Fermat's last theorem

If you know the Pythagorean theorem, you will know that the sides of a right triangle x, y, z satisfy

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

A well-known example of natural numbers x, y, z that satisfy the above equation is 3, 4, 5. In other words, we have

$$3^2 + 4^2 = 5^2 \tag{2}$$

Actually, there are infinite sets of natural number solutions to (1). Here are some examples:

$$\begin{aligned} 6^2 + 8^2 &= 10^2 \\ 5^2 + 12^2 &= 13^2 \\ 7^2 + 24^2 &= 25^2 \\ 9^2 + 40^2 &= 41^2 \end{aligned} \tag{3}$$

Inspired by these examples, one may want to know if there are natural number solutions to the following equation:

$$x^3 + y^3 = z^3 \tag{4}$$

or,

$$x^4 + y^4 = z^4 \tag{5}$$

Actually, around 1637, the French mathematician Pierre de Fermat wrote in margin of his book that he had found a marvelous proof that there is no natural number solution to

$$x^n + y^n = z^n \tag{6}$$

if n is an integer bigger than 2. However, he noted that he could not write out the full proof because the margin was too narrow. This is called "Fermat's Last Theorem."

Fermat proved this theorem elsewhere when $n = 4$. Then, as we will now explain, it is easy to see that all that are left to be proved are prime n. For example, suppose Fermat's Last Theorem is proved for $n = 3$. In other words, suppose it is proved that there is no natural number solution to

$$x^3 + y^3 = z^3 \tag{7}$$

Then, Fermat's last theorem in all the cases when n is a multiple of 3 is proven. To see why, let's consider $n = 6$ as an example. We want to show that there are no natural number solution (x', y', z') to the following equation

$$x'^6 + y'^6 = z'^6 \tag{8}$$

$$(x'^2)^3 + (y'^2)^3 = (z'^2)^3 \tag{9}$$

If it had a solution, then it would mean that (7) has a natural number solution, namely,

$$x = x'^2, \quad y = y'^2, \quad z = z'^2 \tag{10}$$

which is a contradiction. Thus, we conclude that $n = 6$ has no natural number solution, if $n = 3$ has no natural number solution. Similar arguments can be made for any other n that is not prime, except 4. For example, $n = 35$ has no natural number solution, if $n = 5$ or $n = 7$ has no natural number solution. These arguments fail for $n = 4$, even though 4 is not prime, because there are solutions to $n = 2$. Nonetheless, as we just said, Fermat proved for $n = 4$.

Until 1839, among primes, only $n = 3, 5, 7$ were proven. In the mid-19th century, Ernst Kummer proved the theorem for what is called "regular primes," leaving irregular primes to be proved individually. I do not know much about regular primes or irregular primes, but Wikipedia says that the first irregular primes are 37, 59, 61, 101$\cdots$. Building on this work, other mathematicians proved the theorem for all primes less than four million, using complicated computer codes. Nevertheless, as there are infinitely many irregular primes, there are infinite cases to be proven individually, which means that there are infinite cases left to be proven, even though one proves the theorem for all primes less than four million. This method doesn't work, unless one finds a clever trick to prove it once and for all.

In the mid-20th century, Japanese mathematicians Taniyama and Shimura suspected that there is a link between "elliptic curves" and "modular forms," the two completely different areas of mathematics.[1] This is known as "Taniyama-Shimura conjecture." In the 1980s, by the work of Gerhard Frey, Ken Ribet, Jean-Pierre Serre, it was shown that Fermat's Last theorem automatically follows, if Taniyama-Shimura conjecture is true in certain cases. In other words, if Taniyama-Shimura conjecture is proven, Fermat's Last Theorem is proven. However, at the moment, Taniyama-Shimura conjecture was considered too difficult to prove.

Now comes the story of the English mathematician Andrew Wiles. When he was 10 years old, he read about Fermat's Last Theorem in a local library. In an interview, he said

> This problem had been unsolved by mathematicians for 300 years. It looked so simple, and yet all the great mathematicians in history couldn't solve it. Here was a problem, that I, a 10 year old, could understand, and I knew from that moment that I would never let it go. I had to solve it. [1]

In his early teens, he tried to solve this problem, because Fermat, 300 years ago, would not have known much more math than he did. In college, he studied the methods and the

[1] If you want to learn about this topic at laymen's level, read "Love and Math: The Heart of Hidden Reality" by Edward Frenkel

techniques the 18th and 19th century mathematicians tried to tackle this problem. Then, when he became a professional researcher, he put aside the problem. It didn't seem to him that "these techniques were really getting to the root of the problem." He remarked,

> The problem with working on Fermat was that you could spend years getting nowhere. It's fine to work on any problem, so long as it generates interesting mathematics along the way-even if you don't solve it at the end of the day. [1]

In 1986, Wiles heard in the middle of casual conversation at his friend's house that Ribet had proved the connection between Taniyama-Shimura conjecture and the Fermat's Last Theorem. Wiles was "electrified," and secretly began to work on proving Taniyama-Shimura conjecture. He remarked that he had "carried this problem around in [his] head basically the whole time," except when he played around with his kids. He also said what he did when he got stuck:

> When I got stuck and I didn't know what to do next, I would go out for a walk. I'd often walk down by the lake. Walking has a very good effect in that you're in this state of relaxation, but at the same time you're allowing the sub-conscious to work on you. [1]

He described his research process as follows:

> Perhaps I can best describe my experience of doing mathematics in terms of a journey through a dark unexplored mansion. You enter the first room of the mansion and it's completely dark. You stumble around bumping into the furniture, but gradually you learn where each piece of furniture is. Finally, after six months or so, you find the light switch, you turn it on, and suddenly it's all illuminated. You can see exactly where you were. Then you move into the next room and spend another six months in the dark. So each of these breakthroughs, while sometimes they're momentary, sometimes over a period of a day or two, they are the culmination of-and couldn't exist without-the many months of stumbling around in the dark that proceed them.

In 1993, he made a breakthrough, and thought he had proved the theorem. But, an error was discovered. He invited the mathematician Richard Taylor, worked together with him for a year, and fixed the error.

Before Andrew Wiles proved Fermat's Last Theorem in 1994, many mathematicians tried to prove Fermat's Last Theorem over 300 years. Many claimed to find the proofs, only to be found out later that their proofs had errors. It is certain that Fermat's original proof, if there was indeed one, must be different from Wile's proof, because Fermat didn't know all the 20th century mathematics techniques Wiles used for his proof. Andrew Wiles further remarked,

> I don't believe Fermat had a proof. I think he fooled himself into thinking he had a proof. But what has made this problem special for amateurs is that there's a tiny possibility that there does exist an elegant 17th-century proof.

By "an elegant 17th-century proof," he meant a witty proof that requires only 17th-century mathematics.

In the beginning of the 20th century, the German mathematician Paul Wolfskehl left 100,000 Marks as a will to anyone who solves Fermat's Last Theorem. Even though the prize amount was worth today's £ 1 million at the moment, due to inflation, Wiles only received £ 30,000. Despite proving Fermat's Last Theorem, Andrew Wiles couldn't receive the Fields Medal, because he was over the age limit, which is 40 years old. Nonetheless, he was honored with the Abel Prize in 2016.

References

[1] Andrew Wiles on Solving Fermat. `https://www.pbs.org/wgbh/nova/article/andrew-wiles-fermat/`