Spring 2014. The geometry of numbers.

Warmup problem #1. Sums of two squares.

Arithmetic (mention)

Multiplicities: Can write $13 = x^2 + y^2$ for 8 pairs (x, y).

$65 = x^2 + y^2$ for 16.

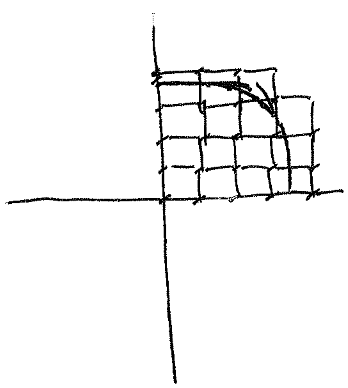
67 in none.

Let $r_2(n)$ = # ways to write n as two squares.

Q. What is $\sum_{n \le N} r_2(n)$? average # of ways?

Same as $\{(x, y) \in \mathbb{Z}^2 : x^2 + y^2 \le N\}$.

Let's estimate this: points inside a circle. $N = 14$



We see:

$$\#\{(x,y) \in \mathbb{Z}^2 : x^2 + y^2 \le N\}$$

$$\sim \text{Area}\{(x,y) \in \mathbb{R}^2 : x^2 + y^2 \le N\}$$

$$= \pi \cdot N.$$

Can we make this rigorous?

0. Assume N is not itself a sum of two squares. (HW: explain what changes)

Get an upper bound:

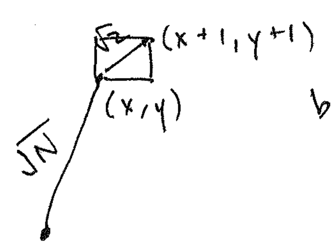
(1) Associate ~~the~~ a unit square to each point:

$$(x, y) \longleftrightarrow [x, x+1] \times [y, y+1].$$

If a circle of radius M contains the whole square, then it certainly contains (x, y).

How big must M be?

If $M \ge \sqrt{N} + \sqrt{2}$ then the circle of radius M will contain the whole box.



Every point in the box is within $\sqrt{N} + \sqrt{2}$ of origin.

1.2.

So: The circle of radius $\sqrt{N}+\sqrt{2}$ contains the box $[x, x+1] \times [y, y+1]$ for each (x,y) with $x^2+y^2 \le N$.

That means,

$$\#\{(x,y) \in \mathbb{Z}^2 : x^2+y^2 \le N\}$$

$$= \#\{\text{boxes } [x,x+1]\times[y,y+1] : (x,y)\in\mathbb{Z}^2,\ x^2+y^2 \le N\}$$

$$= \mathrm{Vol}\left(\{\text{Boxes } [x,x+1]\times[y,y+1] : (x,y)\in\mathbb{Z}^2,\ x^2+y^2 \le N\}\right)$$

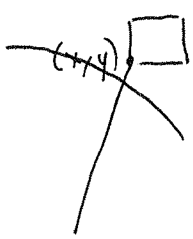
$$\le \mathrm{Vol}(\text{circle of radius } \sqrt{N}+\sqrt{2})$$

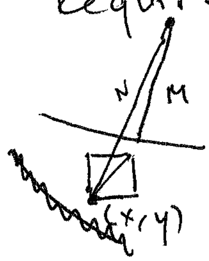
$$= \pi\left(N + 2\sqrt{2}\cdot\sqrt{N} + 2\right).$$

How to get a lower bound? Demand that the boxes $[x,x+1]\times[y,y+1]$ contain the entire circle (with its interior) of radius M.

Here, worry about x or y negative.

Require $M \le \sqrt{N}-\sqrt{2}$.





$$\text{So } \#\{(x,y)\} = \mathrm{Vol}(\{\text{Boxes}\})$$

$$\ge \mathrm{Vol}(\text{Circle of radius } \sqrt{N}-\sqrt{2})$$

$$= \pi\left(N - 2\sqrt{2}\sqrt{N} + 2\right).$$

Notation: $\#\{(x,y)\} = \pi N + O(\sqrt{N})$.

