–100.