I recommend reading these notes with the worksheet in hand so you have some examples ready!!

The subject of this note is the complex integers (often called the Gaussian integers as well). We obtain these special integers by adding a number "i", which squares to -1, to the regular integers. So for brevity, we will often use $\mathbb{Z}[i]$ to denote the complex integers.

For some motivation, let's recall one of our approaches to studying Pythagorean triples, which are integer solutions to the equation

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

First, we subtracted x^2, which leaves us with

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

Being able to perform the factorization on the right hand side was ***crucial*** to our analysis because it let us leverage our understanding of divisibility to narrow down which integers could solve this equation.

But consider a very similar-looking equation:

$$x^2 + y^2 = z^3$$

There are no longer any ways to rearrange the equation to factorize it with integers, and so we seem to be completely stuck. But what if we were able to make a factorization by looking "outside $\mathbb{Z}$". It's probably been a while, but you may remember the "fundamental theorem of algebra", which says that any polynomial factors completely in the complex numbers $\mathbb{C}$, which are the numbers you get by adding in the "imaginary" unit i to the real numbers. The number i has the special property that $i^2 = -1$.

So it seems reasonable to think that if we "add in extra integers" that we might be able to factor more equations. If these "bigger number systems" still have some familiar behavior, especially with respect to factorization, then that might allow us to solve equations like

$$x^2 + y^2 = z^3$$

– or at least to solve them in the "bigger place". That would help us a lot, because we might then have a complete classification of the solutions in this "bigger place", which means all we have to do to solve our original problem (finding integer solutions) is remove from the classification the extra solutions which aren't integers. If our classification is good enough, then in principle this shouldn't be too difficult.

This is exactly what we are going to do!!!!

In particular, there is the following factorization

$$x^2 + y^2 = (x + iy)(x - iy)$$

(check this yourself: distribute and then remember that $i^2 = -1$)

The only "extra integer" we needed is i.

We will see that we gain a lot of leverage from expanding our number system. We will see applications to things we already understand (the pythagorean theorem) as well as new and challenging questions like "when is $x^2 + y^2$ prime?".

Definition. The complex integers $\mathbb{Z}[i]$ are the set of all sums $a + bi$ where a, b are integers and the letter i represents the complex number i such that $i^2 = -1$.

Definition. A complex integer z is called a $\mathbb{Z}[i]$-prime if the only divisors of x in $\mathbb{Z}[i]$ are $\pm z$ and $\pm iz$. In other words, if $z = xy$ is written as a product, one of x or y is ± 1 or $\pm i$.

This is meant to parallel the integer definition of primes: p is a $\mathbb{Z}$-prime if whenever you write $p = xy$, one of x or y is ± 1. What is special about ± 1 and $\pm i$ is that it is possible to divide by them, so it's always possible to create factorizations involving them.

Facts. Addition, multiplication, and subtraction in $\mathbb{Z}[i]$ work the same as you are used to from the integers as far as the usual rules of commutativity, associativity, and distributivity. It's straightforward to add these new integers:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

Multiplying them is slightly trickier, but we can distribute the product like normal and then replace all the i^2's by -1's:

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = ac + (ad + bc)i - bd = (ac - bd) + (ad + bc)i$$

As mentioned previously, one reason that complex integers are important to us is that they will give us more ways to factor equations. But this also means there will be more ways to factor individual integers, even integers that we could not factor before.

Luckily, we have a powerful tool for connecting factorization in $\mathbb{Z}[i]$ and $\mathbb{Z}$: the norm map

Definition. The norm map N is a function from $\mathbb{Z}[i]$ to $\mathbb{Z}$ which is given by

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$$

[note: we will sometimes call $a - bi$ the "conjugate" of $a + bi$, so the norm map can be described as the product of a complex integer with its conjugate]

Important Facts (check these yourself).

(1) The norm map "respects multiplication" in the sense that $N(xy) = N(x)N(y)$. This crucial fact lets us relate $\mathbb{Z}[i]$ and $\mathbb{Z}$ factorizations.

(2) If $N(x) = 1$ then $x = \pm 1$ or $x = \pm i$. These are the elements of $\mathbb{Z}[i]$ which we can divide by without introducing fractions. They are much like ± 1 in $\mathbb{Z}$, which we can also divide by in $\mathbb{Z}$ without introducing new fractions (whereas to divide by 2 forces us to introduce the non-integer fraction $\frac{1}{2}$).

(3) If $N(x) = p$ is a $\mathbb{Z}$-prime, then x is a $\mathbb{Z}[i]$-prime.

Main Goal. We will eventually prove the following fact:

$$\text{a } \mathbb{Z}\text{-prime } p \text{ is the norm of a complex integer (which is a } \mathbb{Z}[i]\text{-prime)}$$
$$\Leftrightarrow$$
$$p \text{ factors into a product of two distinct } \mathbb{Z}[i]\text{-primes (in } \mathbb{Z}[i])$$
$$\Leftrightarrow$$
$$p = 1 \bmod 4$$

It is interesting to note that the norm of a complex integer is $N(a+bi) = a^2 + b^2$, so this answers the question "which primes are sums of two squares?" and shows that the answer is *remarkably* simple - it only depends on p mod 4.

Knowing a prime mod 4 is extremely little information (for instance, you only need the last two digits of any number, no matter how large, to determine what it is mod 4). Yet somehow it determines precisely when that prime can be written as a sum of two squares, which seems like a very difficult question to understand!! After all, there are very few squares, and fairly few primes, so an interaction like this is unexpected.

This is the first case of a powerful theorem called ***quadratic reciprocity***. A very loose statement of quadratic reciprocity is the following:

a $\mathbb{Z}$-prime p is the norm of something in a "larger world of integers" (such as adding $\sqrt{-5}$ to $\mathbb{Z}$)
$\Leftrightarrow$
p splits into a product of two distinct "larger world" primes
$\Leftrightarrow$
p satisfies some congruence conditions

These norms will look like $a^2 + db^2$ for various integers d, and so the full version of quadratic reciprocity tells us how a prime can be written as a (modified) sum of integer squares.

We will not prove this in our class, only some special cases (for instance, the case $d = 1$ corresponds to the larger world of $\mathbb{Z}[i]$), because it is quite difficult. We will get a lot of use out of it though!! This is a powerful tool for understanding the interaction between factorization in the integers and factorization in these "larger worlds of integers".

This will give us the ability to determine the integer solutions to diophantine equations like

$$x^2 + 3y^2 = z^5 \qquad x^2 + 2y^2 = p \text{ (a prime)}$$

Before we start on that, there is a lot of other work to do!! We will begin by studying divisibility in $\mathbb{Z}[i]$ on its own, rather than just comparing to $\mathbb{Z}$. In particular, we will show that it is possible to long divide in $\mathbb{Z}[i]$, and also to make sense of modular arithmetic for $\mathbb{Z}[i]$.

This benefits greatly from having some pictures, so it will be addressed in some hand-written notes that will be posted separately on the website soon.