1.3.

Moral:

(1) {# lattice points} $\sim$ Volume

(2) Error $\ll$ Circumference

(or, equivalently, length of projections).

(3) Used convexity of the region.

(4) Points corresponded nicely to boxes of area 1.

Later:

* How many $\{(x,y)$ with $x^2+y^2 \le N$, $x^2+y^2 \equiv 2 \pmod 7\}$?
* Does this work for ellipses? Other shapes? Higher dimensions?
* Can we get a better error term?
* Connection to L-functions,

$$\frac{1}{4}\sum_{(x,y)\neq(0,0)} (x^2+y^2)^{-s} = \zeta_{\mathbb{Q}(i)}(s) = \zeta(s)\cdot L(s,\chi_{-4}).$$

Warmup 2. The divisor function.

Def. The divisor function $d(n)$ is the # of positive divisors of n.

ex. $d(7)=2$, $d(24)=8$, $d(25)=3$.

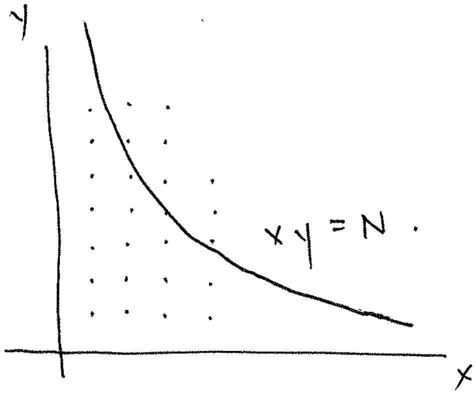
Ask the same questions. How big can $d(n)$ get? (Big.)

And, what is $\sum_{n\le N} d(n)$?

Here, $d(n) = \#\{(x,y) : x,y \ge 1,\ x\cdot y = n\}$

So $\sum_{n\le N} d(n)$ is the number of lattice points (x,y) with $x,y\ge 1$ and $x\cdot y \le N$.

1.4. In other words we want to bound the number of lattice points within the hyperbola



$$\text{Volume} = \int_{x=0}^{\infty} \int_{y=0}^{N/x} dy\, dx$$

$$= \int_{x=0}^{\infty} \frac{N}{x}\, dx$$

$$= N\log(\infty) - N\log(0).$$

[uh....]

Now. We would be ~~bette~~ smater to look at

$$\int_{x=1}^{\cancel{\infty} N} \int_{y=1}^{N/x} dy\, dx = \int_{x=1}^{N} \left(\frac{N}{x} - 1\right) dx$$

$$= \Big[N\log(x) - x\Big]_{x=1}^{N}$$

$$= N\log(N) - (N+1).$$

That first term is right.

Let's be rigorous:

$$\sum_{n \le N} d(n) = \sum_{e \cdot f \le N} 1$$

$$= \sum_{e \le \sqrt{N}} \sum_{f \le \frac{N}{e}} 1 + \sum_{f \le \sqrt{N}} \sum_{e \le \frac{N}{f}} 1 - \sum_{e \le \sqrt{N}} \sum_{f \le \sqrt{N}} 1.$$

The third term is $\lfloor \sqrt{N} \rfloor^2$, between $\underbrace{(\sqrt{N}-1)^2}_{N - 2\sqrt{N} + 1}$ and $\underbrace{(\sqrt{N})^2}_{N}$.

The first two are the same.

(ctd.)

1.5.

