(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. (If n is odd)

Proved before: $r_D(n) > 0 \longrightarrow D$ 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 $\left(\frac{D}{2}\right) = \begin{cases} 0 & \text{if } D \text{ is even} \\ 1 & \text{if } D \equiv 1, 7 \pmod 8 \\ -1 & \text{if } D \equiv 3, 5 \pmod 8 \end{cases}$ (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.

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

Proof. Foil the right side!

Example. Suppose n is coprime to D and squarefree.

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

$= 0$ otherwise.

8.4. Example. Let $D = -4$.

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

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

$((\pm 1)^2 + (\pm 2)^2)$, backwards).

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

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

Example. $D = -15$. ~~$x^2 + y^2 + 4$~~ $x^2 + xy + 4y^2$ #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 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. 3.20.

For $4 \mid D$, and n odd. (Warning: Cox uses different letters)

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.

Suppose d is fundamental.

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

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

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

This is not correct.

We also have

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

(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 GCN problem to solve. We will do this in detail.

9.3.

Strategy of proof.

Hinges on the theorem that

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

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

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

Proof. Foil the right side.

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

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

(8.6) = 9.4

GON and bounds on the class number.

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

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

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

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?

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

$$\sum r_D(n)$$

What are the lengths of the projections?

(z, w) in a box of side length $\frac{1}{\sqrt{a}}$.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & \frac{-b}{2a} \cdot \frac{2a}{\sqrt{-D}} \\ 0 & 2a/\sqrt{-D} \end{bmatrix} \begin{bmatrix} z \\ w \end{bmatrix} = \begin{bmatrix} 1 & \frac{-b}{\sqrt{-D}} \\ 0 & 2a/\sqrt{-D} \end{bmatrix} \begin{bmatrix} z \\ w \end{bmatrix}$$

$$\text{So } |y| < \left| \frac{2a}{\sqrt{-D}} \right| \frac{1}{\sqrt{a}} \leq \frac{2\left|\sqrt{-D}/3\right|}{\sqrt{-D}} \frac{1}{\sqrt{a}} \leq \frac{2\sqrt{3}}{\sqrt{a}}.$$

$$|x| \leq |z| + \left|\frac{b}{2a}\right| |y|$$

$$< \frac{1}{\sqrt{a}} + \frac{1}{2} \cdot \frac{2\sqrt{3}}{\sqrt{a}} = \frac{(1+\sqrt{3})}{\sqrt{a}}.$$

Projections of size $O\left(\frac{1}{\sqrt{a}}\right)$.

So, in general, projections of size $O\left(\frac{\sqrt{N}}{\sqrt{a}}\right) = O(\sqrt{N})$.

The GON question.

What is $\text{Area}(\{ax^2 + bxy + cy^2 < N\})$?

Note it is $N \cdot \text{Area}(\{ax^2 + bxy + cy^2 < 1\})$.
$N^{1/2}$ in each dimension.

$a > 0$ because $b^2 - 4ac < 0$.

$$x^2 + \frac{b}{a}xy + \frac{c}{a}y^2 < \frac{1}{a}$$

$$\left(x + \frac{b}{2a}y\right)^2 + \left(\frac{c}{a} - \frac{b^2}{4a^2}\right)y^2 < \frac{1}{a}$$

$$\left(x + \frac{b}{2a}y\right)^2 + \left(\frac{4ac - b^2}{4a^2}\right)y^2 < \frac{1}{a}.$$

Change of variables $z = x + \frac{b}{2a}y$, $w = \frac{\sqrt{4ac-b^2}}{2a}y$

$$z^2 + w^2 < \frac{1}{a} \text{ with area } \frac{\pi}{a}.$$

Our change of variables is $\begin{bmatrix} z \\ w \end{bmatrix} = \begin{bmatrix} 1 & b/2a \\ 0 & \sqrt{4ac-b^2}/2a \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$

Multiplied volume by $\frac{\sqrt{4ac-b^2}}{2a}$.

So area $= \frac{\pi}{a} \cdot \frac{2a}{\sqrt{4ac-b^2}} = \frac{2\pi}{\sqrt{-D}}$.

9.5.

Therefore, for 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,

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

cheating!!!! come back and fix

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

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

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

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

~~$\sum_{m \le N} \frac{D}{m}$~~ $N \cdot \left(L(1, \chi_D) + o(1)\right)$.

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 careful:

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

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

~~Rise is another section~~

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