11.1. Real quadratic forms.

An indefinite binary real quadratic form $ax^2 + bxy + cy^2$

has:

discriminant $D > 0$,

two real roots $[x : y]$, $\frac{-b \pm \sqrt{D}}{2a}$.

a reduced form in its equivalence class

satisfying

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

Def. Pell's equation is the Diophantine equation

$$t^2 - Du^2 = \pm 4.$$

Can write $\left(\frac{t}{2} - \frac{u}{2}\sqrt{D}\right)\left(\frac{t}{2} + \frac{u}{2}\sqrt{D}\right) = \pm 1$,

and all solutions are given in this form by

$$\pm \left(\frac{t}{2} + \frac{u}{2}\sqrt{D}\right)^k, \quad k \in \mathbb{Z}$$

where u and v are minimal.

Prop. The automorphisms of $ax^2 + bxy + cy^2$, $D > 0$,
are given by

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

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

Lemma 1. These are in $SL_2(\mathbb{Z})$.

Proof. $\det = \frac{1}{4}(t^2 - b^2u^2) + acu^2$

$= \frac{1}{4}(t^2 - Du^2)$.

11.2.

why are the coefficients integers?

D odd $\longleftrightarrow$ b odd.

If D is odd, ~~[illegible]~~ t and u must have the same parity.

If D is even, then so is t.

Lemma 2. As can be verified directly, that gives an automorph, and squaring the matrix gives another of the same shape.

Where do these come from?

Write $ax^2+bxy+cy^2 = a(x-\theta y)(x-\theta' y)$

with $\theta = \dfrac{-b+\sqrt{D}}{2a}$.

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

$= \left(\frac{1}{2}(t-bu)x - cuy\right) - \theta\left[aux + \frac{1}{2}(t+bu)y\right]$

and it can be checked that

$(x-\theta y)\cdot\frac{1}{2}(t-u\sqrt{D})$ is the same thing.

Note: Can write down this matrix.

Figure out the θ coeff because it is the only thing with $\sqrt{D}$'s in it.

Also, $(x-\theta' y)\begin{bmatrix} \frac{1}{2}(t-bu) & -cu \\ au & \frac{1}{2}(t+bu) \end{bmatrix}$ with $\theta' = \dfrac{-b-\sqrt{D}}{2a}$.

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

This is automatic because the computation is conjugate to the previous one.

(11.3) – 12.1.

So our automorph is

$$ax^2 + bxy + cy^2 = a(x - \theta y)(x - \theta' y)$$

$$\downarrow \qquad\qquad \downarrow$$

$$a\left[(x - \theta y)\tfrac{1}{2}(t - u\sqrt{D})\right] \cdot \left[(x - \theta' y)\tfrac{1}{2}(t + u\sqrt{D})\right],$$

which is the same by construction.

Prop. These are all the automorphs.
Easiest proof: Use the correspondence with ideals in QFs.

Def. The fundamental unit $\varepsilon_D := \dfrac{t + u\sqrt{D}}{2}$ is the minimal expression of this shape which is > 1 and of norm ± 1.

Its norm is $\dfrac{t^2 - u^2 D}{4}$, so corresponds to Pell's equation.

Prop. (1) All solutions are $\pm \varepsilon_D^k$.
(2) There is an effective algorithm to find ε.

Def. Write ε_D^+ for the smallest such with norm > 1.
So ε_D^+ is ε_D or ε_D^2 depending on whether $N(\varepsilon_D)$ is 1 or -1.

11. 9. = 12.2

Dirichlet's class number formula for real quadratic fields.

<u>Theorem.</u> $L(1, (\frac{D}{\cdot})) \cdot \sqrt{D} = h(D) \cdot \log(\varepsilon_D^+)$.

Compare to the imaginary case, which said
$$L(1, (\tfrac{D}{\cdot}))\sqrt{D} = h(D) \cdot \frac{2\pi}{w}.$$

How did we prove this?

we looked at $\displaystyle\sum_{n \leq N} r_D(n) \overset{D<0}{=} \frac{1}{w} \sum_f \sum_{\substack{x,y \in \mathbb{Z} \\ 0 < f(x,y) \leq N}} 1$

$$= \frac{1}{w} \sum_f \left(\frac{2\pi N}{\sqrt{|D|}} + O(\sqrt{N}) \right)$$

$$= \frac{2\pi}{w} \left(N \cdot h(D) + O(h(D)\sqrt{N}) \right),$$

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

$$= \sum_{m \leq N} \left(\frac{D}{m}\right) \left\lfloor \frac{N}{m} \right\rfloor = N \left(\sum_{m=1}^{\infty} \left(\frac{D}{m}\right)\frac{1}{m} + o_N(1) \right)$$

$$= N \left(L(1, (\tfrac{D}{\cdot})) + o(1) \right).$$

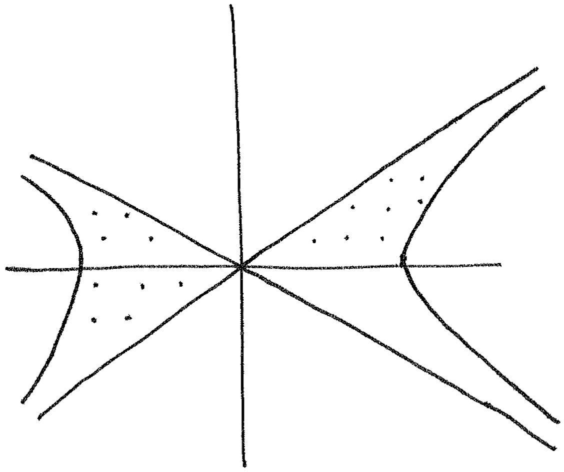
The second half works, but:

$$\sum_{n \leq N} r_D(n) = \frac{1}{\# \mathrm{Aut}(f)} \sum_f \sum_{\substack{x,y \in \mathbb{Z} \\ 0 < f(x,y) \leq N}} 1$$

