4.1.

Recall. Interested in binary quadratic forms $ax^2 + bxy + cy^2$

right action of $SL_2(\mathbb{Z})$

$$(f \circ g)\begin{pmatrix} x \\ y \end{pmatrix} = f\left(g\begin{pmatrix} x \\ y \end{pmatrix}\right).$$

$$\text{So } \left(f \circ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right)(x,y) = f(\alpha x + \beta y, \gamma x + \delta y).$$

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

$$\mathrm{Disc}(f \circ g) = (\det g)^2 \, \mathrm{Disc}(f).$$

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. Then, we choose s, r with $ps - qr = 1$.

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

and so we win!

4.2.

Corollary. (Cox, 2.5)

Let D be an integer $\equiv 0, 1 \pmod 4$

m 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 (mod m).

Proof. If m is prop. rep'd, 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 ~~b~~ 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, coeffs are coprime because $(m, D) = 1$.

Corollary. (Cox, 2.6)

Let n be an integer, p an odd prime. Then

$\left(\frac{-n}{p}\right) = 1 \longleftrightarrow p$ is represented by some primitive form of discriminant $-4n$.

Fact. Any BQF 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 $ax^2 + bxy + cy^2$ (which must have $a, c > 0$) is *reduced* if

(1) $|b| \le a \le c$,

(2) $b \ge 0$ 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: * $SL_2(\mathbb{Z})$ acting on $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ by $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} z = \dfrac{\alpha z + \beta}{\gamma z + \delta}$.

Closely related.

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

(2) Will easily show $a \le \sqrt{-D/3}$.
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.

4.4.

Proof.

Step 1. Given a form, show prop. equiv to one with $|b| \le a \le c$.

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

If $a < |b|$, then

$$g(x,y) = f(x+my, y) = ax^2 + (2am+b)xy + c'y^2$$

$\sim f(x,y)$. If $a < |b|$, choose m with $|2am+b| < |b|$

contradiction!

If $a > c$, swap x and y: $g(x,y) = f(-y, x)$.

Get $|b| \le a \le c$.

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 ~~ue~~ existence, now show uniqueness.

(not in Granville)

4.5.

Lemma. If $f(x,y) = ax^2 + bxy + cy^2$ satisfies $|b| \le a \le c$,
then $$f(x,y) \ge (a - |b| + c)\min(x^2, y^2).$$
(Take for granted, or exercise)

So: If $xy \neq 0$, $f(x,y) \ge a - |b| + c$.
And, by assumption, $a \le c$, 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:

- ⊛ First coeff a must be the same.
- ⊛ ~~First~~ Last coeff c must be the same.
  (Some technical details: Last coeff can't be a. See Cox.)
- ⊛ Same discriminant, so b must be the same up to $\pm$.

Now, why are $f(x,y) = ax^2 + bxy + cy^2$
$g(x,y) = ax^2 - bxy + cy^2$ inequiv?

Let $g(x,y) = f(\alpha x + \beta y, \gamma x + \delta y)$
$a = g(1,0) = f(\alpha, \gamma)$ $\quad c = g(0,1) = f(\beta, \delta)$
By min. considerations, $(\alpha, \gamma) = \pm(1,0)$
$(\beta, \delta) = \pm(1,0)$

So $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ of det. 1.
Must be ± 1.

Finally: $a = |b|$ or $a = c$. Exercise ...

4.6.

Prop. If $ax^2+bxy+cy^2$ is reduced then $3a^2 \le -D$, i.e. $a \le \sqrt{-D/3}$.

Proof.

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2.$$

And $|b| \le a$.

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?

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

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

But, we do have a bound:

$$4ac = -D + b^2$$
$$\leq -D + a^2, \quad \text{so} \quad c \leq \frac{-D}{4a} + \frac{a}{4}$$
$$\leq \frac{-D}{4} + \frac{1}{4}\sqrt{\frac{-D}{3}}.$$

Def. ~~Ea~~ The class number $h(D)$ is the number of proper equivalence classes of IBQFs of discriminant D.

