4.1. 
Recall, interested in binary quadratic forms \( ax^2 + bxy + cy^2 \) right action of \( \text{SU}_2(\mathbb{Z}) \)

\[(f \circ g)(x, y) = f(g(x, y)).\]

So \((f \circ (\begin{pmatrix} a & b \\ c & d \end{pmatrix}))(x, y) = f(ax + by, cx + dy).\)

Remark. Sometimes you see a left action

\[(g \circ f)(x, y) = f((x, y)g).\]

Basically, but not exactly, the same.

Also saw that

\[\text{Disc}(f \circ g) = (\det g)^2 \text{ Disc } (f).\]

Proposition. (Cox, 2.3)

A form \( f \) properly represents an integer \( m \) if and only if it is properly equivalent to the form \( mx^2 + bxy + cy^2 \) for some \( b, c \in \mathbb{Z} \).

Proof. "If" is obvious, \( b/c \) equiv forms represent same integers

Take \( x = 1, y = 0 \).

So, suppose \( f(p, q) = m \) where \( p \) and \( q \) are coprime.

We choose \( s, r \) with \( ps - qr = 1 \). Then,

\[f(px + ry, qx + sy) = f(p, q) x^2 + (\text{Blah}) xy + f(r, s) y^2\]

and so we win!
4.2.

Corollary. (Cox, 2.5)

Let \( D \) be an integer \( \equiv 0, 1 \pmod{4} \). Then \( m \) is an odd integer coprime to \( D \). Then \( m \) is properly represented by a primitive form of discriminant \( D \) if and only if \( D \) is a quadratic residue \( \pmod{m} \).

Proof. If \( m \) is properly represented, can assume \( f(x, y) = mx^2 + bxy + cy^2 \).

So \( D = b^2 - 4mc \equiv b^2 \pmod{m} \).

Conversely, suppose \( D \equiv b^2 \pmod{m} \).

Because \( m \) is odd, can assume \( D \) and \( b \) have same parity. (Replace \( k \) with \( b + m \))

Because \( D \equiv 0, 1 \pmod{4} \), \( D \equiv b^2 \pmod{4m} \).

So, \( D = b^2 - 4mc \) for some \( c \).

\( mx^2 + bxy + cy^2 \) represents \( m \) properly and has discriminant \( D \).

Also, coeff. are coprime because \( (m, D) = 1 \).

Corollary. (Cox, 2.6)

Let \( n \) be an integer, \( p \) an odd prime. Then

\[
\left( \frac{-n}{p} \right) = 1 \quad \rightarrow \quad p \text{ is represented by some primitive form of discriminant } -4n.
\]

Fact. Any \( \mathcal{B} \& \mathcal{F} \) of disc \( -4 \) is equivalent to \( x^2 + y^2 \), (to be proved)

Cor. An odd prime \( p \) is a sum of two squares if and only if \( p \equiv 1 \pmod{4} \).

(!!!)
4.3.

Reduction theory of forms.

Def. A primitive pos. def. form $ax^2 + bxy + cy^2$ is reduced if

1. $|b| \leq a \leq c$,
2. $b \geq 0$ if either $|b| = a$ or $a = c$.

Thm. (Cox, 2.8) Every primitive positive definite form is properly equivalent to a unique reduced form.

Remarks.
1. The conditions for "reduced" define a fundamental domain for the action of $SL_2(\mathbb{Z})$ on binary quadratic forms.

Other examples: $kSL_2(\mathbb{Z})$ acting on $M = \{ z \in \mathbb{C} : \text{Im}(z) > 0 \}$ by $(a, b) \cdot z = \frac{az + b}{c + z}$.

Closely related.

* Binary cubic forms. Hard to describe.
* Manjul on counting quartic or quintic forms.

2. Will easily show $a \leq \sqrt{-D} / 3$.

Quickly conclude that if $D$ is fixed, only finitely many equivalence classes of discriminant $D$. And we can compute them.

3. Cool fact. $x^2 + x + 41$ is prime for $x = 0, 1, 2, 3, \ldots, 10$. Why?

4. Will use this to estimate # equiv classes with $|D| = x$.

5. $D > 0$ is harder. Will do it too.
Proof.

Step 1. Given a form, show prop. equiv to one with \( |b| \leq a \leq c \).

Among all forms in class, choose \( f = ax^2 + bxy + cy^2 \) with \( |b| \) minimized. Since positive definite, \( a, c \neq 0 \).

If \( a = |b| \), then

\[
g(x, y) = f(x + my, y) = ax^2 + b(2am + b)y + cy^2 = f(x, y).\]

If \( a < |b| \), choose \( m \) with \( |2am + b| < |b| \).

Contradiction!

If \( a = c \), swap \( x \) and \( y \):

\[
g(x, y) = f(-y, x).
\]

Get \( |b| \leq a \leq c \).

So: is reduced unless \( b < 0 \) and \( a = -b \) or \( a = c \).

\( a = -b \):

\[
ax^2 - axy + cy^2 \sim ax^2 + axy + (a + c)y^2
\]

(Cox is wrong?)

\( a = c \):

\[
ax^2 + bxy + ay^2 \sim ax^2 - bxy + ay^2
\]

by \( (x, y) \sim (-y, x) \).

So: shows existence, now show uniqueness.

(not in Granville)
Lemma. If \( f(x, y) = ax^2 + bxy + cy^2 \) satisfies \(|b| \leq a \leq c\),
then \( f(x, y) \geq (a - |b| + c) \min(x^2, y^2) \).

(Take for granted, or exercise)

So: If \( xy \neq 0 \), \( f(x, y) = a - |b| + c \).
And, by assumption, \( a \leq c \), so \( a \) is the minimum value
\( c \) is the next value
properly rep'd.

Now, to show uniqueness:
Assume \( f(x, y) = ax^2 + bxy + cy^2 \) sat.
\( |b| < a < c \).
Then \( a < c < a - |b| + c \) are the three smallest
numbers properly rep'd by \( f(x, y) \).

If \( g(x, y) \) is another reduced form equiv. to it:

1. First coeff \( a \) must be the same.
2. First last coeff \( c \) must be the same.
(Some technical details: Last coeff can't be \( a \).
see Cox.)
3. Same discriminant, so \( b \) must be the same
up to \( \pm \).

