A Novice Investigation of The Pythagorean Triples and Fermat’s Last Theorem

Simon The Huynh (Khanh)
Math 311M Honors Concepts of Discrete Mathematics
The Pennsylvania State University

November 14 , 2017
In the Berlin Papyrus 6619 [8], an important mathematical document of the Middle Kingdom, the Egyptian recorded a puzzle about finding the sides of two squares whose sum is the area of another square with side-length of 10; in addition, the side of one square must be equal to $\frac{3}{4}$ the side-length of the other. Algebraically, we can express this problem as $x^2 + y^2 = 100$ and $y = \frac{3}{4}x$, where $x$ and $y$ represent the side-lengths of two missing squares. As proposed in the papyrus, $x = 8$ and $y = 6$ are solutions of the puzzle. In this problem, the sides of our squares, which are 6, 8, and 10, satisfy the Pythagorean Theorem, which states:

$$a^2 + b^2 = c^2$$

where $a$, $b$, and $c$ are the side-lengths of a right triangle [7]. The ordered triple $(6, 8, 10)$ is an example of a Pythagorean triple.

Formally, a Pythagorean triple is defined as an ordered triple $(a, b, c)$ such that $a^2 + b^2 = c^2$ where $a$, $b$, and $c$ are positive integers. As mentioned, these Pythagorean triples can be interpreted as the side-lengths of a right triangle. In fact, we have infinitely many examples of such triples, in addition to $(6, 8, 10)$. For instances, $(3, 4, 5)$ is another familiar example. We should notice that $(6, 8, 10)$ is a multiple of $(3, 4, 5)$. Significantly, any scalar multiple of a Pythagorean triple is itself a Pythagorean triple [7].

**Proof.** Let $(a, b, c)$ be a Pythagorean triple for positive integers $a$, $b$, and $c$. Thus, $a^2 + b^2 = c^2$. For any positive integer $k$, $(ka)^2 + (kb)^2 = k^2(a^2 + b^2) = k^2c^2 = (kc)^2$. Therefore, $(ka, kb, kc)$ is also a Pythagorean triple.

A Pythagorean triple $(a, b, c)$ is primitive if $a$, $b$, and $c$ are relatively prime. Examples of primitive triples are $(3, 4, 5)$ and $(5, 12, 13)$. Thus, the quest for finding Pythagorean triples can be reduced down to just searching for the primitive ones. For all other triples are simply scalar multiples of the primitive elements. In chapter 7 of *Hidden Harmonies* [8], the author clearly described the thought process of doing such task; the result is summarized by the theorem [7] below.

**Theorem 1.** For any positive integers $m$ and $n$ ($0 < n < m$),

$$a = 2mn, \quad b = m^2 - n^2, \quad c = m^2 + n^2$$

form a Pythagorean triple. This triple is primitive if and only if

(*) $m$ and $n$ are relatively prime, and

(**) either $m$ or $n$ is odd, but not both.

Every primitive Pythagorean triple can be expressed in this form.

Before proving this fascinating theorem, it is worth taking time to investigate the characteristics of $a$, $b$, and $c$. Since $a$, $b$, and $c$ are relatively prime, by definition, they cannot be all even; specifically, it is not permitted for any pair of them to be all even as well. In addition, it would be a contradiction to have $a$, $b$, and $c$ to be
all odd. For if \(a, b\) and \(c\) are odd, \(a = 2s + 1, b = 2t + 1,\) and \(c = 2k + 1\) for some integers \(s, t,\) and \(k.\) Thus,

\[
a^2 + b^2 = (2s + 1)^2 + (2t + 1)^2
= (4s^2 + 4s + 1) + (4t^2 + 4t + 1)
= 4s^2 + 4s + 4t^2 + 4t + 2
= 2(2s^2 + 2s + 2t^2 + 2t + 1)
= 2h \quad \text{where} \quad h = 2s^2 + 2s + 2t^2 + 2t + 1,
\]

which means that \(a^2 + b^2\) is an even integer. However, \(a^2 + b^2 = c^2 = (2k + 1)^2 = 2(2k^2 + 2k) + 1,\) which is odd. This is a contradiction. Hence, \(a, b\) and \(c\) cannot be odd simultaneously.

