# Pythagorean Triples and Fermat's Last Theorem

Donald Rideout(drideout@mun.ca), Memorial University of Newfoundland[1]

The Pythagorean theorem says that the sum of the squares of the sides of a right triangle equals the square of the hypotenuse. In symbols,

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

Since we are interested in Number Theory, that is, the theory of whole numbers, we ask if there are any Pythagorean triangles whose sides are whole numbers. There are many such triangles, the most famous being 3, 4, and 5, and the next being 6, 8, and 10, the ones carpenters use to "square-a-house", since they know that the converse of the Pythagorean theorem is true. Here are a few more examples:

$$3^2 + 4^2 = 5^2,\ 7^2 + 24^2 = 25^2,\ 8^2 + 15^2 = 17^2,\ 65^2 + 72^2 = 97^2,\ 77^2 + 36^2 = 85^2.$$

The study of *Pythagorean triples* began about a thousand years before the time of Pythagoras(585-447B.C.) since there are Babylonian tablets dating about 1500B.C. containing lists of such triples including (3, 4, 5) and (4961, 6480, 8161). (Daniel, Shadrach, Meshach, and Abednego were carried off to Babylon in 605 B.C. and probably knew some of these triples since they were taught the letters and language of the Babylonians. They were four young people who could have made the CMO team!)

Are there infinitely many Pythagorean triples? The answer is "YES" for a trivial reason since, for example, for any integer $d$,

$$(3d)^2 + (4d)^2 = (5d)^2.$$

These new triples are not interesting, so we concentrate only on triples with no common factors. Such triples are called *primitive Pythagorean triples*.

Are there infinitely many of these? The first step is to gather some data. Here are some others:

$$(20, 21, 29),\ (12, 35, 37),\ (9, 40, 41),\ (16, 63, 65),\ (28, 45, 53).$$

We can draw a few tentative conclusions from this list. It looks like one of $a$ and $b$ is even and the other odd, and that $c$ is always odd. This is not hard to prove. If $a$ and $b$ are both even then so is $c$, and so the triple $(a, b, c)$ is not primitive. If $a$ and $b$ are both odd then $c$ is even so that for some integers $x$, $y$, and $z$

$$a = 2x + 1, \quad b = 2y + 1, \quad \text{and } c = 2z.$$

We can substitute these into the equation $a^2 + b^2 = c^2$ to get

$$(2x + 1)^2 + (2y + 1)^2 = (2z)^2.$$

[1]Talk given at CMC Seminar, Waterloo, June 2006

This simplifies to $2x^2 + 2x + 2y^2 + 2y + 1 = 2z^2$. This last equation is impossible, and so $a$ and $b$ cannot both be odd. It isnow obvious that $c$ is odd.

Since we can always switch $a$ and $b$, our problem now is to find all solutions in whole numbers to the equation $a^2 + b^2 = c^2$ with $a$ odd, $b$ even, and $a$, $b$, $c$ having no common factors. Our first observation is that

$$a^2 = c^2 - b^2 = (c - b)(c + b).$$

Here are a few examples from the list earlier, where we always take $a$ odd and $b$ even:

$$\begin{aligned} 3^2 &= 5^2 - 4^2 = (5 - 4)(5 + 4) = 1 \cdot 9 \\ 45^2 &= 53^2 - 28^2 = (53 - 28)(53 + 28) = 25 \cdot 81 \\ 77^2 &= 85^2 - 36^2 = (85 - 36)(85 + 36) = 49 \cdot 121 \\ 65^2 &= 97^2 - 72^2 = (97 - 72)(97 + 72) = 25 \cdot 169 \end{aligned}$$