We have $\sum_{f \le \frac{N}{e}} 1 = \frac{N}{e} + \text{Error} \qquad |\text{Error}| < 1.$

So, make an error bounded by $2\sqrt{N}$ and get

$$\sum_{e \le \sqrt{N}} \frac{N}{e} = N\left[\log\sqrt{N} + \gamma + O\left(\frac{1}{\sqrt{N}}\right)\right]$$

$\gamma = .5772\cdots$ Euler's constant.

and so

$$\sum_{n \le N} d(n) = 2N\left(\log\sqrt{N} + \gamma + O\left(\frac{1}{\sqrt{N}}\right)\right) - N + \underbrace{O(\sqrt{N})}_{\text{bounded this by } 6\sqrt{N}}$$

$$= N \log N + (2\gamma - 1)\cdot N + O(\sqrt{N}).$$

[Wax philosophical if time.]

2.1. The circle problem.

Last time:

$$\#\{(x,y) \in \mathbb{Z}^2 : x^2 + y^2 \le M\} = \pi \cdot M + O(\sqrt{M}).$$

Observations:

(1) This should, and does generalize.

Thm. (Davenport, 1950) Given a region $R \subseteq \mathbb{R}^n$ satisfying:

(a) Any line parallel to one of the coordinate axes intersects R in a set of points which, if not empty, consists of at most h intervals.

(b) The same is true (with m in place of n) for any of the m dimensional regions obtained by projecting R on one of the coordinate spaces defined by equating $n-m$ coordinates to 0, for all m with $1 \le m \le n-1$.

Then:

$$\left| \#(\text{lattice pts in } R) - \mathrm{Vol}(R) \right| \le \sum_{m=0}^{n-1} h^{n-m} V_m,$$

where: V_m is the sum of the m dimensional volumes of R on the coordinate spaces obtained by equating any $n-m$ coordinates to zero. (And $V_0 = 1$.)

2.2.

Write:

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

$$= \frac{1}{4}\sum_{\substack{x\in\mathbb{Z}[i]\\ x\neq 0}} N(x)^{-s}$$

$$= \sum_{\underline{a}\triangleleft\mathbb{Z}[i]} N(\underline{a})^{-s}. \qquad (\text{Here } 4 = |\mathbb{Z}[i]^\times|.)$$

$$\chi_{-4}(n) = \left(\frac{-4}{n}\right) = \begin{cases} 1 \text{ if } & n\equiv 1 \pmod 4)\\ -1 \text{ if } & n\equiv -1 \pmod 4)\\ 0 \text{ if } & n\equiv 0,2 \pmod 4)\end{cases}$$

$$L(s,\chi_{-4}) = \sum_{n\geq 1}\chi_{-4}(n)\,n^{-s} = 1 - 3^{-s} + 5^{-s} - 7^{-s} + \cdots$$

$$\zeta(s) = \sum_{n\geq 1} n^{-s} = 1 + 2^{-s} + 3^{-s} + 4^{-s} + \cdots$$

Theorem. $\zeta_{\mathbb{Q}(i)}(s) = \zeta(s)\,L(s,\chi_{-4})$.

We have

$$\#\{(x,y)\neq(0,0) : x^2+y^2\leq N\}$$

$$= \int_{2-i\infty}^{2+i\infty}\Big(\sum_{(x,y)\neq(0,0)}(x^2+y^2)^{-s}\Big)N^s\frac{ds}{s} \quad (\text{Perron})$$

$$= \int_{2-i\infty}^{2+i\infty} 4\cdot\zeta_{\mathbb{Q}(i)}(s)\,N^s\frac{ds}{s}$$

$$= 4\cdot\Big(\operatorname*{Res}_{s=1}\zeta_{\mathbb{Q}(i)}(s)\Big)\cdot N + O(N^{1/3+\varepsilon}),$$

2.3.

Now $$\operatorname*{Res}_{s=1} \zeta_{\mathbb{Q}(i)}(s) = \underbrace{\operatorname*{Res}_{s=1} \zeta(s)}_{\text{This is } 1} \cdot L(1, \chi_{-4}).$$

If you buy all this, use the fact that

$$L(1, \chi_{-4}) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots = \frac{\pi}{4}.$$

(Taylor series for arctan).

