On sum of squares

Stefanus Koesno[1]

[1] Somewhere in California

San Jose, CA 95134 USA

(Dated: November 28, 2017)

Abstract

Here's my struggle in coming up with a proof of $p = a^2 + b^2$ for $p \equiv 1 \pmod 4$, so, many twists and turns later here it is :)

The first thing I notice was that since $p \equiv 1 \pmod 4$,

$$\begin{aligned}(-1)^{\frac{p-1}{2}} &= (-1)^{\frac{(4m+1)-1}{2}} \\ &= (-1)^{2m} \\ &= +1\end{aligned}$$

and therefore -1 is a quadratic residue say $\equiv a^2 \pmod p$, therefore

$$a^2x^2 \equiv -x^2 \pmod p$$

this is true for **any** $x \in (\mathbb{Z}/p\mathbb{Z})^*$. The trick now is to show that if we transform the above to equality rather than equivalence we get

$$y^2 + x^2 = p$$

But it was not too obvious yet how to get there, the only thing I can see is induction, like so

$$\begin{aligned}a^2x^2 + x^2 &\equiv 0 \pmod p \\ &= pw\end{aligned}$$

My strategy was to show that if all primes (1 mod 4) up to p are of the form $a^2 + b^2$ we can show that p must be a sum of two squares too. But still didn't know where to go yet.

Another thing I stumbled upon in this misadventure is Wilson's Theorem, for a prime p

$$\begin{aligned}(p-1)! &\equiv -1 \pmod p \\ 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdots (-2) \cdot (-1) &\equiv -1 \pmod p \\ \left[\left(\frac{p-1}{2}\right)!\right]^2 (-1)^{\frac{p-1}{2}} &\equiv -1 \pmod p\end{aligned}$$

for $p = 4m + 1$ we have

$$[(2m)!]^2 \equiv -1 \pmod p$$

so the roots of -1 are

$$(2m)! \qquad \text{and} \qquad -(2m)!$$

I was hoping that an "explicit" form of the root of -1 would get me somewhere but it went nowhere quite fast :)

Back to the induction attempt, this shows that

$$\begin{aligned}[(2m)!]^2 + 1^2 &\equiv 0 \pmod{p} \\ &= pw\end{aligned}$$

If we inductively assume that all primes ($\equiv 1 \pmod 4$) up to $p = 4m + 1$ has the form $a^2 + b^2$ we can also deduce that p is also of that form, the problem is that w will certainly contain other prime factors much bigger than p since $(2m)!$ is a very large number, so induction fails at this stage.

But worry not, we still have some tricks up our sleeves :) The good thing is that we work with equivalences, so we can use the smaller equivalence of $(2m)!$ to minimize the factorial, say $r \equiv (2m)! \pmod p$ with $r < p$, this is guaranteed, I even (unnecessarily) minimized it further by noting that we have two roots of -1 and we can choose the smaller one. But again, it's not necessary. So what we have now is

$$\begin{aligned}[(2m)!]^2 + 1^2 \equiv r^2 + 1^2 &\equiv 0 \pmod{p} \\ \rightarrow r^2 + 1^2 &= pw\end{aligned}$$

Another worry I had (again unnecessary) was that w can contain primes bigger than p, and that would render the induction useless because instead of possible infinite descend we will get an infinite ascend :)

A break through came after I played around with the actual numbers using maxima, the code is shown below

```
t:0;
a:1277;
for j:1 thru 100 do
block(
```

```
    a:next_prime(a),
    if (mod(a,4) = 1) then
    block(
        t:mod(factorial((a-1)/2),a),
        t:ifactors(t^2+1),
        display(t),
        display(a),
        for i:1 thru length(t) do
        block(
            if (mod(t[i][1],4)>2) then
            block(
                display(t[i][1])
            )
        )
    )
);
display(t);
```

I saw that w only contains have primes less than p and another thing, which I already observed previously, is that all prime factors of w is either 2 or of the form $4u+1$.

