Last time:

Galois integers:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

You can add, subtract, and multiply Galois integers, but can't always divide (just like with integers).

For $\alpha, \beta \in \mathbb{Z}[i]$, we say α divides β if there is some $\gamma \in \mathbb{Z}[i]$ such that $\alpha\gamma = \beta$.

Ex: Since $2 = 2 \cdot 1 = -2(-1) = (1+i)(1-i)$, the divisors of 2 include $\pm 1, \pm 2, 1 \pm i$.

A unit $u \in \mathbb{Z}[i]$ is a number that has a multiplicative inverse $u' \in \mathbb{Z}[i]$ (which satisfies $uu' = 1$).

Ex: ± 1, $\pm i$ are all units in $\mathbb{Z}[i]$.

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit.

Ex: Since $1 + i$ divides 2, and it is not of the form $2u$ or u for any unit u, 2 is not prime.

Norm

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

Proposition. For $\alpha, \beta \in \mathbb{Z}[i]$, we have

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Back to units: If α is a unit, then there is some β for which $\alpha\beta = 1$. So

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

So $N(\alpha) = N(\beta) = 1$. What are integer solutions to $a^2 + b^2 = 1$?

Theorem

The units in $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$.

Define

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geqslant 0} \quad \text{by} \quad a + bi \mapsto a^2 + b^2.$$

For $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Back to primes: Is 2 prime in $\mathbb{Z}[i]$?

Suppose we have

$$(a + bi)(c + di) = 2.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 4.$$

Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.

$a^2 + b^2 = 2$: Potentially nontrivial factors?

$a^2 + b^2 = 4$: In this case, $c + di$ is a unit.

Are there non-trivial solutions to $a^2 + b^2 = 2$? Yes! For example, $1 + i$. Does $1 + i$ divide 2? Compute:

$$\frac{2}{1+i} = \frac{2(1-i)}{2} = 1 - i.$$

So since $1 + i$ isn't a unit, nor is it a unit multiple of 2, we have 2 is not prime in $\mathbb{Z}[i]$!!

Theorem

Let p be an odd prime. Then there are integers a, b satisfying

$$a^2 + b^2 = p$$

if and only if $p \equiv_4 1$.

Proof. Show $a^2 + b^2 = p$ implies $p \equiv_4 1$ by direct computation. For the reverse, see Ch. 24. □

Ex. There are no integer solutions to $a^2 + b^2 = 3$. So, using the same idea as last time, suppose we have

$$(a + bi)(c + di) = 3.$$

Taking N of both sides, we get

$$(a^2 + b^2)(c^2 + d^2) = 9.$$

Possibilities:

$a^2 + b^2 = 1$: In this case, $a + bi$ is a unit.

$a^2 + b^2 = 3$: No solutions.

$a^2 + b^2 = 9$: In this case, $c + di$ is a unit.

So 3 is a prime in $\mathbb{Z}[i]$.

We say $\beta \in \mathbb{Z}[i]$ is prime if the only divisors of β are of the form u or $u\beta$, where u is a unit (one of $\{\pm 1, \pm i\}$).

Looking for primes so far:

1. If $n \in \mathbb{Z}$ is composite in $\mathbb{Z}$, then it is composite in $\mathbb{Z}[i]$.
2. If $p \in \mathbb{Z}$ is prime in $\mathbb{Z}$, then either
   (a) $p = 2$, which is not prime in $\mathbb{Z}[i]$; (we checked)
   (b) $p \equiv_4 -1$, in which case p is prime in $\mathbb{Z}[i]$; (prove using norms)
   (c) $p \equiv_4 1$, in which case there are $a, b \in \mathbb{Z}$ with $a^2 + b^2 = p$, so that $a + ib \neq u, pu$ for any unit u and
   $$(a + ib)(a - ib) = a^2 + b^2 = p,$$
   i.e. p is not prime in $\mathbb{Z}[i]$.

Proposition

An integer n is prime in $\mathbb{Z}[i]$ if and only if n is a prime in $\mathbb{Z}$ satisfying $n \equiv_4 1$.

Are there any more?

Theorem (Gaussian Prime Theorem)

The Gaussian primes can be described as follows:

(i) *(ramified) 1 + i is a Gaussian prime.*

(ii) *(inert) Let p be a prime in $\mathbb{Z}$ with $p \equiv -1 \pmod 4$. Then p is a Gaussian prime.*

(iii) *(split) Let p be a prime in $\mathbb{Z}$ with $p \equiv 1 \pmod 4$. Then $p = a^2 + b^2$ for $a, b \in \mathbb{Z}_{>0}$, and $a + bi$ is a Gaussian prime.*

Moreover, every Gaussian prime is equal to a unit times a Gaussian prime of the form (i), (ii), or (iii).

We can also use $N(\alpha)$ to find divisors of α.

Lemma (Gaussian Divisibility Lemma)

Let $\alpha \in \mathbb{Z}[i]$.

(a) *If* 2 *divides* $N(\alpha)$ *in* $\mathbb{Z}$, *then* $1+i$ *divides* α *in* $\mathbb{Z}[i]$.

(b) *Let* p *be (an inert) prime, and suppose that* p *divides* $N(\alpha)$ *in* $\mathbb{Z}$. *Then* p *divides* α *in* $\mathbb{Z}[i]$.

(c) *Let* $\pi = u + vi$ *be a split, and let* $\overline{\pi} = u - vi$. *If* $N(\pi)$ *divides* $N(\alpha)$ *in* $\mathbb{Z}$, *then at least one of* π *or* $\overline{\pi}$ *divides* α *in* $\mathbb{Z}[i]$.

To be clear:
a divides b in $\mathbb{Z}$ if there is a $k \in \mathbb{Z}$ such that $ak = b$.
α divides β in $\mathbb{Z}[i]$ if there is a $\gamma \in \mathbb{Z}[i]$ such that $\alpha\gamma = \beta$.