Exhaustively, we get to the point, where one of \(a, b\) or \(c\) is even and the others are odd. However, this list can be reduced more since \(c\) cannot be even. To prove this claim, let \(c\) be an even integer; thus, \(a\) and \(b\) are odd. Since \(c\) is even, \(c = 2v\) for some integer \(v.\) Therefore, \(c^2 = (2v)^2 = 4v^2,\) which implies that \(4\) divides \(c^2.\) However, from (1), \(a^2 + b^2\) is not divisible by \(4,\) which means that \(4\) does not divide \(c^2.\) This is also a contradiction. So, it must be the case that \(c\) is odd, and either \(a\) or \(b\) is even, but not both. Now, we are ready to prove Theorem 1.

**Proof.** \((\Rightarrow)\) Let \((a, b, c)\) be a primitive Pythagorean triple. Due to above discussion, we have established that \(c\) must be odd, and either \(a\) or \(b\) is even, exclusively. Without any loss of generality, let \(a\) be even and \(b\) be odd.

Since \(b\) and \(c\) are both odd, their sum and difference must be even. Thus, \(c - b = 2u\) and \(c + b = 2v\) for some integers \(u\) and \(v.\) Solving this system of equations for \(b\) and \(c\) yields \(c = v + u\) and \(b = v - u.\) For \(b\) and \(c\) are relatively prime, \(u\) and \(v\) must not have any common factors as well.

Because \((a, b, c)\) is a Pythagorean triple, \(a^2 + b^2 = c^2.\) It follows that

\[
a^2 = c^2 - b^2
= (c - b)(c + b) \quad \text{(by the difference of the squares formula)}
= (2u)(2v)
= 4uv
\]

In addition, \(a = 2k\) for some integer \(k\) due to our assumption that \(a\) is even. Hence, \(a^2 = 4k^2,\) which means that \(4k^2 = 4uv\) for some integers \(k, u,\) and \(v.\) From this, we have deduced that the product of \(u\) and \(v\) is a perfect square. We also know that \(u\) and \(v\) are relatively prime. Thus, \(u\) and \(v\) are perfect squares. This claim will be verified as a lemma below.

**Lemma 1.** If positive integers \(x\) and \(y\) are relatively prime and \(xy\) is a perfect square, then \(x\) and \(y\) are perfect squares.

**Proof of Lemma 1.** Let \(x\) and \(y\) be positive integers \((x, y \geq 2),\) which are relatively prime and are not perfect squares.

By the Fundamental Theorem of Arithmetic, \(x = p_1^{n_1}p_2^{n_2}...p_k^{n_k}\) and \(y = q_1^{m_1}q_2^{m_2}...q_l^{m_l},\) for some primes \(p_1, ..., p_k, q_1, ..., q_l\) and some integers \(n_1, ..., n_k, m_1, ..., m_l.\) Due to the fact that \(x\) and \(y\) do not have common factors, \(p_i \neq q_j\) for all \(i \in \{1, ..., n\},\) and
for all \( j \in \{1, ..., m\} \). In addition, at least one of \( n_1, ..., n_k \) must be odd because \( x \) is not a perfect square. Similarly, at least one of \( m_1, ..., m_l \) must be odd. Hence, \( xy = p_1^{n_1} p_2^{n_2} ... p_k^{n_k} q_1^{m_1} q_2^{m_2} ... q_l^{m_l} \), where at least one of \( n_1, ..., n_k \) is odd, at least one of \( m_1, ..., m_l \) is odd, and \( p_i \neq q_j \) for all \( i \in \{1, ..., n\} \) and for all \( j \in \{1, ..., m\} \). Thus, \( xy \) is not a perfect square. Contrapositive, if positive integers \( x \) and \( y \) are relatively prime and \( xy \) is a perfect square, then \( x \) and \( y \) are both perfect squares. QED