Note: $\mathrm{Aut}(f) \cong \mathbb{Z} \times \mathbb{Z}/2$

What is the sum? e.g. $f(x,y) = x^2 - 2y^2$ of discriminant 8.

11.5 $= 12.3$



Count lattice points here.

$$\text{Vol} = 4\int_{y=0}^{\infty}\left(\sqrt{N+2y^2} - \sqrt{2y^2}\right) dy$$

$$= 4\int_{y=0}^{\infty}\sqrt{2y^2}\left[-1+\sqrt{1+\frac{N}{2y^2}}\right] dy$$

$$= 4\int_{y=0}^{\infty}\sqrt{2}\cdot y\cdot\left[-1+1+\frac{N}{4y^2}+o\left(\frac{N^2}{y^4}\right)\right]$$

$$= \sqrt{2}N\int_{y=1}^{\infty}\frac{1}{y}\,dy \quad + o(1)$$

So: $\sum_{n\le N} r_D(n) \approx \frac{1}{\infty}\cdot\sum_f$ (divergent integral).

And, $x^2-2y^2=1$ already has infinitely many solutions. (Take $x^2-8y^2=4$ and prove that some have to be even!) (Exercise.)

How could we have handled this differently?

Consider x^2+y^2 of disc -4.

Considered $\frac{1}{4}\sum_{0<x^2+y^2\le N} 1$ divide by equivalence.

What were the equivalences? $\begin{pmatrix}x\\y\end{pmatrix}\to\begin{pmatrix}0&-1\\+1&0\end{pmatrix}^i\begin{pmatrix}x\\y\end{pmatrix}$ for $i=0,1,2,3$.

Count solutions only up to rotation by $90°$! $\begin{pmatrix}0&-1\\1&0\end{pmatrix}\in SO_2$.

So: enough to count $\sum_{\substack{0<x^2+y^2\le N\\0\le x,y}} 1$, and this will give us a GON problem.

(12.4) 15.1

The setup:

Given $ax^2 + bxy + cy^2$

and two representations (x, y) and (X, Y) of the same integer n.

Then
$$X - \theta' Y = \frac{1}{2}(t + u\sqrt{D})(x - \theta' y)$$
$$X - \theta Y = \frac{1}{2}(t - u\sqrt{D})(x - \theta y)$$

for some solution t, u of the positive Pell equation
$$t^2 - u^2 D = 4$$

i.e.
$$X - \theta' Y = (\varepsilon_D^+)^k (x - \theta' y)$$
$$X - \theta Y = (\varepsilon_D^+)^{-k} (x - \theta y)$$
for some k.

So,
$$\left|\frac{X - \theta' Y}{X - \theta Y}\right| = (\varepsilon_D^+)^{2k} \cdot \left|\frac{x - \theta' y}{x - \theta y}\right|.$$

Therefore:

Proposition. There is a unique representation (x, y) which satisfies
$$1 \leq \frac{x - \theta' y}{x - \theta y} < (\varepsilon_D^+)^2$$
and $x - \theta' y$, $x - \theta y$ are both positive.

Call it primary.

Prop. The number of primary rep'ns of a given integer is finite.

Proof. Given a rep'n (x, y) of n.

Then $(x - \theta' y)(x - \theta y) = \dfrac{n}{a}$

and $1 \leq \dfrac{x - \theta' y}{x - \theta y} < (\varepsilon_D^+)^2$.

(12.5) 13.2.

$x-\theta' y$, $x - \theta y$ are both btn. $\left(\frac{n}{a}\right)(\varepsilon_D^+)^{-1}$, $\left(\frac{n}{a}\right)\varepsilon_D^+$.

So their difference is bounded, which is

$$(\theta - \theta')y = \left(\frac{-b+\sqrt{D}}{2a} - \frac{-b-\sqrt{D}}{2a}\right)y = \frac{\sqrt{D}}{a}y$$