Theorem. (Dirichlet's class number formula: $D<0$ case)
If $D<0$ is a fundamental discriminant, then

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

We will prove it, using GON. (First we will learn what it means.)

Also the real case, which involves a regulator.

* The divisor problem. [1.4 and 1.5].

2.4.

Def. An integral binary quadratic form is an expression of the form

$$ax^2 + bxy + cy^2 .$$

a, b, c integers
x, y variables

Questions. Which integers does it represent?

e.g. $x^2 + y^2$: already discussed this.

$x^2 - y^2$: Similar to divisor problem.
$(x-y)(x+y)$

$5x^2 + 7xy + 13y^2$. (??)

Def. Given $ax^2 + bxy + cy^2$: (i.e. fix a, b, c)

(1) It is positive definite if it only represents ~~positive~~ nonnegative numbers.

(2) Its discriminant is $b^2 - 4ac$.

Easy exercise.

(1) It is positive definite $\longleftrightarrow$ $D = b^2 - 4ac \leq 0$ and it represents at least one positive number.

(2) It has a multiple root if and only if $D = 0$.

(3) The discriminant is always $\equiv 0, 1 \pmod 4$.

(4) Can a form be indefinite but represent only positive integers when $x, y \in \mathbb{Z}$?

Binary quadratic forms. (Sources: Cox, Granville)

Define as $ax^2 + bxy + cy^2$.

A function $\mathbb{Z}^2 \to \mathbb{Z}$ or $\mathbb{C}^2 \to \mathbb{C}$. (not a homomorphism)
$\mathbb{R}^2 \to \mathbb{R}$ etc.)

Representations.

An integer m is represented by f if there are ~~coprime~~ x and y with $f(x,y) = m$.
It is properly represented if there are coprime x and y.

Example. $x^2 + 5y^2$ represents 20, but not properly.

Equivalence (the lowbrow version).

Def. Two forms $f(x,y)$ and $g(x,y)$ are properly equivalent if there are $\alpha, \beta, \gamma, \delta$ with

$$f(x,y) = g(\alpha x + \beta y, \gamma x + \delta y)$$

and $$\alpha\delta - \beta\gamma = 1.$$

(Lose "properly": allow -1.)

Example. Let $g(x,y) = x^2 + 5y^2$.
Let
$$\begin{aligned} f(x,y) &= g(x, 3x+y) \\ &= x^2 + 5\cdot(3x+y)^2 \\ &= 46x^2 + 30xy + 5y^2. \end{aligned}$$

Then $f \sim g$.

Proposition. Proper equivalence is an equivalence relation.

Proof. (1) $f \sim f$. Clear.

(2) Suppose $f(x,y) = g(\alpha x + \beta y, \gamma x + \delta y)$ $\quad \alpha\delta - \beta\gamma = 1$.

Then, $f(\delta x - \beta y, -\gamma x + \alpha y)$

$$= g(\alpha(\delta x - \beta y) + \beta(-\gamma x + \alpha y), \gamma(\delta x - \beta y) + \delta(-\gamma x + \alpha y))$$

$$= g([\alpha\delta - \beta\gamma]x, [\alpha\delta - \beta\gamma]y) = g(x,y)$$

and $\delta\alpha - (-\beta)(-\gamma) = 1$.

(3) Now suppose $f(x,y) = g(\alpha x + \beta y, \gamma x + \delta y)$ $\quad \alpha\delta - \beta\gamma = 1$

$g(x,y) = h(rx + sy, tx + uy)$ $\quad ru - st = 1$

Then, (ugh) do it yourself.

Proposition. If f and g are properly equivalent, then they represent the same integers.

Proof. Suppose $f \sim g$ so that $f(x,y) = g(\alpha x + \beta y, \gamma x + \delta y)$. Suppose f represents m, i.e. $f(X,Y) = m$ for some integers X, Y.

