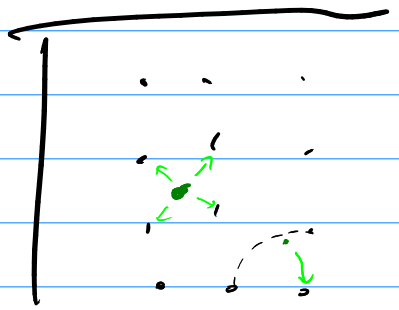
Gaussian integers $\mathbb{Z}[i]$

Worksheet. practice division alg.
notice: answers are not unique.

$$\frac{(4-i)(1-i)}{(1+i)(1-i)} = \frac{3-5i}{2} = \frac{3}{2} - \frac{5}{2}i$$

could take $q = 2-2i$, or $2-3i$
or $1-2i$ or $1-3i$

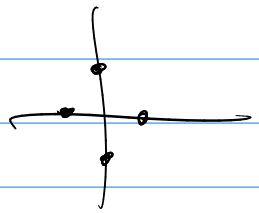
tried to factor some Gaussian integers
— hard!



Goal: Fermat's Christmas thm:
a prime p can be written as a^2+b^2
iff $p=2$ or $p \equiv 1 \pmod 4$
not if $p \equiv 3 \pmod 4$

---

units in $\mathbb{Z}[i]$?
if $z \cdot w = 1$ then $|z|^2 \cdot |w|^2 = |1|^2 = 1$
so $|z|^2 = 1$
so $z = \pm 1$ or $\pm i$



think of $7-i \xrightarrow{\times(-1)} -7+i$
$\times i$ ↓ , $\times(-i)$ ↘
$1+7i$, $-1-7i$

as much the same in factoring in $\mathbb{Z}[i]$
as 12 and -12 were in $\mathbb{Z}$.

zero-divisors in $\mathbb{Z}[i]$?

none - it's a subring of $\mathbb{C}$

$\mathbb{Z}[i]$ is an integral domain.

---

primes and irreducibles in $\mathbb{Z}[i]$

Recall from Monday:

$r \in R$ is prime if $r \mid ab$ implies $r \mid a$ or $r \mid b$, (and r not a unit)

equivalently: $R/\langle r \rangle$ is an int. domain.

if R is an int. dom., say that

$r \in R$ is irreducible if

not zero, not a unit,

and can't be factored as $r = a \cdot b$

unless a is a unit or b is a unit.

in an int. dom., non-zero prime $\Rightarrow$ irreducible

Euclid's lemma: if you have a division alg.

then irreducible $\Rightarrow$ prime.

in $\mathbb{Z}[\sqrt{-5}]$, irred and prime are different

but $\mathbb{Z}[i]$, they're the same thing.

Can happen: $p \in \mathbb{Z}$ is prime, but it factors in $\mathbb{Z}[i]$

e.g. $2 = (1+i)(1-i)$

$5 = (2+i)(2-i)$

$13 = (3+2i)(3-2i)$ — $|3-2i|^2 = 13$ so $3-2i$ is irred.

each of those factors on the right is prime in $\mathbb{Z}[i]$.

Prop for $z \in \mathbb{Z}[i]$, if $|z|^2 =$ prime in $\mathbb{Z}$ then z is irreducible.

(sketch: if $z = vw$ then $|z|^2 = |v|^2 \cdot |w|^2$, $|z|^2 = p$, so $|v|^2 = 1$ or $|w|^2 = 1$ so v or w is a unit.)

Can also happen: $p \in \mathbb{Z}$ is prime and it stays prime in $\mathbb{Z}[i]$

e.g. $p = 3, 7, 11$

On Worksheet 4, you proved that $\mathbb{Z}[i]/\langle 3 \rangle$ is a field

in particular an int. dom.

so $\langle 3 \rangle$ is a prime ideal.

Or we could check: if $3 = z \cdot w$

then $9 = |z|^2 \cdot |w|^2$

and $\nexists\ z \in \mathbb{Z}[i]$ with $|z|^2 = 3$

Prop if $p \in \mathbb{Z}$ is a prime with $p \equiv 3 \pmod 4$ then p remains prime in $\mathbb{Z}[i]$

Pf if p were not prime, write $p = z \cdot w$ where z, w are not units
then $p^2 = |z|^2 \cdot |w|^2$
so $|z|^2 = p$ and $|w|^2 = p$

write $z = a + bi$, then $p = a^2 + b^2$
work mod 4:

$a \equiv 0, 1, 2, 3$ sim. with b
$a^2 \equiv 0, 1, 0, 1$
so $a^2 + b^2 \equiv 0, 1, 2$ but not 3.

so can't have $p \equiv 3 \pmod 4$. ∎

Next HW: if $z \in \mathbb{Z}[i]$ is irred
then $|z| = p$ or $|z| = p^2$...

Return to Worksheet #. #2: factor things in $\mathbb{Z}[i]$

a. $6 = 2 \cdot 3 = (1+i)(1-i) \cdot 3$ and those are all irreducible.

c. 7 is irreducible by prop. above.

d. $z = 4 + 3i$ $|z|^2 = 4^2 + 3^2 = 25 = 5 \cdot 5$
try to factor out some w with $|w|^2 = 5$...

b. $z = 11 + 7i$ $|z|^2 = 121 + 49 = 170 = 2 \cdot 5 \cdot 17$
divide by $1+i$, $17 \equiv 1 \pmod 4$
and something with $|w|^2 = 5$, see where it gets you.