IWORP '24 Notes

Niven Achenjang

November 2024

These are notes on talks given in "Instructional workshop on rational points" which took place at Groningen. Unfortunately for the reader, these notes are live-texed and so their quality is upper bounded both by my (quite) limited ability to understand the material in real time and by my typing speed. With that in mind, they are doubtlessly missing content/insight present in the talks and certainly contain confusions not present in the talks. Despite all this, I hope that you can still find some use of them. Enjoy and happy mathing.

The website for this seminar is available here.

Contents

List of Figures

List of Tables

1 Bianca Viray (University of Washington): Algebraic points on curves

1.1 Lecture 1 (11/4)

Note 1. Slide talk, so we'll see how note taking goes...

(Upcoming preprint with Balcik, Chan, and Liu)

Theorem 1.1.1 (Mordell conjecture, Faltings 1983)**.** *Let C be a nice curve over a number field k. If $g(C) \geq 2$, then $C(k)$ is finite.*

Slogan. Geometry controls arithmetic!

Remark 1.1.2. $C(k)$ reveals very little about C as a whole. Can't hope to understand all of the arithmetic of C by looking just at the rational points over a fixed number field. ◦

Question 1.1.3 (Main)**.** *Can we understand the arithmetic of all of C, e.g. $G_k \curvearrowright C(\overline{k})$?*

Today focused on definitions and perspectives, not proofs.

Example 1.1.4 ($C = \mathbb{P}^1$)**.** $\mathbb{P}^1(\overline{k}) = \mathbb{A}^1(\overline{k}) \cup \{\infty\} = \overline{k} \cup \{\infty\} \curvearrowleft G_k$. Over k, can't distinguish points in a Galois orbit,

$$\mathbb{P}^1(\overline{k}) = \{\infty\} \cup \bigcup_{d \in \mathbb{N}} \left\{\alpha \in \overline{k} \colon \#(G_k \cdot \alpha) = d\right\}.$$

In other words,

$$\mathbb{P}^1(\overline{k}) = \{\infty\} \cup \bigcup_{d \in \mathbb{N}} \bigcup_{f \in k[x] \text{ irred, deg } d} \{\alpha \in \overline{k} : f(\alpha) = 0\}.$$

Closed points on $\mathbb{P}^1_k$ are partitioned by their degree. Degree $d > 1$ points on $\mathbb{P}^1_k$ are parameterized by monic irreducible degree d polynomials in $k[x]$. Better put, degree d points on $\mathbb{P}^1_k$ are parameterized by homogeneous irreducible degree d polynomials in $k[x_0, x_1]$, modulo scaling. Note this sets in

$$\{\text{homogeneous degree } d \text{ polynomials in } k[x_0, x_1], \text{ modulo scaling}\} \sim \mathbb{P}^d(k).$$

This is the same as $\{\text{degree } d, \text{ 0-dimensional } k\text{-subschemes of } \mathbb{P}^1\} = \mathrm{Hilb}^d_{\mathbb{P}^1}(k)$. △

Remark 1.1.5. We'll go back and forth between the language of Galois orbits of $\overline{k}$-points and the language of closed points on C. ◦

Always have

$$\{\text{Degree } d \text{ points on } C\} \subset \mathrm{Hilb}^d_C(k).$$

Question 1.1.6 (Main, reformulated)**.** *Can we understand all (degree d) closed points of C? Maybe to start, how about a Zariski dense set of closed points?*

Example 1.1.7 ($C \colon y^2 = -2(x^2-2)(x^2-3)(x^2-2x-4)$)**.** Note this has a Zariski dense set of degree 2 (= quadratic) points, coming from the projection $C \to \mathbb{P}^1_k, (x, y) \mapsto x$.[1] This holds for the same reason for any hyperelliptic C. △

Example 1.1.8. Say there is a finite map $C \to \mathbb{P}^1$ of degree $d > 2$. The fibers are degree d subschemes. By Hilbert irreducibility, there's a Zariski dense subset of $\mathbb{P}^1(k)$ over which the fibers are irreducible, so degree d points on C are Zariski dense. △

[1] Faltings' theorem says $\#C(\mathbb{Q}) < \infty$, so most fibers must be irreducible

Definition 1.1.9. The density degree set is

$$\delta(C/k) \coloneqq \left\{ \begin{array}{c} d \in \mathbb{N} : \text{degree } d \text{ points on} \\ C \text{ are Zariski dense.} \end{array} \right\} \qquad \diamond$$

Example 1.1.8 shows that the Lüroth semigroup

$$\delta_{\mathbb{P}^1}(C/k) \coloneqq \left\{ \deg(C \to \mathbb{P}^1) : C \to \mathbb{P}^1 \text{ nonconstant} \right\}$$

is a subset of $\delta(C/k)$. Can the containment $\delta_{\mathbb{P}^1}(C/k) \subset \delta(C/k)$ be strict?