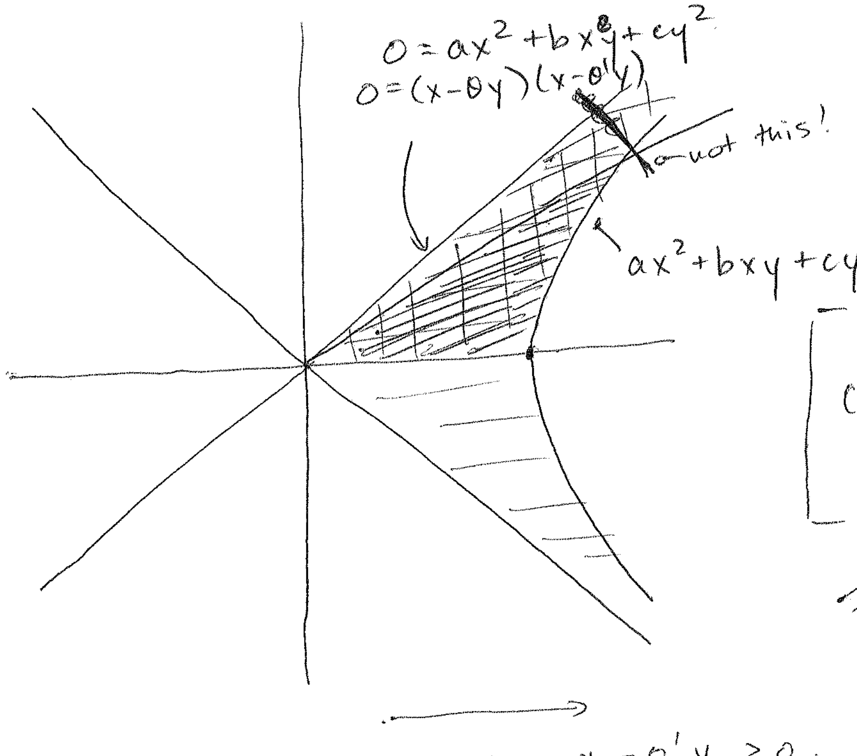
so a bounded number of choices for y.

Therefore:

$$\sum_{n \leq N} r_D(n) = \sum_{\substack{f \\ \text{(in class gp of } N)}} \sum_{n \leq N} r_f(n)$$

$$= \sum_f \sum_{\substack{n \leq N \\ 0 < f(x,y) \leq N \\ x - \theta y > 0 \\ 1 \leq \left|\frac{x-\theta' y}{x - \theta y}\right| < (\varepsilon_D^+)^2}} 1 .$$

How does our picture change?



Note: The picture assumes $b = 0$ and $\theta = \sqrt{\frac{c}{a}}$.

||||: $x - \theta' y > x - \theta y$.
(In picture: $x + \sqrt{\frac{c}{a}}y > x - \sqrt{\frac{c}{a}}y$.

////: $\frac{x-\theta' y}{x - \theta y} < (\varepsilon_D^+)^2$.

$x - \theta' y = \varepsilon^2(x - \theta y)$

$x(\varepsilon^2 - 1) = y(-\theta' + \theta\varepsilon^2)$

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

There is our GON problem!

12.6. (13.3.)

Two questions. (1) Estimate area.

(2) Estimate perimeter.

Max of the coordinates:

$$x - \theta y < \sqrt{N}$$
$$x - \theta' y < \sqrt{N}\,\varepsilon_D^+ .$$

$$(\theta - \theta')y = \frac{\sqrt{D}}{a} y < \sqrt{N}\left(\varepsilon_D^+ - (\varepsilon_D^+)^{-1}\right),$$

so: $y \ll \sqrt{N}$, where the implied constant depends on f.

$x \ll \sqrt{N}$, again ditto.

So the perimeter has size $\ll \sqrt{N}$.

(or use Davenport's lemma.)

Estimation of the area.

Change of variables $\xi = x - \theta y$, $\eta = x - \theta' y$.

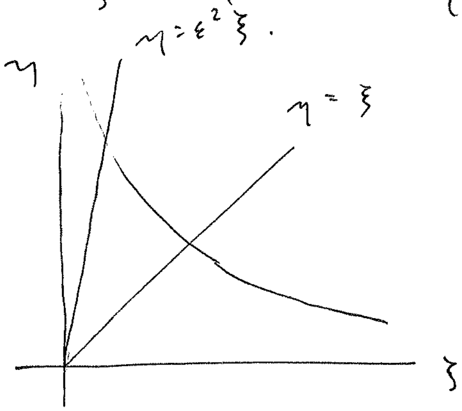
Conditions $0 < ax^2 + bxy + cy^2 \le N \longleftrightarrow 0 < \xi\eta \le \frac{N}{a}$.

$x - \theta y > 0 \longleftrightarrow \xi > 0$.

$\frac{x - \theta' y}{x - \theta y} \in [1, (\varepsilon_D^+)^2) \longleftrightarrow \xi \le \eta \le \varepsilon^2 \xi$. $(\varepsilon = \varepsilon_D^+)$

So: $0 < \xi \le \left(\frac{N}{a}\right)^{1/2}$.

$\xi \le \eta < \min(\varepsilon^2\xi, {}^N/a\xi)$.



