Parabola Volume 60, Issue 3 (2024)

Parameterising the solution of a Diophantine equation

$$a^2 + pb^2 = c^2$$

Koshiro Fujiwara, Konoha Natori, Kosei Kaku, Manami Suwa, Nobuaki Komeda, Tomoya Kaneshiro, Yoshino Kasahara[1] and Kohhei Yasuda[2]

1 Introduction

A triple of coprime natural numbers (a, b, c) satisfying $a^2 + b^2 = c^2$ is called a *primitive Pythagorean triple*. Since a, b and c are coprime, we immediately see that $a \not\equiv b \pmod 2$. Therefore, we consider a as an odd number and b as an even number.

The following Theorem 1 is known [1, 2] to hold for primitive Pythagorean triples.

Theorem 1. *Any primitive Pythagorean triple (a, b, c) can be uniquely represented by the following equation using coprime natural numbers m, n ($m > n$):*

$$a = m^2 - n^2\,, \qquad b = 2mn\,, \qquad c = m^2 + n^2\,. \tag{1.1}$$

Formula 1.1 can be derived using elementary functions as follows [3].

Proof. Dividing both sides of $a^2 + b^2 = c^2$ by c^2 gives

$$\frac{a^2}{c^2} + \frac{b^2}{c^2} = 1\,. \tag{1.2}$$

Now consider a point $\mathrm{P}(x, y) = \left(\frac{a}{c}, \frac{b}{c}\right)$ on the coordinate plane, which exists on the unit circle with rational numbers in both x and y coordinates; see Figure 1.

Let $\mathrm{A}(-1, 0)$ be a point on the unit circle as shown in Figure 1. The slope of the line segment AP is a rational number, say $\frac{n}{m}$, where m and n are coprime natural numbers. Substituting the expression for each point $(x, y) = \left(x, \frac{n}{m}(x + 1)\right)$ on AP into $x^2 + y^2 = 1$ and re-organizing the resulting expression, we obtain

$$(m^2 + n^2)x^2 + 2n^2x + n^2 - m^2 = 0\,. \tag{1.3}$$

Solving Equation 1.3 for x, the positive solution is $x = \frac{m^2-n^2}{m^2+n^2}$. It therefore follows that $y = \frac{n}{m}(x + 1) = \frac{2mn}{m^2+n^2}$, and so $(a, b, c) = (m^2 - n^2, 2mn, m^2 + n^2)$. $\square$

[1]Students at Narita High School, Japan

[2]Kohhei Yasuda teaches mathematics at Narita High School and received a Master's degree in 2024.

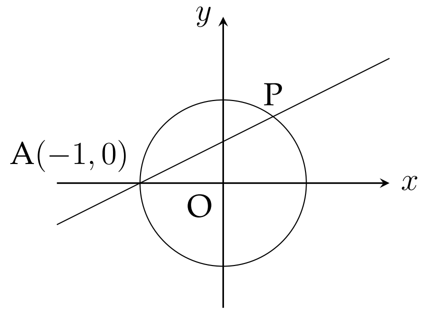

Figure 1: Line AP and circle $x^2 + y^2 = 1$

Similar to Theorem 1, it is known that the integer solution of the Diophantine equation $x^2 + py^2 = z^2$, where p is a prime number, can be expressed in terms of the parameters m and n which are natural numbers. In this paper, we derive the parametric solution of this Diophantine equation in two different ways. The first way is based on elementary functions as in the proof of Theorem 1. The second way uses elementary geometry. In particular, the second way is, as far as we know, a new solution that has not been published anywhere previously.

2 A parameteric solution to $x^2 + py^2 = z^2$

Let p be a prime number. It is known [4] that the parameter solution of the Diophantine equation $x^2 + py^2 = z^2$, where p is a prime number, can be expressed as follows.

Theorem 2. *Let p be a prime number. The solutions to the Diophantine equation*

$$a^2 + pb^2 = c^2 \tag{2.1}$$

can be expressed as follows using the natural number parameters m, n:

$$(a, b, c) = \left(m^2 - pn^2, 2mn, m^2 + pn^2\right). \tag{2.2}$$

Note that in Theorem 2, $a, b,$ and c are coprime natural numbers. Theorem 2 is proved algebraically in [4]. We give other proofs of Theorem 2. One is a proof using elementary functions as in the proof of Theorem 1. The other is a proof using elementary geometry.

3 Proof of Theorem 2 using elementary functions

Proof. Dividing both sides of $a^2 + pb^2 = c^2$ by c^2 gives

$$\frac{a^2}{c^2} + p\frac{b^2}{c^2} = 1\,. \tag{3.1}$$

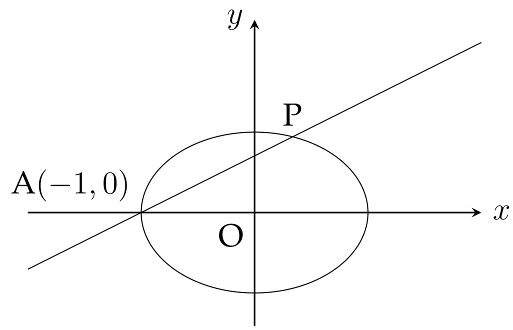

Figure 2: Line AP and ellipse $x^2 + py^2 = 1$

Now consider a point $\mathrm{P}(x_P, y_P) = \left(\frac{a}{c}, \frac{b}{c}\right)$ on the coordinate plane, which exists on the ellipse $x^2 + py^2 = 1$ with rational numbers in both x and y coordinates; see Figure 3.

