I will give you HW 5 soon.
Today I will give you a couple problems.

Goal for today: Given $d \in \mathbb{Z}$ with $\sqrt{d} \neq \mathbb{Z}$ (and hence $\sqrt{d} \notin \mathbb{Q}$) we want to classify/describe elements of the following set:

$$S_d = \{|x^2 - dy^2| : x, y \in \mathbb{Z}\}.$$

Remark: If $d < 0$ then absolute value is not necessary.

Prototype: $S_{-1} = \{x^2 + y^2 : x, y \in \mathbb{Z}\}$

Fermat's Christmas Theorem (1640):

$n \in S_{-1} \iff$ every prime $p \mid n$ such that $p = 3 \bmod 4$ occurs with even multiplicity.

Today we will prove the following more general result:

Let $d \in \{-2, \boxed{-1}, 1, 2, 3, 6, 7, 11, 19\}$.
Then for all integers $n \geq 1$,

$n \in S_d \iff$ every $p \mid n$ with $\left(\frac{d}{p}\right) = -1$ occurs with even multiplicity.

$n = |x^2 - dy^2|$

Warning: For d outside this set the problem is in principle solved, but it is very complicated!!!

"Number Theory is Hard"

Consider the ring

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$$

Since $\sqrt{d} \notin \mathbb{Q}$ we have

$$a + b\sqrt{a} = a' + b'\sqrt{d} \iff a = a' \ \& \ b = b'.$$

Define conjugation

$$(a + b\sqrt{d})^* = (a - b\sqrt{d})$$

and norm $N(a + b\sqrt{d}) = |(a + b\sqrt{d})(a - b\sqrt{d})|$

$$= |a^2 - b^2 d| \geq 0.$$

Last time we proved the following for all $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$:

- $(\alpha\beta)^* = \alpha^* \beta^*$ AMAZING!
- $N(\alpha\beta) = N(\alpha)N(\beta)$
- $N(\alpha) = 0 \iff \alpha = 0 \ (= 0 + 0\sqrt{d})$

Another Fact:

α is a unit $\iff N(\alpha) = 1$.

(i.e., $\exists\, \beta, \alpha\beta = 1$)

Proof: Suppose $\alpha\beta = 1$. Taking norms:

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

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

$$\Rightarrow \quad N(\alpha) = \pm 1 \qquad \boxed{N(\alpha) \geq 0}$$

$$N(\alpha) = +1 \ \checkmark$$

Conversely, suppose $N(\alpha) = 1$.

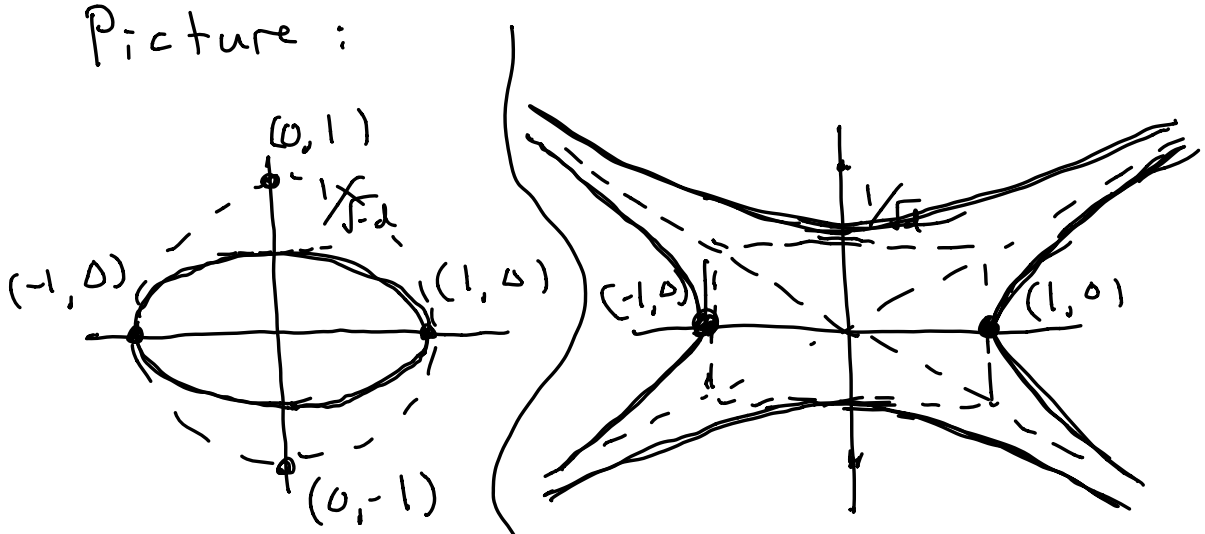
Then by definition, $\alpha\alpha^* = \pm 1$

hence $\alpha^{-1} = \pm\alpha^*$ exists. ///

If we view $x+y\sqrt{d}$ as a point (x,y) in the plane, then the units are the integer points on the ellipse/hyperbola defined by

$$|x^2 - dy^2| = 1$$

Picture:



$d<0$

$$\text{units} = \begin{cases} \pm 1 & d \le -2 \\ \pm 1, \pm i & d = -1 \end{cases}$$

$d>0$

Theorem: ∞ many units

"Pell's Equation" (next week)

What is special about the numbers

$$d = -2, -1, 1, 2, 3, 6, 7, 11, 19 \; ?$$

In these cases we say the ring $\mathbb{Z}[\sqrt{d}]$ is "norm Euclidean," meaning:

For all α, β $(\beta \neq 0)$ $\exists$ χ, ρ such that

$$\begin{cases} \alpha = \chi\beta + \rho \\ N(\rho) < N(\beta) \end{cases}$$

This means that Euclidean Algorithm also works in the ring $\mathbb{Z}[\sqrt{d}]$.

Bézout's Identity: (not "the")

Given α, β we say δ is a gcd

if • $\delta \mid \alpha$ & $\delta \mid \beta$

• $\varepsilon \mid \alpha$ & $\varepsilon \mid \beta \Rightarrow \varepsilon \mid \delta$.

If δ is a gcd of α, β then from Euclidean Alg. we can obtain some (non-unique) ω, ζ such that

$$\delta = \alpha w + \beta \zeta .$$

[Remark: GCD is defined up to units.
If $\delta \in \mathbb{Z}[\sqrt{-1}]$ is a gcd of α, β,
then there are 4 GCD's: $\pm\delta, \pm i\delta$.]

Jargon: Say α, β are coprime if
their GCD's are the units themselves.
Alternatively:

α, β coprime $\iff$ $\alpha x + \beta \zeta = 1$
for some x, ζ.

From this we also obtain

Euclid's Lemma:
Recall that $\pi \in \mathbb{Z}[\sqrt{d}]$ is called <u>prime</u>
if • π not a unit,
• $\pi = \alpha\beta \Rightarrow \alpha$ or β is a unit.

If $\alpha, \beta, \pi \in \mathbb{Z}[\sqrt{d}]$ with π prime, then

$$\pi \mid \alpha\beta \implies \pi \mid \alpha \text{ or } \pi \mid \beta.$$

Proof: Assume $\pi \mid \alpha\beta$ & $\pi \nmid \alpha$.

I claim α, π are coprime. Indeed,
if $\delta \mid \pi$ & $\delta \mid \alpha$ then

$\delta \mid \pi \Rightarrow \delta \sim 1$ or $\delta \sim \pi$

But since $\pi \nmid \alpha$ & $\delta \mid \alpha$ we
cannot have $\delta \sim \pi$. Hence $\delta \sim 1$.

Finally, from Bézout we have

$$\alpha \exists x + \pi \exists \zeta = 1$$

$$\alpha\beta x + \pi\beta\zeta = \beta$$

$$\pi(\alpha\beta)x + \pi\beta\zeta = \beta$$

$$\pi(\alpha\beta x + \beta\zeta) = \beta. \quad \checkmark$$

[From Euclid's Lemma we get
unique prime factorization in $\mathbb{Z}[\sqrt{d}]$.]

Okay. So let d be nice (as above).
Then we can prove the following Theorem.

Theorem: Let $d \in \{-1, -2, 1, 2, 3, 6, 7, 11, 19\}$ and $S_d = \{|x^2 - dy^2| : x, y \in \mathbb{Z}\}$.

(1) $n \in S_d \iff$ every $p \mid n$ with $p \notin S_d$ occurs with even mult.

(2) prime $p \in S_d \iff \left(\frac{d}{p}\right) = +1$

Proof: (1)

Suppose $n = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k} q_1^{2e_1} q_2^{2e_2} \cdots q_l^{2e_l}$

where p_i, q_i are primes,

$p_i \in S_d$

$q_i \notin S_d$.

Then I claim $n \in S_d$. Indeed,

note that $q_i^2 = |q_i^2 - d0^2| \in S_d$.

