Square Sums

R

The title probably evokes the Pythagoras Theorem that claims $c^2 = a^2 + b^2$.
These are sides of a triangle, so distances and thus real numbers.
But the Babylonians were already obsessed with the question when these values can be whole numbers. The simplest is $5^2 = 4^2 + 3^2$ the first Pythagorean triplet, as these later became called. Most amazingly, 5 itself is a square sum as $2^2 + 1^2$.
And indeed, this is the key behind the triplets.
The fundamental fact is that not just the squares inherit the square sumness rather products in general. So a square being square sum is just a special case of a bigger picture. But the really big picture is even more amazing.
By the Fundamental Theorem Of Arithmetic all numbers break down to primes in a unique way and this square sum break down continues this vision.
Fermat who discovered so many laws of the natural numbers observed that:
Only "half of" the primes are square sums but they have a unique square sum form.
The above mentioned case is the simplest, so 5 is the first prime in this "half".
The next 7 , 11 are not square sums and 13 is the next as $3^2 + 2^2$.
Fermat also realized the law behind this splitting of the primes:
Those primes that are $4k + 1$ valued are square sums, in fact exactly one way, while the rest that are $4k - 1$ valued are never.
The only even prime 2 is also square sum as $1^2 + 1^2$.
The uniqueness of square sum forms for the $4k + 1$ primes and the impossibility for $4k - 1$ primes are quiet easy to prove but the existence of square sum form for $4k + 1$ was quite difficult up until quite recently when an amazingly easy proof was found.
At the end of this article I will show this proof.
Half of the primes having these unique forms already suggests that these should be just as fundamental "God given" basic values as the primes themselves.
And indeed, there is no formula that would give the x , y values that $p = x^2 + y^2$.
But then by the same logic, we should expect that all other products made from these primes if turn out to be square sums then should have square sum forms derivable from the "God given" primal square sums. The only even prime 2 is exceptional so we could accept the fact that $2 \cdot 2 = 4$ is not square sum or that $2 \cdot 5 = 10 = 1^2 + 3^2$ is not relating to $5 = 1^2 + 2^2$. But then the $5 \cdot 5 = 25 = 4^2 + 3^2$ Pythagorean triplet or the first non square product from the first two square sum primes 5 and 13 , that is $5 \cdot 13 = 65$ should have a square sum form derivable from the factors' forms.
And here the situation is even more surprising! It is indeed square sum but actually in two ways: $65 = 8^2 + 1^2 = 7^2 + 4^2$.
Two forms and neither relates to the square sum forms of 5 and 13.
The formal solution to all this is $\sqrt{-1}$ which seems as an impossible use of the square root because a square is always positive. But if we accept such imaginary unit number then somehow things come out by themselves.
The start of the calculations is always the simple rule that : $(\sqrt{-1})^2 = -1$.
Therefore, we can even abbreviate $\sqrt{-1}$ as i if we know that $i^2 = -1$.
This was first used for other non natural number problems, namely solving equations.
There it seemed that all we need is the dual combinations, that is the sums of a real and a multiple of this imaginary unit. In other words, the $x + y\,i$ numbers.
Euler went very far with these but still couldn't prove that these dual combinations indeed give always roots for any algebraic equation. This claim, the Fundamental Theorem Of Algebra finally was proven by Gauss. These dual numbers became called complex numbers and the whole valued cases as Gaussian integers.
In my view, these are a better introduction to complex numbers than equations.

Remember that: $(X + Y)(x + y) = Xx + Xy + Yx + Yy.$

Which gives that: $(x + y)(x - y) = xx - xy + yx - yy = x^2 - y^2.$

And then: $(x + y\,i)(x - y\,i) = x^2 - (y\,i)^2 = x^2 - y^2 i^2 = x^2 - y^2(-1) = x^2 + y^2.$

In reverse of course : $x^2 + y^2 = (x + y\,i)(x - y\,i).$

So with these complex numbers we can turn into products not just the square differences but the square sums too. This is the basic trick.
Now let's see some magic!

$$5^2 = 5 \cdot 5 = (2^2 + 1^2)(2^2 + 1^2) = (2 + i)(2 - i)(2 + i)(2 - i) = (2 + i)(2 + i)(2 - i)(2 - i) = (4 + 2i + 2i + i^2)(4 - 2i - 2i + i^2) = (3 + 4i)(3 - 4i) = 3^2 + 4^2$$

