Fermat's Last Theorem

Read Section 6.4

Turn in Explain the method of decent in your own words

After the Diophantine equation $x^2+y^2=z^2$, one generalization is $x^n+y^n=z^n$ for $n \geq 3$. Fermat's Last Theorem was first conjectured in 1637 and proven in 1995 by Andrew Wiles. Attempts to solve this problem through the centuries have created new branches of mathematics.

Theorem 1 (Fermat's Last Theorem)**.** The Diophantine equation $x^n + y^n = z^n$ has no nonzero integer solutions for $n \geq 3$.

We will show that it suffices to prove Fermat's Last Theorem for the cases of n and odd prime and $n = 4$.

Theorem 2. The Diophantine equation $x^n + y^n = z^n$ has a solution no solutions for $n \geq 3$ if and only if there are no solutions for n an odd prime or $n = 4$.

Proof Let $n \in \mathbb{Z}$ and $n \geq 3$. Let $n = ab$ where $a, b \in \mathbb{Z}$ and b is either an odd prime or 4. If x, y, z is a solution to $x^n + y^n = z^n$, then x^a, y^a, z^a is a solution to $x^b + y^b = z^b$. By contraposition, if $x^b + y^b = z^b$ has no solutions, then $x^n + y^n = z^n$ has no solutions. ■

We will prove the case where $n = 4$ using the *method of decent.* This is the only case that Fermat proved. The next 400+ years were spent proving the theorem for odd primes. We will go through the decent arguement slowly on Monday. However, we can prove other facts about solutions to $x^n + y^n = z^n$. We can also use a similar decent arguement to show $x^4 - y^4 = z^2$ has no nontrivial integer solutions.

In-class Problem 1 (Chapter 6, Exercise 20) Let $x, y, z \in \mathbb{Z}$ and let p be a prime number.

(a) Prove that if $x^{p-1} + y^{p-1} = z^{p-1}$, then $p \mid xyz$.

(b) Prove that if $x^p + y^p = z^p$, then $p \mid (x + y - z)$.

Hint: *Recall* **??** *and* **??**.

Hint: *For the first, try contradiction.*

Theorem 3 (Fermat's Right Triangle Theorem)**.** There are no right triangles with integer side lengths whose area is a perfect square.

Proof For a contradiction, assume that there exists a right triangle with integer side lengths a, b, c and area n^2 for some integer n. Then $a^2 + b^2 = c^2$ from the Pythagorean Theorem and $\frac{ab}{2} = n^2$ from the triangle area formula. Multiplying the second equation by 4 gives $2ab = 4n^2$. Thus,

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

Multiplying these two equations together gives

$$(a + b)^2(a - b)^2 = c^4 - (2n^2)^4.$$

Thus, $x = c, y = 2n^2$, and $z = (a + b)(a - b)$ is a solution to $x^4 - y^4 = z^2$, which we will prove has no solutions. ■

Learning outcomes:

Author(s): Claire Merriman

The idea of the method of decent for proving no solution exists for a Diophantine equation is to assume a solution exists. Then use this solution to construct one that has one component that is strictly smaller than the original solution. This process could be repeated indefinitely, but it is not possible to construct an infinitely decreasing list of positive integers. Thus, no solution exists.

Theorem 4. The Diophantine equation $x^4 + y^4 = z^2$ has not solutions in nonzero integers x, y, z.

Note: If x, y, z is a solution to $x^4 + y^4 = z^4$, then

Multiple Choice:

(a) x, y, z

(b) x, y, z^2 ✓

is a solution to $x^4 + y^4 = z^4$. By contraposition, if $x^4 + y^4 = z^2$ has no solutions, then $x^4 + y^4 = z^4$ has no solutions.

Proof Assume by way of contradiction, that $x^4 + y^4 = z^2$ has a solution x_1, y_1, z_1 nonzero integers. Without loss of generality, we may assume $x_1, y_1, z_1 > 0$ and $(x_1, y_1) = 1$. We will show that there is another solution x_2, y_2, z_2 positive integers such that $(x_2, y_2) = 1$ and $0 < z_2 < z_1$. Now, $(x_1)^2, (y_1)^2, z_1$ is a Pythagorean triple with $(x_1^2, y_1^2, z_1) = 1$, and without loss of generality, y_1^2 is even. Thus, by **??** says that there exists $m, n \in \mathbb{Z}$ such that $(m, n) = 1, m > n > 0$, and exactly one of m and n is even such that $x_1^2 = m^2 - n^2, y_1^2 = 2mn, z_1 = m^2 + n^2$. Now, $x_1^2 = m^2 - n^2$ implies $x_1^2 + n^2 = m^2$ and x_1, m, n is a Pythagorean triple with $(x_1, m, n) = 1$ and n is even.

Applying the **??** again, we get that there exists $a, b \in \mathbb{Z}$ with $(a, b) = 1, a > b > 0$, exactly one of a and b is even, with $x_1 = a^2 - b^2, n = 2ab, m = a^2 + b^2$.

We want to show that m, a and b are perfect squares. Now, $y_1^2 = 2mn = m(2n)$ and $(m, 2n) = 1$, we have that

Select All Correct Answers:

(a) m ✓

(b) n

(c) 2n ✓

are perfect squares. Thus, there exists $c \in \mathbb{Z}$ such that $2n = 4c^2$ or, equivalently, $n = 2c^2$. Now, $n = 2ab$ and $(a, b) = 1$, we have that

Select All Correct Answers:

(a) a ✓

(b) b ✓

(c) 2b

are perfect squares.

There exists x_2, y_2, z_2 such that

Multiple Choice:

(a) $m = x_2^2$

(b) $m = y_2^2$

(c) $m = z_2^2$ ✓

Multiple Choice:

(a) $a = x_2^2$ ✓

(b) $a = y_2^2$

(c) $a = z_2^2$

and

Multiple Choice:

(a) $b = x_2^2$

(b) $b = y_2^2$ ✓

(c) $b = z_2^2$.

Without loss of generality, we may assume $x_2, y_2, z_2 > 0$. Then $m^2 = a^2 + b^2$ implies $z_2^2 = x_2^4 + y_2^4$, so that x_2, y_2, z_2 is a solution with positive integers to $x^4 + y^4 = z^2$. Also $(x_2, y_2) = 1$ and $0 < z_2 \leq z_2^2 = m \leq m^2 < m^2 + n^2 = z_1$.

Thus, we have constructed another solution as desired. That is, we assumed the existence of a solution to $x^4 + y^4 = z^2$ in the positive integers, we can construct another solution with a strictly smaller value of z. This is a contradiction since there are only finitely many positive integers between a given positive integer and zero. So $x^4 + y^4 = z^2$ has no solutions on nonzero x, y, z. ■