Now, why one \( f(x, y) = ax^2 + bxy + cy^2 \)
\( g(x, y) = ax^2 - bxy + cy^2 \) inequiv?
Let \( g(x, y) = f(x + \beta y, \delta x + \delta y) \)
\( a = g(1, 0) = f(1, 0) \)
\( c = g(0, 1) = f(\beta, 0) \)
By min. considerations,
\( (1, 0) = (0, 1) \)
\( (\beta, 0) = (0, 1) \)
So \( (\beta, 0) = (0, 1) \) of det. 1.
Finally: \( a = |b| \) or \( a = c \). Exercise...
\( \beta \) must be \( \pm 1 \).
Prop. If \( ax^2 + bx + cx^2 \) is reduced then \( 3a^2 \leq -D \), i.e. \( a \leq \sqrt{-D/3} \).

Proof. \( -D = 4ac - b^2 \)
\[ \geq 4a^2 - a^2 = 3a^2. \]

And \( |b| \leq a \).

This lets us enumerate classes of BQFs.
5.1. The class number.

From (4): Review def. of "reduced".
Main theorem.
Proof on 4.4.
Summarize 4.5.
Definitely do 4.6.

So do we have useful bounds on the coefficients?

$$|b| \leq \frac{8a}{3} \leq \sqrt{\frac{-D}{3}}.$$ 

Now, $c$ can be big. Indeed, $x^2 + \frac{(-D)}{4}y^2$ is reduced.

But we do have a bound:

$$4ac = -D + b^2 
\leq -D + a^2; \text{ so } c \leq \frac{-D}{4a} + \frac{a}{4}$$

$$\leq \frac{-D}{4} + \frac{1}{4} \sqrt{-\frac{D}{3}}.$$ 

Def. The class number $h(D)$ is the number of proper equivalence classes of IB&FS of discriminant $D$.

Theorem.

(1) $h(D) \neq 0 \iff D \equiv 0, 1 \pmod{4}$.

(2) For each negative $D$, $h(D)$ is finite and can be computed in $O(D)$ time.

(3) The IB&FS form a group. (Later)
5.2.

Proof. (2) follows from the fundamental domain and our bounds.

(1) \(b^2 - 4ac \equiv 0, 1 \pmod{4}\).

Conversely, if given \(D \equiv 0 \pmod{4}\), take

\[ x^2 - \frac{D}{4}y^2 \]

given \(D \equiv 1 \pmod{4}\), take

\[ x^2 + xy - \frac{D-1}{4}y^2 \]

Class number computations.

Ex. Compute \(h(-4)\).

Sol'n. Have \(1b|a| \leq a \leq \sqrt{\frac{4}{b}}\).

So: \(a = 1\), \(b = -1, 0, 1\).

(Note: \(-1\) because \(1b|a| = a\))

\[a = 1, b = 0 \Rightarrow 0^2 - 4c = -4 \Rightarrow c = 1.\]

\[a = 1, b = 1 \Rightarrow 1^2 - 4c = -4 \text{ (nope)}\]

So \(h(-4) = 1\).

We observe that \(h(D) \leq 10D\).

Why? Check \(a^2 \leq \sqrt{-\frac{D}{3}}\) and \(1b|a| \leq a\).

Then \(c\) is determined.

So, in fact,

\[h(D) \leq \left(\sqrt{-\frac{D}{3}}\right) \left(2\sqrt{-\frac{D}{3}} + 2\right)\]

\[= \frac{2}{3} \cdot 10D + \sqrt{\frac{10D}{3}}\]

which is less than \(10D\) except for \(D\) really small.
5.3.

Ex. Compute \( h(-23) \).

Have \( |b| \leq a \leq \sqrt{\frac{23}{3}} \) so \( a = 1 \) or \( 2 \).

\( a = 1 : \ b = 0 \) or \( 1 \).

\( b = 0 \Rightarrow -4c = -23 \) (no)

\( b = 1 \Rightarrow 1 - 4c = -23 \) (c = 6)

\( x^2 + xy + 6y^2 \)

\( a = 2 : \ b = -1, 0, 1, 1, 2 \)

\( b = -1 \Rightarrow 1 - 8c = -23 \), \( c = 3 \)

\( 2x^2 - xy + 3y^2 \)

\( b = 0 \Rightarrow -8c = -23 \) (no)

\( b = 1 \Rightarrow 1 - 8c = -23 \)

\( 2x^2 - xy + 3y^2 \)

\( b = 2 \Rightarrow 4 - 8c = -23 \) (no). So \( h(-23) = 3 \).

(Note: latter two are improperly equivalent)

Homework. Keep doing this until you get bored.

The \( D > 0 \) case.

Theorem. (Cox, 2.8) Any form of discriminant \( D > 0 \) is properly equivalent to \( ax^2 + bxy + cy^2 \) not a perfect square with

\( |b| \leq |a| \leq |c| \).

This implies \( |a| \leq \sqrt{\frac{D}{2}} \).

So still can compute class number.
6.1. Class numbers.

Review: Def. of reduced (4.3).

Bound on a (4.6).

Do computations on (5.2) and (5.3).

So now we understand how to compute.

Goals:

1. Understand this quantity for individual $D$ and on average. For example, it is true that

$$\sum_{n \leq N} h(-n) = \frac{\pi}{18 \sqrt{3}} N^{3/2} - \frac{3}{2 \pi^2} N + O\left(\frac{29}{44} + \varepsilon\right),$$

and

$$h(-n) = \frac{\sqrt{n}}{\pi} \cdot L\left(1, \chi_{-n}\right) \text{ for } n > 1.$$

We will investigate these.

2. The set of equivalence classes forms a group. Why??

(a) Ugly classical formulas — see Cox’s book.

(b) Correspondence to quadratic fields.

(c) Bhargava’s boxes.

3. Counting of representations.

$$r(n) = \# \text{ of inequivalent representations of } n.$$

$$r(n) = \sum_{m | n} \left(\frac{d}{m}\right).$$

Explain why it’s true, relate to $L(s, \chi_d)$ and Dedekind zeta fns. (Need for DCNF; then G0V)

4. Relation to $H$.

5. Why $n^2 + n + 41$ is prime so often.
6.2.
Relation to \( \mathcal{H} \) first.

If \( g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \), \( (f \circ g) \begin{pmatrix} u \\ v \end{pmatrix} = f \left( \gamma u + \delta v \right) \).