13.4. The Jacobian change of variables formula says,

$$\iint_{\xi,\eta} d\xi\, d\eta = \iint_{x,y} \left|\frac{\partial(\xi,\eta)}{\partial(x,y)}\right| dx\, dy.$$

$$\frac{\partial(\xi,\eta)}{\partial(x,y)} = \begin{bmatrix} \frac{\partial \xi}{\partial x} & \frac{\partial \xi}{\partial y} \\ \frac{\partial \eta}{\partial x} & \frac{\partial \eta}{\partial y} \end{bmatrix} = \begin{bmatrix} 1 & -\theta \\ 1 & -\theta' \end{bmatrix} \text{ of det} = \theta - \theta' = \frac{\sqrt{D}}{a}.$$

So,

$$\iint_{x\ y} dx\, dy = \frac{a}{\sqrt{D}} \iint_{\xi\ \eta} d\xi\, d\eta$$

$$= \frac{a}{\sqrt{D}}\left[\int_0^{\frac{N^{1/2}}{\varepsilon\sqrt{a}}} (\varepsilon^2 \xi - \xi)\, d\xi + \int_{\frac{N^{1/2}}{\varepsilon\sqrt{a}}}^{(N/a)^{1/2}} \left(\frac{N}{a\xi} - \xi\right) d\xi\right]$$

$$= \frac{a}{\sqrt{D}}\left[(\varepsilon^2 - 1)\frac{\xi^2}{2}\Big|_0^{\frac{N^{1/2}}{\varepsilon\sqrt{a}}} + \left(\frac{N}{a}\log \xi - \frac{\xi^2}{2}\right)\Big|_{\frac{N^{1/2}}{\varepsilon\sqrt{a}}}^{(N/a)^{1/2}}\right]$$

$$= \frac{a}{\sqrt{D}}\Bigg[(\varepsilon^2 - 1)\cdot\frac{1}{2}\cdot\frac{N}{\varepsilon^2 a} + \left(\frac{1}{2}\frac{N}{a}\log\left(\frac{N}{a}\right) - \frac{1}{2}\cdot\frac{N}{a}\right)$$
$$- \left(\frac{N}{a}\log\left(\frac{N^{1/2}}{\varepsilon\sqrt{a}}\right) - \frac{1}{2}\cdot\frac{N}{\varepsilon^2 a}\right)\Bigg]$$

$$= \frac{a}{\sqrt{D}}\cdot\frac{N}{a}\cdot\log\varepsilon = \boxed{\frac{N}{\sqrt{D}}\log\varepsilon}$$

13.5. And so now what?

$$\sum_{n \le N} r_D(n) = \sum_f \sum_{\substack{n \le N \\ \text{in our} \\ \text{region}}} 1$$

$$= \sum_f \left(\frac{N}{\sqrt{D}} \log \varepsilon + o(\sqrt{N}) \right)$$

$$= h(D) \cdot \left(\frac{N}{\sqrt{D}} \log \varepsilon_D^+ + o(\sqrt{N}) \right)$$

$$= N\left(L\left(1, \left(\tfrac{D}{\cdot}\right)\right) + o(1) \right)$$

So: $L\left(1, \left(\tfrac{D}{\cdot}\right)\right) = \dfrac{h(D) \log \varepsilon_D^+}{\sqrt{D}}$, Q.E.D.

14.1.

(1) Recap. What have we done?

Studied binary quadratic forms.

Definition, action of $SL_2(\mathbb{Z})$, automorphism groups.

Reduction theory.

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

Representations of integers by $SL_2(\mathbb{Z})$-classes of forms.

Class numbers.

The class number formula,

$$\frac{L(1,\chi_{\cancel{d}})\sqrt{|d|}}{h(\cancel{d})} = \begin{cases} \dfrac{w}{2\pi} & (D<0) \\ \log \varepsilon_D^+ . & (D>0) \end{cases}.$$

Example.

Take $D=-163$ so that $L(1,\chi_D) = \prod_p \left(1-\left(\frac{D}{p}\right)\cdot\frac{1}{p}\right)^{-1}$.

Then $L(1,\chi_{-163}) = \frac{2}{2\pi}\cdot\frac{1}{\sqrt{163}} = .02493\ldots$

So $L(1,\chi_{-163})^{-1} = 40.109\ldots$

What is

$$\Big(1-\underbrace{\left(\tfrac{-163}{2}\right)}_{-1}\cdot\tfrac{1}{2}\Big)\cdot\Big(1-\underbrace{\left(\tfrac{-163}{3}\right)}_{-1}\cdot\tfrac{1}{3}\Big)\cdot\Big(1-\left(\tfrac{-163}{5}\right)\cdot\tfrac{1}{5}\Big)\cdot\ \cdots\cdots$$

$$= \underbrace{(1+\tfrac{1}{2})(1+\tfrac{1}{3})(1+\tfrac{1}{5})(1+\tfrac{1}{7})\cdots(1+\tfrac{1}{37})}_{4.11}\cdots$$

We see this is a tall order.

Theorems: $h(D) \ll \sqrt{|D|}\log|D|$.

Expect a similar lower bound for negative D, but can't prove it.

14.2.

Question. For $D < 0$, how can we see $h(D) \asymp \sqrt{|D|}$ on average?

