# Welcome! Everything is fine.

When you're connected by zoom:

- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.

# Review of 13.7

$d = 2$ or $3 \pmod 4$, $d < 0$, $\delta = \sqrt{d}$, $R = \mathbb{Z}[\delta]$.

**Definition**

If $A\overline{A} = (n)$, $n > 0$, then $N(A) = n$.

**Definition**

$\mu(d) = 2\sqrt{|d|/3}$ when $d = 2$ or $3 \pmod 4$.

**Theorem**

*$\mathcal{C}(R)$ generated by $P$ such that $N(P) = p \leq \mu$, $p$ splits as $(p) = P\overline{P}$.*

So first step of computing the class group is to find split $p \leq \mu$, i.e., $p$ such that $x^2 - d$ factors over $\mathbb{F}_p$.

# Analyzing elements of the class group

*Relations:* Suppose (e.g.) $(p) = P\overline{P}$, $(q) = Q\overline{Q}$, $(s) = S\overline{S}$ are split primes.

If $N(\alpha) = p^i q^j s^k$, then

find elements by guessing!!!

can't have both P, Pbar dividing (\alpha)

$$P^i \overline{P}^i Q^j \overline{Q}^j S^k \overline{S}^k = (\alpha)(\overline{\alpha}) = (n)$$

is principal, and if no real integer divides $\alpha$, we must have (up to switching $P$ and $\overline{P}$, etc.) that

$$\langle P \rangle^i \langle Q \rangle^j \langle S \rangle^k = 1.$$

So we look for $\alpha$ such that $N(\alpha)$ is a product of those small split primes.

*Nontriviality:* If $P\overline{P} = (p)$ and $p$ irreducible in $\mathbb{Z}[\delta]$ (check by brute force), then $\langle P \rangle \neq 1$.

$p = 2$ *ramifies:* For $d = 2$ or $3 \pmod 4$, $(2) = P\overline{P}$ ramifies, and for $d \neq -1, -2$, $\langle P \rangle$ has order 2 in the class group.

# Example: $d = -26$

- $\lfloor \mu \rfloor = \left\lfloor 2\sqrt{26/3} \right\rfloor = 5$, so check $p = 2, 3, 5$; 2 ramifies (always).

we calculate (mod 3):

3 and 5 split:

$x^2 + 26 = x^2 - 1$

This factors, so 3 splits in R, as (say) (3) = Q\bar{Q}.

So let $(2) = P\overline{P} = P^2$, $(3) = Q\overline{Q}$, $(5) = S\overline{S}$.

Now look for relations. (relns among gens P, Q, S)

$N(1+\delta) =$

$1^2 + 26 = 27 = 3^3$

$\Rightarrow \langle Q \rangle = e$ b/c $Q^3\overline{Q}^3 = (27) = (1+\delta)(1-\delta)$

any prin ideal = identity !

$N(2+\delta) =$

$2^2 + 26 = 2 \cdot 3 \cdot 5$

Can't have both a Q and a \bar{Q} factor of (1+\delta) b/c then (3)=Q\bar{Q} would divide (1+\delta).

$\Rightarrow \langle P \rangle \langle Q \rangle \langle S \rangle = e$

So S is a redundant generator, and we know that <P> has order 2 b/c 2 ramifies, so class group must then be gen by <P><Q>, and must have order 6 = Z_2 x Z_3

# Example: $d = -74$

$\lfloor \mu \rfloor = \left\lfloor 2\sqrt{74/3} \right\rfloor = 9$, so check $p = 2, 3, 5, 7$; 2 ramifies (always).

3 and 5 split, 7 remains:

So let $(2) = P\overline{P} = P^2$, $(3) = Q\overline{Q}$, $(5) = S\overline{S}$.
Now look for relations.
$N(1 + \delta) =$

$N(4 + \delta) =$

# Example: $d = -74$ cont

$(2) = P\overline{P} = P^2$, $(3) = Q\overline{Q}$, $(5) = S\overline{S}$.
$N(13 + \delta) =$

$N(14 + \delta) =$

# Example: $d = -61$

$\lfloor \mu \rfloor = \left\lfloor 2\sqrt{61/3} \right\rfloor = 9$, so check $p = 2, 3, 5, 7$; 2 ramifies (always).