So, \( f \circ g \begin{pmatrix} u \\ v \end{pmatrix} = 0 \)
\[
\begin{pmatrix} \alpha \cdot u + \beta \cdot v \\ \gamma \cdot u + \delta \cdot v \end{pmatrix} = 0.
\]

i.e. \( [u: v] \) is a root of \( f \circ g \)
\[
\begin{pmatrix} \alpha \cdot u + \beta \cdot v \\ \gamma \cdot u + \delta \cdot v \end{pmatrix} = 0.
\]

Set \( v = 1 \) and think of BQFs as being determined by their roots. We definite real quadratic.

i.e. \( u + \Pi' \) is a root of \( f \circ g \)
\[
\begin{pmatrix} \gamma \cdot u + \delta \cdot v \\ \gamma \cdot u + \delta \cdot v \end{pmatrix} = 0.
\]

\( \mathbb{Q} \cdot u + \Pi' \) is a root of \( f \).

Definitions. \( \mathcal{H} = \{ z \in \mathbb{C} : \text{Im}(z) > 0 \} \).

\( \text{GL}_2(\mathbb{C}) \) acts on \( \mathcal{H} \cup \{0\} \) by \( \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \circ z = \frac{\alpha \cdot z + \beta}{\gamma \cdot z + \delta} \).

(Must check! Is a left (covariant) action.)

Prop. An \( \text{definite real} \) binary quadratic form has one of its roots in \( \mathcal{H} \cup \{0\} \).

Prop. If \( \Pi \) \( \text{f} \) has root \( z \in \Pi' \mathcal{C}(\mathbb{C}) \), then \( \Pi \) \( \text{can go back and forth} \).

\( (f \circ g) \) has root \( f^{-1}(z) \).

Prop. A fundamental domain for the action of \( \text{GL}_2(\mathbb{C}) \) on \( \mathcal{H} \) is:

This is equivalent to being reduced in Gauss's sense.
Indeed, the roots of \( ax^2 + bx + c \) are
\[
\frac{-b \pm \sqrt{D}}{2a}.
\]

We have \(|\text{Re}(z)| \leq \frac{1}{2} \iff |b| \leq a\).

What about \( |z| \geq 1?\)

\[
\left| \frac{-b \pm \sqrt{D}}{2a} \right|^2 = \frac{b^2 - D}{4a^2} = \frac{b^2 - (b^2 - 4ac)}{4a^2} = \frac{c}{a}.
\]

So \( |z| \geq 1 \iff a \leq c \).

So the conditions exactly correspond.

---

The \( n^2 + n + 41 \) is prime result.

**Theorem.** If \( D < 0 \), then \( h(D) = 1 \iff D \in \{ -3, -4, -7, -8, -11, -14, -43, -67, -163 \} \).

and also \(-12, -16, -27, -28\) if one counts non-fundamental discs.

**Proof.** Easy homework exercise. [Much, much, MUCH harder homework exercise. (Warning: Gauss, Heilbronn, Siegel, etc. couldn't do it)]

**Rabinowicz's Theorem.** Let \( A \geq 2 \) be an integer. Then \( n^2 + n + A \) is prime for \( 0 \leq n \leq A - 2 \) if and only if \( h(1 - dA) = 1 \).
7.1. Counting and representation theorems.

The general BQF is

\[ ax^2 + bxy + cy^2. \]

Two questions:

1. BQFs form a lattice. \((a, b, c)\)
   How many equiv classes are there with \(|D| < K|\)?
   (Gauss, Mertens, Siegel)

2. Pick \(a, b, c\) and plug in \(x, y\).
   How many \(D\) are represented by a fixed \(ax^2 + bxy + cy^2\) as \(x, y\) vary?

Use CON to answer both. (2) leads to a formula for \(h(D)\) (for \(D < 0\)).

(1) we can straight out do but is not so easy.

(2) — we need representation theorems.

Recall. Prop. (Cox 2.5) \(D \equiv 0, 1 \pmod{4}\), \(m\) odd integer.

Then \(m\) is properly rep'd by a form of disc \(D\)

\[ D \] is a quadratic residue \((\mod{4m})\).

Sketch of proof.

\(m\) properly rep'd by \(f\)

\(f\) equiv. to \(mx^2 + bxy + cy^2\) with \(D = b^2 - 4mc\)

\(D \equiv b^2 \pmod{4m}\).

Application. (Rebinovitch) Let \(A > 2\) integer. Then,

\(n^2 + n + A\) is prime for \(0 \leq n < A - 2\) iff

\(h(1 - 4A) = 1\).
Proof. Suppose $\omega(d) = 1$ with $d = 1 - 4A$.

Then $x^2 + xy + Ay^2$ only BQF of disc $d$, up to equivalence.

Suppose $m = n^2 + u + A$ composite for some $u \in [0, A - 2]$.

Then:
* $m$ has a prime factor $p \leq \sqrt{n^2 + u + A} < A$
* $d$ is a square mod $4m$, hence mod $4p$, and so $p$ is properly represented by a form of disc $d$, hence by $x^2 + xy + Ay^2$.

\[ 4p = 4u^2 + 4uv + 4Av^2 \]
\[ = (2u + v)^2 + (4A - 1)v^2 < 4A - 1 \]
(because $p < A$).

So $v = 0$, so $4p = 4u^2$... no. we lose.

Other way: See Granville's notes.

This is really nice.
Now. Beef up the representation theorem.

**Notation**

**Definition.** An integer $D$ is a **discriminant** if $D \equiv 0, 1 \pmod{4}$

$D$ is a **fundamental discriminant** if in addition
* $p^2 + D$ for any $p > 2$
* if $4 \mid D$ then $D \equiv 2, 3 \pmod{4}$. 


Prop. 12.31. If \( D \) is a fundamental discriminant then all forms of discriminant \( D \) are primitive.

Proof. Suppose the contrary,

Given a form \( (pa) x^2 + (pb) xy + (pc) y^2 \).

It has discriminant \( p^2(b^2 - 4ac) \).

Cannot have \( p > 2 \) by definition.

Moreover, \( p = 2 \) is impossible as \( b^2 - 4ac \equiv 0, 1 \pmod{4} \).

The converse is also true. If \( D \) is not fundamental, use the above to cook up an imprimitive form.

Ex. (uses alg. NT)

1. The fundamental discriminants are 0, 1 and the discriminants of quadratic fields.

2. (Better) (Bhargava, HCL I) (to be discussed!) The fundamental discriminants are precisely the discriminants of maximal quadratic rings.

If \( D \equiv 0 \pmod{4} \), associate \( \mathbb{Z}[x]/(x^2 - \frac{D}{4}) \).

