Geometry of Numbers

TCC module: Term 3 2024

Simon L Rydin Myerson

University of Warwick

For link to course webpage see `https://maths.fan`

Manin's conjecture, $x \cdot y = 0$

Idea of application

Corollary

$L^\perp$ has rank $n-d$ and $\det(L^\perp) = \det(L)$.

- $Z(N) = \#\{x, y \in \mathbb{Z}^n \setminus \{0\} : x \cdot y = 0, \|x\| \cdot \|y\| \le N\}$, let $L = L(x/\gcd(x))$.
- $\#\{y \in L^\perp : \|y\| \le \frac{N}{\|x\|}\} = (\frac{N}{\|x\|})^{n-d} \frac{\mathrm{Vol}(B(0;1))}{\det L}(1 + O_n(\frac{\lambda_{n-d}(L^\perp)}{N/\|x\|}))$ if $\frac{N}{\|x\|} > \lambda_d(L^\perp)$.
- WLOG $\|x\| \le \|y\|$. We will (eventually) prove that most lattices are 'balanced', in the sense that $\lambda_i(M) \asymp \det(M)^{1/\operatorname{rank}(M)}$. One has to be careful: for given constants in $\asymp$, a positive proportion of lattices violate this.
- So for $n \ge 3$, $Z(N)$ we will prove

$$\sum_{x \in \mathbb{Z}^n \setminus \{0\}, \|x\| \le N} (N/\|x\|)^{n-1} \frac{\gcd(x)}{\|x\|} \sim c_n N^{n-1} \log N$$

for some explicit $c_n > 0$.

- Different proofs were given by Franke-Manin-Tschinkel (89), Thunder (93), Robbiani (01), and Spencer (08). Morally speaking we follow Thunder.

Rational points

We can understand $x, y \in \mathbb{Z}^n \setminus \{0\} : x \cdot y = 0$ as rational points on a projective variety.
$\mathbb{P}^{n-1}$ has rational points $[x]$: $x \in \mathbb{Z}^n$, $(x_1, \ldots, x_n) = 1$, with height $h(P) = \|x\|$.
Moreover $\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}$ has rational points

$$\{([x],[y]) : x, y \in \mathbb{Z}^n, \gcd(x) = \gcd(y) = 1\},$$

with height $\|x\| \cdot \|y\|$.
The equation $x \cdot y = 0$ defines a hypersurface H in $\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}$, with the number of points of height $\leq N$ given by

$$\frac{1}{4}\#\{x, y \in \mathbb{Z}^n : \gcd(x) = \gcd(y) = 1, \|x\| \cdot \|y\| \leq N\}$$

$$= \frac{1}{4} \sum_{d_1, d_2 \in \mathbb{N}} \mu(d_1)\mu(d_2) Z(N/d_1 d_2).$$

Here $\mu(d) = \pm 1$ is the Möbius function, and the proof uses the identity $\sum_{d|m} \mu(d) = \mathbf{1}_{m=1}$ valid for $\|m\| \in \mathbb{Z} \setminus \{0\}$

The Manin-Peyre conjecture

$F = g(W(\mathbb{Q}))$, $g : W \to V$ degree ≥ 2

$T = C \cup F$, C = Zariski closed proper subset of $V(\mathbb{Q})$

Conjecture

Let V be a Fano variety and let H be an anticanonical height on $V(\mathbb{Q})$. There is a thin subset $T \subset V(\mathbb{Q})$ such that

$$\#\{P \in V(\mathbb{Q}) \setminus T : H(P) \leq X\} \sim c_{MP} X (\log X)^{\operatorname{rank} \operatorname{Pic}_{\mathbb{Q}}(V) - 1},$$

for a certain explicit constant $c_{MP} \geq 0$.

E.g. for a hypersurface in $\mathbb{P}^{n-1}$, $H([x]) = \|x\|^{n - \deg V}$.