Now going a bit faster:

$$65 = 5 \cdot 13 = (2^2 + 1^2)(3^2 + 2^2) = (2 + i)(2 - i)(3 + 2i)(3 - 2i) = (2 + i)(3 + 2i)(2 - i)(3 - 2i) = (4 + 7i)(4 - 7i) = 4^2 + 7^2.$$

$$65 = 5 \cdot 13 = (2^2 + 1^2)(3^2 + 2^2) = (2 + i)(2 - i)(3 + 2i)(3 - 2i) = (2 + i)(3 - 2i)(2 - i)(3 + 2i) = (8 + i)(8 - i) = 8^2 + 1^2.$$

I left to the end the simplest case of complex break down $2 = (1 + i)(1 - i)$. So:

$$10 = 2 \cdot 5 = (1 + i)(1 - i)(2 + i)(2 - i) = (1 + i)(2 + i)(1 - i)(2 - i) = (1 + 3i)(1 - 3i) = 1^2 + 3^2.$$

$$10 = 2 \cdot 5 = (1 + i)(1 - i)(2 + i)(2 - i) = (1 + i)(2 - i)(1 - i)(2 + i) = (3 - i)(3 + i) = 3^2 + 1^2.$$

Which kind of explains why we end up with only one square sum for 10.
The true understanding comes a bit later.
But now we start without complex numbers.

D

In the followings all letters denote the naturals : 1 , 2 , 3 . .

An n number is square sum if $n = x^2 + y^2$.

The simplest way to get a square sum is to double a square, that is as $n = 2x^2$.
We call this as trivial square sum form and we call an n number a non trivial square sum if it has some non trivial square sum form even if it has trivial form too.
The first three double squares $2 \cdot 1^2 = 2$, $2 \cdot 2^2 = 8$, $2 \cdot 3^2 = 18$ have only this trivial form, but then $2 \cdot 5^2 = 50 = 7^2 + 1^2$, so 50 is a non trivial square sum.
Amazingly, we are already able to claim a strong theorem:

T

1. The product of two square sums of which at least one is non trivial, is again a non trivial square sum.

2. A product of square sums having among them at least one non trivial is again such.

P

1.

Let the two non both trivial square sum forms be $X^2 + Y^2$ and $x^2 + y^2$.
Observe the following two identities:

$$\left(X^2 + Y^2\right)\left(x^2 + y^2\right) = \begin{cases} \left(X\,x + Y\,y\right)^2 + \left(X\,y - Y\,x\right)^2 \\ \left(X\,x - Y\,y\right)^2 + \left(X\,y + Y\,x\right)^2 \end{cases}$$

They can be verified by simply calculating the product on the left and the squares on the right. These two algebraically produced squares sum forms would both fail only if the squares having minus signs in them would become both 0.
But then $Xy = Yx$ and $Xx = Yy$ would stand and thus:
$Xy - Xx = X(y-x) = Yx - Yy = Y(x-y)$ and so $X = -Y$ and so $X^2 = Y^2$. But also:
$Xy - Yy = y(X-Y) = Yx - Xx = x(Y-X)$ and so $x = -y$ and so $x^2 = y^2$.
So both of our original forms were trivial which we assumed not to be true.
Now we show that one of our resulting forms is non trivial.
If both were trivial then $Xx + Yy = Xy - Yx$ and $Xx - Yy = Xy + Yx$.
Adding them we get that $2\,Xx = 2\,Xy$ and so $x = y$.
Subtracting them we get that $2\,Yy = -2\,Yx$ and so $x = -y$.
Both can not be true so both forms could not be trivial either.
2.
Let's start with the non trivial form assumed and multiply it with any other.
We get a non trivial and so we can continue again.

R

A trivial consequence of 1. is that the square of a non trivial square sum is again a non trivial square sum. The reverse is not true as $15^2 = 12^2 + 9^2$ shows.
The reason for this pretty large counter example comes out by first going into refining the good direction itself. Not only multiplying square sums can lead to new ones!
An easy way is to multiply one with a square. Indeed, $(x^2 + y^2)\,k^2 = (xk)^2 + (yk)^2$.
This by the way is a generalization of the triviality because $2\,x^2 = (1^2 + 1^2)\,x^2$.
The reverse of this square multiplication is to take out from an $X^2 + Y^2$ square sum a k common divider of X and Y as: $X^2 + Y^2 = (kx)^2 + (ky)^2 = k^2(x^2 + y^2)$.
So we simplified $X^2 + Y^2$ by taking out k^2. This of course was only useful if k is not 1 so X and Y had a common divider beside the trivial 1.
Thus it's logical to call an $X^2 + Y^2$ square sum form simple if it is not simplifiable.
That is, X and Y have only the trivial common divider 1 and this is also called as them being relative primes. But now again we encounter the same dilemma.
Can such simple square sum form give a number that has non simple form too?
Yes, and the simplest example is the same again: $50 = 5^2\,(1^2 + 1^2) = 1^2 + 7^2$.
Or another: $125 = 25\,(1^2 + 2^2) = 2^2 + 11^2$.