If \( D \equiv 1 \pmod{4} \), associate \( \mathbb{Z}[x]/(x^2 + x + \frac{1 - D}{4}) \).

So for \( D = 1 \), get \( \mathbb{Z}[x]/(x^2 + x) \equiv \mathbb{Z} \oplus \mathbb{Z} \).

For \( D = 0 \), get \( \mathbb{Z}[x]/(x^2) \).

The "quadratic fields" are \( \mathbb{Q} \oplus \mathbb{Q} \) and \( \mathbb{Q}(x)/(x^2) \).
7.4. Automorphisms of quadratic forms.

**Definition.** An automorphism of a quadratic form is a change of variables (i.e., an elt. of $\mathrm{SL}_2(\mathbb{Z})$) mapping $f$ to itself.

**Ex.** Compute the automorphism group of $x^2 + y^2$.

**Sol'n.** Suppose $(x^2 + y^2) \circ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = x^2 + y^2$.

\[
(x^2 + y^2) \circ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = (\alpha x + \beta y)^2 + (\gamma x + \delta y)^2
\]

\[
= [\alpha^2 + \gamma^2] x^2 + [2\alpha \beta + 2\gamma \delta] xy
\]

\[
+ [\beta^2 + \delta^2] y^2.
\]

**Case 1.** $\alpha = \pm 1$.

Then $\gamma = 0$ and $\delta = \pm 1$, $\beta = 0$ by $(\alpha \beta \gamma \delta) \in \mathrm{SL}_2(\mathbb{Z})$.

So $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

**Case 2.** $\gamma = \pm 1$.

Then $\alpha = 0$, $\delta = 0$, $\beta = \pm 1$.

Get $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ or $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

So $|\text{Aut}(x^2 + y^2)| = 4$ and $\text{Aut}(x^2 + y^2) \cong \mathbb{Z}_4$.

**Note.** This group is naturally isomorphic to $\mathbb{Z}[i]$, $\{1, i, -1, -i\}$.

$(0, -1) \in \mathrm{SO}(2)$ is counter-clockwise rotation in $\mathbb{R}^2$ by $90^\circ$.

$\mathbb{R}^2 \cong \mathbb{C}$ as real vector spaces.

This rotation is multiplication by $i$. 
Automorphisms of quadratic forms.

Review def., result of computation on 7.4.
Prop. If two quadratic forms are equivalent then their automorphism groups are isomorphic and indeed conjugate in $\text{SL}_2(\mathbb{Z})$.

Proof. If $f' = f \circ g$, then

$$h \in \text{Aut}(f') \implies f' \circ h = f' \circ f \circ g \circ h = f \circ g \circ h = f \circ g \circ g^{-1} = f \implies ghg^{-1} \in \text{Aut}(f).$$

So, $\text{Aut}(f') = g \cdot \text{Aut}(f) \cdot g^{-1}$.

(Also note, $(ghg^{-1})(gh'g^{-1}) = ghg^{-1}$ so RHS is a group isomorphic to $\text{Aut}(f')$.)

Remark: This principle is extremely familiar, master it!

Prop. If $f$ is a primitive quadratic form of disc $D < 0$, then

$$|\text{Aut}(f)| = \begin{cases} 4 & \text{if } D = -4 \ (\text{proved above}) \\ 2 & \text{if } D = -3 \ (\text{homework!!}) \\ 2 & \text{if } D = -4. \end{cases}$$

Isomorphic to the unit group of the ring of integers of $\mathbb{Q}(\sqrt{D})$.

If $D > 0$ then $\text{Aut}(f)$ is infinite.

Example: Look at $x^2 - 2y^2$ of discriminant $\delta$.

Ex. (1. easy) Verify that $\begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix} \in \text{Aut}(f)$ and is of infinite order.

Hints. $x^2 - 2y^2 = (x - \sqrt{2}y)(x + \sqrt{2}y)$ and $(\sqrt{2} - 1)(\sqrt{2} + 1) = 1$.
The representation theorem.

Let \( r_D(n) := \# \) representations of \( n \) by all \( \mathbb{Q} \) of disc \( D \), up to equivalence.

Proved before: \( r_D(n) > 0 \quad \Rightarrow \quad n \equiv D \mod 4 \).

**Theorem.** \( r_D(n) = \sum_{m | n} \left( \frac{D}{m} \right) \).

**Note.** We only defined \( \left( \frac{D}{m} \right) \) for odd prime \( m \).

Define \( \left( \frac{D}{2} \right) = \begin{cases} 0 & \text{if } D \text{ is even} \\ 1 & \text{if } D \equiv 1 \mod 8 \\ -1 & \text{if } D \equiv 3, 5 \mod 8 \end{cases} \)

(2 ram in \( \mathbb{Q}(\sqrt{D}) \))

(2 splits in \( \mathbb{Q}(\sqrt{D}) \))

(2 inert in \( \mathbb{Q}(\sqrt{D}) \))

and \( \left( \frac{D}{m \cdot m'} \right) = \left( \frac{D}{m} \right) \left( \frac{D}{m'} \right) \) for all \( m, m' \).

This defines \( \left( \frac{D}{m} \right) \) for all positive integers \( m \), and is periodic in the top.

**Analytic number theory lemma.**

\[
\sum_{m | n} \left( \frac{D}{m} \right) = \prod_{p | n} \left( 1 + \left( \frac{D}{p} \right) + \left( \frac{D}{p^2} \right) + \cdots + \left( \frac{D}{p^e} \right) \right).
\]

**Proof.** Follow the right side!

**Example.** Suppose \( n \) is coprime to \( D \) and squarefree.

Then, \( r_D(n) = \prod_{p | n} \left( 1 + \left( \frac{D}{p} \right) \right) = 2^{ω(n)} \) \( ω(n) \) *dist prime factors:

\[
= \begin{cases} 2 & \text{if } D \text{ is a residue mod } p, \\ 0 & \text{otherwise} \end{cases}
\]
8.4. Example. Let \( D = -4 \).

Then \( r_{-4}(1) = 1 \). \((1^2 + 0^2, 1^2 + 0^2, 0^2 + 1^2, 0^2 + (-1)^2)\)
\( r_{-4}(5) = 2 \). \((1^2 + 2^2, 1^2 + 2^2)\)
\((1^2 + 2^2, 2^2 + 2^2)\), (backwards).
\( r_{-4}(2) = 1 \). (Note: \((-\frac{4}{2}) = 0\).)

