The Equation $x^2 + y^2 = z^2$

The equation $x^2 + y^2 = z^2$ is associated with the Pythagorean theorem: In a right triangle the sum of the squares on the sides is equal to the square on the hypotenuse.

We all learn that $(3, 4, 5)$ is a “Pythagorean triple”: $3^2 + 4^2 = 5^2$. A Pythagorean triple is a “triple” of three positive integers $(x, y, z)$ so that $x^2 + y^2 = z^2$. The triple is said to be primitive if $x$ and $y$ have no common factors other than ±1. In other words $(x, y, z)$ is primitive if $x^2 + y^2 = z^2$ and $\gcd(x, y) = 1$.

Examples: $(3, 4, 5), (5, 12, 13), (7, 24, 25), (8, 15, 17), (9, 40, 41), (11, 60, 61), (12, 35, 37), (13, 84, 85), (16, 63, 65), (20, 21, 29), (28, 45, 53), (33, 56, 65), (36, 77, 85), (39, 80, 89), (48, 55, 73), (65, 72, 97)$

Remark: Notice we are interested in positive integer solutions. Certainly for any positive $x$ and $y$ there is a $z$ defined by $z = \sqrt{x^2 + y^2}$ but “usually” $z$ is irrational.

Interest in Pythagorean triples precedes Pythagoras by more than 1000 years. The Babylonian tablet “Plimpton 322” is dated to 1900-1600 BCE contains a table which is 15 rows by 3 columns of integers. In the first column are values of $y$ and in the second are values of $z$ and the third column is simply an enumeration 1-15. The largest triple on Plimpton 322 is $(13500, 12709, 18541)$:

$$13,500^2 + 12,709^2 = 18,541^2$$
The Chinese were aware of the Pythagorean theorem 1000 BCE. They call it the "Gougu Theorem." Ancient Egypt is rumored to have been aware of it before Pythagoras.

We have no evidence that Pythagoras or the Pythagoreans were the first to prove his famous theorem. The oldest known axiomatic proof is found in Euclid’s *Elements*. The converse is also true If \( x^2 + y^2 = z^2 \) then the triangle is a right triangle.

There is another geometric interpretation of the equation \( x^2 + y^2 = z^2 \):

\[
\left( \frac{x}{z} \right)^2 + \left( \frac{y}{z} \right)^2 = 1
\]

How many rational points \( \left( \frac{x}{z}, \frac{y}{z} \right) \) lie on the unit circle.

Ancient tradition attributes to Pythagoras and the Pythagoreans, the following method for generating Pythagorean triples:

\[
x = 2n + 1 \quad y = 2n^2 + 2n \quad z = 2n^2 + 2n + 1
\]

so that

\[
z^2 = ((2n^2 + 2n) + 1)^2 = (2n^2 + 2n)^2 + 2(2n^2 + 2n) + 1 = y^2 + 4n^2 + 4n + 1 = y^2 + x^2
\]

Since \( n \) is arbitrary this generates infinitely many triples. Note that \( \gcd(y, z) = 1 \) so that we know there are infinitely many primitive Pythagorean triples: For any odd number \( x = 2n + 1 \) there is a primitive Pythagorean triple. However not all Pythagorean triples are of this form: \( (8, 15, 17) \).

Another result of the same ilk is found in Euclid’s *Elements* (ca. 300 BCE) and Diophantus’ *Arithmetica* (ca. 250). It states

\[
x = 2st, \quad y = s^2 - t^2 \quad z = s^2 + t^2
\]
defines a Pythagorean triple. Here $s$, $t$ are positive integers and $s > t$. Observe

$$x^2 + y^2 = 4s^2t^2 + s^4 - 2s^2t^2 + t^4 = s^4 + 2s^2t^2 + t^4 = (s^2 + t^2)^2 = z^2$$

**Fibonacci and the Pythagorean Problem:** Leonardo of Pisa (Fibonacci) (1175-1250) showed was that all primitive Pythagorean triples were of this form. (But not all triples of this form are primitive, for take $s$ and $t$ both even.) His proof may be from Arab mathematicians who apparently knew this result.

