Recall: Proved: Euclidean $\Rightarrow$ PID $\Rightarrow$ Noetherian $\Rightarrow$ UFD.

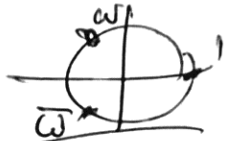
$\mathbb{Z}[\omega]$ = Eisenstein integers $\quad \omega = e^{2\pi i/3}$

$(\omega-1)(\omega^2+\omega+1) = \omega^3 - 1 = 0 \qquad \omega^3 = 1 \qquad \omega^2+\omega+1=0$

Recall: Wanted to know which $n = x^2+y^2$.

Answered question using $\mathbb{Z}[i]$. $N(z)$ "$x+iy$".

This quadratic form, $Q(x,y) = x^2+y^2$ is the norm form for $\mathbb{Z}[i]$.



$N(x+\omega y) = (x+\omega y)(x+\bar{\omega} y) = x^2 - xy + y^2$.

Q: Which integers $n = x^2 - xy + y^2$? ("$Q(x,y)$")

Look at some n's?

y \ x	0	1	2	3	4
0	0	1	4	9	16
1	1	1	3	7	13
2	4	3	4	7	12
3	9	7	7	9	13
4	16	13	12	13	16

homogeneous quadratic form

$$Q(kx, ky) = k^2x^2 - kx\cdot ky + k^2y^2.$$
$$= k^2\left(x^2 - xy + y^2\right) = k^2\, Q(x,y).$$

$Q(1,2) = 3$, $Q(2,4) = 4\cdot 3 = 12$.

$Q(3,6) = 9\cdot 3 = 27$. ($\times 2$)

Seeing $n = Q(x,y) \in \{0, 1, 3, 4, 7, 9, 12, 13, \ldots\}$,

With x^2+y^2, it was clear that #s get bigger the farther out you go.

What about $x^2 - xy + y^2$, can this take negative values? $= (x-y)^2 + xy$.

To see this in general, ex: $7x^2 - 32xy + 12y^2$.

Does this take large/small/positive/negative values? ~~To do~~: Idea: Pull out y^2:

$$y^2\left[\left(\frac{x}{y}\right)^2 - \left(\frac{x}{y}\right) + 1\right]$$ If we set $z = \frac{x}{y} \in \mathbb{Q}$.

Then $Q(x,y) = \underset{\geq 0}{y^2}\cdot Q(z)$ $\quad Q(z) = z^2 - z + 1$.

Q(z):

Is our Q ↑ ↗ ?

If we try to solve $Q(z) = 0 = z^2 - z + 1$.

$$\Rightarrow z = \frac{1 \pm \sqrt{1 - 4 \cdot 1}}{2}$$

For a general form $Q = [A, B, C] = Ax^2 + Bxy + Cy^2$

Will abuse "$[A, B, C]$" for both quad polynomial & quadratic form.

$Q(z, 1) = Az^2 + Bz + C$.

So Q takes both pos & neg values $\Leftrightarrow B^2 - 4AC > 0$.

For our form $Q = x^2 - xy + y^2$, discriminant $= -3 < 0$.

So Q only takes larger & larger positive values.

Aside: Make $x^3 + 4x^2y^2 - 5xy$ homogeneous.

Add auxiliary variable, z, to make all monomials have same degree. Total degree $= 4$.

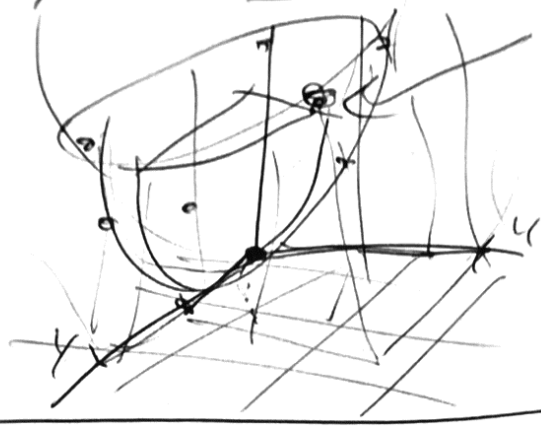
$\Rightarrow x^3 z + 4x^2y^2 - 5xyz^2 := P(x, y, z)$.

To get back to original (de-homogenize), Set $z=1$.

The $\mathbb{R}$-values taken by $Q = x^2 - xy + y^2$ are:

$z = x^2 - xy + y^2$.

$7 \quad 1 \quad 3$



Back to Q: What values does $Q = x^2 - xy + y^2$ take? Ans: $0, 1, 3, 4, 7, 9, 12, 13, 16, \ldots, \boxed{19}$ ← Any patterns?

mod 5: $0, 1, 3, 4, 2, 4$, all values.

mod 3: $0, 1, 0, 1, 1, 0, 0, 1, 1$.

$w^3 = 1$
$w = 1^{1/3}$

~~Conjecture:~~ Theorem: $\forall x, y \in \mathbb{Z}$, $x^2 - xy + y^2 \not\equiv 2 \pmod 3$.

$y \backslash x$	0	1	2
0	0	1	1
1	1	1	0
2	1	0	1

mod 3 only takes 0 or 1.

Claim: For Every $p \equiv 1 \pmod 3$. $\exists x, y \in \mathbb{Z}$ s.t. $x^2 - xy + y^2 = p$. (i.e. all primes $\equiv 1 (3)$ are represented).

$10 \equiv 1 (3)$, $10 = 5 \cdot 2$.

If Claim is true, then $19 = x^2 - xy + y^2$.

How to find x & y? $Q(3,5) \Rightarrow 19$ ✓,

$Q(2,5) \neq$ ✓.

Recall FLT: $a^{p-1} \equiv 1 \ (p)$.

If $a \not\equiv 0 (p)$, $a^{\frac{p-1}{3}} \in \mathbb{Z}$.

If $p \equiv 1 (3)$, then $a^{\frac{p-1}{3}}$ makes sense.

(Recall for $p \equiv 1 (4)$ & $x^2 + y^2$, looked at $a^{\frac{p-1}{4}}$...)

Set $z \equiv a^{\frac{p-1}{3}} (p)$. What is $z^3 \equiv 1 \ (p)$?

$\left(a^{\frac{p-1}{3}}\right)^3 \equiv a^{p-1} \equiv 1$

If we can find a s.t. $z = a^{\frac{p-1}{3}} \neq 1$, then $z \neq 1$ but $z^3 \equiv 1$.

How likely are we to find such an a?

$7^3 = 7^2 \cdot 7 \equiv -6 \equiv 1$

$7^2 = 49 \equiv 11 \equiv -8$.

Ex: $p = 19 \equiv 1 (3)$, $\frac{p-1}{3} = 6$. $2^6 = 2^4 \cdot 2^2 \equiv 4$. $\binom{6}{3} = 12 \equiv 7$.

a	1	2	3	4	5	6	7	8	9	...
$a^{\frac{p-1}{3}} = a^6$	1	7	7							

We've found $z = 7 \equiv 2^{\frac{19-1}{3}}$ with $z^3 \equiv 1 \ (19)$.

$3^6 = 3^4 \cdot 3^2 = 9 \cdot \underbrace{81}_{\underbrace{5 + 76}_{19 \cdot 4}} \equiv 9 \cdot 5 \equiv \underbrace{45}_{\underbrace{7 + 38}_{2 \cdot 19}} \equiv 7 \ (19)$.

Exercise 7: Fill out this table

a vs $a^{\frac{p-1}{3}}$ for $a = 1, \ldots, p-1$,

& $p = 19$, & $p = 31$