Recall that because \( |\text{Aut}(x^2 + y^2)| = 4 \), there are 4 equivalent relations for each.

Example. \( D = -15 \).

\[ \frac{x^2 + y^2}{2} 4 \quad \frac{x^2 + xy + 4y^2}{2} \quad \frac{2x^2 + xy + 2y^2}{2} \]

\( \left(\frac{-15}{13} \right) = 1 \), so \( r_{-15}(13) = 2 \). \#1: \( x = 1, y = -3 \)
\( x = -1, y = 3 \)
\( x = -3, y = 1 \)
\( x = 3, y = -1 \).
These are two equivalent classes.

Similarly, \( \left(\frac{-15}{19} \right) = 3 \), so \( r_{-15}(19) = 2 \). rep'd by first form only.

Two ways to prove this.
1. Correspondence to ideals.
2. Work with binary quadratic forms directly.

Proofs of (2).
A bit messy. See Cox, ex. 2.20.
For \( 4 \nmid D \), and \( n \) odd. (Warning: Cox uses different letters).

(a) The number of solutions to \( x^2 \equiv D \pmod{n} \)
is \( \prod_{p \mid n} \left(1 + \left(\frac{D}{p}\right)\right) \).
9.1. Dirichlet’s class number formula.
Suppose \( d \) is fundamental.

**Theorem.** Let \( L(1, \chi_d) := \sum_{n} \left( \frac{d}{n} \right) \cdot \frac{1}{n} \).

Then, \( h(d) = \frac{w}{2\pi} \cdot |d|^{1/2} \cdot L(1, \chi_d) \),

where \( w = \begin{cases} 
2 & \text{if } d < -4 \\
1 & \text{if } d = -4 \\
6 & \text{if } d = -3 
\end{cases} \).

**Examples.**

\[ d = -4: \]
\[ h(-4) = \frac{4}{2\pi} \cdot \sqrt{4} \cdot \left( 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots \right) \]
\[ = \frac{4 \cdot 2}{2\pi} \cdot \frac{\pi}{4} = 1. \]

\[ h(-3) = \frac{6}{2\pi} \cdot \sqrt{3} \left( 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \frac{1}{7} - \frac{1}{8} \ldots \right) \]
\[ = \frac{6 \sqrt{3}}{\pi} \cdot \frac{\pi}{3 \sqrt{3}} = 1. \]

\[ h(-23) = \frac{2}{2\pi} \cdot \sqrt{23} \left( 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} - \frac{1}{5} + \frac{1}{6} - \frac{1}{7} + \ldots \right) \]
\[ = \frac{\sqrt{23}}{\pi} \left( \frac{3\pi}{\sqrt{23}} \right). \]

**Consequences.**

1. Since \( \left( \frac{d}{n} \right) \) is equally likely to be 0 or 1, expect \( h(d) = \frac{\sqrt{|d|}}{\pi} \) on average.
9.2. Question: What is $\sum_{-d < x} h(d)$ asymptotically?

$$\sum_{-d < x} \frac{\sqrt{|d|}}{\pi} \sim \frac{3}{\pi^2} \int_{0}^{x} \frac{1}{\pi t^{1/2}} dt = \frac{2}{\pi^2} x^{3/2}.$$ 

This is not correct.

We also have

$$\sum_{-d < x} h(-d) = \# \{ (a, b, c) : b^2 - 4ac \in [-x, 0], \text{satisfy inequalities for being reduced, b}^2 - 4ac \text{ is fundamental} \}.$$ 

(2) $L(1, Xd)$ is easy to bound from above, so we can prove $h(d) < \sqrt{|d|} \log |d|$.

(Will prove this directly.)

(3) $L(1, Xd) \neq 0$.

This proves, e.g. half of primes are $\equiv 1 \pmod{4}$.

half one $\equiv 3 \pmod{4}$.

Note: A similar formula holds for $d > 0$ also. It is harder because there is a harder GON problem to solve. We will do this in detail.

Hinges on the theorem that

\[ r_D(n) = \sum_{m|n} \left( \frac{D}{m} \right) \]

Lemma. We have [explain "\( \prod p^{e_p} \ln n \)]

\[ \sum_{m|n} \left( \frac{D}{m} \right) = \prod_{p|n} \left( 1 + \left( \frac{D}{p} \right) \right) + \left( \frac{D}{p^2} \right) + \ldots + \left( \frac{D}{p^{e_p}} \right) \]

Proof. Foil the right side.

In particular, if \( n \) is coprime to \( D \) and squarefree,

\[ r_D(n) = \prod_{p|n} \left( 1 + \left( \frac{D}{p} \right) \right) = \begin{cases} 2^{\omega(n)} \text{ if } D \text{ is a residue } \mod n \\ 0 \text{ if } \text{D is not a residue } \mod n \end{cases} \]

\( \omega(n) \): # of distinct prime divisors
Prop. If \( d < 0 \) then

\[
h(d) \ll |d| \log |d|.
\]

Proof. The key identity is that, for a fixed form \( f = ax^2 + bxy + cy^2 \),

\[
\sum_{\substack{n \leq N \atop 0 \leq f(x,y) \leq N}} \frac{1}{w} = \frac{1}{w} \sum_{x,y \in \mathbb{Z}} \frac{1}{w} \quad \sum_{0 < f(x,y) \leq N}
\]

where \( w = \begin{cases} 2 & \text{if } \text{Disc}(f) < -4 \\ 4 & \text{if } \text{Disc}(f) = -4 \\ 6 & \text{if } \text{Disc}(f) = -3 \end{cases} \).

This is obvious. The proof is by staring at it.

That said, \( w \) gives the number of equivalent representations by \( f \), so you do need to prove that if \( g \) is a nontrivial automorphism of \( f \), then \( g \left[ \begin{array} { c } { x } \\ y \end{array} \right] \neq \left[ \begin{array} { c } { x } \\ y \end{array} \right] \) for \( \left[ \begin{array} { c } { x } \\ y \end{array} \right] \neq \left[ \begin{array} { c } { 0 } \\ 0 \end{array} \right] \).

For \( \text{Disc}(f) < -4 \), \( \text{Aut}(f) \cong \{ (1,0), (-1,0) \} \).

For \( \text{Disc}(f) = -4, -3 \), it's obvious.

For \( \text{Disc}(f) = -4, -3 \), just check it.