We conjecture that $c - b$ and $c + b$ are always squares of odd numbers. How can we prove this? First, we observe that $c-b$ and $c+b$ seem to have no common factors. Suppose that $d$ is a common factor of $c-b$ and $c+b$; that is, $d$ divides both $c-b$ and $c+b$. It is an exercise to show that $d$ also divides $(c + b) + (c - b) = 2c$ and $(c + b) - (c - b) = 2b$. But $b$ and $c$ have no common factors since $(a, b, c)$ is primitive, and hence $d$ must equal 1 or 2. But $d$ also divides $(c-b)(c+b) = a^2$, and $a$ is odd, so $d$ must be 1. In other words, the only whole number dividing both $c - b$ and $c + b$ is 1, and $(c - b)(c + b) = a^2$. The only way this can happen is if $c - b$ and $c + b$ are themselves squares. This is intuitively clear but not entirely trivial to prove! You are asked in grade school to accept this by faith. Hence, we can now write $c + b = s^2$ and $c - b = t^2$ where $s > t \geq 1$ are odd integers with no common factors. Solving for $b$ and $c$ yields $c = \frac{s^2+t^2}{2}$ and $b = \frac{s^2-t^2}{2}$, and hence $a = \sqrt{(c - b)(c + b)} = st$. The proof is now finished!

**Pythagorean Triples Theorem.** *You will get every primitive Pythagorean triple $(a, b, c)$ with $a$ odd and $b$ even by using the formulas*

$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2},$$

*where $s > t \geq 1$ are chosen to be any odd integers with no common factors.*

Alternatively, since $b$ is even, we could have started with $b^2 = c^2 - a^2$. Hence $\left(\frac{b}{2}\right)^2 = \frac{c-a}{2} \cdot \frac{c+a}{2}$ and, by a similar argument as above, we conclude that $\frac{c+a}{2} = u^2$ and $\frac{c-a}{2} = v^2$ so that $c = u^2 + v^2, a = u^2 - v^2$ and $b = 2uv$ where $u > v \geq 1, (u, v) = 1$, and $u$ and $v$ have opposite parity.

We list some of the examples above as well as a few others. You should extend this list and make other conjectures.

| $s$ | $t$ | $a = st$ | $b = \frac{s^2-t^2}{2}$ | $c = \frac{s^2+t^2}{2}$ |
|---|---|---|---|---|
| 3 | 1 | 3 | 4 | 5 |
| 5 | 1 | 5 | 12 | 13 |
| 7 | 1 | 7 | 24 | 25 |
| 9 | 1 | 9 | 40 | 41 |
| 11 | 1 | 11 | 60 | 61 |
| 13 | 1 | 13 | 84 | 85 |
| 5 | 3 | 15 | 8 | 17 |
| 9 | 5 | 45 | 28 | 53 |
| 9 | 7 | 63 | 32 | 65 |
| 11 | 3 | 33 | 56 | 65 |
| 11 | 5 | 55 | 48 | 73 |
| 11 | 7 | 77 | 36 | 85 |
| 11 | 9 | 99 | 20 | 101 |
| 13 | 3 | 39 | 80 | 89 |
| 13 | 5 | 65 | 72 | 97 |
| 15 | 7 | 105 | 88 | 137 |
| 35 | 3 | 105 | 608 | 617 |
| 21 | 5 | 105 | 208 | 233 |
| 121 | 41 | 4961 | 6480 | 8161 |

Is it always true that 60 divides $abc$? Which odd numbers appear in a primitive triple $(a, b, c)$? It is a fact that $c$ can occur if and only if the only odd primes dividing $c$ are of the form $4n + 1$. Can you find three primitive triples with the same $c$?

Since the Diophantine[2] equation $a^2 + b^2 = c^2$ has infinitely many solutions, it is natural to investigate the situation where the exponent 2 is replaced by 3, and then 4, and so on. For example, do the equations

$$a^3 + b^3 = c^3 \quad \text{and} \quad a^4 + b^4 = c^4 \quad \text{and} \quad a^5 + b^5 = c^5$$

have solutions in nonzero integers $a, b, c$? In 1637 Pierre de Fermat(1601-1665) showed that there is no solution for exponent 4.