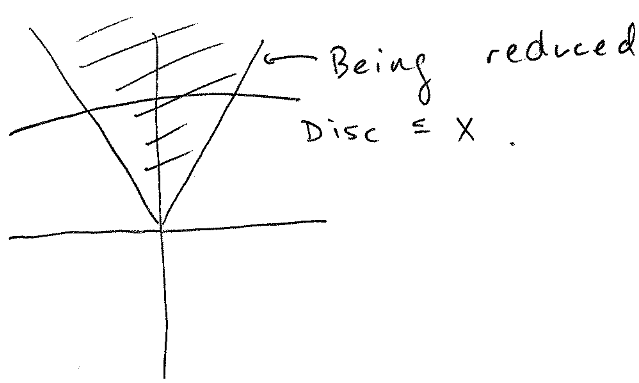
We have $\displaystyle\sum_{\substack{|D| \leq X \\ D<0}} h(D) \asymp X^{3/2}$. (Gauss)

To see this: We are counting

$$\left\{ (a,b,c) \in \mathbb{Z}^3 : \begin{array}{l} 0 < b^2 - 4ac < X, \\ |b| \leq a \leq c, \\ b \geq 0 \text{ if either } |b| = a \text{ or } a = c \end{array} \right\}.$$

The conditions
$\{ |b| \leq a \leq c,\ b \geq 0 \text{ if either } |b| = a \text{ or } a = c \}$ define a cone in $\mathbb{R}^3$.
This means that (a,b,c) in this set $\iff$ $\lambda(a,b,c)$ is for all $\lambda \in \mathbb{R}^+$.

Schematic:



Heuristic: Approximately equal to the volume.

$$\mathrm{Vol}(\{(a,b,c) \in \mathbb{R}^3 : 0 < b^2 - 4ac < X, \text{ is reduced}\})$$
$$= X^{3/2} \cdot \mathrm{Vol}(\{(a,b,c) \in \mathbb{R}^3 : 0 < b^2 - 4ac < 1, \text{ is reduced}\})$$
$$\asymp X^{3/2}.$$

But careful. This region is not compact.

(14.3) = 15.1

Return for now to lattice point counting questions.

Davenport's lemma.

Warmup. Suppose V is a convex region in the plane.

Theorem. $\Big|$ Area of V $-$ #lattice points of $V\Big|$

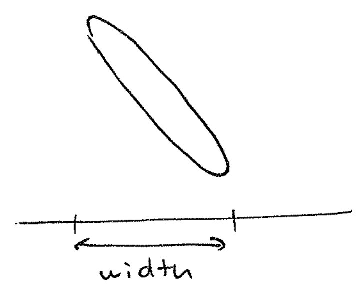
$\leq$ (width of V) + (height of V).

Definitions.

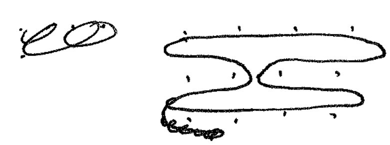
Convex means that if $z_1, z_2 \in V$ then so is $\lambda z_1 + (1-\lambda) z_2$ for any $\lambda \in (0,1)$.

Here we will need less.

Width and height are the lengths of the projections.



The hypotheses are necessary!



We will give a proof of this with an eye to its generalization.

Notation. $f(x,y)$ = char. fn. of V.

So, we are interested in bounding

$$\Big| \int_x \int_y f(x,y)\,dx\,dy - \sum_x \sum_y f(x,y) \Big|.$$

(14.4) = 15.2

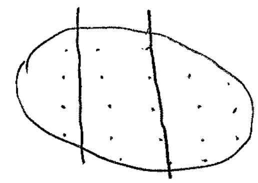
The one-dimensional version.

If V is ~~compact~~ convex, $f(x)$: char fn. of V, then

$$\left| \int_X f(x)\,dx - \sum_X f(x) \right| \leq 1. \quad \text{(obvious)}.$$

Apply this. For fixed x_0,

$$\left| \int dy\, f(x_0, y) - \sum_Y f(x_0, y) \right| \leq 1.$$



So,

$$\left| \int dx \int dy\, f(x,y) - \sum_Y \int_X f(x,y)\,dx \right| \leq \text{width},$$

where width means the length of the projection onto the x-axis.

very important!

In Davenport's notation,

$$\left| \int dx \int dy\, f(x,y) - \sum_Y \int_X f(x,y)\,dx \right| \leq \int_X f(x)\,dx$$

where $f(x) = \begin{cases} 1 & \text{if there is some } y \text{ with } f(x,y) = 1 \\ 0 & \text{otherwise.} \end{cases}$

Careful. This involves an abuse of notation.

The function "remembers" which coordinate x was.

Will write $f(y)$ with a different meaning.

(14.5) = 15.3.

But, we also have

$$\left|\sum_y \int_x f(x,y)\,dx - \sum_x \sum_y f(x,y)\right|$$

$$\leq \sum_y \left| \int_x f(x,y)\,dx - \sum_x f(x,y)\right|$$

(bounded by 1, and 0 if both sides are 0.

$$\leq \sum_y f(y) \leq \text{height} + 1.$$

So total difference $\leq$ width + height + 1.

Q. Do we need convexity?

No, only really used that $\left|\int_x f(x)\,dx - \sum_x f(x)\right| \leq 1$.

Can replace with h if we don't mind powers of h.

This will happen if $f(x)$ is defined by a bunch of polynomial inequalities.

This works in higher dimension.

Get an induction argument that will be presented next time.

15.4. The <u>full argument</u>.

Given a region R in $\mathbb{R}^n$, closed and bounded. Assume:

(1) Any line parallel to a coord. axis intersects R in at most h intervals.