Prop. If \( f \) is positive definite, then

\[
\sum_{x,y \in \mathbb{Z} \atop 0 \leq f(x,y) \leq N} 1 = \frac{2\pi N}{|1d|} + o(\sqrt{N}).
\]

Now why is this interesting?

\[
\sum_{\text{disc } D \leq N} \sum_{f \in \text{disc } D} f(n) = h(D) \left( \frac{2\pi N}{|1d|} + o(\sqrt{N}) \right).
\]
Therefore, for any $N$,

$$\sum_{n \leq N} r_D(n) = \sum_{n \in \mathbb{N}} \sum_{f \text{ f of disc } D} r_f(n) = h(D) \left( \frac{2\pi N}{\sqrt{|D|}} + o(\sqrt{N}) \right).$$

Simultaneously,

$$\sum_{n \leq N} r_D(n) = \sum_{n \leq N} \sum_{m|n} \left( \frac{D}{m} \right) = \sum_{m \leq N} \left( \frac{D}{m} \right) \sum_{n \leq N} \frac{1}{m|n}$$

 cheating!!!! come back and fix

$$= \sum_{m \leq N} \left( \frac{D}{m} \right) \left\lfloor \frac{N}{m} \right\rfloor$$

$$= \sum_{m \leq N} \left( \frac{D}{m} \right) \frac{N}{m}$$

$$= N \cdot \sum_{m \leq N} \left( \frac{D}{m} \right) \cdot \frac{1}{m}.$$

Now, because $\sum_{m} \left( \frac{D}{m} \right) \cdot \frac{1}{m}$ is convergent, this is

$$N \cdot \left( L(1+D) + o(1) \right).$$

So,

$$N \left( L(1+D) + o(1) \right) = \frac{2\pi N}{\sqrt{|D|}} + o(\sqrt{N})$$

$$= N \left( \frac{2\pi h(D)}{\sqrt{|D|}} + o(1) \right).$$

So,

$$L(1+D) = \frac{2\pi h(D)}{\sqrt{|D|}}.$$
4.6. Being more careful:

For any $A$ and $B$ we have $|\sum_{A \leq m \leq B} (\frac{D}{m})| \leq 1D$.

So, for any $k$,

$$\sum_{m \leq N} \left( \frac{D}{m} \right) \left\lfloor \frac{N}{m} \right\rfloor = \sum_{m \leq \frac{N}{K}} \left( \frac{D}{m} \right) \left\lfloor \frac{N}{m} \right\rfloor + \sum_{\frac{N}{K} < m \leq N} \left( \frac{D}{m} \right) \left\lfloor \frac{N}{m} \right\rfloor$$

$$= \sum_{m \leq \frac{N}{K}} \left( \frac{D}{m} \right) \cdot \frac{1}{m} + O\left( \frac{N}{K} \right) + \sum_{r=1}^{K} \sum_{\frac{N}{K} < m \leq \frac{N}{r}} \left( \frac{D}{m} \right)$$

$$= \sum_{m \leq \frac{N}{K}} \left( \frac{D}{m} \right) \cdot \frac{1}{m} + O\left( \frac{N}{K} \right) + O\left( K|1D| \right)$$

Choose $K = \sqrt{N/|1D|}$, get

$$\sum_{m \leq N} \left( \frac{D}{m} \right) \left\lfloor \frac{N}{m} \right\rfloor = \sum_{m \leq \frac{N}{K}} \left( \frac{D}{m} \right) \cdot \frac{1}{m} + O\left( \sqrt{N|1D|} \right)$$

This is much better.

This is still $N \cdot (L(1, X_0) + o(1))$. 
10.1. Real quadratic forms

We are now interested in indefinite quadratic forms
\[ ax^2 + bxy + cy^2, \quad D > 0. \]

Fact. If \( D > 0 \) it is indefinite and has two real roots \([x : y]\).
(Do it by pure thought!)

Gauss. Any such form is equivalent to a reduced form satisfying
\[ 0 < \sqrt{D} - b < 2|a| < \sqrt{D} + b. \]

[A. What word is missing?]

Cor. If \( D > 0 \) then \( h(D) \) is finite.

Proof. We have \( b < \sqrt{D} \), and \( |a| < 2\sqrt{D} \).
\( c \) is determined by \( a \) and \( b \).

So \( h(D) < (\sqrt{D} + 1)(4\sqrt{D} + 1) \ll D \).

Consider the roots \( p_1 = \frac{-b + \sqrt{D}}{2a}, \quad p_2 = \frac{-b - \sqrt{D}}{2a} \).

One is between 0 and 1 and the other is less than -1.

Reduction theory.

Def. \( ax^2 + bxy + cy^2 \), \( cx^2 + b'xy + c'y^2 \) are neighbors if they have the same discriminant and \( b \equiv -b' \pmod{2c} \).

In this case, \( cx^2 + b'xy + c'y^2 = (ax^2 + bxy + cy^2) \begin{bmatrix} 0 & -1 \\ 1 & \frac{b + b'}{2c} \end{bmatrix} \).
10.2.

So, given $ax^2 + bxy + cy^2$.

Let $b'_0$ be the least residue in absolute value of $-b \pmod{2c}$ with $|b'_0| \leq c$.

- If $|b'_0| > \sqrt{D}$ then let $b' = b'_0$.
  
  We have $0 < (b')^2 - D \leq c^2 - D$.
  
  So $|c'| = \frac{(b')^2 - D}{4|c|} < \frac{|c|}{4}$ . (Decreased $|c|$)

- If $|b'_0| \leq \sqrt{D}$, choose $b' \equiv -b \pmod{2c}$ so $b'$ as large as possible s.t. $|b'| < \sqrt{D}$.
  
  We have $-D = (b')^2 - D = 4c c' < 0$.
  
  If $2|c| > \sqrt{D}$ then $|c'| \leq \frac{|D|}{4c} < |c|$. 

In case we hit one of the cases, $2|c| \leq \sqrt{D}$:

$\sqrt{D} = 2|c|$ and $\sqrt{D} - 2|c| \leq |b'| < \sqrt{D}$.

So: $0 < \sqrt{D} - |b'| \leq 2|c| < \sqrt{D} + |b'|$.

Idea: Keep reducing $a$ and $c$ until we got suit reduced.

Note: Don't have uniqueness, get a cycle (see Grenville).
10.3. The automorphs.

Def. Pell's equation is $v^2 - Dw^2 = \pm 4$.

