4.1.

Recall. Interested in binary quadratic forms $ax^2 + bxy + cy^2$ right action of $SL_2(\mathbb{Z})$

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

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

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

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

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 $\equiv 0, 1 \pmod 4$

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) $|b| \leq a \leq c$,

(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: * $SL_2(\mathbb{Z})$ acting on $\mathcal{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$ by $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tau = \frac{\alpha\tau + \beta}{\gamma\tau + \delta}$

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 $x = 0, 1, 2, 3, \cdots, 10$. 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 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 one $f(x,y) = ax^2 + bxy + cy^2$
$g(x,y) = ax^2 - bxy + cy^2$ 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.

4.6.

Prop. If $ax^2 + bxy + cy^2$ 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?

$$|b| \le |a| \le \sqrt{\frac{-4D}{3}}.$$

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

But. We do have a bound:

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

Def. The class number $h(D)$ is the number of proper equivalence classes of IBQFs 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. (in fact $h(D) \ll |D|^2$)
(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 $|b| = a$)

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

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

So $h(-4) = 1$.

We observe that $h(D) << |D|$.

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

Then c is determined.

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

$= \frac{2}{3} \cdot |D| + \sqrt{\frac{-D}{3}}$

~~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)

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

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

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

$b = 0 \Rightarrow -8c = -23$ (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, Ex. 2.10) 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

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

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 $|\text{Ш}|$.

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

6.2.

(C) 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. ~~[illegible]~~

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

$$\Updownarrow$$

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

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

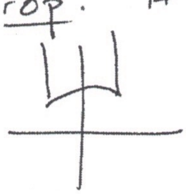
$GL_2(\mathbb{C})$ acts on $\mathbb{H} \cup \{\infty\}$ by $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \circ z = \frac{\alpha z + \beta}{\gamma z + \delta}$.

(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 $g^{-1}(z)$. 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 $|\mathrm{Re}(\tau)| \leq \frac{1}{2} \iff |b| \leq a$.

What about $|\tau| \geq 1$?

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

So $|\tau| \geq 1 \iff a \leq c$.

So the conditions exactly correspond.

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

Theorem. If $D < 0$, then

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

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 $A \geq 2$ be an integer. Then $n^2 + n + A$ is prime for $0 \leq n \leq A - 2$ if and only if $h(1 - 4A) = 1$.

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

$$4p = 4u^2 + 4uv + 4Av^2$$
$$= (2u+v)^2 + (4A-1)v^2 \leq 4A - 1$$
(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 $\frac{D}{4} \equiv 2, 3 \pmod 4$.

[7.3].

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

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

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

$D = 0$, 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.