**Theorem:** *Fermat(1637)* $a^4 + b^4 = c^4$ *has no nontrivial solutions in integers.*

**Proof:** We will prove a slightly more general result, that $a^4 + b^4 = c^2$ has no solutions in integers. It is an exercise to show then that $a^4 + b^4 = c^4$ cannot have a solution either.

[2]Called such in honour of Diophantus who lived in Alexandria around 250 A.D. and who wrote *Arithmetic*, one of the great classics of ancient Greek mathematics. All that we know about his life is what is given in the following problem in a collection called the *Palatine Anthology*, written roughly a century after Diophantus' death: Here you see the tomb containing the remains of Diophantus, it is remarkable: artfully it tells the measures of his life. The sixth part of his life God granted him for his youth. After a twelfth more his cheeks were bearded. After an additional seventh he kindled the light of marriage, and in the fifth year he accepted a son. Alas, a dear but unfortunate child, half of his father he was when chill Fate took him. He consoled his grief in the remaining four years of his life. By this devise of numbers, tell us the extent of his life.

Assume that $a^4 + b^4 = c^2$ where $(a, b, c)$ have no common factor and say $b$ is even. Then

$$\begin{aligned} b^2 &= 2uv \\ a^2 &= u^2 - v^2 \\ c &= u^2 + v^2 \end{aligned}$$

where $u > v \geq 1$, $(u, v) = 1$, and $u$ and $v$ of opposite parity. In fact, $v$ must be even for if not and $u$ is even, then from $a^2 = u^2 - v^2$, we have $a^2 \equiv -1 \equiv 3 \pmod 4$ which is not possible. Since $a^2 + v^2 = u^2$, then as above

$$\begin{aligned} v &= 2pq \\ a &= p^2 - q^2 \\ u &= p^2 + q^2. \end{aligned}$$

Therefore $b^2 = 2uv = 4pq(p^2 + q^2)$ and hence $p$, $q$, $pq$ and $p^2 + q^2$ are squares since $p$, $q$, $pq$ and $p^2 + q^2$ have no factors in common. Let $p = A^2$ and $q = B^2$. Then $A^4 + B^4 = p^2 + q^2$ is a square and

$$A^4 + B^4 = p^2 + q^2 = u < u^2 + v^2 = c < c^2 = a^4 + b^4.$$

This sets up an *infinite descent* chain of squares of whole numbers of the form $x^4 + y^4$ which is clearly impossible. (The above argument is called the *method of infinite descent* and was invented by Fermat.)

The proof that there is no solution for exponent 3 turned out to be much harder. Leonhard Euler(1707-1783), who was the greatest mathematician of his time, proved the case $n = 3$ in 1753 and observed that the proof seemed very different from the case $n = 4$.

**Theorem:** *(Euler (1753)) $a^3 + b^3 = c^3$ has no nontrivial solutions.*

**Proof:** Assume a solution $a$, $b$, and $c$ with no factors in common. Only one is even. If $c$ is even, then $a$ and $b$ are odd, and writing $a + b = 2p$ and $a - b = 2q$, we have $a = p + q$ and $b = p - q$, and

$$c^3 = (p + q)^3 + (p - q)^3 = 2p^3 + 6pq^2 = 2p(p^2 + 3q^2).$$

(Similarly, if $a$ or $b$ is even.) Assume first that 3 does not divide $p$. Then $2p$ and $p^2 + 3q^2$ have no factors in common, so each must be a cube. (The case where 3 divides $p$ is similar.) It is at this point that Euler introduced complex numbers. He showed that $p^2 + 3q^2 = (c^2 + 3d^2)^3$, where $c$ and $d$ are chosen so that $p = c^3 - 9cd^2$ and $q = 3c^2d - 3d^3$. He factored $p^2 + 3q^2$ into $p + \sqrt{-3}q$ and $p - \sqrt{-3}q$ and worked with these numbers, and made statements about them that were not completely justified. That is, he claimed and did not completely justify that if $p^2 + 3q^2$ is a cube, then there must exist $c, d$ such that $p$ and $q$ are given by the above equations. Assuming that this can be justified we have