~~[illegible]~~

Theorem.
(1) $h(D) \neq 0 \longleftrightarrow D \equiv 0, 1 \pmod 4$.
(2) For each negative D, $h(D)$ is finite,
~~and can be~~ $h(D) \ll |D|^2$ (in fact $h(D) \ll |D|$),
and can be computed in $O(|D|)$ time.
(3) The IBQFs 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, 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 $|b| \le a \le \sqrt{\frac{4}{3}}$.

So: $a = 1$. $b = -1, 0,$ or 1.
(not -1 because $|b| = a$)

$a = 1, b = 0 \implies 0^2 - 4c = -4 \implies c = 1$.

$a = 1, b = 1 \implies 1^2 - 4c = -4$ (nope)

So $h(-4) = 1$.

We observe that $h(D) \ll |D|$.

Why? Check $a \le \sqrt{\frac{-D}{3}}$ and $|b| \le a$.

Then c is determined.

So, in fact, $h(D) \le \left(\sqrt{\frac{-D}{3}}\right)\left(2\sqrt{\frac{-D}{3}} \cancel{+1}\right)$
$$= \frac{2}{3} \cdot |D| \cancel{+ \sqrt{\frac{|D|}{3}}}$$

~~which is less than $|D|$ except for $|D|$ really small.~~

5.3.

Ex. Compute $h(-23)$.

Have $|b| \le a \le \sqrt{\frac{23}{3}}$ so $a = 1$ or 2.

$a = 1$: $b = 0$ or 1.

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

$b = 1 \Rightarrow 1 - 4c = -23$ $(c = 6)$ $\quad x^2 + xy + 6y^2$

$a = 2$: $b = -1, 0, 1, 2$

$b = -1 \Rightarrow 1 - 8c = -23$, $\quad c = 3$ $\quad 2x^2 - xy + 3y^2$

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

$b = 1 \Rightarrow 1 - 8c = -23$ $\quad 2x^2 + xy + 3y^2$.

$b = 2 \Rightarrow 4 - 8c = -23$ (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, Ex. 2.8) Any form of discriminant $D > 0$ not a perf. square is properly equivalent to $ax^2 + bxy + cy^2$ with $|b| \le |a| \le |c|$. This implies $|a| \le \frac{\sqrt{D}}{2}$.

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

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

and

$$h(-n) = \frac{\sqrt{n}}{\pi} \cdot L(1, \chi_{-n}) \quad \text{for } n > 4.$$

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.

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

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

Explain why it's true, rel'n to $L(s, \chi_d)$ and Dedekind zeta fns.

(Need for DCNF, then GON)

(4) Relation to $\mathbb{H}$.

(5). Why $n^2 + n + 41$ is prime so often.

6.2.

Relation to $\mathbb{H}$ first.

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

So, $f\circ g(u,v) = 0$

$$\Updownarrow$$

$f(\alpha u + \beta v, \gamma u + \delta v) = 0$.

i.e. $[u:v]$ is a root of $f\circ g$

$$\Updownarrow$$

$[\alpha u + \beta v : \gamma u + \delta v]$ is a root of f.

Set $v = 1$ and think of BQFs as being determined by their roots.

i.e. $u \in \mathbb{P}^1$ is a root of $f\circ g$

$$\Updownarrow$$

$\dfrac{\alpha u + \beta}{\gamma u + \delta} \in \mathbb{P}^1$ is a root of f.

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

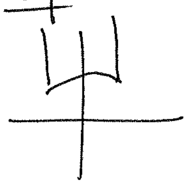
$GL_2(\mathbb{C})$ acts on $\mathbb{H} \cup \{\infty\}$ by $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \circ z = \dfrac{\alpha z + \beta}{\gamma z + \delta}$.

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

Prop. A definite real binary quadratic form has one of its roots in $\mathbb{H}\cup\{\infty\}$

Prop. If f has root $z \in \mathbb{P}^1(\mathbb{C})$, then $(f\circ g)$ has root $f^{-1}(z)$. Can go back and forth!

Prop. A fundamental domain for the action of $GL_2(\mathbb{Z})$ on $\mathbb{H}$ is:



This is equivalent to being reduced in Gauss's sense.

6.3. Indeed, the roots of ax^2+bx+c are

$$\frac{-b \pm \sqrt{D}}{2a}.$$

We have $|\mathrm{Re}(z)| \le \frac{1}{2} \Longleftrightarrow |b| \le a$.