D

Numbers that have non simplifiable square sum form are called simple square sums.
Even if they have other forms that are simplifiable.

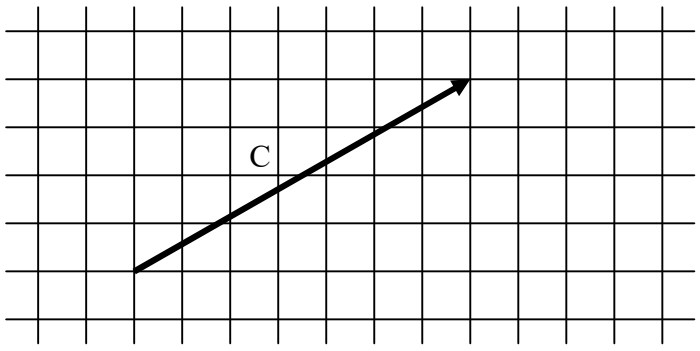
T

1. A product of simple square sums is simple square sum if and only if:
   There is maximum one even member.

2. Every factor of a simple square sum is also a simple square sum.

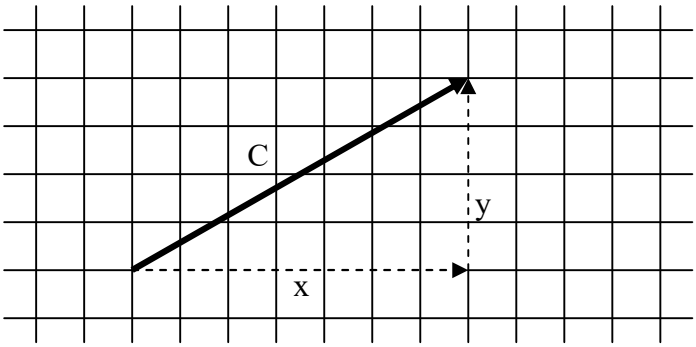
R The proof of 1. and 2. within the natural numbers are quite difficult.
What's worse, they have no meaning behind. We'll get very visual proofs for both.
A hint for our road is already present in the seemingly strange x , y letters we used.
The x , y letters are of course common for the Descartes coordinates and so our notation suggests that the complex numbers are actually the points of the plane.
The complex wholes or the Gaussian integers are the grid points.
This is an Elementary School level vision that for some insane reason is still missing from all curriculums. Even more surprisingly, these complex wholes are not the only and shouldn't be the first use of the grid points.
The fractions can also be identified with these and in the article about the Fundamental Theorem Of Arithmetic I explain this.
That should be a lower Elementary School subject and then there is a third relating educational problem. The total lack of vectors as foundation of Coordinate Geometry.
This is definitely a High School subject and strangely, in all tertiary educations, they say, "Forget everything you learnt in High School" and start with vectors.
One advantage is that the three dimensional handling is just as easy.
So the (x , y , z) points are then x **i** + y **j** + z **k** sums or linear combinations from the three unit vectors of the axes. Everything that in High School was so difficult comes out then with ease. There is no reason for this at all, because High School kids can grasp this abstract approach perfectly.
But now back to our subject, this in-between third use of the coordinate system probably should be in upper Elementary School.
A fundamental common over complication in all three applications of the coordinate system is the coordination itself. This is so deeply rooted problem that probably it will never change. I myself fell back to the error of coordination many times.
The simple truth is that the arbitrary axes and the origin are not necessary!
Most results are about the differences of the coordinates and the whole Euclidian vision is that actually any point could be the origin. So then why can not we start without an origin? Well we can and here where we only use the whole valued coordinates, that is regard the grid points, the concept of the "connector" should be the start. In the mentioned earliest fractional application in lower Elementary School we should regard these as just distances without a direction while here with the complex integers we can introduce the direction that is using vectors as connectors.
These two is then a perfect preparation for the mentioned High School Coordinate Geometry based on vectors.