Then since S_d is closed under multiplication [$N(\alpha\beta) = N(\alpha)N(\beta)$.]

we conclude that

$n = p_1^{d_1} \cdots p_k^{d_k} (q_1^2)^{e_1} \cdots (q_l^2)^{e_l} \in S_d$ ✓

Conversely, suppose $n \in S_d$, i.e., suppose $n = |x^2 - dy^2|$ some x, y.

$$n = N(x + y\sqrt{d}).$$

Factor $x + y\sqrt{d}$ into primes in $\mathbb{Z}[\sqrt{d}]$:

$$x + y\sqrt{d} = \pi_1 \pi_2 \cdots \pi_h .$$

Taking norms gives

$$n = N(\pi_1) N(\pi_2) \cdots N(\pi_h).$$

For any prime $\pi \in \mathbb{Z}[\sqrt{d}]$ we will show that $N(\pi) = p$ or p^2 for some prime $p \in \mathbb{Z}$, from which the desired result follows.

Indeed, if $N(\pi) = p$ is prime then we're done. ✓

Otherwise, suppose $p \mid N(\pi)$

for some prime $p \in \mathbb{Z}$.

Then $p \mid |\pi\pi^*|$

$\Rightarrow p \mid \pi\pi^*$ (because d is nice)

$\overset{\text{Euclid}}{\Rightarrow} p \mid \pi$ or $p \mid \pi^*$

Say $p \mid \pi$. Then $\pi = \alpha p$, $\alpha \in \mathbb{Z}[\sqrt{d}]$.

Since π is prime in $\mathbb{Z}[\sqrt{d}]$, this means ~~p is a unit~~ or α is a unit.

Hence α is a unit and

$$N(\pi) = N(\alpha) N(p)$$
$$= 1 \cdot p^2 = p^2 \quad \checkmark$$

(2) Which primes $p \in \mathbb{Z}$ have the form $p = |x^2 - dy^2|$?

(i.e. $p \in S_d$.)

Claim: $p \in S_d \iff \left(\frac{d}{p}\right) = +1$.

If $p = |x^2 - dy^2|$ then I claim $p \nmid y$. Otherwise, say $y = py'$ then

$p \mid x^2 - dy^2 \implies p \mid x^2 \implies p \mid x$

Say $x = px'$. But then

$p = |(px')^2 - d(py')^2|$

$p = p^2 |x'^2 - dy'^2|$. Contradiction.

Hence we have $p = |x^2 - dy^2|$

$p \nmid y$. (y^{-1} exists mod p.)

$\implies x^2 - dy^2 \equiv 0 \mod p$

$x^2 \equiv dy^2$

$\left(\frac{x}{y}\right)^2 \equiv d \mod p$.

$\implies \left(\frac{d}{p}\right) = +1$.

Conversely, suppose $\left(\frac{d}{p}\right) = +1$

so $d \equiv m^2 \bmod p$, some $m \in \mathbb{Z}$.

Thus $p \mid (m^2 - d)$ in $\mathbb{Z}$

$p \mid (m+\sqrt{d})(m-\sqrt{d})$ in $\mathbb{Z}[\sqrt{d}]$.

We want to show that $p \in S_d$,
so suppose for contradiction that
$p \notin S_d$. Recall that this implies
p is <u>prime</u> in $\mathbb{Z}[\sqrt{d}]$.

Then since d is nice, Euclid's
Lemma says that

$\rightarrow$ $p \mid (m+\sqrt{d})$ or $p \mid (m-\sqrt{d})$

Hence $p(a+b\sqrt{d}) = m + \sqrt{d}$

$pa + pb\sqrt{d} = m + 1\sqrt{d}$ $(\sqrt{d} \notin \mathbb{Q})$

$\Rightarrow$ $pb = 1$. Contradiction.

QED.

What have we done? E.g.:

- $d=-1$ is nice.

$$p = x^2+y^2 \iff \left(\frac{-1}{p}\right) = +1$$

$$\iff p=2 \text{ or } p=1 \bmod 4.$$

- $d=-2$ is nice.

$$p = x^2+2y^2 \iff \left(\frac{-2}{p}\right) = +1$$

$$\overset{\text{HW4}}{\iff} p=2 \text{ or } p=1,3 \bmod 8$$

- $d=2$ is nice.

$$p = |x^2-2y^2| \iff \left(\frac{2}{p}\right) = +1$$

$$\iff p=2 \text{ or } p=1,7 \bmod 8.$$

- $d=3$ is nice.

$$p = |x^2-3y^2| \iff \left(\frac{3}{p}\right) = +1$$

$$\iff p=3 \text{ or } p=1,11 \bmod 12.$$

Of course, to complete these proofs one still needs to prove that these values of d are nice, i.e. that these $\mathbb{Z}[\sqrt{d}]$ are norm Euclidean.

You will prove $d=-1$ on HW5; but in general this is quite hard.

In fact, the main theorem of this lecture holds more broadly whenever $d \not\equiv 1 \bmod 4$ and $\mathbb{Z}[\sqrt{d}]$ has unique prime factorization.

It is an open problem to classify such nice d.

[HW5: $d=-5$ is not nice.]