$N^{r-1} \log N$

Rational points: a heuristic

Let $\vec{f}(\vec{x}) \in \mathbb{Z}[x_1, \ldots, x_n]^R$ be a system of homogeneous forms. Let $V(\vec{f}) \subset \mathbb{P}^{n-1}$ be the zero locus. Rational points: $(x_1, \ldots, x_n) = 1$, $\vec{f} = \vec{0}$ with height $h(P) = \|x\|$.

We assume $V(\vec{f})$ is irreducible$/\overline{\mathbb{Q}}$, and that the f_i generate $I(V(\vec{f}))$.

Let $U \subset V(\vec{f})$ be a sufficiently small Zariski open subset. Define

$$M(B) = \text{measure}\{\vec{t} \in \mathbb{R}^n : \|\vec{f}(\vec{t})\| \leq 1\}.$$

$, \|t\| \leq B$

1. If $M(B) \ll 1$ as $B \to \infty$, we hope:

    - The degree of $V(\vec{f})$ is large and/or its dimension is small,
    - The number of rational points on U is finite.

$|x^k + y^k + z^k| \leq 1$

$k > 3$

Rational points heuristically, II

2. If $M(B) \to \infty$ but $M(B) \ll_\epsilon B^\epsilon$ as $B \to \infty$, we hope:
   - $V(\vec{f})$ has some kind of group structure,
   - $\{P \in U(\mathbb{Q}) : h(P) \leq B\} \sim C(\log B)^{r/2}$ for suitable $C \geq 0$, $r \in \mathbb{N}$, h.
3. If for some $\delta > 0$ we have $M(B) \gg B^\delta$ as $B \to \infty$, we hope:
   - The degree of $V(\vec{f})$ is small and/or its dimension is large,
   - $\{P \in U(\mathbb{Q}) : h(P) \leq B\} \sim CB(\log B)^{r-1}$ for suitable C, r, h.

The Hardy-Littlewood heuristic

- $\vec{f}(\vec{x}) \in \mathbb{Z}[x_1, \ldots, x_s]^R$ will be a system of R homogenous forms of degrees d_i in $s > 2\sum d_i$ variables with integer coefficients.
- We assume: $\vec{\alpha} \cdot \vec{f} = \sum^R \alpha_i F_i$ is nonzero and indefinite for all $\vec{\alpha} \in \mathbb{R}^R \setminus \{\vec{0}\}$.
- We study $Z_{\vec{f}}(B) = \#\{\vec{x} \in \mathbb{Z}^s : \vec{f}(\vec{x}) = \vec{0}, \|\vec{x}\| \leq B\}$.

Heuristic

- Model $\vec{x}$ by a random real vector $\vec{X}$, and model $f_i(\vec{x})$ by $\lfloor f_i(\vec{X}) \rfloor$.
- That is, let $\vec{X}$ be a uniform random variable on $[-B, B]^s$. Maybe $Z_{\vec{f}}(B) \sim (2B)^s \cdot \mathbb{P}[\vec{f}(\vec{X}) \in [0,1)^R]$, which is typically $\sim c_{\vec{f}} B^{s - 2\sum d_i}$.
- But: if $R = 1$, $f(\vec{x}) = x_1^2 + x_2^2 - 3x_3^2$, then $Z_f(B) = 1$.
- Fix: let $\vec{X}_p$ be uniformly distributed on $\mathbb{Z}_p^s$. Predict

$$Z_{\vec{f}}(B) - 1 = (1 + o(1))(2B)^s \cdot \mathbb{P}[\vec{f}(\vec{X}) \in [0,1)^R] \prod_p \lim_{N \to \infty} p^{nR} \mathbb{P}[p^N \mid \vec{f}(\vec{X}_p)].$$

Predict

$$Z_{\vec{f}}(B) - 1 = (1 + o(1))(2B)^s \cdot \mathbb{P}[\vec{f}(\vec{X}) \in [0,1)^R] \prod_p \lim_{N\to\infty} p^{nR}\mathbb{P}[p^N \mid \vec{f}(\vec{X}_p)].$$

$\sim$ const $\cdot B^{r-\Sigma d_i}$ some constant

Let V be a smooth projective variety in $\mathbb{P}^n_{\mathbb{Q}}$ defined by $f_1 = \cdots = f_r = 0$.