D So imagine an infinite bathroom tiling with simple square tiles.
No fashionable pictures on the tiles, no coordinates in the plane either, just squares.
The "connectors" are arrows from any corners to any other in this tiling:

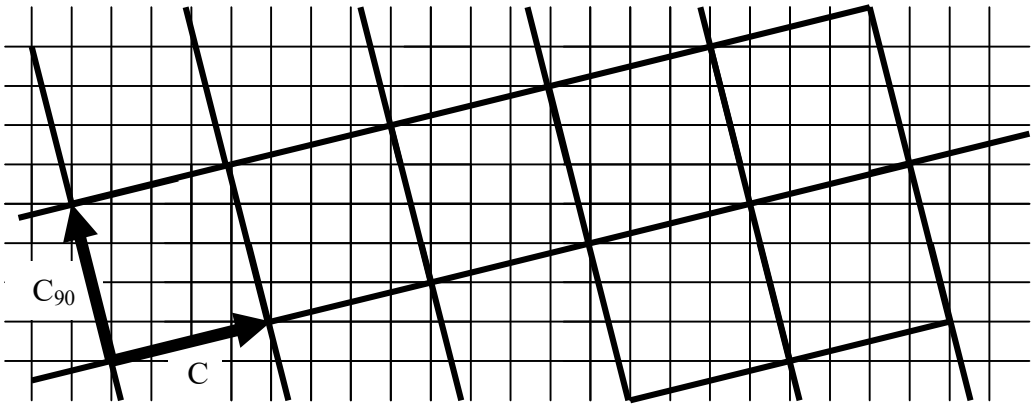


These C connectors are our new numbers that will represent the x + y i sums.

As we can guess from this, x will mean the horizontal and y, the vertical steps that achieve the same motion as C itself:

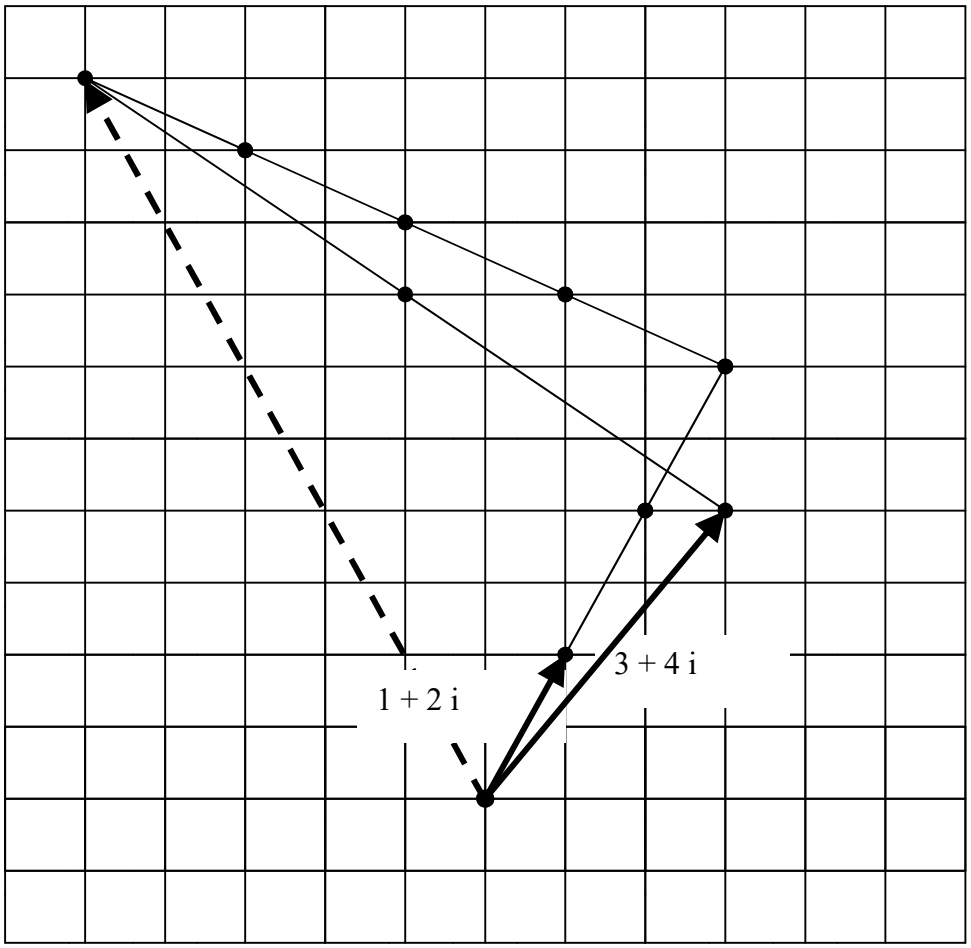


Of course, x , y can be zero or negative whole numbers too.
Zero means not moving horizontally or vertically at all, and minus means moving left or down.
This acceptance of the right and up as plus is merely our human convention.
So, the combined or complex number (– 2 + 3 i) for example means:
Go 2 tiles horizontally to the left and then go three tiles vertically up.
As an other example : (7 – 2 i) means go 7 right and 2 down.
The crucial first recognition about our new universe is this:
Our tiling has hidden sub-tilings in it. Namely, every fix C connector generates one.



The repeated continuations of C in its line, falling onto exact corner points, that is being connectors, is obvious. The less obvious fact is that turning C with 90 degrees, this C_{90} will be a connector again. Of course, it follows from turning both of the x , y components of C too.
Then, the repeated continuations of C_{90} give the other perpendicular sides of the new tiles.
This vision is elementary school stuff. Every kid should see it as early as possible.

The second important vision is using any U connector as new unit or fixed sub-tiling and to measure a second C connector in this system. The surprising fact is the following:
C measured in the U sub-system leads to the same point as U measured in C.
For example:



The two connectors are the black arrows: $1 + 2\,i$ and $3 + 4\,i$.
The resulting connector is the dashed arrow and easy to see through the black dots we placed, that it is both $1 + 2\,i$ measured in the $3 + 4\,i$ unit system or in reverse.
This common end result is quite surprising as a general fact.
Yet trying every concrete example, it turns out to be true.
One "ugly" way to prove this sameness is to realize that the representations of the connectors in each other's sub-system is actually the product of them, using the i compositions.
For example, above, the resulting vector is $-5 + 10\,i$. And voila:
$(1 + 2\,i)(3 + 4\,i) = 3 + 4\,i + 6\,i + 8(-1) = -5 + 10\,i$.
The same can be seen in general.
But there is a nicer way to see this fact by reinterpreting the multiplication itself.
We have to regard connectors determined in an other way than from the x and y components. Namely, from their length $|C|$ and their angle to the horizon.
Then, using U as unit, means replacing the x, y, C triangle with a similar one, but using as unit, not the original tiles rather new $|U|$ tiles. So this means a $|U|$ stretching of $|C|$ and a turn of its angle with U's angle. So the representation of C in U will have $|U|\,|C|$ length and the sum of their angles. This at once shows that the order is immaterial and U's representation in C is the same.

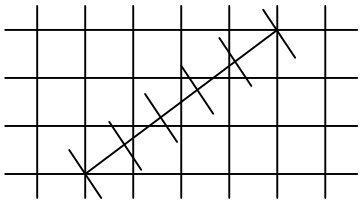
The third crucial thing to "see" is what we can't really see, namely that the square sums are the squares of these $|C|$ connector lengths, that is $|C|^2$.
Indeed, $x^2 + y^2$ of a C connector is obviously the square of its length, that is, $|C|^2$ by Pythagoras theorem. But the $|C|$ length is all we can see. Of course, we could place a square on top of C but that wouldn't fit into our tiling at all.
So we simply have to accept that $|C|$ is not a whole number, but $|C|^2$ is.

Yet the $|C\,U| = |C|\,|U|$ rule implies $|C|^2\,|U|^2 = |C\,U|^2$ too.
So this gives a new proof of that square sums multiplied remain square sum.
A result for whole numbers thus obtained by temporarily stepping out to the real numbers. Indeed, $|C|, |U|, |C\,U|$ are not wholes but produce the product as square sum. Observe the concrete example:

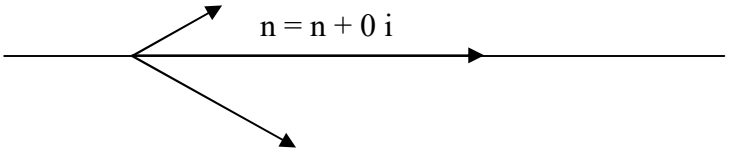
$(1^2 + 2^2)(3^2 + 4^2) = |1 + 2\,i|^2\,|3 + 4\,i|^2 =$

