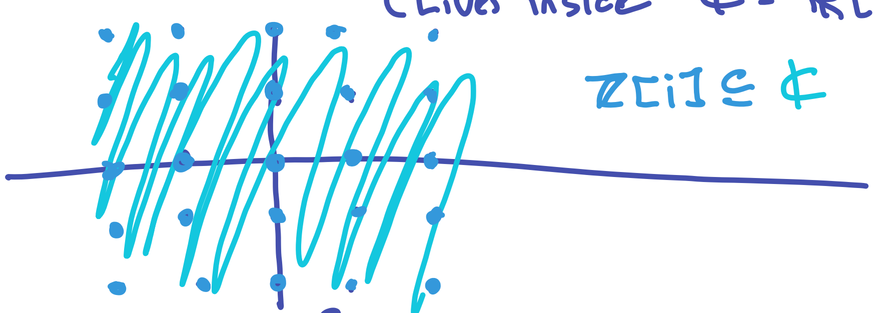
Math 4400

Week 12, Thursday

Gaussian primes and unique factorization.

Recall: Gaussian integers $\mathbb{Z}[i]$ - $a+bi$ with $a,b \in \mathbb{Z}$.

(Lives inside $\mathbb{C} = \mathbb{R}[i]$).



$\mathbb{Z}[i] \subseteq \mathbb{C}$

$N(z) = z\bar{z} = \|z\|^2$ ← square of distance from origin.

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

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

$N: \mathbb{C} \setminus \{0\} \to \mathbb{R}_{>0}$ (positive real numbers)

$\mathbb{Z}[i] \setminus \{0\} \to \mathbb{Z}_{>0}$ (positive integers).

Crucial reformulation of sums of two squares problem:

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

$$\Updownarrow$$

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

$$n = a^2 + b^2 \iff n = N(a+bi).$$

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 <u>indecomposable</u> if
$z = \alpha\beta \Rightarrow \alpha$ or β 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 $\alpha = a+bi$, $11 = a^2+b^2$ X
not possible — $11 \equiv 3 \bmod 4$!

$N(\alpha) = 11^2$ $N(\beta) = 1$. $N(\beta) = 1$ $\beta = a+bi$.
$(a+bi)(a-bi) = 1$ so β is a unit!

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

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

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

<u>Proof</u>: (1) If $N(z) = 1$ $z = a+bi$ $1 = N(z) = (a+bi)(a-bi)$
so z is a unit.

△ Can be indecomp. but N not prime, e.g. $N(11) = 121$.

If z is a unit, so there is $t \in \mathbb{Z}[i]$
s.t. $st = 1$ then $N(s)N(t) = 1 \Rightarrow N(s) = N(t) = 1$.
$1 = N(a+bi) = a^2+b^2 \Rightarrow$ one of a, b is ± 1
the other is zero.

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

$$p = N(\alpha\beta) = N(\alpha)N(\beta) \Rightarrow N(\alpha)=1 \text{ or } N(\beta)=1$$

so by (1) α or β is a unit.

Example:

- $10 = 5\cdot 2$ is decomposable.

Decomposable/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

- $(1+2i)$, $(1-2i)$, $(1+i)$, $(1-i)$ indecomposable.

Norm 5   Norm 2

Prime norm $\Rightarrow$ indecomposable

Note: $10 = \underbrace{(1+2i)(1-2i)}_{5}\underbrace{(1+i)(1-i)}_{2}.$

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

So also $10 = (-i)(1+2i)(1-2i)(1+i)^2$.

unit   "Prime factorization of 10"

Definition: A Gaussian prime is a set of indecomposables 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
- $1+i$
- $a+bi$ or $a-bi$ where $a>b$ are positive integers with a^2+b^2 an integer prime $\equiv 1 \bmod 4$.
- p an integer prime $\equiv 3 \bmod 4$

(2) Any Gaussian integer z has a unique factorization

$$z = i^m \gamma_1 \cdot \gamma_2 \cdot \ldots \gamma_n$$

where γ_i are indecomposables as in (1) unique up to reordering and $m \in \mathbb{Z}/4\mathbb{Z}$.

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 $p_i \equiv 3 \bmod 4$.

<u>Proof of corollary assuming theorem</u>: 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:

Division for Gaussian integers:

If α, β are Gaussian integers,

$\beta = q\alpha + r \quad$ for $\quad N(r) \leq \frac{N(\alpha)}{2}$.

Proof/construction of q:

In $\mathbb{C}$, $\frac{\beta}{\alpha} = \frac{\beta\bar{\alpha}}{N(\alpha)} = x + yi$.

to get q, round x and y to nearest integers

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

$$61 = q_1(11+i) + r_1$$

$$\frac{11}{2} + \left(-\frac{1}{2}\right)i$$

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

$$61 = 6(11+i) + (-5-6i).$$

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

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

$$(11+i) = (-1+i)\underline{\underline{(-5-6i)}} + 0$$

$$-5-6i = \gcd(11+i, 61).$$

Note: $11^2 + 1^2 = 2 \cdot 61$
$N(-5-6i) = (-5)^2 + (-6)^2 = 61.$