Then I realized, of course!, w can only contain prime factors less than (or equal to) p because since $r < p$, we must have $r^2 + 1 \leq p^2$ and so w cannot have factors bigger than p (if $r^2 + 1 = p$ then we are done so we need not care of this case). So our induction is on track.

The next thing we need to show is that w can only contain prime factors of the form $4u + 1$ or 2, it cannot contain a prime factor of the form $4u - 1$ because assume the opposite, then

$$\begin{aligned} r^2 + 1 &= psw', \qquad s \text{ of the form } 4u-1, \quad w = sw' \\ &\equiv 0 \pmod{s} \\ r^2 &\equiv -1 \pmod{s} \end{aligned}$$

but for a prime of the form $4u-1$, (-1) cannot be a quadratic residue so the above is false and we show that w cannot contain a prime factor of the form $4u-1$.

The next and final ingredient we need what I saw some time ago regarding the multiplication of two sums of squares

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

i.e. if we have two sums of squares we can multiply them together to get another sum of squares. It can be easily seen if we express them in complex numbers

$$\begin{aligned} A \cdot C &= (a+ib)(c+id) \\ \rightarrow |A||C| &= |(a+ib)(c+id)| \\ (a^2+b^2)(c^2+d^2) &= (ac-bd)^2 + (ad+bc)^2 \end{aligned}$$

Note that this relationship enjoys obvious symmetries because

$$|a+ib| = |b+ia| = |a-ib| = |b-ia|$$

the first equality is from $a \leftrightarrow b$, the second is from $b \rightarrow -b$ and the last is from $a \rightarrow -a$, and they also apply to c and d therefore

$$\begin{aligned} (a^2+b^2)(c^2+d^2) &= (ac-bd)^2 + (ad+bc)^2 \\ &= (bc-ad)^2 + (bd+ac)^2, && a \leftrightarrow b \\ &= (ac+bd)^2 + (ad-bc)^2, && b \rightarrow -b \\ &= (ac+bd)^2 + (bc-ad)^2, && a \rightarrow -a \end{aligned}$$

Note also that $a \leftrightarrow b$ is the same as $a \rightarrow -a$ and $c \leftrightarrow d$ is the same as $b \rightarrow -b$ but $a \rightarrow -a$ is the same as $b \rightarrow -b$ and of course doing both will get us back to where we started. The above two are the only symmetries we have, negating c or d will get us one of those two. Another way of looking at it, which is my favorite is to write them down as matrices, write the complex numbers as follows

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad C = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \longrightarrow AC = \begin{pmatrix} (ac-bd) & (ad+bc) \\ -(ad+bc) & (ac-bd) \end{pmatrix}$$

If we now take the determinant, noting that determinant of a product is the product of the determinants

$$|AC| = |A||C| = \begin{vmatrix} (ac-bd) & (ad+bc) \\ -(ad+bc) & (ac-bd) \end{vmatrix}$$
$$\rightarrow (a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$$

Why do we need all this? From our induction we know that

$$r^2 + 1^2 = pw$$

w might only contain 2 or primes less than p of the form $4u+1$ and by our hypothesis they are all sums of squares and from above we know that product of sums of squares is again a sum of squares (note that $2 = 1^2 + 1^2$) and so we peel of this equation one layer (one prime factor) at a time

$$r^2 + 1^2 = pw$$
$$r^2 + 1^2 = pw_1 w_2 \cdots w_n$$

say $w_1 = a^2 + b^2 \rightarrow (r^2 + 1^2) = P(a^2 + b^2) = Pw_1$, if we write this in matrix form

$$\begin{pmatrix} r & 1 \\ -1 & r \end{pmatrix} = P \cdot \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$
$$\rightarrow \frac{1}{(a^2+b^2)} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} r & 1 \\ -1 & r \end{pmatrix} = P$$
$$\frac{1}{(a^2+b^2)} \begin{pmatrix} ar+b & a-br \\ -(a-br) & a+br \end{pmatrix} = P$$