What about $|z| \ge 1$?

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

So $|z| \ge 1 \Longleftrightarrow a \le c$.

So the conditions exactly correspond.

The $n^2 + n + 41$ is prime result.

Theorem. If $D < 0$, then

$h(D) = 1 \Longleftrightarrow D \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$.

and also $-12, -16, -27, -28$ if one counts non-fundamental discs.

Proof. $\Longleftarrow$: Easy homework exercise.

$\Longrightarrow$: Much, much, MUCH harder homework exercise.

(Warning: Gauss, Heilbronn, Siegel, etc. couldn't do it)

Rabinowicz's Theorem. Let $A \ge 2$ be an integer. Then $n^2 + n + A$ is prime for $0 \le n \le A-2$ if and only if $h(1-4A) = 1$.

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 $|D| < X$?
(Gauss, Mertens, Siegel)

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

Use GoN 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
$$\Updownarrow$$
D is a quadratic residue $\pmod{4m}$.

Sketch of proof.

m properly rep'd by f
$$\Updownarrow$$
f equiv. to $mx^2 + bxy + cy^2$ with $D = b^2 - 4mc$
$$\Updownarrow$$
$D \equiv b^2 \pmod{4m}$.

Application. (Rabinowicz) Let $A \geq 2$ integer. Then,
$n^2 + n + A$ is prime for $0 \leq n \leq A-2$ iff
$h(1-4A) = 1$.

(6.4) = 7.2.

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

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

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

Then:

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

$$4p = 4u^2 + 4uv + 4Av^2$$
$$= (2u+v)^2 + (4A-1)v^2 \quad < 4A - 1$$

(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

* $p^2 \nmid D$ for any $p > 2$
* If $4 \mid D$ then $\frac{D}{4} \equiv 2, 3 \pmod 4$.

12.31.

Prop. 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 $\mathbb{Z}[x] / \left(x^2 - \frac{D}{4}\right)$

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

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

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

The "quadratic fields" are ~~$\mathbb{Q}(x)$~~ $\mathbb{Q} \oplus \mathbb{Q}$

and $\mathbb{Q}(x) / (x^2)$.

7.4. Automorphisms of quadratic forms.

Definition. An automorphism of a quadratic form f is a change of variables (i.e. an elt. of $SL_2(\mathbb{Z})$) 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 $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\in SL_2(\mathbb{Z})$.

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 $|\mathrm{Aut}(x^2+y^2)| = 4$ and $\mathrm{Aut}(x^2+y^2)\cong C_4$.

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

$\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\in SO(2)$ is counter-clockwise rotation in $\mathbb{R}^2$ by 90°

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

This rotation is multiplication by i.

8.1. Automorphisms of quadratic forms.

Review def., result of computation on 7.4.

(7.5) = 8.2.

Prop. If two quadratic forms are equivalent then their automorphism groups are isomorphic, and indeed conjugate in $SL_2(\mathbb{Z})$.

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

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

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

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

Rk. This principle is extremely familiar, master it!

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

$$|Aut(f)| = \begin{cases} 4 & \text{if } D=-4 \quad \text{(proved above)} \\ 6 & \text{if } D=-3 \quad \text{(homework!!)} \\ 2 & \text{if } D<-4. \end{cases}$$

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

If $D>0$ then $Aut(f)$ is infinite.

Example. Look at $x^2 - 2y^2$ of discriminant 8.

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

(2. hard) Figure out how I wrote down that matrix.

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

8.3.

The representation theorem.

Let $r_D(n) :=$ # representations of n by all QF of disc. D, up to equivalence.

Proved before: $r_D(n) > 0 \longleftrightarrow$ (If n is odd) D is a quadratic residue mod 4.

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

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

Define $$\left(\frac{D}{2}\right) = \begin{cases} 0 & \text{if } D \text{ is even} \quad (2 \text{ ram in } \mathbb{Q}(\sqrt{D})) \\ 1 & \text{if } D \equiv 1, 7 \pmod 8 \quad (2 \text{ splits in } \mathbb{Q}(\sqrt{D})) \\ -1 & \text{if } D \equiv 3, 5 \pmod 8 \quad (2 \text{ inert in } \mathbb{Q}(\sqrt{D})) \end{cases}$$

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

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

Analytic number theory lemma.

$$r_D(n) = \sum_{m \mid n} \left(\frac{D}{m}\right) = \prod_{p^{e_p} \parallel n} \left(1 + \left(\frac{D}{p}\right) + \left(\frac{D}{p^2}\right) + \cdots + \left(\frac{D}{p^{e_p}}\right)\right).$$

Proof. Foil the right side!