$= |(1 + 2\,i)(3 + 4\,i)|^2 = |-5 + 10\,i|^2 = 5^2 + 10^2$

The i meant the vertical component and so repeated application should mean 180° turn. On the other hand, we know that $i\,i = -1$. These two mean the same thing.
Indeed, 180° turn is actually multiplication with -1. So i is not imaginary at all!
It is the half turn of negativity or 180° turn, that is a 90° turn.
These $x + y\,i$ complex numbers used with x, y real numbers instead of wholes, became the real language of modern physics. Gauss had this vision, but couldn't foresee the electromagnetic fields, quantum mechanics or relativity yet.
This was the root of his bitterness.
What is important from our subject is that these complex numbers of the full plane, should be approached through the tilings as new whole numbers first.
Just as the real numbers must be approached through the naturals and fractions.
Back to our subject, when $x^2 + y^2 = z^2$ is true with a whole z, that is the Pythagorean Triples, simply mean a C connector that $|C| = z$.
For these connectors, quite accidentally, our tiles could be placed to cover the z length. The simplest case of course is $3^2 + 4^2 = 5^2$.
So this is also a certain "sub-tiling", but it has no meaning to be used further.

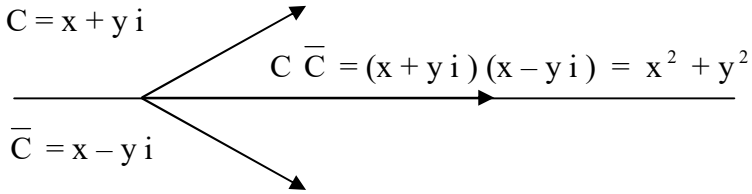


This fact, that already the Pythagorean Triples don't fit into the tiling system or Gaussian integers, is a sign that probably Fermat's Last Theorem also has nothing to do with this vision.
The final, fourth crucially visible fact that lead to the understanding of square sums is that the horizontal connectors as old fashioned natural numbers, can be the products of two connectors, only if these two are symmetrically angled to the horizontal.



This fact is true in general, for the complex or plane numbers. The horizontal old fashioned x real numbers can only be products of symmetrical pairs.
Indeed, this follows from multiplication adding the angles.
The horizontal 0 angle can be the sum of only α and $-\alpha$.
Equal long, symmetrical complex factors thus must be $x + y\,i$ and $x - y\,i$, so called conjugates and these are indeed the crucial in all physical applications to bridge the abstract complex numbers to the measurements as real numbers.

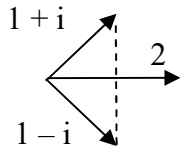
Among the integers or connectors, these C, $\overline{C}$ conjugates give the square sums:



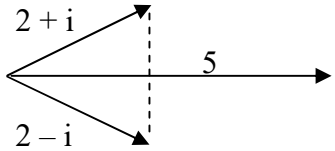
Observe that this fourth vision simply goes back to the algebraic start.
This is how we introduced the imaginary members to make a square sum a product.

The best use of the mirroring vision is that the particularity of why "half" of the old primes are square sums, becomes geometrically visible.
Indeed, these are the old primes that are not primes in the plane anymore, rather products of two symmetrical primes of the plane:

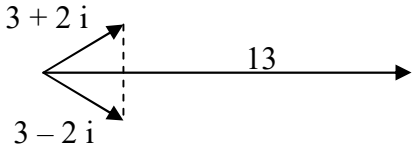
$2 = (1 + i)(1 - i) = 1^2 - i^2 = 1 + 1$



$5 = (2 + i)(2 - i) = 2^2 - i^2 = 4 + 1$



$13 = (3 + 2i)(3 - 2i) = 3^2 - (2i)^2 = 9 + 4$



In the last two, we could have used the "opposite" pairs $1 + 2i$ and $1 - 2i$ for 5 and $2 + 3i$ and $2 - 3i$ for 13. But these are not new primes!
Indeed, $1, -1, i$ and $-i$ are the four units of the plane numbers.
So multiplying with these counts as same numbers or merely unit variants.
So, for example: $1 + 2i = i(2 - i)$ and $1 - 2i = -i(2 + i)$.