We assume that the last listed member of the triple is the largest.

**Lemma** Let $(x, y, z)$ be a primitive Pythagorean triple. Then $x$ or $y$ is even and the other is odd.

**Proof:** Clearly at most one of $x$ and $y$ can be even since $\gcd(x, y) = 1$. Suppose that neither was even: $x = 2h + 1$ and $y = 2k + 1$. Then

$$z^2 = 4h^2 + 4h + 1 + 4k^2 + 4k + 1 = 4(h^2 + h + k^2 + k) + 2$$

This says that $2|z^2$ but $4 \nmid z^2$ which is impossible because $z^2$ is a perfect square. \qed

We shall choose $x$ to be even.

**Theorem** The triple $(x, y, z)$ is a primitive Pythagorean triple if and only if there exist two relative prime integers $s$ and $t$ so that $s > t > 0$ and

$$x = 2st \quad y = s^2 - t^2 \quad \text{and} \quad z = s^2 + t^2$$

where one of $s$ and $t$ is even and the other is odd.

**Proof:** We have already seen that $(x, y, z)$ is a Pythagorean triple. (See the text, page 275). We need only check that it is primitive. If $d$ is a common divisor of $x$ and $y$ then $d^2|z^2$, and so $d|z$. Therefore $d|(s^2 + t^2)$ and this says $d$ is not even (because $s$ and $t$ are even and odd). Also $d|(s^2 - t^2)$ so $d|2s^2$ and $d|2t^2$ and so $d|s^2$ and $d|t^2$. If $d \geq 2$ then this says $s^2$ and $t^2$ have a common prime factor. That is impossible ($\gcd(s, t) = 1$) $d = \pm 1$.

Conversely suppose that $(x, y, z)$ is a primitive Pythagorean. We would like to set $s^2 = (z + y)/2$ and $t^2 = (z - y)/2$ but of course that is problematic since we don’t know either of these is a perfect square. We therefore introduce

$$u = \frac{z + y}{2} \quad v = \frac{z - y}{2}$$

Because $z$ and $y$ are odd, $u$ and $v$ are integers. Observe that $\gcd(u, v) = 1$ because if $u$ and $v$ have a common factor $d$ then $d|(u + v)$ that is $d|z$ and similarly $d|y$ and so $d = \pm 1$. Moreover

$$uv = \left(\frac{z + y}{2}\right)\left(\frac{z - y}{2}\right) = \frac{z^2 - y^2}{4} = \left(\frac{x}{2}\right)^2$$

That is $uv$ is a perfect square. This and the fact $\gcd(u, v) = 1$ implies $u$ and $v$ are perfect squares: $u = s^2$ and $v = t^2$. To check this observe that every prime $p$ in the prime decomposition of $uv$ must appear to an even power: $p^{2u}|uv$. Of course $p$ must divide either $u$ or $v$ but because $\gcd(u, v) = 1$ it can’t divide both and so if $p^{2v}$ divides $u$ or $v$.  

Therefore every prime in the prime decomposition of \( u \) appears to an even power and similarly for \( v \). We have therefore verified the relationships between \( x, y, z \) and \( s \) and \( t \). We further know that \( \gcd(s^2, t^2) = 1 \) and so \( \gcd(s, t) = 1 \). We also know \( s > t > 0 \) because \( u > v > 0 \) by their definitions.

Finally it remains to check that \( s \) or \( t \) is even but not both. Certainly \( \gcd(s, t) = 1 \) implies they are not both even. On the other hand if both were odd then \( z^2 = s^2 + t^2 \) would be even which we know is not possible for a primitive Pythagorean triple. So exactly one of \( s \) and \( t \) is even. \( \square \)

Theorem: If \((x, y, z)\) is a Pythagorean triple than either \( x \) or \( y \) is divisible by 3.