If we take the determinant of the LHS

$$\frac{1}{(a^2+b^2)^2}[(ar+b)^2 + (a-br)^2] = \frac{1}{(a^2+b^2)^2}[(a^2+b^2)(r^2+1^2)]$$
$$\left(\frac{ar+b}{a^2+b^2}\right)^2 + \left(\frac{a-br}{a^2+b^2}\right)^2 = \frac{(r^2+1^2)}{(a^2+b^2)}$$

The RHS is just P and it is an integer, we need to show that each term in the LHS is an integer to show that we can decompose P in terms of sum of two squares. From

$$\begin{aligned}(ar+b)(ar-b) &= a^2r^2 - b^2 \\ &= a^2r^2 + (b^2r^2 - b^2r^2) - b^2 \\ &= r^2(a^2+b^2) - b^2(r^2+1^2)\end{aligned}$$

since a^2+b^2 divides r^2+1^2 it divides the LHS and since it is prime it either divides $(ar+b)$ or $(ar-b)$, say it divides $(ar+b)$ we need to show that it divides $(a-br)$ but it follows immediately since

$$(a^2+b^2)(r^2+1) = (ar+b)^2 + (a-br)^2$$

since the LHS and the first term in the RHS are divisible by a^2+b^2 it must divide the last term on the RHS as well.

Now suppose a^2+b^2 divides $(ar-b)$ we need to rewrite the above as (from the fact that $(a^2+b^2)(c^2+d^2) = (a^2+b^2)(d^2+c^2)$, *i.e.* the product of sum of squares formula is invariant under $a \leftrightarrow b, c \leftrightarrow d$)

$$\left(\frac{ar+b}{a^2+b^2}\right)^2 + \left(\frac{a-br}{a^2+b^2}\right)^2 = \left(\frac{a+br}{a^2+b^2}\right)^2 + \left(\frac{ar-b}{a^2+b^2}\right)^2$$

and from

$$(a^2+b^2)(r^2+1) = (a^2+b^2)(1+r^2) = (a+br)^2 + (ar-b)^2$$

using the same argument, since a^2+b^2 divides the LHS and the last term on the RHS it must also divide the first term in the RHS. And so what we have is

$$P = \begin{cases} \left(\frac{ar+b}{a^2+b^2}\right)^2 + \left(\frac{a-br}{a^2+b^2}\right)^2 & \text{if } a^2+b^2 \text{ divides } (ar+b) \\ \left(\frac{a+br}{a^2+b^2}\right)^2 + \left(\frac{ar-b}{a^2+b^2}\right)^2 & \text{if } a^2+b^2 \text{ divides } (a-br) \end{cases}$$

so what we need is just repeat the process with $w_2, w_2, \ldots$ until we only have p on the RHS of $r^2+1^2 = pw_1w_2\cdots w_n$ and therefore p is also a sum of two squares, doing this continually inductively we show that every prime $p = 4m+1$ can be expressed as a sum of two squares.

Another feature is that this sum is unique (up to ordering of course since $a^2 + b^2 = b^2 + a^2$), so let's choose a convention that if $p = a^2 + b^2$ then $a < b$ (since p is prime $a \neq b$), so say we have two sums representing the same prime

$$\begin{aligned} p &= a^2 + b^2 \\ &= c^2 + d^2 \\ \rightarrow p^2 &= (ac + bd)^2 + (ad - bc)^2 \\ &= (ad + bc)^2 + (ac - bd)^2 \end{aligned}$$

again using the product of sums of squares formula, since p is prime, the three terms are all co-prime and and we get a primitive pythagorean triple

$$\begin{aligned} p^2 = (m^2 + n^2)^2 &= (2mn)^2 + (m^2 - n^2)^2 = (ac + bd)^2 + (ad - bc)^2 \\ = (k^2 + l^2)^2 \quad &= (2kl)^2 + (k^2 - l^2)^2 \qquad = (ad + bc)^2 + (ac - bd)^2 \end{aligned}$$

at this point I got somewhat stuck, because even if we generate two more sums it's still OK as long as they don't generate infinitely many more, my initial strategy was to show there's an infinite descend but it might not exist. So, this endeavor turned out to be quite tricky, I thought this would be a quick proof by contradiction but then again :)

We can also try solutions to Diophantine equations of the form $m^2 + n^2 = k^2 + l^2$ but this is just over the top.