Example. Suppose n is coprime to D and squarefree.

Then, $$r_D(n) = \prod_{p \mid n} \left(1 + \left(\frac{D}{p}\right)\right) = 2^{w(n)}$$ ($w(n) =$ # dist prime factors) if D is a residue mod p,

$= 0$ otherwise.

8.4. <u>Example</u>. Let $D = -4$.

Then $r_{-4}(1) = 1$. $(1^2+0^2, (-1)^2+0^2, 0^2+1^2, 0^2+(-1)^2)$

$r_{-4}(5) = 2$. $\cancel{1^2+2^2, 1^2+(-1)^2}$

$((\pm1)^2+(\pm2)^2)$, backwords).

$r_{-4}(2) = 1$. (Note: $\left(\frac{-4}{2}\right) = 0$.)

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

<u>Example</u>. $D = -15$.

$\cancel{x^2+y^2\pm4}$ $x^2+xy+4y^2$ #1

$2x^2+xy+2y^2$. #2

$\left(\frac{-15}{17}\right) = 1$, so $r_{-15}(17) = 2$.

#2: $x = 1, y = -3$

$x = -1, y = 3$

$x = -3, y = 1$

$x = 3, y = -1$.

These are two equiv. classes.

Similarly, $\left(\frac{-15}{19}\right) = 1$, $r_{-15}(19) = 2$. rep'd by <u>first</u> 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. 3.20. (Warning: Cox uses different letters)

For $4 \mid D$, and n odd. D negative,

(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.

Theorem. Suppose d is fundamental. Let $L(1, \chi_d) := \sum_n \left(\frac{d}{n}\right) \cdot \frac{1}{n}$.

Then, $h(d) = \frac{w}{2\pi} \cdot \sqrt{|d|}\; L(1, \chi_d)$,

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

Examples.

$d = -4$:

$$h(-4) = \frac{4}{2\pi} \cdot \sqrt{4} \cdot \left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots\right)$$

$$= \frac{4 \cdot 2}{2\pi} \cdot \frac{\pi}{4} = 1.$$

$$h(-3) = \frac{6}{2\pi} \sqrt{3} \left(1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \frac{1}{7} - \frac{1}{8} \cdots\right)$$

$$= \frac{3\sqrt{3}}{\pi} \cdot \frac{\pi}{3\sqrt{3}} = 1.$$

$$h(-23) = \frac{2}{2\pi} \sqrt{23} \left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} - \frac{1}{5} + \frac{1}{6} - \frac{1}{7} + \cdots\right)$$

$$= \frac{\sqrt{23}}{\pi} \left(\frac{3\pi}{\sqrt{23}}\right).$$

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?

Guess $\displaystyle\sum_{-d<X} \frac{\sqrt{|d|}}{\pi} \sim \underbrace{\frac{3}{\pi^2}}_{\substack{\text{Proportion of}\\ d \text{ which are}\\ \text{fundamental}}} \int_0^X \frac{t^{1/2}}{\pi}\,dt = \frac{2}{\pi^3} X^{3/2}$.

This is not correct.

We also have

$$\sum_{-d<X} h(-d) = \#\left\{(a,b,c) : \begin{array}{l} b^2 - 4ac \in [-X, 0], \\ \text{satisfy inequalities} \\ \text{for being reduced}, \\ b^2 - 4ac \text{ is fundamental} \end{array}\right\}$$

(2) $L(1, \chi_d)$ is easy to bound from above, so we can prove $h(d) \ll \sqrt{|d|} \log |d|$.
(Will prove this directly.)

(3) $L(1, \chi_d) \neq 0$.
This proves, e.g. half of primes are $\equiv 1 \pmod 4$
half are $\equiv 3 \pmod 4$.

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.