Proof: We may suppose that \((x, y, z)\) is primitive. By the preceding Theorem \( x = 2st \) and \( y = s^2 - t^2 = (s - t)(s + t) \). Thus we need only check that \( s \) or \( t \) or \( s - t \) or \( s + t \) must be divisible by 3. Every integer is of the form \( 3m \) or \( 3m + 1 \) or \( 3m - 1 \) for some integer \( m \) because the set of all multiples of 3 forms a lattice of integers from which all integers differ by at most one. We may suppose that neither \( s \) nor \( t \) is divisible by 3. If \( s = 3m + 1 \) and \( t = 3n + 1 \) then \( s - t \) is divisible by 3. If \( s = 3m + 1 \) and \( t = 3n - 1 \) then \( s + t \) is divisible by 3. Similarly if \( s = 3m - 1 \) and so either \( x \) or \( y \) is divisible by 3. \( \square \)

Fermat’s Last Theorem:

Pierre de Fermat (1601-1665) wrote in 1637 in the margin of his copy of Diophantus’s *Arithmetica* (ca. 250) that

“It is impossible to write a cube as a sum of two cubes, a fourth power as an sum of two fourth powers, and, in general, any power beyond the second as a sum of two similar powers. For this I have discovered a truly wonderful proof, but the margin is too small to contain it.”

In our notation: There are no positive integers \( n, x, y \) and \( z \) so that

\[ x^n + y^n = z^n \]

if \( n \geq 3 \). See page 514-517 (about) of our text (Burton, 7th ed). Compare this with the case \( n = 2 \): \( x^2 + y^2 = z^2 \) which we will show has infinitely many primitive solutions. It is generally believed that Fermat who gave a proof of the case \( n = 4 \) (by his method of “infinite descent”) and quite possibly handled the case \( n = 3 \), erroneously thought that it would extend to all values of \( n \).

Observe that, if \( n = pk \) where \( p \) and \( k \) are integers then

\[ x^n + y^n = z^n \]

becomes \( (x^k)^p + (y^k)^p = (z^k)^p \). This says that if there is not integers \( a, b, \) and \( c \) of \( a^p + b^p = c^p \) then there is not solution to \( x^n + y^n = z^n \). Therefore it is enough to prove Fermat’s Last Theorem when \( n = 4 \) (as Fermat did) and for all primes \( n = p \geq 3 \). (This is because of the prime decomposition theorem for positive integers.) Leonhard Euler established the \( n = 3 \) case in a book *Algebra* (1770) by Fermat’s method of infinite descent and so it is possible that indeed Fermat could have really known the \( n = 3 \) case as well. Lejeune Dirichlet dealt with the case \( n = 5 \) in 1825; Lamé did the case \( n = 7 \) in 1839 and claimed to have a proof of the
general case in 1847 but it was immediately refuted by J. Liouville. In 1850 a 3000 franc prize was offered for the solution and in 1908 100,000 marks was offered as a prize and indeed Wiles got 75,000 marks. Over 1000 false proofs were published.

By 1976 the result was known for $3 \leq n \leq 125,000$. Gerd Faltings showed in 1983 that if $n \geq 3$ then there are at most finitely many solutions $(x, y, z)$. Credit for the proof of Fermat’s Last Theorem is given, not to Fermat but to Andrew Wiles. Andrew Wiles announced a proof in summer 1993 in Cambridge (his doctoral school) but a gap was found in his argument. There was a collective gasp when the gap was realized but most people agreed that it was just a matter of time and in fact Wiles, in collaboration with Richard Taylor worked their way around the gap by September 1994 and their results appeared in the Annals of Mathematics 141 in 1995 in a series of 2 papers. More precisely Weil and Taylor proved the Shimura-Taniyama-Weil Conjecture for semistable elliptic curves over the rationals. It links the subject areas of elliptic curves to modular forms and is considered an important component of Robert Langland’s Program for number theory. It was already known that this conjecture would establish Fermat’s Last Theorem.

Wiles devoted 7 years straight working on this problem and not much else and that he set his sights on cracking this problem while he was still at Cambridge. He is a professor at Princeton University.

Reference: Fermat’s Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem, by Amir D. Aczel