$$2p = 2c(c - 3d)(c + 3d) = \alpha^3\beta^3\gamma^3$$

since $2p$ is a cube and $2c, c \pm 3d$ have no factors in common. Since $2p \mid c^3$ then $\alpha^3\beta^3\gamma^3 = 2p < c^3$ since we can assume without loss of generality that $c$ is positive. Since

$$\beta^3 + \gamma^3 = (c - 3d) + (c + 3d) = 2c = \alpha^3,$$

and since we can assume also that $\alpha$ is positive, we have $\alpha < c$, and so by a descent argument, the result follows.

The proof for exponent 5 is shared by two very eminent mathematicians, the young, 20 years old, Peter Gustav Lejeune Dirichlet(1805-1859) and the aged, 73 years old, Adrien-Marie Legendre(1752-1833). They proved the result for $n = 5$ in 1825 using one of the first general results on the general $a^n + b^n = c^n$ case proved by a Monsieur Le Blanc in 1823, namely, that if $p$ and $2p + 1$ are primes[3], then the equation $a^p + b^p = c^p$ has no solutions in integers $a, b, c$ with $p$ not dividing the product $abc$.

This result was communicated to Legendre (and Cauchy) so that they could present the result to the Académie des Sciences de Paris. Why? Because Monsieur Le Blanc was really Sophie Germain(1776-1831) and regulations of the Academy prevented women from presenting their discoveries in person. Sophie Germain is best known for her Number Theory results and so impressed the famous Gauss[4] that he recommended her for an honorary degree at the University of Göttingen. Unfortunately, Sophie Germain died in Paris before the University of Göttingen could award her the honorary doctorate which Gauss had recommended she receive.

The exponent 6 case is trivial, since if there is a non-trivial solution to $a^6 + b^6 = c^6$ then we would have a solution to the exponent 3 case since $(a^2)^3 + (b^2)^3 = (c^2)^3$. This we know is not possible. In general then, we need only consider the cases $n = p$ where $p$ is an odd prime. Note that every integer greater than 2 is either a multiple of 4 or an odd prime.

In 1832, seven years after his and Legendre's proof of the case $n = 5$, Dirichlet published a proof of the case $n = 14$. This is of course weaker than the case $n = 7$ and his publication of this proof is in a way a confession of his failure with the case $n = 7$. Another seven years passed before the first proof of the case $n = 7$ was published by Gabriel Lamé(1795-1870) in 1839.

I think it is about time that we state the general conjecture. In the margin of his copy of Bachet's Latin translation of the complete works of Diophantus, Fermat wrote:

> "*Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet*" (It is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or in general any power higher than the second into powers of like degree; I have discovered a truly remarkable proof which this margin is too small to contain.)

This copy is now lost, but the remark appears in the 1670 edition of the works of Fermat, edited in Toulouse by his son Samuel de Fermat. It is stated in Dickson's *History of the The-*

[3]There are many primes $p$ for which $2p + 1$ is also prime, but it is still not known whether there are infinitely many such primes.

[4]"Carl Friedrich Gauss(1777-1855) was the greatest of all mathematicians and perhaps the most richly gifted genius of whom there is any record. This gigantic figure, towering at the beginning of the nineteenth century, separates the modern era in mathematics from all that went before. He surpassed the levels of achievement possible for ordinary men of genius in so many ways that one sometimes has the eerie feeling that he belonged to a higher species." (Quoted from George F. Simmons' delightful book entitled *Calculus Gems* from McGraw-Hill.)

*ory of Numbers, Volume II*, that Fermat's assertion was made about 1637. Even though no correct proof was discovered until recently the following has always been known as *Fermat's Last Theorem*[5].