Keep in mind the containments

$$\{\text{degree } d \text{ points on } C\} \subset \left\{ \begin{array}{c} \text{degree } d, \text{ 0-dim'l} \\ \text{subschemes of } C \end{array} \right\} = \mathrm{Hilb}^d_C = \mathrm{Sym}^d_C \,.$$

Remark 1.1.10. If $d \in \delta(C/k)$, there is a positive dimensional $Z \subset \mathrm{Sym}^d_C$ with Zariski dense k-points (take the closure of the image of the degree d points). $\circ$

Question 1.1.11. *What are the positive dimensional $Z \subset \mathrm{Sym}^d_C$ with Zariski dense k-points?*

Note Sym^d_C parameterizes degree d effective divisors on C, so get map

$$\rho = \rho_d \colon \mathrm{Sym}^c_C \longrightarrow \mathrm{Pic}^d_C,$$

and Pic^d_C is an abelian variety if it has any rational points.

- Assume $\dim \rho(Z) = 0$.

  Then, Z is mapping to a point, so $Z \subset |D| \simeq \mathbb{P}^N$ for some $N \geq 1$ (note: $|D| \simeq \mathbb{P}^N$ b/c Z has a rational point). Note that there's always some $\mathbb{P}^1 \hookrightarrow \mathbb{P}^N \simeq |D| \supset Z$, and the existence of this $\mathbb{P}^1$ translates into the existence of a degree d map $C \to \mathbb{P}^1$. This are the points we saw before.

  Construction 1.1.12 (map to $\mathbb{P}^1$, response to audience question). Having $\mathbb{P}^1 \hookrightarrow |D|$ gives two line distinct, but linearly equivalent divisors $D_0 \sim D_1$. Hence, there's some rational function $f \in k(C)$ with $\mathrm{div}(f) = D_0 - D_1$. This f is the map $C \to \mathbb{P}^1$. $\bigcirc$

  Slogan. $Z = |D|$ gives $\mathbb{P}^1$-parameterized points.

  Definition 1.1.13. A closed point $x \in C$ is $\mathbb{P}^1$-parameterized if any of the following equivalent conditions holds:

  (1) $\exists \pi \colon C \to \mathbb{P}^1$ with $\pi(x) \in \mathbb{P}^1(k)$ and $\deg \pi = \deg x$.

  (2) $\exists \mathbb{P}^1 \hookrightarrow \mathrm{Sym}^d_C$ whose image contains x.

  (3) $h^0(C, \mathscr{O}(x)) \geq 2$.

  Otherwise, we say x is $\mathbb{P}^1$-isolated. $\diamond$

- Assume $\dim \rho(Z) > 0$.

  Let $W^d \coloneqq \rho(\mathrm{Sym}^d_C) \supset \rho(Z)$. Note that $\rho(Z)$ has a Zariski dense set of k-points.

  Theorem 1.1.14 (Mordell–Lang Conjecture, Faltings '94)**.** *If $Y \subset A$ has Zariski dense k-points, then Y is a translate of a positive rank abelian subvariety.*

  Thus, $\rho(Z)$ is a positive rank abelian variety.

Definition 1.1.15. A closed point $x \in C$ is `AV-parameterized` if there is a positive rank abelian subvariety $B \subset \mathrm{Pic}^0_C$ such that $[x] + B \subset W^d$. Otherwise, x is `AV-isolated`. ◇

Definition 1.1.16. A point is `parameterized` if its $\mathbb{P}^1$- or AV-parameterized. It is `isolated` if it is $\mathbb{P}^1$- and AV-isolated. ◇

Theorem 1.1.17 (Bourdon, Ejder, Liu, Odumodu, Viray 2019, Faltings' 1994 proof of Mordell–Lang + ε)**.** *Let C/k be a nice curve. Then,*

(1) *$d \in \delta(C/k) \iff \exists$ degree d parameterized point, i.e.*

$$\delta(C/k) = \delta_{\mathbb{P}^1}(C/k) \cup \delta_{AV}(C/k),$$

where these are the sets of (degrees of) $\mathbb{P}^1$- or AV-parameterized points.

