Euler's Work on Fermat's Last Theorem

Karthik Balakrishnan

April 18, 2018

Lemma 1

The product of distinct primed can never be a power of any kind (for example a square).

Proof. This lemma has already been proven by Fermat, so Euler didn't feel like proving it. It is a trivial proof that stems from the Fundamental Theorem of Arithmetic.

Lemma 2

If $a^2 + b^2 = c^2$ such that a and b are co-prime. Then we can represent $a = p^2 - q^2$, and $b = 2pq$, where p and q are co-prime. If p is odd then q is even and vice versa.

Proof. Because $a^2 + b^2$ is a square, we set its root equal to $a + \frac{bp}{q}$ where $\frac{q}{p}$ is expressed in the smallest terms. Thus we get ...

$$a^2 + b^2 = a^2 + \frac{2abq}{p} + \frac{b^2q^2}{p^2}$$

... and can then say ...

$$a : b = (p^2 - q^2) : 2pq.$$

The integers $p^2 - q^2$ and $2pq$ are either co-prime or have a common divisor of 2. In the former, we have completed the construction of the three terms and proven the lemma. In the latter, $2|(p^2 - q^2) = (p - q)(p + q)$ meaning that either $(p - q)$ or $(p + q)$ is even. Quickly we realize that since both p and q are positive integers if one of the two factors of $p^2 - q^2$ is divisible by 2, then both must be divisible by 2 due to parity. Therefore, we can say $p + q = 2s$ and $p - q = 2s$ and then manipulate to get $p = r + s$ and $q = r - s$ where r and s are co-prime. Substituting this into $b = 2pq$, we get $b = 2(r + s)(r - s) = 2(r^2 - s^2)$ and $a = p^2 - q^2 = 2(2rs)$. Thus we see that when both numbers are even, we have a non primitive pythagorean triple which can be reduced to its primitive case where one term is odd and the other is even.

Corollary 1

If the sum of two mutually primitive squares is a square, it is necessary that the one square is even, the other is odd. It follows that the sum of two odd squares is not a square.

Corollary 2

If $a^2 + b^2$ is a primitive square, one of the numbers is odd and the other is even. The odd can be written as $a = p^2 - q^2$ and the even can be expressed as $b = 2pq$.

A Stronger Version of Fermat's Last Theorem for N=4

There are no three integers x, y, and z such that $xyz \neq 0$ and $x^4 + y^4 = z^2$.

Proof. Proof by contradiction. Assume that the hypothesis is true for integers x, y, and z We begin by invoking corollary 2, which states that if ...

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

... then we can write, without loss of generality, that ...

$$x^2 = a^2 - b^2$$

$$y^2 = 2ab.$$

Where a and b are relatively prime numbers. Now we can take the first statement and rewrite it as another Pythagorean Triple ...

$$x^2 + b^2 = a^2$$

... and once again we can say that ...

$$b = 2cd$$

$$x = c^2 - d^2$$

$$a = c^2 + d^2$$

Now notice that $y^2 = 2ab$. Using our new equations we can rewrite the expression as $y^2 = 2(c^2+d^2)(2cd) = 4cd(c^2+d^2)$. Since a and b are relatively prime, cd must be some square number e^2 and c^2+d^2 must be some square number f^2. If $cd = e^2$, and c and d are co-prime, c must be some square g^2 and $d = h^2$. Plugging this in ...

$$c^2 + d^2 = f^2 \rightarrow (g^2)^2 + (h^2)^2 = f^2.$$

We have arrived to an equation of the same form as our initial equation and f^2 is strictly less than z^2. We can repeat these same steps again and again, creating infinitely smaller cases. But alas, there are only a finite amount of integers below z^2 and above 0. Thus we have reached a contradiction, and by infinite descent our assumption must be false.

Another Impossible Diophantine Equation

There are no three integers x, y, and z such that $xyz \neq 0$ and $x^4 - y^4 = z^2$.

Proof. Proof by Contradiction. Assume that we do have three numbers of the form mentioned above, we can rewrite the above to give us ...

$$x^4 = y^4 + z^2.$$

Now when we invoke corollary 2, we get one of two cases:

Case 1

Since $(x^2)^2 = (y^2)^2 + z^2$, we can say ...

$$z = 2mn, \;\; y^2 = m^2 - n^2, \;\; x^2 = m^2 + n^2$$

.

If so, we can multiply x^2 and y^2 and rewriting the product we get ...

$$m^4 - n^4 = (xy)^2.$$

Because $x, y < z$, $xy < z^2$, meaning that we have generated three numbers of the same form as our initial case that are strictly smaller than the original. We can do this process infinitely, but between z and 0, there are only finitely many integers. We have reached a contradiction and our assumption must be false.

Case 2

Since $(x^2)^2 = (y^2)^2 + z^2$, we can say ...

$$z = m^2 - n^2, \;\; y^2 = 2mn, \;\; x^2 = m^2 + n^2.$$

From this we can write $(\frac{y}{2})^2$ as ...

$$\left(\frac{y}{2}\right)^2 = \frac{mn}{2}.$$

From corollary 2, we know that either m or n is even. Without loss of generality, we can say that $\frac{m}{2} = k$. Since $2mn$ must be a square number and n is relatively prime to m and $\frac{m}{2}$, we can say that $n = a^2$ for integer some a and $\frac{m}{2} = b^2$ for some integer b. Plugging these values into our equation for x^2 we get ...

$$x^2 = n^2 + m^2 = a^4 + 4b^4.$$

We can rewrite this equation and invoke corollary 2 to get ...

$$x^2 = (a^2)^2 + (2b^2)^2$$

$$a^2 = c^2 - d^2, \;\; 2b^2 = 2cd, \;\; x = c^2 + d^2$$

... therefore $b^2 = cd$ meaning that $c = e^2$ and $d = f^2$ for some integers e and f. Plugging this into our equation to the equation for a^2 we get ...

$$e^4 - f^4 = a^2.$$

Thus we have constructed a smaller case of the same form and can do this infinitely. But there are only finitely many triplets of numbers under the original and above 0. We have reached a contradiction and our assumption must be false.