This new insight into the square sumness of the 2 , 5 , 13 , . . . primes, still leaves the actual break downs or decompositions empirical.
In fact, they are more surprising than the old primes because we can tell practically nothing about them. The only thing we know that one component must be odd and one even because their square sum must be odd.
I list the first few prime square sums after the already mentioned 2 , 5 , 13.
$17 = 4^2 + 1^2$, $29 = 5^2 + 2^2$, $37 = 6^2 + 1^2$, $41 = 5^2 + 4^2$, $53 = 7^2 + 2^2$
$61 = 6^2 + 5^2$, $73 = 8^2 + 3^2$, $89 = 8^2 + 5^2$, $97 = 9^2 + 4^2$.

I went up to 97 because this is the first where both components are composite.

The crucial fact of the grid numbers is that just like the naturals they break down into prime or irreducible ones that can not be decomposed any more.

To prove the uniqueness of these can go similarly as among the naturals.
This might sound surprising because here we have no linear ordering of them.
The necessary Euclid's Lemma however can be proven with remainders and this is meaningful here too by the lengths.
The most striking difference is the mentioned four units.

The old primes that lose their primality, which we revealed are exactly the $4k+1$ ones and 2, can obviously break down into only simple factors.
Meaning that their two coordinates are relative primes and so the connector can not be divided into equal sections.
The mentioned earliest Elementary School use of the connectors for the fractions has the result that these simple connectors are actually the same as the minimal ones.
Those that have no grid points on them.
We might jump to the conclusion that these simple or minimal C connectors are then the prime numbers of the plane. But this is not true!
On the line, among the naturals, we only have numbers and primes. In the plane, these minimal connectors are an in between class. All primes must be such, but not all of them are primes. A simple rule can tell which minimal connectors are prime, just like the rule of being $4k+1$ can tell which primes of the naturals lose their primality in the plane and become products of conjugates.
Actually, the two rules are connected in a strange way.
Those and only those C are prime connectors for which $|C|^2$ is a square sum prime number. These of course are the $4k+1$ primes but this form is not important.
The actual rule is only that $|C|^2$ has to be a prime number because then by the first rule it's already trivial that it must be $4k+1$ since $|C|^2 = x^2 + y^2$.
And this primality of $|C|^2$ for a prime connector is trivial because the lengths of the connectors multiply when connectors are multiplied.
So the only question is whether all $4k+1$ primes can become a connector length.
And this follows by simply decomposing any $4k+1$ prime into its two conjugate.
Indeed, these must be primes in the plane because otherwise we had more square sum forms for the $4k+1$ prime. And as we mentioned it is quite easy to see that a number having more square sum forms must be composite.

But let's get back to four amazing visual consequences of the plane numbers.
The first explains why we have multiple square sum forms. The second what numbers are square sums at all. From this follows the third, why all factors of a simple square sum are also such. And from this a fourth, an explanation for the Pythagorean triples.

Breaking down a natural number into plane primes, those that are not lying on the x axis must form conjugate pairs.
They are above and under the horizontal line symmetrically.
The product above and under are two conjugate numbers giving a square sum form of our natural number for sure. But by switching conjugate members, that is using mixed above and under members we get new square sum forms with same total product.
We can achieve this in an other way too: By picking a member and its conjugate pair, we can multiply one with i while the other with $-i$.
These actually mean perpendicular turnings of them in opposite directions.
Using these in place of the original pair we get again new square sum above and under. The total of course remains the same because $i(-i) = 1$.

The question of being a square sum is a bit trickier.
It depends not only on the prime factors lying on the x axis but on a special feature of the $1+i$ and $1-i$ conjugate prime factors of 2.

These are in 45° to the horizontal x axis and so multiplied even many times will fall onto the y or x axis. The conjugate factors coming from the other, that is odd square sum primes in x, that is from $5, 13, 17, \ldots$ have the opposite feature:
They can not combine in multiplyings, that is by angle additions to fall onto any axis.
By the way, these are exactly the $4k + 1$ ones but this fact is not a visual triviality so we'll just mention this feature in bracket from now on.
Similarly, the primes on x that are not 2 or these odd square sum primes, that is the ones that stay plane primes: $3, 7, 11, \ldots$ are exactly the $4k - 1$ ones.
Having even many of such is no problem because they can increase both components of an existing 2 or $4k + 1$. But even many 2 is a problem when we must have at least one odd square sum prime factor $(4k + 1)$ to have at least one conjugate pair in the total product. So the end result is that a number is square sum if and only if:
It has no or even many of each plane prime factor $(4k - 1)$. And if it has no or even many 2 factors then it has at least one odd square sum prime factor $(4k + 1)$.