As a result, we can express \( u \) and \( v \) as \( n^2 \) and \( m^2 \), respectively, for some positive integer \( n \) and \( m \). Therefore, \( a^2 = 4uv = 4n^2m^2 \) implies that \( a = 2mn \). Substituting \( m^2 \) and \( n^2 \) for \( v \) and \( u \), respectively, into \( b = v - u \) and \( c = v + u \) gives us \( b = m^2 - n^2 \) and \( c = m^2 + n^2 \). So, \((a, b, c) = (2mn, m^2 - n^2, m^2 + n^2) \) for some positive integer \( m \) and \( n \).

Clearly, since \( u \) and \( v \) are relatively prime, \( m \) and \( n \) do not have any factors in common. This deduction satisfies condition (*) in theorem 1. It also implies that \( m \) and \( n \) cannot both be even. Also, if \( m \) and \( n \) are odd simultaneously, \( b = m^2 - n^2 \) and \( c = m^2 + n^2 \) will be even simultaneously, which contradicts the fact that \((a, b, c) \) is primitive. Hence, \( m \) and \( n \) has opposite parity. This reasoning fulfills condition (**) in our theorem.

\[ (\Leftarrow) \] Now, let \( m \) and \( n \) be positive integers that are relatively prime. Without any loss of generality, let \( m \) be even and \( n \) be odd. Then, we define \( a = 2mn \), \( b = m^2 - n^2 \), and \( c = m^2 + n^2 \).

First, we have:

\[
a^2 + b^2 = (2mn)^2 + (m^2 - n^2)^2
= 4m^2n^2 + (m^4 - 2m^2n^2 + n^4)
= m^4 + 2m^2n^2 + n^4
= (m^2 + n^2)^2
= c^2
\]

Thus, \((a, b, c) \) satisfies the condition of being a Pythagorean triple. The remaining task is to show that it is primitive. Since \( b = m^2 - n^2 \) and \( c = m^2 + n^2 \) are odd in addition to \( \gcd(m, n) = 1 \), it follows that \( b \) and \( c \) are relatively prime. Besides, because \( a = 2mn \) is even, it could not have any common factors with \( b \) or \( c \). Hence, \( a, b, \) and \( c \) are relatively prime, which confirms that the triple is primitive. QED

This theorem, in fact, provides us a powerful method to generate Pythagorean triples. The only ingredients that we need is two positive integers, which are co-prime; one of them must be odd and the other must be even. For example, 13 and 14. Let \( m = 14 \) and \( n = 13 \). From our theorem, \( a = 2mn = 2(14)(13) = 364 \), \( b = m^2 - n^2 = (14)^2 - (13)^2 = 27 \), and \( c = m^2 + n^2 = (14)^2 + (13)^2 = 365 \). Thus, \((364, 27, 365) \) is a primitive Pythagorean triple. Indeed, \((364)^2 + (27)^2 = (365)^2 \). Because of their beauty and significance, the Pythagorean triples have been studied by mathematicians of different eras, even before the time of Pythagoras himself [8]. For an instance, in book X, proposition 28 of Euclid’s Elements, the author described his own method of "find[ing] two square numbers such that their sum is also square [4]."
Like many problems in mathematics, we should ask ourselves whether we can do it better. In the own words of Richard Feynman, a renowned physicist, he said that "mathematicians prepare abstract reasoning that’s ready to be used if you will only have a set of axioms about the real world [5]." Truly, mathematicians take great delight in sending their problems into the realm of abstraction. For an example, they often talk about mathematical puzzles that involved the n-dimensional space rather than settling for just ordinary two or three-dimensional ones. In other words, "special cases", as they called them, are not good enough. Back to our context, we could generalize the equation $a^2 + b^2 = c^2$ by replacing the power of 2 with any positive integer $n$. Doing so yields us the equation $a^n + b^n = c^n$ for positive integers $a, b, c,$ and $n$. In the book *Arithmetica* by Diophantus of Alexandria, a significant Greek mathematician, he provided ways of solving the special case of such equation when $n = 2$, which was similar to what Euclid did.