(2) *There are only finitely many isolated (closed) points on C.*

"These are the points without a good reason to exist."

Equivalently, there is an open $U \subset C$ s.t. every closed $x \in U$ is parameterized.

Question 1.1.18 (Main, final form)**.** *Can we understand all parameterized points on C?*

1.2 Lecture 2 (11/5)

1.2.1 Recall from last time

We defined $\delta(C/k) = \{d \in \mathbb{N} : \deg d \text{ points are Zariski dense}\}$.

Recall 1.2.1. A closed point $x \in C$ is

- $\mathbb{P}^1$`-parameterized` if $\exists \pi \colon C \to \mathbb{P}^1$ s.t. $\pi(x) \in \mathbb{P}^1(k)$ and $\deg \pi = \deg x$.
- `AV-parameterized` if $\exists B \subset \mathrm{Pic}^0_C$ postive rank abelian subvar s.t. $[x]+B \subset W^d := \mathrm{im}\left(\mathrm{Sym}^d_C \xrightarrow{\rho_d} \mathrm{Pic}^d_C\right)$. ⊙

Theorem 1.2.2 (Cor of Faltings '94, BELOV)**.** *Let C be a smooth projective geometrically integral curve over a number field k. Then,*

(1) *$\delta(C/k) = \delta_{\mathbb{P}^1}(C/k) \cup \delta_{AV}(C/k)$.*

(2) *There are only finitely many isolated points on C.*

1.2.2 Today's Content

Theorem 1.2.3 (Faltings '94, `Mordell--Lang Conjecture`)**.** *Let A be an abelian variety over a number field k. Let $X \subset A$ be a closed subvariety. Then, there exists f.many points $x_1, \dots, x_r \in X(k)$ and finitely abelian subvarieties $B_1, \dots, B_r \subset A$ such that*

(1) *$x_i + B \subset X$ for all i; and*

(2) *$X(k) = \bigcup_{i=1}^r x + B_i(k)$.*

Remark 1.2.4. If $[D] \in \mathrm{Pic}^d_C(k)$, then $\mathrm{Pic}^d_C \simeq \mathrm{Pic}^0_C$ via translation by $[D]$. Thus, Pic^d_C is either an abelian variety or is pointless (in which case, Sym^d_C is also pointless and we don't care about it in these lectures). ◦

We want to apply Faltings to $A = \mathrm{Pic}^0_C \simeq \mathrm{Pic}^d_C \supset W_d = X$. We immediately get that there exists $[D_1], \dots, [D_r] \in W^d(K)$ and $B_1, \dots, B_r \in \mathrm{Pic}^0_C$ such that

(1) $[D_i] + B_i \subset W^d$; and

(2) $W^d(k) = \bigcup_{i=1}^r [D_i] + B_i(k)$.

Now, view $\mathrm{Hilb}^d_C(k) \supset \{\text{isolated pts on } C\} \xrightarrow{\rho_d} W^d(k)$. By definition, any (AV-)isolated point must land inside

$$\bigcup_{\substack{i=1 \\ \text{rank } B_i = 0}}^{r} [D_i] + B_i(k),$$

so there are only finitely many possibilities for $\rho_d(\text{an AV-isolated point})$.

Corollary 1.2.5. *$\#\rho_d(\{AV\text{-isolated points}\}) < \infty$.*

Now assume $d \in \delta(C/k)$. What does Falting's theorem tell us? To start, we have an infinite set $\{\text{degree } d \text{ pts on } C\} \subset \mathrm{Hilb}^d_C(k)$. The image of this set under $\rho_d \colon \mathrm{Hilb}^d_C = \mathrm{Sym}^d_C \to \mathrm{Pic}^d_C$ is either infinite or has some infinite fiber. In the first case, there sill be some B_i with positive rank (containing an image of a degree d point), so we there exists some AV-parameterized point (of degree d). In the second case, there must be a $\mathbb{P}^1$-parameterized point (by Definition 1.1.13**(2)**).

"If you say 'any of the following are equivalent', that's not a definition, it's also a definereom." (Apparently Bianca learned this word from Tony).

Corollary 1.2.6. *$\delta(C/k) \subset \delta_{\mathbb{P}^1}(C/k) \cup \delta_{AV}(C/k)$.*

To finish the proof of Theorem 1.2.2, need to show

- If there is a degree d parameterized point, then $d \in \delta(C/k)$ (+ Definereom)
- $\rho_d|_{\{\text{isolated pts}}$ is finite-to-one. Also, there are no isolated points of degree $d \gg 0$.