This then implies that a number is simple square sum if and only if:
It has no plane prime factors $(4k - 1)$ and has maximum one 2 factor.
This implies at once both 1. and 2. of our theorem on page 3.

c^2 can only have no or even many of both the plane prime and 2 factors! So:
c^2 is square sum if and only if c has <u>some</u> odd square sum $(4k + 1)$ prime factor.
But:
c^2 is simple square sum if and only if c has <u>only</u> odd square sum $(4k + 1)$ prime factors. Or in an even simpler way, if c is an odd simple square sum.

Finally, to be quite specific about the plane primes, we can concretely list them.
Here it's better to use coordination and go on the x axis from the origin.
We start with 2 then we go through all $p = 4k + 1$ primes and regard their empirical square sum break downs using the larger member first. These will each give a single grid point on the $\sqrt{p}$ radius circle under the 45° line. These then can be copied eight times to get all of them on the same circle.
So each circle has only eight primes and the increasing circles give all primes.
In spite of this simple list, we know nothing about how these primes are distributed.
Even the simple question is open whether on a single line parallel with the axes we have infinite many primes. In particular, we do not know for sure if there are infinite many $n^2 + 1$ primes. This shows that the abstraction of the plane numbers still leaves some stubborn problems lying at the origins, within the naturals.

Appendix: Proving that all $p = 4k + 1$ primes are $x^2 + y^2$.

$4k + 1$ is odd and an odd's square is odd and even's square is even, so one of x , y is odd and one is even. Let's assume that x is the odd.
So $4k + 1 = x^2 + (2w)^2 = x^2 + 4w^2$.
The big idea is to replace w^2 with uv and to regard the (x , u , v) triplets for which $4k + 1 = x^2 + 4uv$.
A smaller second idea, helping to crystallize the proof, is that we still don't restrict $4k + 1$ to be a p prime. Instead, we'll make exclusions from the possible triplets.
Then if:
1. For a $4k + 1 = p$ prime the excluded ones are always a single triplet.
2. In general, the non excluded triplets are even many.

Then we are finished!
Indeed, then firstly for the prime situations the total set of triplets is odd.
Secondly, observe that in the total set, that is including the single excluded triplet, for every $(x , u , v) , u \neq v$ triplet we get a new one by exchanging u and v.
So these non equal u , v triplets are even many. Thus if the total is odd then there have to be even many $u = v = w$ triplets where $4k + 1 = p = x^2 + 4w^2 = x^2 + y^2$.
As we mentioned earlier, it is easy to show that a number that has two square sum forms must be composite and so actually this odd number has to be 1.
But for us now the task is to prove the oddity or in more general the evenness of the non excluded cases.
The above argument exchanging u , v suggests that we should find some other pairing of triplets among the non excluded ones.
A straight forward pairing is not known, probably because the wider world of triplets allowing integers lies behind. But we can make a compromise and thus find two very simple pairings that can only take out v from the positive values.
But the two pairings work in tandem, so all those cases where the first main pairing goes to negative v, the second pairing will change it back to positive.
Thus we have three subsets among the non excluded triplets:
Those where the main pairing is usable and v stays positive, those where the main pairing is applicable but leads to negative v, and finally those where the main pairing is not applicable. But these last two are paired by our second pairing. So then if our pairings are perfect, that is always make new triplets and self reversing, then the first subset is even and the other two are equal numbered, so the total is indeed even.
Now the details:
The excluded triplets are those where $x = u$ or $x = u – v$.
The second exclusion is impossible for a $4k + 1 = p$ prime because:
$(u – v)^2 + 4uv = (u + v)^2$ can not be a prime.
The first exclusion at primes implies $x = u = 1$ so as we claimed it is a single case.
Indeed, $u^2 + 4uv = u (u+4v) = p \quad \rightarrow \quad u = 1$.
Now the two alterations:
$(x , u , v) \quad \leftrightarrow \quad (2u – x , u , x + v – u)$
$(x , u , v) \quad \Leftrightarrow \quad (x + 2v , x + v – u , –v)$
Observe that :
$(2u – x)^2 + 4 u (x + v – u) = x^2 + 4uv$ and
$(x + 2v)^2 + 4 (x + v – u) (–v) = x^2 + 4uv$
So the $\rightarrow$ and $\Rightarrow$ altered triplets are indeed correct triplets.
In $\rightarrow$ the u remains, while $2u – x$ is a mirroring of x to u.
The first exclusion guarantees that we don't get same x value and the mirroring itself that we get a new triplet and the reversal of x. The rest are just as trivial.