As we fast-forward to the 17th century in France, a lawyer named Pierre de Fermat had in his hand a copy of the surviving part of Diophantus’ *Arithmetica*. Despite his occupation, Fermat studied mathematics as a leisure activity; in fact, he contributed significant results in some fields of mathematics. As Fermat read a proposition in Diophantus’ book, which asked "to divide a given square number into two squares [6]", he thought about this problem in a more abstract way. As we discussed, Fermat tried to find solutions for the equation $a^n + b^n = c^n$ for any positive integer $n$. Specifically, when $n = 3$, he wondered if there exist $a, b,$ and $c$ that satisfy the equation $a^3 + b^3 = c^3$. He, then, wrote down a note for himself in the margin of that page, which stated that:

"It is impossible for a cube to be the sum of two cubes, a fourth power to be the sum of two fourth powers, or in general for any number that is a power greater than the second to be the sum of two like powers. I have discovered a truly marvelous demonstration of this proposition that this margin is too narrow to contain [10]."

After Fermat’s death, his copy of Diophantus’ *Arithmetica* was found and re-published with all Fermat’s notes. According to critics, the assertion above was one of many claims that Fermat made without providing any legitimate proofs [12]. However, these claims were gradually verified by later mathematicians, with the exception of Fermat’s conjecture that was quoted above. Because this was the last of his assertions that was left unproved, it was well-known as "Fermat’s Last Theorem." Ironically, people often incorrectly thought of "Fermat’s Last Theorem" as his "final statement [3]" because of its name. We should restate this proposition using our modern mathematical language.

**Theorem 2** (Fermat’s Last Theorem). There exist no positive integers $a, b,$ and $c$ that satisfy the equation $a^n + b^n = c^n$, for any integer $n$ greater than 2.

Clearly, we have seen that this equation has infinitely many solutions for the case $n = 2$. In addition, one should agree that the trivial case, $a + b = c$ has infinitely many solutions as well. Surprisingly, Fermat affirmed with great confidence that this equation will not have any integer solutions for $n$ that is at least 3. However, "[the] margin [was] too narrow" for him to provide the full proof, he declared. Yet, whether Fermat truly had a valid verification of this theorem is evermore a mystery.
Despite its innocent appearance and elementary meaning, Fermat’s Last Theorem is extremely hard to prove [3].

To show that the conjecture is incorrect, we have to simply provide a counterexample of three positive integers that fulfill the equation \(a^3 + b^3 = c^3\), or \(a^4 + b^4 = c^4\), etc. During the Information Age, computer scientists and mathematicians employed their new tool, namely the computer, with a hope of finding just one counterexample. However, they could only find "near misses", such as \(135^3 + 138^3 = 172^3 - 1\); the Indian mathematician Srinivasa Ramanujan (1887-1920) discovered a way to generate infinitely many near misses like this, as recorded in his manuscript [1].

On the other hand, if a brave person accepts Fermat’s challenge of proving this theorem, he or she needs to provide solid logical arguments for the general case. William Dunham, the author of The Mathematical Universe, mentioned that Euler’s proof of the special case when \(n = 3\) differed from the one for \(n = 4\), which was proven by Fermat himself [3]. In order words, the structure of this problem changes with respect to the value of \(n\). Besides Euler, Fermat, and Ramanujan, mathematicians Dirichlet, Legendre, and Gabriel Lame proved the cases \(n = 14, 5,\) and \(7\), respectively [3]. They were just a few names among those who contributed to the process of solving Fermat’s Last Theorem.