Note: if $D$ is even, so is $v$, can rewrite
$$(\frac{v}{2})^2 - (\frac{D}{4})w^2 = \pm 1.$$

Example. Let $D = 8$. $v^2 - 8w^2 = \pm 4$.

A solution is $v = 2, w = 1$.

Rewrite this as $(v')^2 - 2w^2 = \pm 1$ with $v' = \frac{v}{2}$,

$$[v' - \sqrt{2}w][v' + \sqrt{2}w] = \pm 1.$$

$(1 - \sqrt{2})(1 + \sqrt{2}) = 1$,
and $(1 - \sqrt{2})^k(1 + \sqrt{2})^k = 1$ for any $k$.

Thus, Pell's equation has a solution in $\mathbb{Z}$.

Cor. It has infinitely many.

Case 1. $4 | D$. As above. $(v')^2 - \frac{D}{4}w^2 = \pm 1$

$$(v' - \frac{\sqrt{D}}{2}w)(v' + \frac{\sqrt{D}}{2}w)$$

Take kth powers to get infinitely many solutions.

Case 2. $4 \nmid D$. Write $(v')^2 - D(w')^2 = \pm 1$ with

$v' = \frac{v}{2}, w' = \frac{w}{2}$

both half integers.

Either both or neither are in $\mathbb{Z}$.

If integers, do as above.

If half,

$$(v' + \sqrt{D}w')^2 = [v'^2 + Dw'^2] + \sqrt{D} \cdot 2v'w'.$$

Check: Because $D \equiv 1 \mod 4$, both of above are half integers.

(Not $\frac{1}{4}$-integers).
10.4. Exercise. The automorphisms of a form are all given by
\[ \begin{bmatrix} \frac{1}{2}(u-vu) & -cu \\ au & \frac{1}{2}(u+vu) \end{bmatrix} \]
with \( u^2 - au^2 = +q \). \((-q\) gives \( \det = -1 \).)

Simple exercise. Check that this gives an automorphism, and that squaring this matrix preserves this property.

Better exercise. Factor \( ax^2 + bxy + cy^2 = a(x - \Theta y)(x - \Theta' y) \),
\[ \Theta = \frac{-b + \sqrt{D}}{2a}, \]
and check that our automorphism corresponds to
\[ x' - \Theta y' = \frac{1}{2}(u \sqrt{D})(x' - \Theta' y) \]
\[ x' + \Theta y' = \frac{1}{2}(+u \sqrt{D})(x' + \Theta' y). \]

Definitions.
The fundamental unit \( \epsilon_B := \frac{u_0 + \sqrt{D}}{2} \) is the minimal such expression which is \( > 1 \) and of norm \( \pm 1 \).

Here the norm is \( \epsilon_B \cdot \epsilon_B = \frac{u_0^2 - Dw_0^2}{4} \).

So corresponds to Pell’s equation.

Prop. All solutions are \( \pm \epsilon_B \).

Def. Let \( \epsilon_B^+ \) be the smallest unit \( > 1 \) with norm 1.

So, \( \epsilon_B^+ = \epsilon_B \) or \( \epsilon_B^2 \), depending on whether \( N(\epsilon_B) = 1 \) or \(-1\).
Consider the expression \( \left| \frac{x - \Theta y}{x - \Theta'y} \right| \) for given \( x \) and \( y \).

If we change variables, \( \begin{bmatrix} x' \\ y' \end{bmatrix} = g \cdot \begin{bmatrix} x \\ y \end{bmatrix} \), then

\[
\left| \frac{x' - \Theta y'}{y' - \Theta'y} \right| = \left| \frac{(\xi_D)^k (x - \Theta y)}{(\xi_D)^{-k} (x - \Theta y)} \right| = (\xi_D)^k \cdot \left| \frac{x - \Theta y}{y' - \Theta'y} \right|
\]

Therefore, there is a unique \( k \) for which this quantity is between 1 and \((\xi_D)^2\).

Choose where \( x - \Theta y > 0 \) (by replacing \( x, y \) with \( -x, -y \) if nec.)

So: We want to count \( \sum_{n \in \mathbb{N}} r_D(n) \).

This is still equal to \( N \cdot (L(1, \xi_D) + o(1)) \) for the same reason as before.

So we need to count, for each fixed value \( \xi \), how many integer points \((x, y)\) there are with:

\( 0 < ax^2 + bxy + cy^2 \leq N, \)

\( x - \Theta y > 0, \)

\( \left| \frac{x - \Theta y}{x - \Theta'y} \right| \in \left[ 1, (\xi_D)^2 \right). \)

Counting lattice points in a hyperbola.
E1.1.

Def. A quadratic field is

\[ \mathbb{Q}(\sqrt{d}) = \{ a + b \sqrt{d} : a, b \in \mathbb{Q} \} . \]

Its ring of integers is

\[ \mathcal{O} = \left\{ \frac{a + b \sqrt{d}}{2} : a, b \in \mathbb{Z}, a \text{ and } b \text{ have the same parity} \right\} \]

if \( d \equiv 2, 3 \pmod{4} \)

\[ \mathcal{O} = \left\{ x \in \mathbb{Q}(\sqrt{d}) : x \text{ satisfies a monic poly. with coefficients in } \mathbb{Z} \right\} \]

is maximal f.g. subring of \( \mathbb{Q}(\sqrt{d}) \).

Its discriminant is \( \text{disc}(\mathcal{O}) = \text{det} \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix} = 4d \)

or \( \text{det} \begin{vmatrix} \frac{1 + \sqrt{d}}{2} \\ \frac{1 - \sqrt{d}}{2} \end{vmatrix} = \sqrt{d} \)

for squarefree \( d \).

So \( \text{Disc}(\mathcal{O}) = \text{Disc}(\mathbb{Q}(\sqrt{d})) = \begin{cases} d & \text{if } d \equiv 1 \pmod{4} \\ 4d & \text{if } d \equiv 2, 3 \pmod{4} \end{cases} \)

Prop. The set of quadratic fields is in bijection with the set of fundamental discriminants, other than 1.

Notation. Let \( K \) be a \( \mathbb{Q} \)- and \( \mathcal{O} \) its ring of integers.

Thm. \( \mathcal{O} \) admits unique factorization of ideals into prime ideals.

If \( p \) is a prime of \( \mathcal{O} \), then \( p \mathcal{O}_K \) is:

- prime in \( \mathcal{O} \) (inert)
- \( p \mathcal{O}_K \) in \( \mathcal{O} \) (split)
- or \( p^2 \) in \( \mathcal{O} \) (ramified)
Def. A fractional ideal of $\mathcal{O}$ is an $\mathcal{O}$-submodule of $K$.

