Recall: Gaussian integers $\mathbb{Z}[i]$ - $a+bi$ with $a, b \in \mathbb{Z}$. (Lives inside $\mathbb{C} = \mathbb{R}[i]$).

For $z \in \mathbb{Z}[i]$, $N(z) = z \overline{z} = |z|^2$ - square of distance from origin.

If $z = a+bi$, $N(z) = (a+bi)(a-bi) = a^2 + b^2$.

$N(z_1z_2) = N(z_1)N(z_2)$. 

Math 4400
Week 12, Thursday
Gaussian primes and unique factorization.
\[ \mathbb{C} \setminus \{0\} \rightarrow \mathbb{R}_{>0} \text{ (positive real numbers)} \]
\[ \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{Z}_{>0} \text{ (positive integers)} \]

**Crucial reformulation of sums of two squares problem:**

Which positive integers \( n \) can be written as \( n = a^2 + b^2, \ a, b \in \mathbb{Z} \)?

\[ n = a^2 + b^2 \]

\[ n = \mathcal{N}(a + bi). \]

Which positive integers \( n \) can be written as \( n = \mathcal{N}(z), \ z \in \mathbb{Z}[i] \)

Allows us to use structure of \( \mathbb{Z}[i] \) to study sums of 2 squares.

Today: unique factorization and primes in \( \mathbb{Z}[i] \)

Indecomposables, units, and primes.
Definition: A Gaussian integer $z$ is **indecomposable** if $z = \alpha \beta \Rightarrow \alpha$ or $\beta$ is a unit in $\mathbb{Z}[i]$. (otherwise decomposable).

Example. $11$ is indecomposable in $\mathbb{Z}[i]$. ($11 + 0i$).

Suppose $11 = \alpha \beta$, $\alpha, \beta \in \mathbb{Z}[i]$.

$N(11) = N(\alpha \beta) \Rightarrow 11^2 = N(\alpha)N(\beta)$

Possibilities are:

$N(\alpha) = N(\beta) = 11$: But if $\alpha = a + bi$, $11 = a^2 + b^2 \times$

not possible $- 11 \equiv 3 \mod 4$ !

$N(\alpha) = 11^2$, $N(\beta) = 1$. $N(\beta) = 1$ $\beta = a + bi$.

$(a + bi)(a - bi) = 1$ so $\beta$ is a unit!

$N(\alpha) = 1$, $N(\beta) = 11^2$ similarly get $\alpha$ is a unit!

Lemma: (1) $z$ is a unit in $\mathbb{Z}[i] \iff N(z) = 1$ 

($\iff \exists 1, -1, i, -i$)

(2) If $N(z)$ is prime, then $z$ is indecomposable.

Proof: (1) If $N(z) = 1$ $z = a + bi$, $1 = N(z) = (a + bi)(a - bi)$ so $z$ is a unit.

△ Can be indecomposable

N not prime.

If $z$ is a unit, so there is $t \in \mathbb{Z}[i]$ s.t. $st = 1$ then $N(s)N(t) = 1 \Rightarrow N(s) = N(t) = 1$.

e.g. $1 = N(a + bi) = a^2 + b^2 \Rightarrow$ one of $a, b$ is $\pm 1$ the other is zero.

(2) If $N(z) = p$, $z = \alpha \beta$. 

\[ N(11) = 121. \]
\[ p = N(2iB) = N(cA)N(B) \Rightarrow N(cA) = 1 \text{ or } N(B) = 1 \]

So by (1), \( \alpha \) or \( B \)

is a unit.

Example:

- \( 10 = 5 \cdot 2 \) is decomposable.

Decompose/Composite as an int. \Rightarrow decomposable Gaussian integer:

- \( 5 = (1+2i)(1-2i) \) is decomposable.

Prime as an integer \( \not\Rightarrow \) indecomposable as a Gaussian integer.

- \( 2 = (1+i)(1-i) \) is decomposable

\[ (1+2i), (1-2i), (1+i), (1-i) \]

\( \text{in decomposable: } \]

\[ \text{Norm } 5 \quad \text{Norm } 2 \]

Prime norm \( \Rightarrow \) indecomposable

Note: \( 10 = (1+2i)(1-2i)(1+i)(1-i) \)

\( \equiv \)

\[ 5 \quad 2. \]

But \( 1-i = (-i)(1+i) \).

So also \( 10 = (-i)(1+2i)(1-2i)(1+i)^2 \), a prime factorization of 10!

Definition: A Gaussian prime is a set of indecomposable in \( \mathbb{Z}[i] \) which
differ by multiplication by a unit.

Example: \{11, -11, 11i, -11i\}.
- \{1+2i, -1-2i, -2+i, 2-i\}
- \{1-2i, -1+2i, 2+i, -2-i\}
- \{1+i, -1-i, -1+i, 1-i\}.

Theorem:
(1) Any Gaussian prime contains exactly one indecomposable of the form
   a+bi or a-bi where a>b
   are positive integers with
   \(a^2+b^2\) an integer prime \(\equiv 1 \, \text{mod} \, 4\),
   or an integer prime \(\equiv 3 \, \text{mod} \, 4\).
(2) Any Gaussian integer \(z\) has a unique factorization
    \(z = i^m r_1 \cdot r_2 \cdot \ldots \cdot r_n\)
    where \(r_i\) are indecomposables as in (1).
unique up to reordering and \( n \in \mathbb{Z}/4\mathbb{Z} \).

Corollary: A positive integer \( n \) is a sum of two squares \( \iff \)
\[ n = p_1^{k_1} \cdots p_m^{k_m} \]
where \( p_i \) are distinct integer primes and \( k_i \) is even if \( p_i \equiv 3 \mod 4 \).

Proof of corollary assuming theorem: Apply norm to unique factorization in \( \mathbb{Z}[i] \).

Just like for integers, proof of theorem boils down to a Euclidean algorithm for \( \gcd \) (plus stuff from Tuesday for part (1)).

Exactly like Euclidean alg for integers using:

\[ \text{Division for Gaussian integers:} \]
\[ \text{If } \alpha, \beta \text{ are Gaussian integers,} \]
\[ B = qA + r \quad \text{for} \quad N(r) \leq \frac{N(A)}{2}. \]

**Proof/Construction of q:**

In \( C \), \[ \frac{B}{A} = \frac{B}{N(A)} = x + yi. \]

to get \( q \), round \( x \) and \( y \) to nearest integer

**Example:** \( \gcd(11+i, 61) \).

\[ 61 = q_1(11+i) + r_1 \]

In \( C \), \[ \frac{61}{11+i} = \frac{61(11-i)}{122} = \frac{11}{2} - \frac{i}{2} \rightsquigarrow q_1 = 6. \]

\[ 61 = 6(11+i) + (-5-6i). \]

\( 11+i = q_2(-5-6i) + r_2 \)

\[ \frac{11+i}{-5-6i} = \frac{(11+i)(-5+6i)}{61} = \frac{(-61+61i)}{61} = -1+i \]

\( 11+i = (-1+i)(-5-(i)) + 0 \)

\[ -5-6i = \gcd(11+i, 61). \]
Note: \[ 1^2 + 1^2 = 2 \cdot 6^1 \]
\[ N(-5 - 6i) = (-9^2 + (-6)^2) = 6^1. \]