(2) Same is true for all <u>projections</u> of R onto coord. subspaces obtained by setting some coords to 0.

Then:

$$\cancel{\sum_{x\in R}} \left| \#\{x \in \mathbb{Z}^n \cap R\} - \mathrm{Vol}(R) \right| \le \sum_{m=0}^{n-1} h^{n-m} V_m,$$

<u>where</u>: V_m = sum of m-dim volumes of projections of R onto subspaces, obtained by setting coords. $= 0$. ($V_0 = 1$.)

Note: If convex then $h = 1$.

<u>Proof</u>. Induction.

For any <u>particular</u> x_1 we have (by hyp. for $n-1$)

$$\left| \int dx_2 \cdots \int f(x_1, \ldots, x_n)\, dx_n - \sum_{x_2} \cdots \sum_{x_n} f(x_2, \ldots, x_n) \right|$$

$$\le \sum_{r=0}^{n-2} h^{n-1-r} \sum_{\substack{i_1 < \cdots < i_r \\ i_1 \ge 2}} \int \cdots \int f(x_1, x_{i_1}, \ldots, x_{i_r})\, dx_{i_1} \cdots dx_{i_r}.$$

Here (as before) $f(x_1, x_{i_1}, \ldots, x_{i_r}) = 1$ or 0 depending on whether there are values of the other coords. making the argument 0.

15.5. Integrate w.r.t. x_1.

$$\left| \int \cdots \int f(x_1, \cdots, x_n)\, dx_1 \cdots dx_n - \sum_{x_2} \cdots \sum_{x_n} \int_{x_1} f(x_1, \cdots, x_n)\, dx_1 \right|$$

$$\leq \sum_{r=0}^{n-2} h^{n-1-r} \sum_{\substack{i_1 < \cdots < i_r \\ i_1 \geq 2}} \int dx_1 \int dx_{i_1} \cdots \int f(x_1, x_{i_1}, \cdots, x_{i_r})\, dx_{i_r}$$

$(m = r+1)$

$$= \sum_{m=1}^{n-1} h^{n-m} \sum_{\substack{j_1 < \cdots < j_m \\ j_1 = 1}} \int dx_{j_1} \cdots \int f(x_{j_1}, \cdots, x_{j_m})\, dx_{j_m}.$$

(Note: Fubini. Can rearrange anything.)

Also, (by hyp. for 1), for any particular $x_2, \cdots, x_n$,

$$\left| \int f(x_1, \cdots, x_n)\, dx_1 - \sum_{x_1} f(x_1, \cdots, x_n) \right| \leq h\, f(x_2, \cdots, x_n).$$

Sum over $x_2, \cdots, x_n$.

$$\left| \sum_{x_2} \cdots \sum_{x_n} \int f(x_1, \cdots, x_n)\, dx_1 - \sum_{x_1} \cdots \sum_{x_n} f(x_1, \cdots, x_n) \right|$$

$$\leq h \sum_{x_2} \cdots \sum_{x_n} f(x_2, \cdots, x_n)$$

$$\leq h \left[\int \cdots \int f(x_2, \cdots, x_n)\, dx_2 \cdots dx_n + \sum_{m=0}^{n-2} h^{n-1-m} \sum_{\substack{i_1 < \cdots < i_m \\ i_1 \geq 2}} \int dx_{i_1} \cdots \int f(x_{i_1}, \cdots, x_{i_m})\, dx_{i_m} \right]$$

$$= \sum_{m=0}^{n-1} h^{n-m} \sum_{\substack{i_1 < \cdots < i_m \\ i_1 \geq 2}} \int dx_{i_1} \cdots \int f(x_{i_1}, \cdots, x_{i_m})\, dx_{i_m}.$$

Add our two error terms! Get

$$\sum_{m=0}^{n-1} h^{n-m} \sum_{i_1 < \cdots < i_m} \int dx_1 \cdots \int f(x_{i_1}, \cdots, x_{i_m})\, dx_{i_m}.$$

QED.

16.1. The study of lattices.

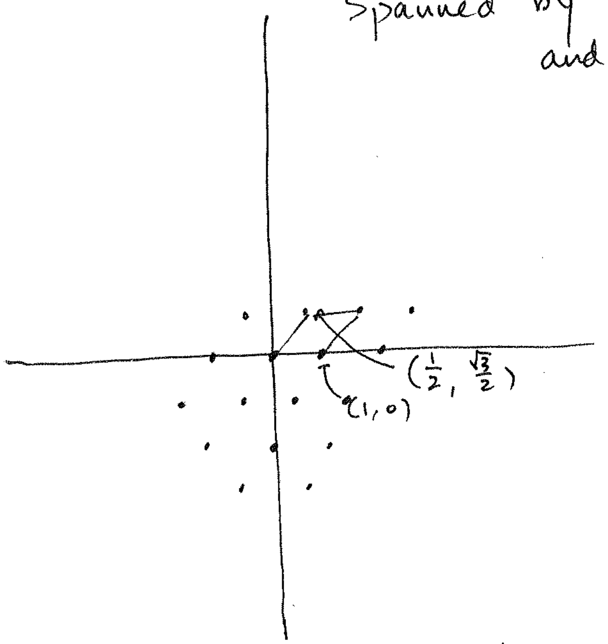
Cor. 1. Every prime $p \equiv 1 \pmod 4$ can be written as a sum of two squares.