**Fermat's Last Theorem.** *The Diophantine equation*

$$a^n + b^n = c^n$$

*where $n$ is a natural number larger than 2, has no solution in integers all different from 0.*

It is doubtful that Fermat had a correct proof. The person who made the greatest contribution in the latter part of the 19th century was Ernst Eduard Kummer(1810-1893) who developed a whole new area of mathematics called algebraic number theory and used this theory to prove Fermat's Last Theorem for many exponents, but still only a finite list. Kummer worked with complex numbers arising naturally from the factorization

$$a^p + b^p = (a+b)(a+\zeta b)(a+\zeta^2 b)(a+\zeta^3 b)\cdots(a+\zeta^{p-1}b)$$

where $\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$. Gauss had worked with these numbers in the case $p = 3$ where $\zeta = \frac{-1+\sqrt{3}i}{2}$. This is a *primitive* cube root of one since $\zeta^3 = 1$. If $a$ and $b$ are integers then Kummer tried to work with the "integers" $a + \zeta^n b$. He was successful in certain cases to show that if

$$c^p = (a+b)(a+\zeta b)(a+\zeta^2 b)(a+\zeta^3 b)\cdots(a+\zeta^{p-1}b)$$

then each $a+\zeta^n b$ is a $p$th power, leading to a contradiction. He encountered many difficulties which he was able to resolve in a large number of cases, and was able to prove the theorem for *regular* primes. No one knows if there are infinitely many of these primes, but there are infinitely many of the other kind, the *irregular* ones, the first one being $p = 37$. He was able to overcome some of the difficulties with irregular primes and prove the theorem for all prime $p < 100$. The statement of Fermat's Last Theorem is often divided into two cases:

**First Case.** There do not exist integers $a$, $b$, $c$ such that $abc$ is NOT divisible by $p$ and $a^p + b^p = c^p$.

**Second Case.** There do not exist integers $a$, $b$, $c$, all different from 0, such that $p$ is a divisor of $abc$ and $a^p + b^p = c^p$.

The first case of Fermat's Last Theorem is considered easier than the second case. In 1909 Wieferich discovered a simple criterion for the first case. If the first case fails for exponent $p$ then $p^2$ is a factor of $2^{p-1} - 1$. Then in 1910 Mirimanoff, after understanding Wieferich's proof, showed that if the first case fails for $p$ then $p^2$ is a factor of $3^{p-1} - 1$. Then by 1971 the first case was proved for all $p < 3 \times 10^9$. The second case is harder and up to 1993 the theorem was proved for all primes $p < 4,000,000$.

In 1983, Gerd Faltings showed that if $a^n + b^n = c^n$ for $n > 2$ had a solution, then there could only be finitely many of them.

[5]Fermat's Last Theorem has been featured in science fiction; attempting a solution was even mentioned as a hobby of Captain Jean-Luc Picard in a Star Trek New Generation episode called "The Royale".

In 1985 L.M. Adleman, D.R. Heath-Brown, and E. Fouvry used Sophie Germain's results together with difficult analytic estimates to prove that there are infinitely many primes $p$ such that $a^p + b^p = c^p$ has no solutions with $p$ not dividing $abc$.

In 1985 Gerhart Frey suggested a new line of attack on Fermat's problem using a notion called modularity. He wrote down the cubic curve

$$y^2 = x(x + a^n)(x - b^n)$$

where $(a, b, c)$ is a primitive solution of $a^n + b^n = c^n$ where $n > 2$. This curve is called an elliptic curve[6]. In general, elliptic curves are given by equations of the form

$$y^2 = x^3 + ax^2 + bx + c.$$

The numbers $a$, $b$, and $c$ are fixed and the notion of modularity came about from studying the rational points on such curves[7]. Frey suggested in a lecture at Oberwolfach in 1985 that the above curve might contradict the Taniyama-Shimura conjecture that every elliptic curve with coefficients that are rational numbers is modular. He highlighted several features of these elliptic curves that seemed too good to be true. Kenneth Ribet(1990) proved that this elliptic curve is NOT modular. But Andrew Wiles(1994) proved that it had to be! Hence the contradiction proving Fermat's Last Theorem.