9.3. Strategy of proof.

Hinges on the theorem that

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

Lemma. We have [explain "$p^{e_p} \| n$"]

$$\sum_{m|n} \left(\frac{D}{m}\right) = \prod_{p^{e_p} \| n} \left(1 + \left(\frac{D}{p}\right) + \left(\frac{D}{p^2}\right) + \dots + \left(\frac{D}{p^{e_p}}\right)\right).$$

Proof. FOIL the right side.

In particular, if n is coprime to D and squarefree,

$$r_D(n) = \prod_{p|n} \left(1 + \left(\frac{D}{p}\right)\right) = \begin{cases} 2^{w(n)} & \text{if } D \text{ is a residue mod } n \\ & (w(n): \# \text{ of dist prime divisors}) \\ 0 & \text{o/w}. \end{cases}$$

(8.6) = 9.4

GON and bounds on the class number.

~~**Prop.** If $d<0$ then~~ (A.G., p. 9)

$$\cancel{h(d) \ll \sqrt{|d|}\log|d|.}$$

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

$$\sum_{n \le N} r_f(n) = \frac{1}{w} \sum_{\substack{x,y \in \mathbb{Z} \\ 0<f(x,y)\le N}} 1,$$

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

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 $g\begin{bmatrix} x \\ y \end{bmatrix} \ne \begin{bmatrix} x \\ y \end{bmatrix}$ for $\begin{bmatrix} x \\ y \end{bmatrix} \ne \begin{bmatrix} 0 \\ 0 \end{bmatrix}$.

For $\mathrm{Disc}(f) < -4$, $\mathrm{Aut}(f) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ so it's obvious.

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

Prop. If f is positive definite, then

$$\sum_{\substack{x,y \in \mathbb{Z} \\ 0<f(x,y)\le N}} 1 = \frac{2\pi N}{\sqrt{|D|}} + O(\sqrt{N}).$$

~~Now why is this interesting?~~

$$\sum_{\substack{f \\ f \text{ of disc } D}} \sum_{n \le N} r_f(n) = \cancel{h(D)\left(\frac{2\pi N}{\sqrt{|D|}} + O(\sqrt{N})\right)}.$$

$$\parallel$$

$$\sum_{n \le N} r_D(n)$$

9.5.

Therefore, for $\underset{\approx}{\underline{\text{any}}}$ N,

$$\sum_{n \le N} r_D(n) = \sum_{\substack{f \\ f \text{ of disc} \\ D}} \sum_{n \le N} r_f(n) = h(D)\left(\frac{2\pi N}{w\sqrt{|D|}} + O(\sqrt{N})\right).$$

Simultaneously,

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

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

cheating!!!! come back and fix

$$\sim \sum_{m \le N} \left(\frac{D}{m}\right) \frac{N}{m}$$

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

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

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

So,

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

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

So, $L(1, \chi_D) = \dfrac{2\pi h(D)}{w\sqrt{|D|}}$.

9.6. Being more coreful :

For any A and B we have $\left|\sum_{A<m\le B}\left(\frac{D}{m}\right)\right| \le |D|$.

So, for any k

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

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

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

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

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

~~This is much smaller~~

This is still $N\cdot\left(L(1,\chi_D)+o(1)\right)$.

10.1. Real quadratic ~~fields~~ 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

$$0 < \sqrt{D} - b < 2|a| < \sqrt{D} + b.$$

[Q. 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 $\rho_1 = \dfrac{-b + \sqrt{d}}{2a}$, $\rho_2 = \dfrac{-b - \sqrt{d}}{2a}$.

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 $|b_0'| \le c$.

* If $|b_0'| > \sqrt{d}$ then let $b' = b_0'$.

We have $0 < (b')^2 - \cancel{D} \le c^2 - d$,

so $|c'| = \dfrac{(b')^2 - D}{4|c|} < \dfrac{|c|}{4}$. (Decreased $|c|$)

* If $|b_0'| < \sqrt{D}$, choose $b' \equiv -b \pmod{2c}$ w/ b' as large as possible s.t. $|b'| < \sqrt{D}$.

We have $-D \le (b')^2 - D = 4cc' < 0$.

If $2|c| > \sqrt{D}$ then $|c'| \le \left|\frac{D}{4c}\right| < |c|$.

