Theorem: An odd prime number can be written as the sum of two square numbers if and only if it is one more than a multiple of 4. Also, this can only be done in one way except for reording the two squares. For example, 37 is prime and one more than 4*9 and it can be written as $6^2 + 1^2$ and is not the sum of two squares in any other way, and 43 is prime and not one more than a multiple of 4 and cannot bewritten as the sum of 2 squares.

Levels recommended for proof: 4

Proof:

The proof that every prime number that is 3 more than a multiple of 4 is not the sum of two squares is the easy part. An even number squared is a multiple of 4, and an odd number can be written as 2k+1, so its square is $4k^2 + 4k + 1$ by simple alebgra which is clearly 1 more than a multiple of 4. Therefore any square number is 0 or 1 more than a multiple of 4, so the sum of 2 square numbers can never be 3 more than a multiple of 4.

Now if we have an odd prime, it is not the sum of two odd numbers squared or two even numbers squared because otherwise it would be an even. So we want to investigate whether it is the sum of an even number squared and an odd number squared. The even number can be written as 2k and therefore we are looking at $p = x^2 + (2k)^2 = x^2 + 4k^2$ where p is prime. We now write $p = x^2 + 4yz$ and we want to solve for when $y = z$. What happens is that if y is not z, we can interchange the order of y and z to get a pair of solutions. Therefore if we could somehow show that there were an odd number of different solutions with x, y and z positive integers and p an odd prime 1 nore than a multiple of 4 to $p = x^2 + 4yz$, we would know there has to be at least one with y and z the same so we would be done.

Now here comes the fun part:

We represent the x^2 part as an $x * x$ grid square. We represent the $4yz$ part as 4 $y * z$ grid rectangles. We place them in a windmill configuration like this:

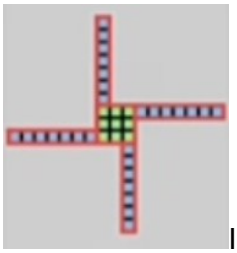
Image of the windmill configuration. The area is clearly $p = x^2 + 4yz$ squares.

Lets suppose that y is the length of the side that touches the square, so in the image above $y = 1$. In cases like these where $y < x^2$, we can generate another solution by modifying the windmill diagram slightly as shown below:

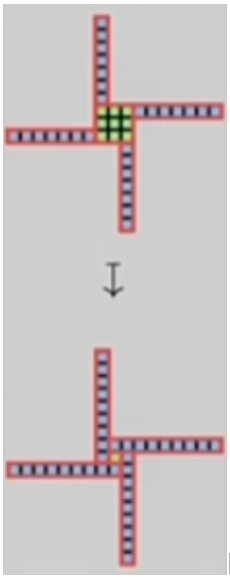
Image of the transformation

This transforms a solution of the $y < \frac{x}{2}$ case into the $y > z + x$ case. So we have a pairing between two solutions in the two cases.

Now lets look into the $\frac{x}{2} < y < x$ case and the $x < y < x + z$ case. They are also a pair, as shown below.

So this leaves three cases. $y = \frac{x}{2}, y = x, y = x + z$. If you are smart, you will realize that we have not yet used the fact that p is prime, which we need to do. If p is not prime, the theorem is not generally true (consider 21).

If $y = \frac{x}{2}$ then $x^2 + 4yz = x^2 + 2xz = x(x + 2z) = 2y(x + 2z)$ which is a problem as that is divisible by y.

If $y = x + z$ then our diagram will look like a square, and a square number is not prime.

If $y = x,\ x^2 + 4yz = x^2 + 4xz$, which is divisible by x. Therefore the only possibility is that $x = y = 1$. In this case, $z = \frac{p-1}{4}$ always gives us a solution that looks like the straight cross in the image below.

To put it another way, p is a 1 more than a multiple of 4, so write p as 1+4k, so the straight cross with a block in the middle and four rectangles of length k will always exist. This is the only way that we do not have a pairing with another windmill diagram, as we have ruled out all the cases.

Therefore, since there are a bunch of pairs and the straight cross, we have no shown that $p = x^2 + 4yz$ has an odd number of solutions. This means p can be written as the sum of two squares by the logic above.

Now here comes the boring part:

Now it remains to show that this can be done in a unique way.

Side note: This can be done really elegantly by factoring $p = x^2 + y^2 = (x + iy)(x - iy)$ and using the fact that the complex integers factor uniquely, but we do not assume that you know what this means or how to prove it, so I will now do this in a more elementary way.

So suppose $p = a^2 + b^2$ and $p = c^2 + d^2$ and $a \neq c, d, b \neq c, d$. Then one can check by expanding everything that

$$p^2 = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

Also $p - a^2 = b^2$ and $p - c^2 = d^2$. Therefore $(p - a^2)d^2 = b^2d^2 = (p - c^2)b^2$. Therefore we can rearrange $(p - a^2)d^2 = (p - c^2)b^2$ to get $p(d^2 - b^2) = (ad)^2 - (bc)^2 = (ad - bc)(ad + bc)$. One can check by expanding everything and moving all terms to one side that these equations are indeed equivalent. p is prime so it either divides $ad - bc$ or $ad + bc$. p cannot divide $ad - bc$ because we know from earlier that $p^2 = (ac + bd)^2 + (ad - bc)^2$, but if p did divide $ad - bc$, we would know that $(ad - bc)^2 \geq p^2$ so $(ac + bd)^2 \leq 0$. This would force $ad - bc = 0$ so we could conclude that $p(d^2 - b^2) = (ad - bc)(ad + bc) = 0$ so $d^2 = b^2$, hence contradicting the assumption that we have a non-unique solution. Otherwise, if p divides $ad + bc$, then note that $p^2 = (ac + bd)^2 + (ad - bc)^2$ and this is just equal to $(ad + bc)^2 + (ac - bd)^2$, so therefore either $ad + bc = 0$, or we are in the situation where $p = ad + bc$ and $ac = bd$ as if both of these were false $(ad + bc)^2 + (ac - bd)^2$ would be greater than p^2 for the same reason as in the first case. If $ad + bc = 0$ then again $p(d^2 - b^2) = (ad - bc)(ad + bc) = 0$ so $d^2 = b^2$. So the last case is when $ac = bd$. Note that the highest common factor of a and b must be 1, otherwise $p = a^2 + b^2$ is divisible by that factor squared, same for c and d. Therefore a and b do not share any prime factors and neither do c and d. Therefore in the equation $ac = bd$ all the prime factors in a have to go into d and all prime factors of d have to go into a, so a and d have the same prime factors, so $a = d$, so there is no case where $a \neq c, d, b \neq c, d$.