Let $\mathrm{A}(-1, 0)$ be a point on the unit circle as shown in Figure 1. The slope of the line segment AP is a rational number, say $\frac{n}{m}$, where m and n are coprime natural numbers. Furthermore, since $m = x_P + 1$, $n = y_P$ and $1 > \frac{1}{\sqrt{p}} > y_P$, it is clear that $m > n$. Substituting the expression for each point $(x, y) = \left(x, \frac{n}{m}(x+1)\right)$ on AP into $x^2 + py^2 = 1$ and re-organizing the resulting expression, we obtain

$$(m^2 + pn^2)x^2 + 2pn^2x + pn^2 - m^2 = 0\,. \tag{3.2}$$

The positive solution to this equation is $x = \frac{-pn^2+m^2}{m^2+pn^2}$. Substituting $x = \frac{-pn^2+m^2}{m^2+pn^2}$ into equation $x^2 + py^2 = 1$ and solving gives the positive solution $y = \frac{2mn}{m^2+pn^2}$. Therefore, $x = \frac{a}{c} = \frac{-pn^2+m^2}{m^2+pn^2}$ and $y = \frac{b}{c} = \frac{2mn}{m^2+pn^2}$, so $(a, b, c) = (m^2 - pn^2, 2mn, m^2 + pn^2)$. □

4 Proof of Theorem 2 using elementary geometry

Proof. Consider a right triangle $\triangle\mathrm{ABC}$ whose hypotenuse AC has length 1 and the other two sides AB and BC have lengths x and $y\sqrt{p}$, respectively; see Figure 4. When the side-length of BC is divided by $(1 + x)\sqrt{p}$, it becomes $(y\sqrt{p}/\left((1 + x)\sqrt{p}\right) = \frac{y}{1+x}$, a rational number. Therefore,

$$\frac{n}{m}(1 + x) = y \tag{4.1}$$

for some coprime natural numbers m and n. Note that $(1 + x) > y$; hence $m > n$.

By Equation 4.1 and the equation $x^2 + py^2 = 1$, we obtain

$$(m^2 + pn^2)x^2 + 2pn^2x + pn^2 - m^2 = 0\,. \tag{4.2}$$

The positive solution to this equation is $x = \frac{-pn^2+m^2}{m^2+pn^2}$. Substituting this expression into the equation $x^2 + py^2 = 1$ and solving it gives the positive equation solution $y = \frac{2mn}{m^2+pn^2}$.

Since $x = \frac{a}{c}$ and $y = \frac{b}{c}$, it follows that $(a, b, c) = (m^2 - pn^2, 2mn, m^2 + pn^2)$. □

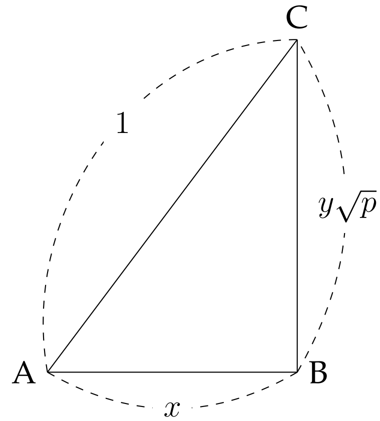

Figure 3: Right triangle $\triangle\mathrm{ABC}$

5 Conclusion

In this paper, we gave two separate proofs of Theorem 2.

As can be seen by comparing the two proofs in Sections 3 and 4, the formulas are the same in the middle. In both cases, $(m^2+pn^2)x^2+2pn^2x+pn^2-m^2=0$ is derived by substituting $y=\frac{n}{m}(1+x)$ for $x^2+py^2=1$. However, the process of obtaining equations $y=\frac{n}{m}(1+x)$ and $x^2+py^2=1$ is quite different. Since it is sufficient to derive the equations $y=\frac{n}{m}(1+x)$ and $x^2+py^2=1$ using some property, it can be expected that there are other alternative proofs of Theorem 2 that have not yet been discovered.

6 Acknowledgements

We would like to thank the many people who assisted us in writing this paper.
We would like to take this opportunity to express our appreciations to them.

References

[1] A.R. Kanga, The family tree of Pythagorean triples, *IMA Bulletin* **26** (1990), 15–27.

[2] K.R. Rosen, *Elementary Number Theory And Its Applications*, Addison-Wesley, 1988.

[3] T. Jaklitsch, T.C. Martinez, S.J. Miller and S. Mukherjee, *Class numbers and Pell's equation* $x^2+105y^2=z^2$, arXiv:2203.16709v1, 2022.

[4] Stack Exchange Mathematics, *Characterize the solution of a Diophantine equation* $x^2+py^2=z^2$, last accessed on 2024-12-28.