In case ~~we hit none of the "if"s~~. $2|c| \le \sqrt{D}$:

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

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

Idea: Kept reducing a and c until we got such reduced.

Note, Don't have uniqueness, get a cycle (see Granville).

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

$$\left(\frac{v}{2}\right)^2 - \left(\frac{D}{4}\right) w^2 = \pm 1.$$

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.

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

Cor. It has infinitely many.

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

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

Take kth powers to get inf. 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 $D \equiv 1 \pmod 4$, both of above are half integers (not $\frac{1}{4}$-integers).

10.4. <u>Exercise</u>. The automorphisms of a form are all given by

$$\begin{bmatrix} \frac{1}{2}(t-bu) & -cu \\ au & \frac{1}{2}(t+bu) \end{bmatrix}$$

with $t^2 - du^2 = +4$. (-4 gives det $= -1$.)

<u>Simple exercise</u>. Check that this gives an automorphism, and that squaring this matrix preserves this property.

<u>Better exercise</u>. Factor $ax^2 + bxy + cy^2 = a(x - \theta y)(x - \theta' y)$,

$$\theta = \frac{-b + \sqrt{D}}{2a},$$

and check that our automorph corresponds to

$$x' - \theta y' = \tfrac{1}{2}(t - u\sqrt{D})(x' - \theta' y)$$
$$x' + \theta y' = \tfrac{1}{2}(t + u\sqrt{D})(x' + \theta' y).$$

<u>Definitions</u>.

The <u>fundamental unit</u> $\varepsilon_D := \dfrac{u_0 + \sqrt{D}\, w_0}{2}$ is the minimal such expression which is > 1 and of norm ± 1.

Here the norm is $\varepsilon_D \cdot \overline{\varepsilon_D} = \dfrac{u_0^2 - D w_0^2}{4}$.

So corresponds to Pell's equation.

<u>Prop</u>. All solutions are $\pm \varepsilon_D^k$.

<u>Def</u>. Let ε_D^+ be the smallest unit > 1 with norm 1.

So, $\varepsilon_D^+ = \varepsilon_D$ or ε_D^2, depending on whether $N(\varepsilon_D) = 1$ or -1.

10.5.

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

$$\left|\frac{x'-\theta y'}{x'-\theta' y'}\right| = \left|\frac{(\varepsilon_D^+)^k (x-\theta y)}{(\varepsilon_D^+)^{-k}(x-\theta' y)}\right| = (\varepsilon_D^+)^k \cdot \left|\frac{x-\theta y}{x-\theta' y}\right|.$$

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

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

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

This is still equal to $N \cdot \left(L(1, \chi_D) + o(1)\right)$

for the same reason as before.

So we need to count, for each fixed QF $ax^2 + bxy + cy^2$, how many integer points (x, y) there are with:

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

$$x - \theta y > 0,$$

$$\left|\frac{x-\theta y}{x-\theta' y}\right| \in [1, (\varepsilon_D^+)^2).$$

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~~

Its ring of integers is

$$\mathcal{O} = \begin{cases} a + b\sqrt{d} : a, b \in \mathbb{Z} & \text{if } d \equiv 2, 3 \pmod 4 \\ \dfrac{a+b\sqrt{d}}{2} : a, b \text{ same parity} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

It is:

$$\mathcal{O} = \{ x \in \mathbb{Q}(\sqrt{d}) : x \text{ satisfies a monic poly. with coeffs in } \mathbb{Z} \}$$

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

Its discriminant is $(\mathrm{Tr}(\alpha_i \alpha_j)) = \det \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4\sqrt{d}$

or $\det \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix} = \sqrt{d}$

as above,

so for squarefree d, $\mathrm{Disc}(\mathcal{O}) = \mathrm{Disc}(\mathbb{Q}(\sqrt{d})) = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$

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

Notation. Let K be a QF and $\mathcal{O}$ its ring of integers.

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

If p is a prime of $\mathbb{Q}$, then $p\mathcal{O}_K$ is:

prime in $\mathcal{O}$ (inert)

$\mathfrak{p} \cdot \bar{\mathfrak{p}}$ in $\mathcal{O}$ (split)

or $\mathfrak{p}^2$ in $\mathcal{O}$. (ramified)

E1.2.