We can assume that f_i has integral coefficients with gcd 1. Then V has a reduction mod p, a variety V_p in $\mathbb{P}^n_{\mathbb{F}_p}$.

Let N_p be the number of $\mathbb{F}_p$-points on V_p. The natural guess for N_p is that it is roughly $p^{\dim V}$. Indeed one could project onto the first D co-ordinates and in some sense this gives a way to parametrise most of the points on V_p.

For all but finitely many p, we have $\lim_{N\to\infty} p^{nR}\mathbb{P}[p^N \mid \vec{f}(\vec{X}_p)] = N_p/p^{\dim V}$.

If the product $\prod N_p/p^{\dim V}$ diverges, we actually have a natural way to correct this prediction too.

$$\int \prod_p c_p \left(1 - \frac{1}{p^s}\right) \Rightarrow \int \prod \left(1 - \frac{1}{p^s}\right) L(s,p)$$

where $L(1,p) = c_p$

$$\#\{n \le N\} \approx \int_{1 - i\sigma + 1}^{1 + i\infty + 1} \zeta(s)(\cdot)\, ds \quad f(s) = \sum_N n^{-s} = \prod \left(1 - \frac{1}{p^s}\right)$$

$$N \prod c_p = \infty$$

$$N (\log N)^{1/2}, \quad \zeta = 1(\cdot) - 1$$

An extra power of log

The following is an explanation of what is written in section 2.1 of `https://archive.mpim-bonn.mpg.de/id/eprint/2194/1/preprint_1993_79.pdf`, which assumes some slightly more technical maths (and is also in French). I will look around to see if there is a good introduction to some of these ideas.

We look at

$$F(s) = \prod_p \left(1 - p^{1-s}\frac{N_p - p^{\dim V}}{p^{\dim V}}\right)^{-1}.$$

This is well defined for $\Re s > 1$, where $\Re s$ is the real part. What is more, it is (up to a bounded multiplicative factor) the same as the “Artin L-function $L_S(s, \operatorname{Pic} V_{\bar{Q}})$ of the Picard group of $V_{\bar{Q}}$”, which has a meromorphic continuation to the whole complex plane. And, crucially, $L_S(s, \operatorname{Pic} V_{\bar{Q}})$ has a pole at $s = 1$ with multiplicity equal to the rank of $\operatorname{Pic} V_{\bar{Q}}$.

$Z(N) = \#\{x, y \in \mathbb{Z}^n \setminus \{0\} : x \cdot y = 0, \|x\| \cdot \|y\| \le N\}$, let $L = L(x/\gcd(x))$.

if $\|y\| < \|x\|$, swap x & y

$$Z(N) = \sum_{x \in \mathbb{Z}^n \setminus \{0\}, \|x\| \le \sqrt{N}} \#\{y : y \cdot x = 0, \|x\| \le \|y\| \le \sqrt{N}/\|x\|\}$$

$$+ \#\{y : y \cdot x = 0, \|x\| < \|y\| \le \sqrt{N}/\|x\|\}$$

Let $B(R) = \{y \in \mathbb{R}^n : \|y\| \le R\}$ or $\{y \in \mathbb{R}^n : \|y\| < R\}$, let $\gcd(z) = 1$.

$$\#L(z)^{\perp} \cap B(R) = \frac{\mathrm{Vol}(B(R))}{\|z\|} + O(1 + \frac{R}{\lambda_1(L(z)^{\perp})})^{n-1}$$

$$\sum_{\|z\| \le \sqrt{N}/g, \gcd(z)=1} \#L(z)^{\perp} \cap D(N/d\|z\|)$$
$$- \sum_{\|z\| \le \sqrt{N}/g, \gcd(z)=1} \#L(z)^{\perp} \cap D(d\|z\|)$$