Another strategy was to show that all pythagorean triples are unique, *i.e.* no two triples have the same hypotenuse, but this is evidently wrong as 65 serves as a counter example, $(16, 63, 65)$ and $(33, 56, 65)$, but this counter example also gave me an idea.

So $65 = 1^2 + 8^2 = 4^2 + 7^2$, since we have two sums of squares I tried combining them, but in doing so I found the new solutions are $(25, 60, 65)$ and $(39, 52, 65)$, it's no longer primitive, so this means that the new solutions above are actually divisible by p. So here it goes

$$\begin{aligned} (ac + bd)(ac - bd) &= a^2c^2 - b^2d^2 \\ &= a^2c^2 + (b^2c^2 - b^2c^2) - b^2d^2 \\ &= (a^2 + b^2)c^2 - b^2(c^2 + d^2) \\ &= p(c^2 - b^2) \end{aligned}$$

since p is prime, it must either divides $(ac+bd)$ or $(ac-bd)$ (c^2-b^2 cannot be zero by assumption). If it divides $(ac+bd)$ then since

$$p^2 = (ac+bd)^2 + (ad-bc)^2 \longrightarrow (ac+bd)^2 \leq p^2$$

we must have $(ac+bd)^2 = p^2$ but this means

$$\begin{aligned} 0 &= (ad-bc)^2 \\ \rightarrow \frac{a}{b} &= \frac{c}{d} \end{aligned}$$

the only possible solution for this is that $a=c, b=d$. If p divides $(ac-bd)$, from the other representation

$$p^2 = (ad+bc)^2 + (ac-bd)^2 \longrightarrow (ac-bd)^2 \leq p^2$$

we have

$$0 = (ad+bc)^2$$

which is just not possible, therefore there is only one possible sum of squares representation for p.

This uniqueness part can be proven mighty easily using the Gaussian Integer field, since this field is Euclidean (for any two numbers in this field a, b we can express them as $a = bq + r$), every number can be factorized uniquely, therefore

$$p = (a+ib)(a-ib)$$

since $a \pm ib$ are not related by units (the only units are ± 1 and $\pm i$) the above factorization of p is unique and we are done.

Bonus Featurette

Another thing I observed during this misadventure was that any number (not just primes) of the form $n = 4m-1$ cannot be expressed as a sum of two squares, this is because n must have a prime factor p of the form $4u-1$, if n can be expressed as a sum of two squares

$$\begin{aligned} a^2 &\equiv -b^2 \pmod{n} \\ a^2 &\equiv -b^2 \pmod{p} \\ \left(\frac{a}{b}\right)^2 &\equiv -1 \pmod{p} \end{aligned}$$

but -1 cannot be a quadratic residue mod $p = 4u - 1$.

The other lemma, another thing is that a prime power of $p^k, p = 4u - 1$ can be expressed a sum of two squares if k is even and one of the number in the sum is zero, *i.e.* $p^k = 0^2 + (p^{k/2})^2$ is the only sum of square representation for $p = 4u - 1$, this is due to the same reasoning above, say we assume the opposite

$$\begin{aligned} a_0^2 &\equiv -b_0^2 \pmod{p^k} \\ \left(\frac{a_0}{b_0}\right)^2 &\equiv -1 \pmod{p} \end{aligned}$$

which is not allowed (since -1 is not a quadratic residue) unless both $a_0 \equiv b_0 \equiv 0 \pmod{p}$ but in this case, p divides both a_0 and b_0 thus

$$\begin{aligned} p^2 a_1^2 &= -p^2 b_1^2 + p^k \\ a_1^2 &= -b_1^2 + p^{k-2} \end{aligned}$$

and we have the same situation again, repeating the process, if k is even then we will get

$$a_n^2 = -b_n^2 + 1$$

which means that either a_n or b_n is zero, they can't both be zero because $a_0^2 + b_0^2 = p^k$, if k is odd then

$$a_n^2 = -b_n^2 + p$$

but this time we've got no solution, not even if a_n or b_n is zero, thus if k is odd there's no solution while if k is even then $p^k = (p^{k/2})^2 + 0^2$.