Def. A *fractional ideal* of $\mathcal{O}$ is an f.g. $\mathcal{O}$-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* $Cl(K) := I(K)/P(K)$.

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

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

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

$$Cl(K) \cong Cl(D).$$

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

Construct a map

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

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

In other words:

$$a(x+\theta y)(x+\theta' y) \longrightarrow a[1, \theta].$$

E1.3.

Now, let $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ act on $ax^2 + bxy + cy^2$.

Get $a\left([\alpha x + \beta y] + [\gamma x + \delta y]\theta\right) \cdot \text{conj}.$

$= a\left([\alpha + \gamma\theta]x + [\beta + \delta\theta]y\right) \cdot \text{conj}.$

$= a \cdot (\alpha + \gamma\theta)\left(x + \frac{\beta + \delta\theta}{\alpha + \gamma\theta} y\right) \cdot \text{conj}.$

So maps to $a \cdot (\alpha + \gamma\theta)\left[1, \frac{\beta + \delta\theta}{\alpha + \gamma\theta}\right]$

$= a\left[\alpha + \gamma\theta, \beta + \delta\theta\right].$

$= a \cdot [1, \theta]\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}.$

We wrote an ideal of $\mathcal{O}$ ~~as~~ in terms of its $\mathbb{Z}$-basis which we simply permuted.

So it's well defined.

You can go backwards too, so injective.

Why is it surjective? Given $[\alpha, \beta]$ for some $\alpha, \beta \in K$.

WLOG $\tau := \frac{\beta}{\alpha}$ is in $\mathbb{H}$.

Then $[\alpha, \beta] \sim [1, \tau]$ in $Cl(K)$.

Let $ax^2 + bx + c$ be min poly of τ.

Check: This maps to it.

E1.4. <u>Corollary</u>. $Cl(D)$ is a group.

As Dirichlet discovered, if
$$f(x,y) = ax^2 + bxy + cy^2$$
$$g(x,y) = a'x^2 + b'xy + c'y^2$$
with $\gcd(a, a', \frac{b+b'}{2}) = 1$

both of disc D, then their <u>composition</u> is

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

<u>where</u> B is the unique integer (mod $2aa'$) with
$$B \equiv b \pmod{2a}$$
$$B \equiv b' \pmod{2a'}$$
$$B^2 \equiv D \pmod{4aa'}.$$

<u>Proof</u>. Multiply ideals!

<u>Claim</u>. If f is a form of disc D, then
$$\mathrm{Aut}(f) \cong \mathcal{O}^\times.$$

<u>Proof</u>. Let $\frac{u + v\sqrt{d}}{2}$ be a unit, with $\left(\frac{u+v\sqrt{d}}{2}\right)\left(\frac{u-v\sqrt{d}}{2}\right) = 1$.
(Similar if -1.)

$$ax^2 + bxy + cy^2 = a(x + \theta y)(x + \theta' y)$$
$$= a\underbrace{\left(\frac{u+v\sqrt{d}}{2}\right)(x+\theta y)\left(\frac{u-v\sqrt{d}}{2}\right)(x+\theta' y)}_{\text{FOIL.}}$$

Get a change of variables.

E1.5.

The zeta function.

Def. If $\underline{a}$ is an (integral) ideal then $N(\underline{a}) = [\mathcal{O} : \underline{a}]$.

If $\underline{a} = (a)$ then $N(\underline{a}) = N(a)$.

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

$$\zeta_K(s) = \sum_{\underline{a} \neq 0} (N\underline{a})^{-s} = \prod_{\mathfrak{p}} (1 + (N\mathfrak{p})^{-s} + (N\mathfrak{p})^{-2s} + \dots)$$
$$= \prod_{\mathfrak{p}} (1 - (N\mathfrak{p})^{-s})^{-1}.$$

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

Ex. $\mathbb{Z}[i]$ is a PID, with unit group 4, so

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

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 $\left(\frac{D}{p}\right) = 1$.

$(1 - p^{-s})^{-1}$ if ramified

$(1 - p^{-2s})^{-1}$ if inert.

Implies: # of ideals of norm n is

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

i.e. # of inequivalent representations.

We recognize this now!