Andrew Wiles(1953- ) received his Ph.D. at Cambridge University where his supervisor was an Australian, John Coates. He accepted a full professorship at the prestigious Harvard University in the early eighties, and very soon after that he decided to spend all of his research time trying to prove Fermat's Last Theorem. This was done with much secrecy since he was afraid that others, who also knew the results that he was using to try to prove the theorem, might also get interested and prove the theorem before he did. In particular, he wanted to keep it secret from Gerd Faltings, a brilliant, and brusque, young German who for several years was a Princeton Institute of Advanced Study colleague of Wiles's. In May of 1993 Wiles thought he had a proof and had taken Professor Nick Katz into his confidence, to check the details of his arguments. The proof was completed just in time to be delivered at a conference in Cambridge, England, in June, organized by his former supervisor John Coates. He told Professor Coates that he wanted to have three lectures to present his ideas instead of the one hour offered. The title of Wiles' talks was "Modular Forms, Elliptic Curves, and Galois Representations," but the title gave no hint where the lectures would lead.

The write-up of his results took 200 pages and Wiles was done just in time to catch his plane for England. After his first two lectures on Monday and Tuesday June 21st and 22nd, 1993, the question from Kenneth Ribet and others in the audience was "What can he possibly say on Wednesday?" When Wiles finally delivered the coup de grâce the last day of the conference a little after 10:30a.m. on June 23rd, he did it with characteristic understatement and, he admits, a little dramatic forethought. He turned from the blackboard, covered in algebraic script, faced the audience and smiled: "I'd better stop there."

[6]An elliptic curve is not an ellipse. Elliptic curves first arose when mathematicians tried to compute the circumference of an ellipse, and hence the name.

[7]The delightful book by Joseph H. Silverman entitled *A Friendly Introduction to Number Theory* from Prentice Hall gives an excellent explanation of how these ideas help to prove Fermat's Last Theorem.

The roof fell in in September when his colleague Nick Katz had a problem working out some details. By December Wiles was persuaded to enlist the help of another mathematician. He settled on Richard Taylor, a promising young Cambridge mathematician who had been taught by Wiles and who was familiar with the "proof". Finally around 10a.m. on the morning of September 19, 1994 Wiles had closed the gap and the seven-year quest for the mathematician's Holy Grail was over! With Taylor's help in writing up and "TEX-ing" the report it was ready on October 6, 1994 and sent off by Federal Express to three mathematicians to check all the details. They were Henri Darmon, a French-Canadian mathematician at McGill, Fred Diamond, a young American mathematician at Princeton, and Gerd Faltings at the Max Planck Institute in Bonn, who all said it was correct and complete. The full manuscript is published in *Annals of Mathematics* vol 141, no. 3, May 1995 containing Wiles' original Cambridge paper and the correction by Taylor and Wiles.

There was a conference on Fermat's Last Theorem at Boston University in August 1995. On Friday afternoon, August 18, 1995, the last day of the conference, while giving a talk entitled "Modularity of Semistable Elliptic Curves," Andrew Wiles thanked Gerhart Frey for his great ideas and asked him if he had any ideas about certain zeros of the Riemann Zeta function. At this conference t-shirts were sold with a very brief proof on the front and references on the back. This proof is given on the last page.

Amateur mathematicians (often cranks) came out of the woods in large numbers after the so called Wolfskehl prize of 1908 for a solution was announced. It was an enormous amount of money — 100,000DM at a time when the mark was transferable into gold. At the time 100,000DM was worth roughly 38 kgs of gold! The competition for the Wolfskehl prize is now over since Andrew Wiles was awarded this prize amounting to £30,000 on June 27, 1997[8].