Lemma 1.2.7 (Defineorem Definition 1.1.13)**.** *Let $x \in C$ be a closed point of degree $d = \deg x$. Then, TFAE*

(1) *There exists $\pi \colon C \to \mathbb{P}^1$ with $\pi(x) \in \mathbb{P}^1(k)$ and $\deg \pi = \deg x$.*

(2) *There exists a nonconstant morphism $\mathbb{P}^1 \to \mathrm{Hilb}^d_C = \mathrm{Sym}^d_C$ whose image contains x.*

(3) $\dim \mathrm{H}^0(C, \mathscr{O}(x)) \geq 2$.

"My notes just say proof **(1)** $\implies$ **(2)** $\implies$ **(3)** $\implies$ **(1)**."

Proof.

($\mathbf{(1)} \implies \mathbf{(2)}$) Taking fibers gives a (non-constant) map $\pi^* \colon \mathbb{P}^1 \to \mathrm{Hilb}^d_C$. Furthermore, by assumption, $\pi^*(\pi(x)) = x$.

($\mathbf{(2)} \implies \mathbf{(3)}$) Consider composition $\mathbb{P}^1 \to \mathrm{Hilb}^d_C \to \mathrm{Pic}^d_C$. The image is a single point and also contains $[x]$. Thus, $\dim \rho_d^{-1}([x]) \geq 1$, which implies $h^0([x]) \geq 2$.

More explicitly, get two effective divisors $D_1 \neq D_2$ linearly equivalent to $[x]$, so get functions $f_1, f_2 \in k(X)$ s.t. $\dim f_i = D_i - x$. These span a 2-dimensional subspace of $\mathrm{H}^0(C, \mathscr{O}(x))$.

($\mathbf{(3)} \implies \mathbf{(1)}$) Since $h^0([x]) \geq 2$, there exists a non-constant function $f \in k(C)$ such that $\mathrm{div}(f) + [x] \geq 0$. This gives a morphism $f \colon C \to \mathbb{P}^1$ whose fiber above ∞ is x, so $\deg f = \deg x$. ∎

Lemma 1.2.8. *Fix $d \in \mathbb{Z}^+$. TFAE,*

(1) *$\exists \pi\colon C \to \mathbb{P}^1$ of degree d.*

(2) *$\exists D \in \mathrm{Div}^d(C)$, $h^0([D]) \geq 2$ AND $|D|$ is basepoint free.*

(3) *$\exists$ a degree d $\mathbb{P}^1$-parameterized point.*

(4) *$\exists \infty$-many deg d $\mathbb{P}^1$-parameterized points.*

Proof. I'm too lazy to type this. Do divisor stuff and then say Hilbert irreducibility for **(3)**.

Actually, I'll write **(1)** to **(4)**. Say we have $\pi\colon C \to \mathbb{P}^1$ Galois w/ group G. We want some fiber to be integral. Given $z \in \mathbb{P}^1$ (away from branch locus), it's fiber will be a bunch of points $x_1, \dots, x_r$ of equal degree. Let $G_z = \mathrm{Stab}(x_i) \leq G$ (decomposition/stabilizer group). Then, the fiber C_z is integral $\iff G_z = G$. Have some finite subset of maximal proper subgroups $H \leq G$. Now, if C_z is not integral, then z will be the image of a rational point under $C/H \to \mathbb{P}^1$ (for some such H). Thus, the set of z s.t. C_z is not integral is a thin set. However, Hilbert irreducility tells us that $\mathbb{P}^1(k)$ is not thin, so we win. ■

Theorem 1.2.9 (`Hilbert Irreducibility`)**.** *If $\Omega \subset \mathbb{P}^1(k)$ is a thing set, then $\mathbb{P}^1(k) \setminus \Omega$ is Zarski dense.*

1.3 Lecture 3 (11/6)

Yesterday we were going through the proof of (most of) Theorem 1.2.2.

Note 2. There are no chargers and I don't think my laptop has enough battery for two lectures, so these notes might be kinda scant as I attempt to preserve power.

From yesterday's stuff, we can easily deduce that

- ρ_d is injective on isolated points.
- If $d > g$, all degree d points are $\mathbb{P}^1$-parameterized (use Riemann-Roch).