Cor. 2. Every positive integer can be written as a sum of four squares.

What is a lattice? [Discussion]

Properties of lattices.

Spanned by $(1,0)$ and $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$.



Draw some more.

Discuss: what different properties do they have?

What theorems should they satisfy?

Let V be a real vector space of dim n.

Def. A lattice $\Lambda \subseteq V$ is an additive subgroup

$$\mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r, \text{ where the } e_i \text{ are linearly independent over } \mathbb{R}.$$

The e_i form a basis for the lattice.

It is full if $r = n$.

Example. $\mathbb{Z}\cdot(1,0) + \mathbb{Z}(\sqrt{2},0)$ is not a lattice.

Prop. Λ is a lattice iff it is free of rank n and $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = V$.

16.2. Volumes (or covolumes)

For any $\lambda_0 \in \Lambda$ (a full lattice) we have a fundamental parallelepiped

$$D_{\lambda_0} := \{ \lambda_0 + \sum_{i=1}^{n} a_i e_i \ , \quad 0 \le a_i < 1 \} .$$

A fundamental domain for Λ acting on $\mathbb{R}^n$ by addition.

Note: This depends on a choice of basis.

Def. The volume (covolume) of the lattice is $\mathrm{Vol}(D_{\lambda_0})$.

Def. 2. The volume of the lattice is $\mu(\mathbb{R}^n/\Lambda)$, where μ is Lebesgue measure on $\mathbb{R}^n$ and then induced to a quotient measure on $\mathbb{R}^n/\Lambda$.

Def. 3. Let $v_1, \dots, v_n$ be the standard basis for $\mathbb{R}^n$.

So, $\mathbb{Z}v_1 + \dots + \mathbb{Z}v_n$ has volume 1.

If $\Lambda = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_n$ with $e_i = \sum_{j=1}^{n} a_{ij} v_j$,

then $\mathrm{Vol}(\Lambda) = |\det(a_{ij})|$.

Prop. The volume does not depend on the choice of basis.

Proof. If also $\Lambda = \mathbb{Z}f_1 + \dots + \mathbb{Z}f_n$, then

$$\begin{bmatrix} f_1 \\ \vdots \\ f_n \end{bmatrix} = M \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} \quad \text{with } M \in GL_n(\mathbb{Z}) .$$

(Think about it!! It's a tautology.)

So, $\mathrm{Vol}(\Lambda) = |\det(M \cdot (a_{ij}))| = |\det(a_{ij})|$.

~~18.3.~~ 16.3 = 17.1.

Lemma. Let $S \subseteq V = \mathbb{R}^n$ measurable.

Λ full lattice in V.

If $\mu(S) > \mathrm{Vol}(\Lambda)$ then we can find $\alpha, \beta \in S$, $\alpha \neq \beta$, and $\beta - \alpha \in \Lambda$.

Proof. Think of this as obvious. (draw a picture)

(Prove the mapping $S \subseteq V \to V/\Lambda$ is not injective.)

A proof. Write $S = \bigcup_{\lambda_0 \in \Lambda} (S \cap D_{\lambda_0})$

By countable additivity $\mu(S) = \sum_{\lambda_0 \in \Lambda} \mu(S \cap D_{\lambda_0})$.

Now, $\sum_{\lambda_0 \in \Lambda} \mu((S \cap D_{\lambda_0}) - \lambda_0) = \mu(S) > \mathrm{Vol}(\Lambda)$.

This means, for some λ_0 and λ_0',

$(S \cap D_{\lambda_0}) - \lambda_0 \cap (S \cap D_{\lambda_0'}) - \lambda_0' \neq \phi$.

i.e. $\alpha - \lambda_0 = \beta - \lambda_0'$ for some $\alpha, \beta \in S$. QED.

Minkowski's lattice point theorem:

Let $\Lambda \subseteq \mathbb{R}^n$ be a full lattice.

Let $T \subseteq \mathbb{R}^n$ be a set which is

convex (when $\alpha, \beta \in T$, the line joining them is in T)

symmetric ($\alpha \in T \to -\alpha \in T$).

If $\mu(T) > 2^n \mathrm{Vol}(\Lambda)$, then T contains a nonzero $\lambda \in \Lambda$.

(16.4). = 17.2.
~~18.4. (=19)~~

Proof. Apply the lemma to the lattice $2\Lambda := \{2 \cdot v : v \in \Lambda\}$.
$\mathrm{Vol}(2\Lambda) = 2^n \mathrm{Vol}(\Lambda)$,
so if $\mu(T) > 2^n \mathrm{Vol}(\Lambda)$ there exist $\alpha, \beta \in T$ with
$\alpha - \beta \in 2\Lambda$.

By symmetry, $-\beta \in T$.
By convexity, $\frac{\alpha - \beta}{2} \in T$. It's also in Λ. Q.E.D.

Note. If T is compact, can prove for $\mu(T) \geq 2^n \mathrm{Vol}(\Lambda)$.
Can cook up counterexamples when less.