3 remains, 5 and 7 split: 2 is not a square (mod 3) by brute force

$x^2 - 2$, 2 is NR // $x^2 + 61 \equiv x^2 - 4 \pmod 5$

So let $(2) = P\overline{P} = P^2$, $(5) = Q\overline{Q}$, $(7) = S\overline{S}$.

<P>,<Q>,<S> generate class gp

Now look for relations.

$a^2 + 61 =$ 62, 65, $70 = 2 \cdot 5 \cdot 7$

<P>^2 = e

a=1 a=2 N(3+\delta)

so <P><Q><S> = e

$125 = 5^3$

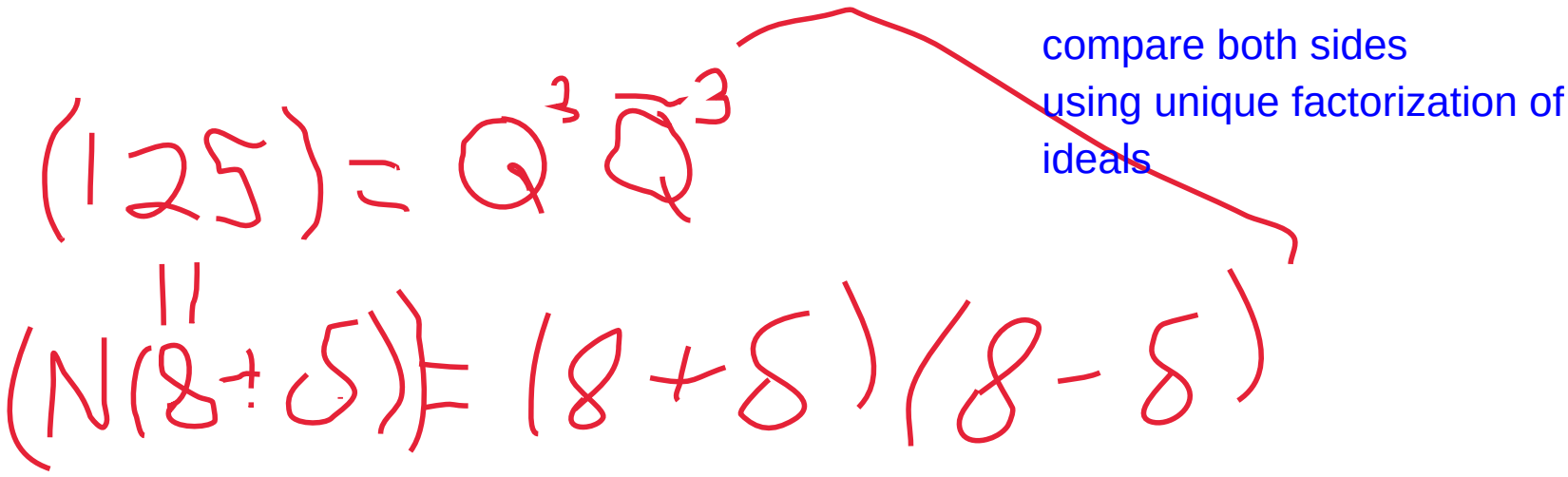
<Q>^3 = e

( same true for \bar{Q} b/c <\bar{Q}>=<Q>^{-1} )

N(8+\delta)

So again, class group generated by <P> and <Q>, and is = Z_2 x Z_3.

# Example: $d = -61$ cont




So (for ex) (8+\delta) must be the product of half of the Qs & \bar{Q}s, and (8-\delta) must be the product of the other half (b/c conjugate).
If there's a mix in the factors of (8+\delta), then Q\bar{Q} divides (8+\delta), which means that 5 divides 8+\delta, and that can't happen.
So (8+\delta) must be the product of all Qs or all \bar{Q}s; after changing names, WLOG all Qs: (8+\delta) = Q^3
But (8+\delta) is a principal idea, so its ideal class is trivial, i.e., <(8+\delta)> = e.
So <Q>^3 = e.

# Why does $\mu$ work?

(sticking to the $d = 2, 3 \pmod 4$ case)

- $N(A) = [R : A]$
  $=$ area of fund domain of $A$ in terms of $R$-rectangles
- If $\alpha$ is a minvec of a lattice $A$, $N(A) \geq \frac{\sqrt{3}}{2} N(\alpha)$.

- If $\alpha$ is a minvec of an ideal $A$, $N(\alpha) \leq N(A)\mu$.
- Every ideal class contains $A$ such that $N(A) \leq \mu$; prime factors of $A$ have even smaller norm.