Then $g(\alpha X + \beta Y, \gamma X + \delta Y) = m$ and so we are done.

Similarly, if g represents m, then f does, because it's an equivalence relation.

3.3.1

Equivolence (the highbrow version).

Def. $SL_2(\mathbb{Z})$ is the set of 2×2 metrices $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ with

deteminant $\alpha\delta - \beta\gamma = 1$.

Prop. $SL_2(\mathbb{Z})$ is a group.

Proof. * matrix mult. is associative

* inverse $\begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix}$ also in $SL_2(\mathbb{Z})$.

Prop. There is a right action of $SL_2(\mathbb{Z})$ on BQFs given by

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

Remorks. (1) Think of BQFs as functions $\mathbb{Z}^2 \to \mathbb{Z}$, naturol to represent elements of $\mathbb{Z}^2$ as column vectors.

(2) what is being claimed is that

(a) $f \circ I_2 = f$. (trivial)

(b) $(f\circ g)\circ g' = f \circ (gg')$

(3) There is not a left action. Suppose we wrote $g \circ f$ instead of $f \circ g$. Then, would have

$$(gg')\circ f = g' \circ (g \circ f). \qquad [\text{UGH.}]$$

Writing actions on the right corresponds to contravariance.

Proof. (of 2b)

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

3.4. Idea: Follows directly from the fact that $SL_2(\mathbb{Z})$ acts on $\mathbb{Z}^2$.

Exercise. For an example, verify you do get a right action and not a left one.

Disadvantage of highbrow approach:

Lots of parentheses. Eyes can glaze over.

Advantage: Immediate that equivalence is an equiv. rel'n.

Question. Are all BQFs equivalent?

Definition. The discriminant of a binary quadratic form $ax^2 + bxy + cy^2$ is $D = b^2 - 4ac$.

Proposition / Exercise.

If $f(x,y) = g(\alpha x + \beta y, \gamma x + \delta y)$ then

$$\mathrm{Disc}(f) = (\alpha\delta - \beta\gamma)^2 \, \mathrm{Disc}(g).$$

To say exactly the same thing:

If $f = g \circ \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$, then

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

In particular, if $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in SL_2(\mathbb{Z})$ then $\mathrm{Disc}(f) = \mathrm{Disc}(g)$.

But. This is not required.

Example. Let $g(x,y) = x^2 + y^2$, $\mathrm{Disc}(g) = -4$.

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix}.$$

Then $\left(g \circ \begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix}\right)\begin{pmatrix} x \\ y \end{pmatrix} = g\left(\begin{pmatrix} 2x \\ 5y \end{pmatrix}\right) = 4x^2 + 25y^2$.

$\mathrm{Disc}(g) = -400$.

$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$. $\left(g \circ \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}\right)\begin{pmatrix} x \\ y \end{pmatrix} = g(x + 2y, 0)$

$= (x+2y)^2 = x^2 + 4xy + 4y^2$

$\mathrm{Disc} = 0$.

3.5.

Q. How many BQFs are there of discriminant -4?, up to equivalence

Ex. $2x^2 + 6xy + 5y^2$. Disc $= -4$.

Equivalent to

$$2(x-y)^2 + 6(x-y)y + 5y^2 \qquad \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x-y \\ y \end{pmatrix}$$

$$= 2x^2 - 4xy + 2y^2 + 6xy - 6y^2 + 5y^2$$

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

Equivalent to

$$2x^2 + 2x(y-x) + (y-x)^2$$

$$= 2x^2 + 2xy - 2x^2 + y^2 + x^2 - 2xy$$

$$= x^2 + y^2,$$ our old friend.

Can we always do this?

Guess. Given any discriminant D and form f of disc. D. Then any other form g of discriminant D is equivalent to f.

This is not true.

Example. $D = -20$.

Prove that $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ are not equivalent.