(ANT notes()

~~Ideals and lattices.~~

~~Let $[K : \mathbb{Q}] = n$.~~
~~Then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.~~
~~So is an ideal, because it's a submodule of $\mathcal{O}_K$.~~
~~So is a fractional ideal, because d times it is an ideal for some $d \in \mathbb{Z}$.~~

~~Want to regard it in $\mathbb{R}^n$.~~
~~Suppose K has r real embeddings $\sigma_1, \ldots, \sigma_r$ $K \hookrightarrow \mathbb{R}$~~
~~$2s$ complex ones $\sigma_{r+1}, \ldots \sigma_{r+s}$ and their complex conjugates.~~
~~$n = r + 2s$ by Galois theory.~~

~~Then define $\sigma : K \longrightarrow \mathbb{R}^r \times \mathbb{C}^s \xrightarrow{\sim} \mathbb{R}^n$ (as vector spaces)~~
~~(non-canonically!~~
~~$\mathbb{C} \xrightarrow{\sim} \mathbb{R}^2$~~
~~$1 \longrightarrow (1, 0)$~~
~~$i \longrightarrow (0, 1)$.)~~

~~$\alpha \longrightarrow (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \ldots, \sigma_{r+s}(\alpha))$.~~

(16.5) = 17.3.

Extensions and generalizations.

1. In our lemma, ~~we can find~~ suppose $\mu(S) > m \operatorname{Vol}(\Lambda)$.
Then we can find $q_1, \dots, q_{m+1} \in S$ all nonequal s.t.
$q_i - q_j \in \Lambda$ for all i, j.

And, in Minkowski, given Λ, T as before.
If $\mu(T) > m \cdot 2^n \operatorname{Vol}(\Lambda)$
then T contains at least m pairs of points $\pm q_i$
distinct from each other and zero.

2. We can replace our inequalities with equalities
if S (T) is compact.

Representations by quadratic forms.

Theorem. Every prime $p \equiv 1 \ (4)$ is a sum of two squares.

Lemma. Consider the set of integer points $\vec{u} = (u_1, \dots, u_n) \in \mathbb{Z}^n$
satisfying

$$\sum_{1 \le j \le n} a_{ij} u_j \equiv 0 \pmod{k_i}$$

for positive integers $k_1, \dots, k_m$
integers a_{ij}.
Then this is a complete lattice Λ with
$$\operatorname{Vol}(\Lambda) \le k_1 k_2 \cdots k_m.$$

17.4.

Proof. (Sketch. Will come back and be rigores)

Note that $\mathbb{Z}^n \supseteq \Lambda \supseteq (\prod k_i)\mathbb{Z}^n$.

Imagine this as being enough.

Proof of theorem.

We know that $\left(\frac{-1}{p}\right) = 1$, i.e. there is some a with $a^2 + 1 \equiv 0 \pmod p$.

Consider the set of integers $(x, y) \in \mathbb{Z}^2$ with
$$y \equiv ax \pmod p.$$
Lattice of volume $\leq p$.

So, by Minkowski, there is a point of Λ in the disc
$$D : \{(x, y) : x^2 + y^2 < 2p\}$$
of volume $2\pi p > 2^2 \operatorname{Vol}(\Lambda)$.

So there are integers x, y not both 0,
$$y \equiv ax \pmod p$$
$$x^2 + y^2 < 2p.$$

But $\pmod p$,
$$x^2 + y^2 \equiv x^2 + a^2 x^2$$
$$\equiv x^2 - x^2 \equiv 0.$$

So $p \mid x^2 + y^2$ and so $x^2 + y^2 = p$.

Exercise. Extend to show:

A positive integer is a sum of two squares if it is not divisible by a prime $p \equiv 3 \pmod 4$.

17.5.

Thm (Legendre) Every positive m is a sum of four squares.

Proof. WLOG $m = p_1 \cdots p_q$ with distinct primes p_i.

Claim. For every prime p, there are a_p and b_p with
$$a_p^2 + b_p^2 + 1 \equiv 0 \pmod p.$$

Proof. (for $p \geq 3$) The sets $\{a^2 : a \pmod p\}$

$\{-1 - b^2 : b \pmod p\}$

each contain $\frac{p+1}{2}$ elts. (mod p) and hence overlap.

Now, for each $p = p_i$ from $i = 1$ to q, consider the $\vec{u} = (u_1, \dots, u_4)$ satisfying
$$u_1 \equiv a_p u_3 + b_p u_4 \pmod p$$
$$u_2 \equiv b_p u_3 - a_p u_4 \pmod p.$$

Intersection of all is a lattice Λ of det $\leq m^2$.

So, there is a nonzero lattice point of Λ in the set
$$\{x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2m\}$$
of volume $\frac{1}{2}\pi^2 (2m)^2 > 2^4 m^2 \geq 2^4 \operatorname{Vol}(\Lambda)$.

Call it $\vec{u} = (u_1, u_2, u_3, u_4)$ and then
$$u_1^2 + u_2^2 + u_3^2 + u_4^2 \equiv (a_p u_3 + b_p u_4)^2 + (b_p u_3 - a_p u_4)^2$$
$$\equiv (a_p^2 + b_p^2 + 1) u_3^2 + (a_p^2 + b_p^2 + 1) u_4^2$$
$$\equiv 0 \pmod p.$$

Done as before.