It is principal if it is $x \cdot \mathcal{O}$ for some $x \in K$.

Both are groups under multiplication, $I(K)$ and $P(K)$.

Def. The class group $\text{Cl}(K) = I(K) / P(K)$.

Units. Let $\mathcal{O}^\times$ be the group of units.

Then $|\mathcal{O}^\times| = \begin{cases} 6 & \text{if } K = \mathbb{Q}(\sqrt{-3}) \\ 4 & \text{if } K = \mathbb{Q}(\sqrt{-4}) \\ 2 & \text{if } K = \mathbb{Q}(\sqrt{-D}), \, D \leq 0 \\ \infty & \text{if } D > 0 \end{cases}$.

Theorem. If $K$ is a (the) quadratic field of discriminant $D$, then

$$\text{Cl}(K) \cong \text{Cl}(D).$$

Proof. (Sketch. See Cox, 5.30, 7.7)

Construct a map

$$\text{BQFs} \rightarrow \text{Ideals of } \mathcal{O} :$$

$$ax^2 + bxy + cy^2 \rightarrow \left[ a, \frac{-b + \sqrt{D}}{2} \right]$$

$$= a \cdot \left[ 1, \frac{-b + \sqrt{D}}{2a} \right].$$

In other words:

$$a(x + \theta y)(x + \theta' y) \rightarrow a \left[ 1, \theta \right].$$
Now, let \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) act on \( ax^2 + bxy + cy^2 \).

Get
\[
\begin{align*}
&= a \left( [q + x \theta] y + [p + y \theta] y \right) \cdot \text{conj}
\end{align*}
\]
\[
= a \left( [q + x \theta] y + \frac{p + y \theta}{q + y \theta} y \right) \cdot \text{conj}
\]
\[
= a \cdot \left( q + x \theta \right) \left( 1, \frac{p + y \theta}{q + y \theta} \right)
\]
\[
= a \left[ \begin{array}{c} q + x \theta \\ \frac{p + y \theta}{q + y \theta} \end{array} \right].
\]

So maps to
\[
\begin{align*}
&= a \cdot \left( q + y \theta, \frac{p + y \theta}{q + y \theta} \right) \cdot \text{conj}
\end{align*}
\]
\[
= a \cdot \left[ 1, \theta \right] \left[ \begin{array}{c} q \\ \frac{p + y \theta}{q + y \theta} \end{array} \right].
\]

We wrote an ideal of \( O \) in terms of its \( \mathcal{L} \)-basis which we simply permuted.

So it's well defined.

You can go backwards too, so injective.

Why is it surjective? Given \( \left[ \begin{array}{c} q \\ p \end{array} \right] \) for some \( q, p \in K \).

WLOG \( \tau := \frac{p}{q} \) is in \( \mathcal{H} \).

Then \( \left[ \begin{array}{c} q \\ p \end{array} \right] \sim \left[ \begin{array}{c} 1 \\ \tau \end{array} \right] \) in \( \text{Cl}(K) \).

Let \( ax^2 + bxy + cy^2 \) be any polynomial of \( \tau \).

Check: This maps to it.
E1.4. **Corollary.** \( \text{Cl}(D) \) is a group.

As Dirichlet discovered, if

\[
\begin{align*}
    f(x, y) &= ax^2 + bxy + cy^2 \\
    g(x, y) &= a'x^2 + b'xy + c'y^2
\end{align*}
\]

with \( \gcd(a, a', b + b') = 1 \)

both of disc \( D \), then their composition is

\[
    aa'x^2 + Bxy + \frac{B^2 - D}{4aa'} y^2
\]

where \( B \) is the unique integer \( \pmod{2aa'} \) with

\[
\begin{align*}
    B &= b \pmod{2a} \\
    B &= b' \pmod{2a'} \\
    B^2 &\equiv D \pmod{4aa'}
\end{align*}
\]

**Proof.** Multiply ideals!

**Claim.** If \( f \) is a form of disc \( D \), then

\[
    \mathfrak{A} \mathfrak{A}^t(f) \mathfrak{A} \cong \mathcal{O}^x.
\]

**Proof.** Let \( \frac{u + \sqrt{d}}{2} \) be a unit, with \( \left( \frac{u + \sqrt{d}}{2} \right) \left( \frac{u - \sqrt{d}}{2} \right) = 1 \).

\[
\begin{align*}
    ax^2 + bxy + cy^2 &\cong (x + \Theta y) (x + \Theta' y) \\
    &\cong \left( \frac{u + \sqrt{d}}{2} \right) (x + \Theta y) \left( \frac{u - \sqrt{d}}{2} \right) (x + \Theta' y) \\
    &\text{Foil.}
\end{align*}
\]

Get a change of variables.
1.5. The zeta function.

Def. If $a$ is an (integral) ideal then $N(a) = [\theta : a]$. If $a = (a)$ then $N(a) = N(a)$.

Def. If $\mathcal{O}$ is the ring of integers of (any) number field $K$ then its Dedekind zeta function is

$$\zeta_K(s) = \sum_{a \subseteq \mathcal{O}} (Na)^{-s} = \prod_{P} \left( 1 + (NP)^{-s} + (NP)^{-2s} + \ldots \right)^{-1}$$

Ex. If $K = \mathbb{Q}$ then $\zeta_K(s) = \zeta(s)$.

Ex. $\mathbb{Z}[i]$ is a PID, with unit group $\mathbb{Z}$ so

$$\zeta_{\mathbb{Z}[i]}(s) = \frac{1}{4} \sum_{(a,b) \neq (0,0)} (a^2 + b^2)^{-s}.$$ 

Prop. For any number field $K$ we have

$$\zeta_K(s) = \zeta(s) \cdot L(s, \chi_D).$$

Proof. For each prime $p$, RHS is:

- $(1 - p^{-s})^{-2}$ if $p$ splits
- $(\frac{D}{p}) = 1$.
- $(1 - p^{-s})^{-1}$ if $p$ ramified
- $(1 - p^{-s})^{-1}$ if inert.

Implies: # of ideals of norm $n$ is

$$\sum_{d | n} 1 \cdot (\frac{D}{e}) = \sum_{e | n} (\frac{D}{e}),$$

i.e. # of inequivalent representations.

We recognize this now!