**Bibliography**

Here are some books that are very helpful to start learning some of the mathematics behind Fermat's Last Theorem.

*A Friendly Introduction to Number Theory 3rd ed.*, Joseph H. Silverman, Prentice Hall, Upper Saddle River, NJ 07458, 2006.

This is the best introductory and elementary book in Number Theory that I have read. It is well motivated and explains some of the mathematics behind the proof of FLT.

*Fermat's Enigma*, Simon Singh, Viking Penguin, 1997.

This is a delightful book for the amateur giving the history of FLT. There is a video that complements the above book very well. It is one of the Nova Series videos entitled *The Proof* which is written and produced by John Lynch, and directed by Simon Singh. (See the Internet address: http://www.wgbh.org.)

[8]The prize was greatly decreased by virtue of inflation following the world wars.

# Appendix: A Geometric solution to $a^2 + b^2 = c^2$.

We can attack the problem of finding all the solutions of the Diophantine Equation $a^2+b^2 = c^2$ by dividing this equation by $c^2$, obtaining

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

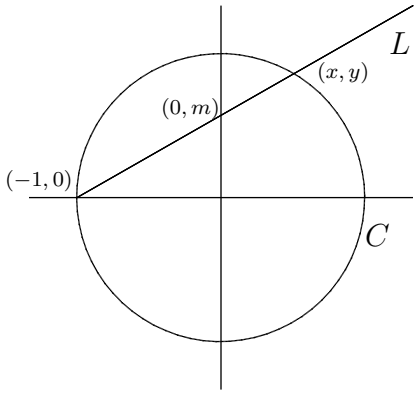
So the pair of rational numbers $(a/c, b/c)$ is a solution to the equation

$$x^2 + y^2 = 1.$$

We know that this is the equation of a circle $C$ with radius 1. We will use the geometry of $C$ to find all the points on $C$ whose $xy$-coordinates are rational numbers. Consider the line through $(-1, 0)$ having slope $m$:

$$L: \quad y = m(x + 1) \qquad \text{(point-slope formula)}.$$

It is clear from the picture that the intersection $C \cap L$ consists of exactly two points, and one of those points is $(-1, 0)$. We want to find the other one.




To find the intersection of $C$ and $L$, we need to solve the equations

$$x^2 + y^2 = 1 \quad \text{and} \quad y = m(x + 1)$$

for $x$ and $y$. We leave that to the reader. We obtain

$$x = \frac{1 - m^2}{1 + m^2} \quad \text{and} \quad y = \frac{2m}{1 + m^2}.$$

Hence, for every rational number $m$ we get the above rational solution to the equation $x^2 + y^2 = 1$. On the other hand, if we have a solution $(x_1, y_1)$ in rational numbers, then the slope of the line through $(x_1, y_1)$ and $(-1, 0)$ will be a rational number. So by taking all possible values of $m$, we get every solution to $x^2 + y^2 = 1$ in rational numbers (except for $(-1, 0)$, which corresponds to the vertical line having "infinite" slope).

How is the formula for rational points on a circle related to our formula for Pythagorean triples? We can write the rational number $m$ as a fraction $v/u$ and then our formula for $x$ and $y$ becomes

$$(x, y) = \left( \frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2} \right),$$

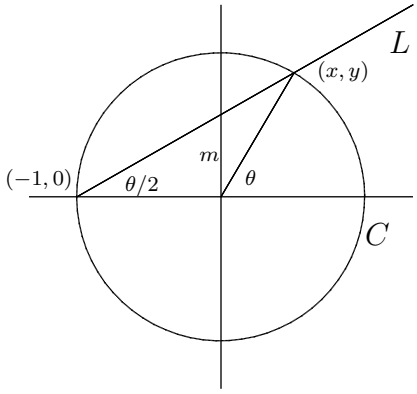
and clearing denominators gives the Pythagorean triple

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2).$$

We can relate this to our formula above by setting

$$u = \frac{s + t}{2} \quad \text{and} \quad v = \frac{s - t}{2}.$$

Let's return to our circle once more, this time to do some trigonometry since we have the point $(x, y)$ written in a form which is very helpful.