Just like many great stories, when hope seems lost, a hero arises and pushes forward with all his might to tame the beast. In this story, our hero is Sir Andrew Wiles, a British mathematician. In the days of his youth, Wiles had obsessed with Fermat’s Last Theorem and devoted his life to solving it [11]. He carried this passion through his years at Oxford University and the University of Cambridge, where he earned his bachelor and Ph.D., respectively.

After the Spring semester of 1986, a professor of UC Berkeley named Ken Ribet announced his discovery of the connection "between Fermat’s last theorem, elliptic curves and the Taniyama-Shimura conjecture [9]." To Wiles, this link was a key to unlock Fermat’s Last Theorem. Then, he spent many hours working on proving the theorem in secret. According to his colleagues, he exhausted more time in his office and even skipped department meetings [11]. In 1993, he surprised the world of mathematics by presenting his proof of Fermat’s Last Theorem. In its early stage, his proof was found to be partially incorrect. It took another two years for Andrew Wiles’ solution to be acknowledged and published in 1995 [9]. Hence, the 368-year-old "beast" was put to rest as the mathematical society celebrated its victory.

As a conclusion of this paper, we will look at the elementary proof of Fermat’s Last Theorem for the case \(n = 4\). Specifically, we will verify that the equation \(a^4 + b^4 = c^4\) has no positive integer solutions. To complete such a task, we first explore the equation \(x^4 + y^4 = z^2\) instead [2]. If we are able to show that there are no positive integers that satisfy the equation \(x^4 + y^4 = z^2\), then our desired result will follow as a corollary [10].

**Proposition 1.** There is no positive integers \(x, y,\) and \(z\) that satisfy the equation \(x^4 + y^4 = z^2\).

**Proof (by contradiction) [2].** Let assume that there exist \(x, y,\) and \(z\) such that \(x^4 + y^4 = z^2\) with \(x, y\) are relatively prime and \(z\) is positive.

If \(x\) and \(y\) are not relatively prime, then let \(k = gcd(x, y)\). Thus, \(k\) divides both \(x\) and \(y\), which implies that \(k^4\) divides both \(x^4\) and \(y^4\). Hence, \(k^4\) divides \(x^4 + y^4 = z^2\). So, \(z^2\) is a multiple of \(k^2\). This means that \(\frac{x}{k}, \frac{y}{k},\) and \(\frac{z}{k^2}\) are another triplet solution
for our original equation for \( \left( \frac{x}{k} \right)^4 + \left( \frac{y}{k} \right)^4 = \frac{x^4}{k^4} + \frac{y^4}{k^4} = \frac{x^4 + y^4}{k^4} = \frac{z^2}{k^4} = \left( \frac{z}{k^2} \right)^2 \). So we are guaranteed to find such \( x \) and \( y \) that are relatively prime. Since \( \gcd(x, y) = 1 \), \( x \) and \( y \) cannot be both even. Let assume that \( x \) and \( y \) are both odd, which implies that \( x^4 \) and \( y^4 \) are both odd as well. Without loss of generality, let \( x = 2l + 1 \) for some integer \( l \); then, \( x^4 = (2l + 1)^4 = 16l^4 + 32l^3 + 24l^2 + 8l + 1 = 4m + 1 \) for \( m = 4l^4 + 8l^3 + 6l^2 + 2l \). Thus, \( x^4 \equiv 1 \pmod{4} \) and \( y^4 \equiv 1 \pmod{4} \). Therefore, \( x^4 + y^4 \equiv 2 \pmod{4} \), which implies that \( z^2 \equiv 2 \pmod{4} \). This is a contradiction since \( z^2 \equiv 0 \text{ or } 1 \pmod{4} \). So, \( x \) and \( y \) cannot be both odd.

Without loss of generality, let \( x \) be even and \( y \) be odd. It follows that \( z \) is odd. Because \( x^4 + y^4 = z^2 \) is equivalent to \( (x^2)^2 + (y^2)^2 = z^2 \), \( (x^2, y^2, z) \) is clearly a Pythagorean triple. Since \( x \) and \( y \) are relatively prime, \( x^2 \) and \( y^2 \) do not have any common factors. Hence, this triple is primitive. By Theorem 1, there exist positive integers \( m \) and \( n \) such that

\[
x^2 = 2mn, \quad y^2 = m^2 - n^2, \quad z = m^2 + n^2,
\]

where \( m \) and \( n \) are relatively prime and have different parity.