To finish the proof of Theorem 1.2.2, all that remains is to show that if a degree d parameterized point exists, then $d \in \delta(C/k)$. If the point is $\mathbb{P}^1$-parameterized, this follows already from Lemma 1.2.8.

Corollary 1.3.1 (of Lemma 1.2.8)**.** *If $d > \max(2g, 1)$, then TFAE*

- $d \in \delta_{\mathbb{P}^1}(C/k)$
- $\mathrm{Hilb}^d_C(k) \neq \emptyset$
- $d \equiv 0 \mod \mathrm{ind}(C)$.

Goal. Prove that if there is a degree d AV-parameterized (and $\mathbb{P}^1$-isolated) point, then $d \in \delta(C/k)$.

1.3.1 AV-parameterized points

Example 1.3.2. Say $\pi\colon C \to E$ is a degree d morphism with E a positive rank elliptic curve. Assume there is some $P \in E(k)$ whose fiber C_P is integral. Then, $[C_P] + \pi^* \mathrm{Pic}^0_E \subset W^d$, so C_P is AV-parameterized. △

Warning 1.3.3. There exists cyclic isogenies $\varphi\colon E' \to E$ with $\varphi(E'(k)) = E(k)$ (e.g. 175.b3 → 175.b1), so Hilbert irreducibility does not hold for elliptic curves. In this case, the image of $\varphi^*\colon \mathrm{Sym}^1_E \to \mathrm{Sym}^{\deg \varphi}_{E'}$ consists only of reducible divisors.

It turns out, in this case, E' will still have an AV-parameterized point of degree $\deg \varphi$, but not coming from where you'd initially expect. •

Proposition 1.3.4 (Viray, Vogt; Prop 2.9)**.** *Let E be a positive rank elliptic curve and let $\pi\colon C \to E$ be a degree d map that does not factor through any étale cover. Then $\{P \in E(K) : C_p$ integral$\}$ is Zariski dense in E.*

Lemma 1.3.5. *Let $d \geq g \geq 1$. Then,*

$$d \in \delta_{AV}(C/k) \iff \mathrm{Pic}^0_C \text{ has positive rank and } \exists x \in C \text{ with } \deg x = d.$$

Proof. If $d \geq g \geq 1$, then $W^d = \mathrm{Pic}^d_C$ (i.e. ρ_d surjective). ■

Example 1.3.6. Bianca wrote down an example where $2 \in \delta_{\mathbb{P}^1}(C/k)$, $3 \in \delta_{AV}(C/k)$, but $5 \notin \delta_{C/k}$. See VV paper. △

Corollary 1.3.7. *$\delta(C/k)$ is not a semigroup.*

Proposition 1.3.8 (BELOV, c.f. VV Prop 4.5)**.** *Let $x \in C$ be a degree d point that is AV-parameterized and $\mathbb{P}^1$-isolated. Let $A \subset \mathrm{Pic}^0_C$ be a positive rank abelian subvariety such that $[x] + A \subset W^d$.*

Then, there is a finite index subgroup $H < A(k)$ such that every element of $[x] + H$ is represented by a degree d point. In particular, $d \in \delta(C/k)$.

Remark 1.3.9. Main point in the proof is that, because x is $\mathbb{P}^1$-isolated, you know that $[x] \notin \bigcup_e \mathrm{im}\big(W^{d-e} \times W^e \to W^d\big)$. Since this union is a finite union of cosets (by Faltings' big theorem), get that it must miss some coset (contained in W^d). ∘

Proposition 1.3.10 (VV Prop 5.9)**.** *Let $n \geq 2$. Then,*

$$n \cdot \delta_{AV}(C/k) \subset \delta_{\mathbb{P}^1}(C/k) \cap \delta_{AV}(C/k).$$

In particular, $\mathbb{N} \cdot \delta(C/k) \subset \delta(C/k)$.

Remark 1.3.11. Idea here is to choose $A \subset \mathrm{Pic}^0_C$ such that $[x] + A \subset W^d$ and then choose infinite order $D_0 \in A(k)$ s.t. D_0 is effective. Then, $y_i = x + iD_0$ is effective for all $i \geq 0$ and $y_i \not\sim y_j$ for $i \neq j$. Furthermore, $nx \sim (n+1)y_i - y_{(n+1)i}$ (or something like this) for all i, so get lots of effective representatives of $n[x]$. ∘

Corollary 1.3.12 (Abramovich, Harris; Frey)**.** $\mathrm{gon}(C/k) \leq 2 \min \delta(C/k)$.

