Howard University Math Department

Pythagorean triples

PYTHAGOREAN TRIPLETS AND FERMAT"S LAST THEOREM

We know $x^2 + y^2 = z^2$ has integer solutions. For example $3^2 + 4^2 = 5^2$. Such solutions are called **Pythagorean triplets**.

Note that $x^3 + y^3 = z^3, x^4 + y^4 = z^4$, etc., have no solutions.

In other words, $x^n + y^n = z^n$ has no solutions for $n > 2$.

This is called Fermat's Last Theorem and was proved by English mathematician Andrew WIles in 1996.

FINDING ALL SOLUTIONS OF $x^2 + y^2 = z^2$.

USING COMPLEX NUMBERS

Recall that $(a + bi)(c + di) = ac - bd + (ad + bc)i$.

Given $z = m + ni$, we have the absolute value given by $|z| = \sqrt{m^2 + n^2}$.

The absolute value is just the distance of the point (a, b) from the origin (0,0).

It is a basic fact that the absolute value of a product is the product of the absolute values.

In other words $|zw| = |z||w|$.

In particular $|z^2| = |z|^2$.

Expanding we get $|m^2 - n^2 + 2mni| = (\sqrt{m^2 + n^2})^2 = m^2 + n^2$.

On the other hand $|m^2 - n^2 + 2mni| = \sqrt{(m^2 - n^2)^2 + (2mn)^2}$.

So we get after squaring both sides

$$(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2.$$

Check this using algebra !

So we get the following formula for Pythagorean triples:

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2 \implies x^2 + y^2 = z^2. \quad (1)$$

In other words, starting with any two natural numbers (or even integers) m, n we can manufacture Pythagorean triplets x, y, z using equation (1).

For example $m = 2, n = 1$ gives $m^2 - n^2 = 3, 2mn = 4, m^2 + n^2 = 5$.

$m = 3, n = 2$ gives $m^2 - n^2 = 5, 2mn = 12, m^2 + n^2 = 13$.

Check that $5^2 + 12^2 = 13^2$.

In fact we see that we can generate infinitely many Pythagorean triplets this way, using equation (1).

QUESTION: ARE ALL PYTHAGOREAN TRIPLETS GENERATED THIS WAY?

We will see the answer on monday.

PROOF THAT ALL PYTHAGOREAN TRIPLES ARE GIVEN BY EQUATION (1)

We will do this in several steps.

All of the below involve only integers.

First note that if $x^2 + y^2 = z^2$ and x, y, z have a common factor d, then writing $x = dx_1, y = dy_1, z = dz_1$ we get $d^2(x_1^2 + y_1^2) = d^2 z_1^2$.

Dividing both sides by d^2 we get $x_1^2 + y_1^2 = z_1^2$ with x_1, y_1, z_1 not having a common factor.

The triples with no common factors are called **Primitive Pythagorean Triples.** In fact they wouln't have a common factor even between any two of the numbers x, y, z, as shown next.

1. Show that if two of x, y, z have a common factor, then all three have a common factor.

   Proof: Same as above, just bring the two terms divisible by a common factor d to one side and show that it divides the third term that is on the other side.

2. Show that if $x^2 + y^2 = z^2$ is a primitive triple then at least one of x, y have to be odd.

   Proof: If both are even then z would also have to be even. But then 2 divides all three and that is not possible since they are primitive.

3. Show that if $x^2 + y^2 = z^2$ is a primitive triple then exactly one of x, y can be odd.

   Hint: What happens if both are odd? First show that 4 divides z^2.

   Proof: If both are odd then x^2+y^2 is even, which means 2 divides z^2. But this means 2 divides z. (If z were odd then z^2 would be odd also). Letting $z = 2z_1$ we get $z^2 = 4z_1^2$. So we have proved that 4 divides z^2.

   Now let $x = 2m + 1, y = 2n + 1$. We get

   $x^2+y^2 = (2m+1)^2+(2n+1)^2 = 4m^2+4m+1+4n^2+4n+1 = 4A+2$, *with* $A = m^2+m+n^2+n$.

   This means that, on the LHS when you divide by 4 you get a remainder of 2.

   On the other hand on the RHS the remainder is 0 because 4 divides the RHS!

   This means that only one of x, y is odd.

   Let x be odd and y be even. [This means z will be odd]. If x is even and y is odd proof will be exactly the same.

   Now we can write $y^2 = z^2 - x^2$. SInce we agreed y is even, we get that $z^2 - x^2 = (z - x)(z + x) = 4k^2$ for some k.

4. Show that since x, z have no common factors and both are odd, the gcd of $z - x$ and $z + x$ is 2.

   Proof. Suppose not. Clearly, since sum and difference of two odd numbers is even, we have that 2 divides $z + x$ and $z - x$. Suppose they have another common factor d after dividing both by 2. Then $z - x = 2da, z + x = 2db$. Then by solving for z and x we get that $z = d(a + b), x = d(b - a)$ divides both, which is a contradiction. So $z - x = 2a, z + x = 2b$ and a, b have no common factors.

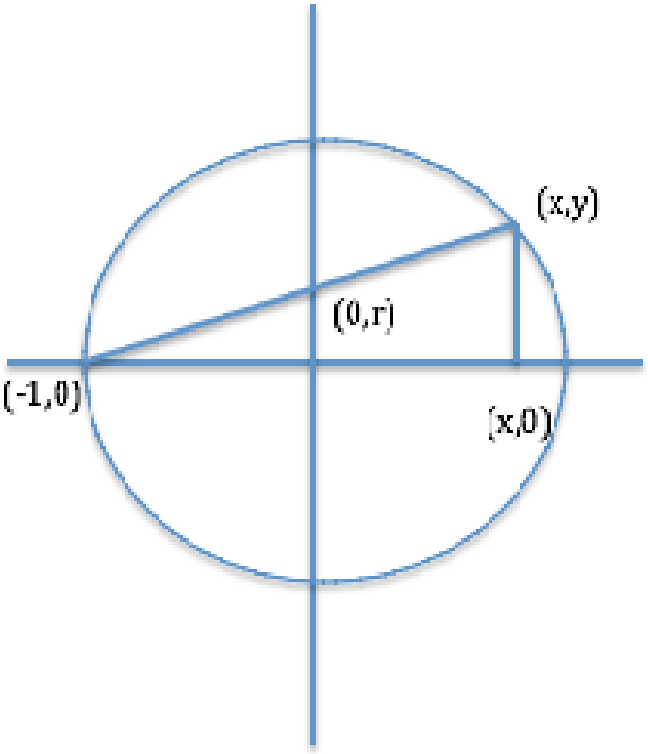
5. Show that in the above if $y^2 = (z - x)(z + x)$ then $a = n^2, b = m^2$ for some m, n.

PROOF USING GEOMETRY

For the geometric proof look of the unit circle below. The points on the $y-$axis are in 1-1 correspondence with the points on the circle.

The idea is to show that, points with rational coordinates on $y-$axis correspond to points with rational coordinates on the unit circle.

So $(0, r)$ will have $r = n/m$ for some integers n, m iff x, y are rational numbers.



6. Prove that if the point on the $y-$axis $(0, r)$ will have $r = n/m$ for some integers p, q iff the point on the circle (x, y) has x, y as rational numbers. Remember that radius of circle is 1.