From the uniqueness claim, we can also say that if you draw a circle in the complex plane whose radius is a prime number, this circle will hit a lattice point exactly twelve or four times. Because if $p = 4m+1 = a^2+b^2$, the points are $2ab \pm i(b^2-a^2), -2ab \pm i(b^2-a^2)$ and the same points with real and imaginary parts exchanged and of course the obvious ones $\pm p, \pm ip$, if on the other hand $p = 4m - 1$ then the only points are just $\pm p, \pm ip$. Or if you like roots, then if $p = 4m+1$, a circle with radius $\sqrt{p}$ has eight lattice points while a circle with radius $\sqrt{p}$ where $p = 4m - 1$ has none.

The reason I even got into this circular business is that because I wanted to prove the uniqueness part geometrically but it was quite troublesome to do so :)

Pythagoras and friends, let's start with the product of sums of squares, say we have three of them, are they associative? The answer is yes since we can represent them in terms of matrices and matrices are associative under multiplication.

Next question, what are the symmetries of this product of sums of squares? from $a \leftrightarrow b$, $c \leftrightarrow d$ and simultaneous $a \leftrightarrow b$ and $c \leftrightarrow d$ we get

$$(ac+bd)^2+(ad-bc)^2$$
$$(bc+ad)^2+(bd-ac)^2$$
$$(ad+bc)^2+(ac-bd)^2$$
$$(bd+ac)^2+(bc-ad)^2$$

we see that there are only two possibilities for the first term while there are four for the second although they come in plus minus pairs.

This plus minus thing is important when we multiply more than two sums of squares, so we need to see what happens when we apply a minus sign to a, b, c, d but from the pattern above doesn't matter where we apply the minus sign or to how many of the elements we will just get the same things with just plus and minus cycled through different elements. Thus, if we ignore the plus minus sign, from two sums of squares we will get only two sets of sums of squares.

Next, how many sum of squares representation does p^k have? $p = 4m+1$ of course. Let's start from $k = 2$, in this case

$$p^2 = (a^2+b^2)^2+0^2$$
$$p^2 = (2ab)^2+(a^2-b^2)^2$$

Let's call a sum of squares where both squares are non-zero and co-prime as a proper sum. Thus, p^3

$$(a(2ab)+b(a^2-b^2))^2+(a(a^2-b^2)-b(2ab))^2$$
$$(a(a^2-b^2)+b(2ab))^2+(a(2ab)-b(a^2-b^2))^2$$

has 2 proper reps, the pattern I saw was for p^k with k even has the same number of proper reps as p^{k-1} and p^{k-1} has twice the number of proper reps of p^{k-2}. This can be shown

quite easily, the key is that multiplication is associative thus

$$p^k = \begin{cases} (p^2)(p^2)\cdots(p^2)p, & k \text{ odd} \\ (p^2)(p^2)\cdots(p^2), & k \text{ even} \end{cases}$$

each p^2 only generates one proper rep, the same with p, thus for k odd we get in total $2^{\frac{k-1}{2}}$ proper reps, for k even we get $2^{\frac{k}{2}-1}$ proper reps or in a fancier expression

$$2^{\lfloor \frac{k-1}{2} \rfloor}$$

The reason of defining these proper reps is to see that for given a hypotenuse how many primitive triples we can build on it. First of a primitive hypotenuse cannot have prime factors of the form $4m-1$, that is quite obvious from our previous discussion. Second, from our preceding discussion, the number of primitive triples of a hypotenuse, h, will be of the form 2^N where

$$2^N = 2^{M-1}\prod_{i=1}^{M} 2^{\lfloor \frac{k_i-1}{2} \rfloor} \qquad \text{with} \qquad h = \prod_{i=1}^{M} p^{k_i}$$