Since \( y^2 = m^2 - n^2 \) implies that \( y^2 + n^2 = m^2 \) with \( m \) and \( n \) relatively prime and of different parity, the triplet \((y, n, m)\) is another primitive Pythagorean triple. Since \( y \) is defined to be odd, \( n \) must be even. By similar argument, there exist positive integer \( u \), and \( v \) such that

\[
n = 2uv, \quad y = u^2 - v^2, \quad m = u^2 + v^2,
\]

where \( u \) and \( v \) are relatively prime and have different parity.

We now have \( x^2 = 2mn \), which means that \( \frac{x^2}{4} = \frac{2mn}{4} = m \left( \frac{n}{2} \right) \). Thus, \( m \left( \frac{n}{2} \right) = \left( \frac{x}{2} \right)^2 \). In other words, the product of \( m \) and \( \frac{n}{2} \) is a perfect square with the property that \( m \) and \( \frac{n}{2} \) are relatively prime. By Lemma 1, \( m \) and \( \frac{n}{2} \) must be perfect squares.

Likewise, we also have \( n = 2uv \). Again, \( u \) and \( v \) are relatively prime and their product is a perfect square, i.e., \( \frac{n}{2} \). Thus, \( u \) and \( v \) are perfect squares.

Therefore, \( m = t^2 \), \( u = g^2 \), and \( v = h^2 \) for some positive integers \( t \), \( g \), \( h \). Now, let replace \( m \), \( u \), and \( v \) with \( t^2 \), \( g^2 \), and \( h^2 \), respectively, in the equation \( m = u^2 + v^2 \).

As a result, we have

\[
t^2 = g^2 + h^2
\]

for \( t > 0 \). Besides, \( t^4 < t^4 + n^2 \), which means that \( t^4 < m^2 + n^2 = z \) since \( t^2 = m \) and \( z = m^2 + n^2 \). Clearly, \( 0 < t < z \).

We just deduce that the positive integers \( g, h, \) and \( t \) also satisfy the equation \( x^4 + y^4 = z^2 \) for \( 0 < t < z \). Hence, if we repeat the whole process, we will find another triplet integer solution \((g_1, h_1, t_1)\) with \( 0 < t_1 < t < z \). As a result, we are able to generate an infinite sequence of these solutions, \((g, h, t), (g_1, h_1, t_1), (g_2, h_2, t_2), (g_3, h_3, t_3), ...\) where \( 0 < \ldots < t_3 < t_2 < t_1 < t < z \). This is a contradiction since it is impossible to have infinitely many integers between 0 and a fixed positive integer \( z \). QED

**Corollary** (Fermat’s Last Theorem for \( n = 4 \)). The equation \( a^4 + b^4 = c^4 \) has no positive integer solutions.
Proof (by contradiction) [10]. Let assume that there exist positive integers $a$, $b$, and $c$ such that $a^4 + b^4 = c^4$. Hence, the equation $a^4 + b^4 = (c^2)^2$ has positive integer solutions, which contradicts Proposition 1. QED

In the opening, we discuss the Pythagorean triples, which are ordered triplets that satisfy the Pythagorean relationship. In addition to learning their properties, we also study the way of generating them. We, then, consider the general case of the problem where our variables $a$, $b$, and $c$ are raised to any positive integer power, $n$. As a connection with this abstract problem, the story of Fermat’s Last Theorem is told one more time. In this story, Fermat’s assertion challenged mathematicians for more than three centuries until it was finally conquered by Andrew Wiles in 1995. His "truly marvelous" proof is more than 500-pages long; there is no margin that would possibly contain it.

References


