Recall: **Thm:** $\mathbb{Z}$ is a PID.

(SCR ring is ideal if $z_1, z_2 \in S \Rightarrow z_1 \pm z_2 \in S$ & $rz \in S$.)

i.e. $S = \text{ideal} = (n_1, \ldots, n_k)$ ideal

If $= \{ n_1 x_1 + n_2 x_2 + \cdots + n_k x_k \mid x_i \in \mathbb{Z} \}$.

then $\exists\, d$ s.t. $S = (d)$. (& $d = \gcd(n_1, \ldots, n_k)$).

Pf: Start with $S = (n, m) = \{ nx + my \}$.

Fact 1: $\ell \mid n$ & $\ell \mid m \Rightarrow \ell \mid nx + my \Rightarrow \gcd(n,m) \mid nx + my$

$\Rightarrow S \subseteq (\gcd(n,m))$.

Fact 2: Claim: $\gcd(n,m) \in S$. ($\Rightarrow (\gcd(n,m)) \subseteq S$).

want x & y s.t. $nx + my = d = \gcd(n,m)$ $\Rightarrow$

Ex: $n_1 = 5$, $n_2 = 17$, $n_3 = 26$. **Claim:** $\exists\, d \in \mathbb{Z}$

↑

s.t. $S = \{ 5x_1 + 17x_2 + 26x_3 \mid x_i \in \mathbb{Z} \}$.

$\psi = \{ dy \mid y \in \mathbb{Z} \}$. $d=1$, $(1) = \mathbb{Z}$.

$0, 5, 17, 26, 22, 2 = (-3)5 + 17$, $2k = (-3k)\cdot 5 + k \cdot 17$.

$1 = 5 - 2\cdot 2 = 5 - ((-3)5 + 17)\,2 = 7\cdot 5 + -2\cdot 17$.

Ex: $S = \{ 35x_1 + 10x_2 + 15x_3 \} = (5)$.

---

pf (Fact 2): Look in S, find $r \in S$, least >0 elem.

$r = nx + my$, Euclidean alg $\Rightarrow \exists$ solution to $nx+my=d$

$nx + my = d$. Claim: $r = d$. (since $d \mid n$ & $d \mid m$ $\Rightarrow d \mid (nx+my)$.

Once we know $(n_1, n_2) = (d_1)$. — $\gcd(n_1, n_2)$

$(n_1, n_2, n_3) = (d_1, n_3) = (d_2)$. And so on...

(?) — $\gcd(d_1, n_3)$

$d_1 = \gcd(n_1, n_2)$, $d_2 = \gcd(d_1, n_3)$.

Exercise 1: $d_2 = \gcd(n_1, n_2, n_3)$

If $S = (n_1, n_2)$, $2n_1 \in S$, $2n_1 - n_2 \in S$.

$= \{n_1 x_1 + n_2 x_2 \mid x_1, x_2 \in \mathbb{Z}\}$.

Now try $R = \mathbb{Z}[i]$ "Gaussian integers".

$= \{x + iy \mid x, y \in \mathbb{Z}\}$ ⇒ $7+3i$, $-2+17i$.

Exercise 2: This is a ring i.e. $z_1, z_2 \in R \Rightarrow z_1 + z_2 \in R$ & $z_1 z_2 \in R$.

Ex: $(7+3i)(-2+17i) = -14 - 6i + 119i - 51 =$

$= -65 + 113i$.

Exercise 3: Let R = linear polys/$\mathbb{Z}$, i.e. $r \in R \Leftrightarrow r = n + mx$. Is R a ring?

Exercise 4: Let $R = \mathbb{Z}[\sqrt{-5}] = \{x + \sqrt{-5}\,y \mid x, y \in \mathbb{Z}\}$.

Is this a ring?

Fact: If R is a PID, $\Rightarrow$ UFD (unique factorization)

Because $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

Back to $R = \mathbb{Z}[i]$. Do we have a division algorithm?

i.e. $n = m \cdot q + r$ with r "smaller" than "m"?

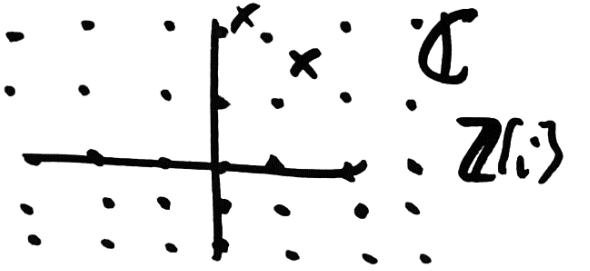
Kevin's "norm" $N(x+iy) = x^2 + y^2 = (x+iy)(x-iy)$.

Ex: $n = -2+17i$, $m = 7+3i$. Find q & r s.t.

$0 \le N(r) < N(m) = \boxed{58}$ | Hint: $171 = 27q + r$, $\left\lfloor \frac{171}{27} \right\rfloor = q$.

$$\frac{n}{m} = \frac{(-2+17i)(7-3i)}{(7+3i)(7-3i)} = \frac{37 + i(125)}{58}$$

$\approx 2i = q$.



Want: $n = mq + r$, $r = n - mq = (-2+17i) - (7+3i)(2i)$,

$\hookrightarrow = 4+3i$, $N(r) = 25 < 58$.

Know: $n = mq_1 + r_1$, $n = -2+17i$, $m = 7+3i$,
r_{-1} r_0 $q_1 = 2i$, $r_1 = 4+3i$

Next: $m = r_1 q_2 + r_2$, $7+3i = (4+3i)\,q_2 + r_3$.
q_2 r_2 q_2 r_3

$\frac{(7+3i)(4-3i)}{(4+3i)(4-3i)} = \frac{37-9i}{25} \approx 1 = q_2$ $\quad$ $N(r_2) = 9 < 25$

Next: $r_1 = r_2 q_3 + r_3$, $4+3i = 3 \cdot q_3 + r_3$.
r_2 q_3 r_3

$\frac{4+3i}{3} \approx 1+i = q_3$, $\quad$ r_2 $1+i$ $\boxed{1}$.

Last: $r_2 = r_3 q_4 + r_4$, $\quad 3 = 1 \cdot q_4 + r_4$.
3 0

$\circlearrowleft$

Exercise 5: Do Euclidean alg on

(1) $n = 5+3i$, $m = 2-8i$

(2) $n = 5+3i$, $m = 2+8i$.