What this means is that given a hypotenuse h, there's only one primitive right triangle we can construct if h is prime or a prime squared otherwise we get multiple primitive triangles out of it :)

On Thue's Lemma, this is one cool application of the pigeons :) let $0 \leq x, y \leq \lfloor \sqrt{n} \rfloor$, n need not be prime and given a number a, construct the following

$$ax - y \pmod{n}$$

since there are possible $(\lfloor \sqrt{n} \rfloor + 1)^2 > n^2$ values for x and y and there are only n values (mod n), there must be duplicates, this is where the pigeons come along :)

Assume we have two different sets of (x, y) such that their construction above is the same then

$$ax_1 - y_1 \equiv ax_2 - y_2 \pmod{n}$$
$$\rightarrow a(x_1 - x_2) \equiv (y_1 - y_2) \pmod{n}$$

let $w = x_1 - x_2$ and $z = y_1 - y_2$ then we claim that both w and z are non-zero because is w is zero then z is also zero but our assumption is that (x_1, y_1) and (x_2, y_2) are two

distinct sets the second and more important (because this is what we want) thing is that $|w|$ and $|z|$ must be $\leq \lfloor\sqrt{n}\rfloor$ but this is guaranteed as $0 \leq x, y \leq \lfloor\sqrt{n}\rfloor$. However, we must be careful that $x_1, x_2, y_1, y_2 \neq 0$ but again this is guaranteed as when $x_1 \equiv 0$ then $y_1 \equiv 0$ again this is fine because (x_2, y_2) are a distinct set from (x_1, y_1) so w and y won't be zero.

From this proof we can see that the solution to $p = a^2 + b^2$ comes from the difference $x_1 - x_2$ rather than from $x_{1,2}$ themselves which explains my pathetic attempt in proving Thue's lemma without them pigeons :) because there I constructed a multiplication table for $ax \equiv y$ and tried to find a pattern I can use but the pattern is in the difference not the direct result of the multiplications.

On 65, now the fun part, if we combine the representations of sum of squares of 65 repeatedly, will we get an infinite descend? The answer sadly is no because now since 65 is not prime

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

we can't claim that $(a^2 + b^2) = (c^2 + d^2) = 65$ divides $(ac + bd)$ or $(ac - bd)$, what we can say is that each prime factor of 65 divides either $(ac + bd)$ or $(ac - bd)$. Say one of its prime factor is q and it divides $(ac + bd)$, this means

$$65^2 = (ac + bd)^2 + (ad - bc)^2$$
$$65^2 = (qq')^2 + (ad - bc)^2$$

but $q|65$ as well, this means what we get is no longer a primitive triple (the triples are no longer co-prime to one another), therefore this new representation is no longer $65 = u^2 + v^2$ instead it's $s \cdot (u^2 + v^2)$, thus we can't combine it we the previous two to get new ones. Thus

65 Stupid Lemma, if the same hypotenuse occurs in two primitive pythagorean triples, then combining these two using the product of sums of squares will not produce other primitive pythagorean triples. This doesn't mean that the same hypotenuse can only have two primitive triples but if you combine it this way it won't produce more primitive triples.

A hypotenuse can have more primitive triples because say it has three prime factors, $p_{1,2,3}$, all of the form $4m+1$, then combining p_1 and p_2 alone (using the product of sums of squares) we already get two possible outputs, combining it with p_3 we get a total of four, for more details see previous subsection.