Note that

$$\cos\theta = x = \frac{1 - m^2}{1 + m^2} \quad \text{and} \quad \sin\theta = y = \frac{2m}{1 + m^2}.$$

If you have a complicated identity in sine and cosine that you want to test, all you have to do is to substitute for $\cos\theta$ and $\sin\theta$ above, collect powers of $m$ and see if you get zero. Trig identities now become an algebra exercise!

Next assume $\theta$ is positive and less than $\pi$ radians. Can you explain why the angle above is $\theta/2$? Clearly then $m = \tan\frac{\theta}{2}$. Hence we have the following trigonometric identities

$$\tan\left(\frac{\theta}{2}\right) = \frac{\sin\theta}{1 + \cos\theta}, \quad \cos\theta = \frac{1 - \tan^2(\theta/2)}{1 + \tan^2(\theta/2)}, \quad \sin\theta = \frac{2\tan(\theta/2)}{1 + \tan^2(\theta/2)}.$$

These identities are very tedious to derive and are useful in calculus for integrating rational functions involving sines and cosines.

**FERMAT'S LAST THEOREM:** *Let $n$, $a$, $b$, $c \in \mathbf{Z}$ with $n > 2$. If $a^n + b^n = c^n$ then $abc = 0$.*

**Proof:** The proof follows a program formulated around 1985 by Frey and Serre [**F,S**]. By classical results of Fermat, Euler, Dirichlet, Legendre, and Lamé, we may assume $n = p$, an odd prime $\geq 11$. Suppose $a, b, c \in \mathbf{Z}$, $abc \neq 0$, and $a^p + b^p = c^p$. Without loss of generality we may assume $2|a$ and $b \equiv 1 \bmod 4$. Frey [**F**] observed that the elliptic curve $E : y^2 = x(x - a^p)(x + b^p)$ has the following "remarkable" properties: (1) $E$ is semistable with conductor $N_E = \prod_{\ell|abc} \ell$; and (2) $\bar{\rho}_{E,p}$ is unramified outside $2p$ and is flat at $p$. By the modularity theorem of Wiles and Taylor-Wiles [**W,T-W**], there is an eigenform $f \in \mathcal{S}_2(\Gamma_0(N_E))$ such that $\rho_{f,p} = \rho_{E,p}$. A theorem of Mazur implies that $\bar{\rho}_{E,p}$ is irreducible, so Ribet's theorem [**R**] produces a Hecke eigenform $g \in \mathcal{S}_2(\Gamma_0(2))$ such that $\rho_{g,p} \equiv \rho_{f,p} \bmod \wp$ for some $\wp|p$. But $X_0(2)$ has genus zero, so $\mathcal{S}_2(\Gamma_0(2)) = 0$. This is a contradiction and Fermat's Last Theorem follows.
Q.E.D.

## References


[**F**] Frey, G.: Links between stable elliptic curves and certain Diophantine equations. *Ann. Univ. Sarav.* **1** (1986), $1 - 40$.

[**R**] Ribet, K.: On modular representations of $\mathrm{Gal}(\bar{Q}/Q)$ arising from modular forms. *Invent. math.* **100** (1990), $431 - 476$.

[**S**] Serre, J.-P.: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{Q}/Q)$, *Duke Math. J.* **54** (1987), $179 - 230$.

[**T-W**] Taylor, R. L., Wiles, A.: Ring-theoretic properties of certain Hecke algebras. *Annals of Math.* **141** (1995), $553 - 572$.

[**W**] Wiles, A.: Modular elliptic curves and Fermat's Last Theorem. *Annals of Math.* **141** (1995), $443 - 551$.