Other failed attempts

Throughout my meandering, the most painful attempt was trying to find an explicit pattern in the mutiplication table mod p, this is after I found out about Thue's Lemma which states that there must be x, y with $0 < |x|, |y| \leq \lfloor \sqrt{n} \rfloor$ such that $ax \equiv \pm y \pmod{n}$, why is this relevant? If both $|x|$ and $|ax|$ is $\leq \lfloor \sqrt{p} \rfloor$ then since

$$\begin{aligned} a^2 &\equiv -1 \pmod{p} \\ \rightarrow a^2x^2 &\equiv -x^2 \pmod{p} \\ a^2x^2 + x^2 &\equiv 0 \pmod{p} \\ &= pw \end{aligned}$$

w cannot be 0 since $0 < |x|, |ax| \leq \lfloor \sqrt{p} \rfloor$, and w cannot be ≥ 2 since $2\lfloor \sqrt{w} \rfloor^2 < 2p$, and it is a strict inequality since p is prime and so $\lfloor \sqrt{p} \rfloor < \sqrt{p}$. Thus w must be 1 and we are done.

The challenge now is to show that we can find such x such that the above is true. In other words, given any $a \in (\mathbb{Z}/p\mathbb{Z})^*$, there must be x, y with $|x|, |y| \in \{1, 2, \ldots, \lfloor \sqrt{p} \rfloor\}$ such that $ax \equiv y \pmod{p}$.

I tried proving Thue's Lemma without the pigeon hole principle and I failed, couldn't find a good way, thought about cross classification but nothing worked so far.

Since I also knew about the product of sums of squares thingy, I was also trying to find a condition where we can divide a sum of squares by another, but this turned out quite complicated as it is the subject of what is called Gaussian integers in algebraic number theory LOL

For the uniqueness part, I tried pigeon holing it to submission :) say from two representations of sum of squares we generate two more, then we have four, from this four we can generate up to 12 (4 choose 2 and each generates two), so some of them must

be duplicates but then it was ok to have duplicates. Another thing I wanted to try was partitioning but was too lazy to work out all the details :)

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

If we generalize the product of sum of squares

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

to include $\sqrt{n}$, using our complex number notation

$$\begin{aligned} A \cdot C &= (a + i\sqrt{n}b)(c + i\sqrt{n}d) \\ \rightarrow |A||C| &= |(a + i\sqrt{n}b)(c + i\sqrt{n}d)| \\ (a^2+nb^2)(c^2+nd^2) &= (ac-nbd)^2 + n(ad+bc)^2 \end{aligned}$$

we get the same rule, the product of a^2+nb^2 and c^2+nd^2 results in x^2+ny^2.

Just like the case of $n=1$, this equation enjoys the same sort of symmetries, $a \leftrightarrow \sqrt{n}b$

$$\begin{aligned} A \cdot C &= (\sqrt{n}b + ia)(c + i\sqrt{n}d) \\ \rightarrow |A||C| &= |(\sqrt{n}b + ia)(c + i\sqrt{n}d)| \\ (a^2+nb^2)(c^2+nd^2) &= (ac+nbd)^2 + n(bc-ad)^2 \end{aligned}$$

which is the same as, $b \rightarrow -b$ which in turn is the same as $a \rightarrow -a$. Note also that we can set $\sqrt{n} \rightarrow \sqrt{-n}$ to get a form of Pell's equation $x^2 - ny^2$. This complex number point view is very helpful.

Suppose a sum of two squares a^2+nb^2 is divisible by a prime, p, of the form c^2+nd^2

$$\begin{aligned} (ad-bc)(ad+bc) &= a^2d^2 - b^2c^2 \\ &= a^2d^2 + nb^2d^2 - nb^2d^2 - b^2c^2 \\ &= c^2(a^2+nb^2) - b^2(c^2+nd^2) \end{aligned}$$

since $p = c^2+nd^2$ is a prime it must divide either $(ad-bc)$ or $(ad+bc)$, say for now it divides $(ad+bc)$, now since p divides $(a^2+nb^2)(c^2+nd^2)$ and $(ad+bc)$ and we know that

$$(a^2+nb^2)(c^2+nd^2) = (ac-nbd)^2 + n(ad+bc)^2$$

so p must also divide $(ac - nbd)$. If p divides $(ad - bc)$ instead we can use the other formulation

$$(a^2 + nb^2)(c^2 + nd^2) = (ac + nbd)^2 + n(bc - ad)^2$$

here also p divides the LHS and the last term in the RHS and therefore divides $(ac+nbd)$, therefore

$$\left(\frac{a^2 + nb^2}{c^2 + nd^2}\right) = \left(\frac{ac + nbd}{c^2 + nd^2}\right)^2 + n\left(\frac{bc - ad}{c^2 + nd^2}\right)^2$$

So the inductive proof should work with other values for n other than 1. The other key in the proof is that all other primes smaller than p of the form $4m+1$ must be a sum of two squares.

If $n = 2$ for example, we are no longer interested in p of the form $4m + 1$, because we now want primes where -2 is a quadratic residue which means that either both -1 and 2 are quadratic residues or both are quadratic non residues.

For 2 to be a quadratic residue, p must be of the form $\pm 1 \pmod 8$, while for -1 to be a quadratic residue, p must be $1, 5 \pmod 8$, so for both to be quadratic residues p must be $1 \pmod 8$, and subsequently for both to be quadratic non-residues p must be $3 \pmod 8$.

Thus in this case a quadratic -2 means $p = 1, 3 \pmod 8$, another way of looking at it is that the first few primes where -2 is a quadratic residue are

$$3, 11, 17$$

and they also happen to be of the form $8m+1$ or $8m+3$, if we just start with $3 = 1^2+2\cdot 1^2$ as our inductive basis, the next prime number where -2 is quadratic is 11 and we can do the same inductive proof as the one for $4m + 1 = x^2 + y^2$ starting with $p = 11$. In the peeling step $r^2 + 2 = pw$, each prime factor of w must have -2 as a quadratic residue and by the above conclusion we know they are of the form $x^2 + 2y^2$.

The same goes for $n = 3$, $x^2 + 3y^2$, for -3 to be a quadratic residue, both -1 and 3 must quadratic or both must be non quadratic but it will be easier if we just use the reciprocity formula. If we express all primes greater than 3 in mod 6, it must be of the

form $6m \pm 1$. Using Gauss's quadratic reciprocity formula

$$\begin{aligned}\left(\frac{-3}{6m+1}\right) &= (-1)^{\frac{6m+1-1}{2}}(-1)^{\frac{3-1}{2}\frac{6m+1-1}{2}}\left(\frac{6m+1}{3}\right)\\ &= (-1)^{6m}\left(\frac{1}{3}\right)\\ &= +1\end{aligned}$$

and if we compute the corresponding Legendre symbol with $6m-1$ we get -1. So the condition that -3 is a quadratic residue is the same to that of $p = 6m+1$.

So here our inductive basis is the first prime where -3 is quadratic, *i.e.* $7 = 2^2 + 3 \cdot 1^2$ and our starting point for the inductive proof is $p = 13$ and the proof follows as usual.

The next case is not $n = 4$ because $x^2 + 4y^2 = x^2 + (2y)^2$ which is the same as the case of $n = 1$. So the next case is $x^2 + 5y^2$. Here what we need is primes where -5 is a quadratic residue.

But we have a problem here because 3 has -5 as a quadratic residue but is not expressible as $x^2 + 5y^2$ (in this case $-5 \equiv 1 \pmod 3$), likewise for 7, -5 is a quadratic residue, $-5 \equiv 2 \pmod 7$ and $4^2 \equiv 2 \pmod 7$ but again 7 is not expressible as $x^2 + 5y^2$.

By these reasons alone we ca no longer use the inductive proof because once we reach $r^2 + 5 = pw$, w might contain 3 and 7 and they are not of the form $x^2 + 5y^2$. So even if we can express the condition for -5 to be quadratic residue as primes of the $y \pmod u$, the proof still doesn't work because 3 and 7 will be of that form but they are not of $x^2 + 5y^2$ so we can't do the peeling step for $r^2 + 5 = pw$ because each prime factor of w must have -5 as a quadratic residue but they might not be of the form $x^2 + 5y^2$.