Summary:

- $\delta(C/k) = \delta_{\mathbb{P}^1}(C/k) \cup \delta_{AV}(C/k)$
- $\delta_{\mathbb{P}^1}(C/k) \supset (\mathrm{ind}(C/k) \cdot \mathbb{N}) \cap \mathbb{N}_{\geq \max(2g+1)}$
- $\delta_{AV}(C/k) \neq \emptyset \iff \mathrm{rank}\,\mathrm{Pic}^0_C(k) > 0$
- $\mathbb{N}_{\geq 2} \cdot \delta_{AV}(C/k) \subset \delta_{\mathbb{P}^1}(C/k) \cap \delta_{AV}(C/k)$
- There are f.many isolated points.

Question 1.3.13. *Can we understand all parameterized points on C, as a scheme (also understanding residue fields).*

1.4 Lecture 4 (11/7): Residue fields of closed points on curves

Open Question 1.4.1. *Let E be a positive rank elliptic curve and let $\pi\colon C \to E$ be a degree d map that does not factor through any isogeny. Is $\{P \in E(k) : C_P \text{ integral}\}$ Zariski dense in E?*

Note: may factor through étale cover but not one with points.

Proposition 1.4.2 (VV; Prop 3.7)**.** *Let C' be a genus 1 curve with $\operatorname{rank}\operatorname{Pic}^0_{C'}(k) > 0$ and let $\pi\colon C \to C'$ be a degree d map. Then, $d \cdot \operatorname{ind}(C'/k) \cdot \mathbb{N} \subset \delta(C/k)$...*

There was more I missed

1.4.1 Residues fields

Notation 1.4.3. Let x be a 0-dimensional scheme over x, so $x = \operatorname{Spec} A$. It's "residue field" is $\mathbf{k}(x) \coloneqq A$ (not necessarily a field, really just the ring of functions on x).

Motivations for studying residue fields of closed points on curves

- Understanding all closed points, as schemes
- Diophantine stability [Mazur, Rubin]
  - A nice variety X/k is Diophantine-stable for L/k if $\nexists x \in X$ with $k \subsetneq \mathbf{k}(x) \hookrightarrow L$.
  - For which types of extensions is an abelian variety Diophantine-stable?
  - If $\{\mathbf{k}(x) : x \in C, \text{closed}\}/\sim = \{\mathbf{k}(x) : x \in C', \text{closed}\}$, then is $C_{\overline{k}} \simeq C_{\overline{k}'}$?

    They prove this for k-isomorphism for genus 0 curves. It's false over k for genus 1 curves (take two with the same Jacobian which generate the same cyclic subgroup of $\mathrm{H}^1(k, E)$).
- Grnwald problem: Fix a finite group G, a finite set S of places, and a set of étale G-algebras $\{L_v/k_v\}_{v\in S}$, does there exist a Galois extension L/k with $\operatorname{Gal}(L/k) \simeq G$ such that $L \otimes_k k_v \simeq L_v$ for all $v \in S$?

Recall we're interested in understanding all parameterized points on C.

Remark 1.4.4. For a fixed degree, parameterized points arise in finitely many families. ∘

Question 1.4.5. *In a given parameterization, how do the residue fields vary?*

Let's first look at $\mathbb{P}^1$-parameterized points. Given a degree d map $\pi\colon C \to \mathbb{P}^1$, how does $\mathbf{k}(C_t)$ vary as t ranges over $\mathbb{P}^1(k)$?

Warning 1.4.6. In trying to make this question precise, be careful to not turn it into an open problem about number fields. •

Possible interpretations:

- Describe/characterize the possible isomorphism classes $\mathbf{k}(C_t)$ for $t \in \mathbb{P}^1(k)$.

  Wait, can we describe all degree d extensions of k? No...
- Describe/characterize the possible local isomorphism classes $\mathbf{k}(C_t) \otimes_k k_v$ for $t \in \mathbb{P}^1(k)$.

  Remark 1.4.7. $\mathbb{P}^1$ satisfies weak approximation, so k points dense in k_v points (for finite set of v's). ∘

  Can reduce to describing $\mathbf{k}(C_t) \otimes_k k_v$ for $t \in \mathbb{P}^1(k_v)$.

Example 1.4.8. Consider $C\colon y^2 = f(t_0, t_1) \subset \mathbb{P}(1, g+1, 1)$, where f is separable with degree $2g+2$. Then,

$$\mathbf{k}(C_t) \simeq \frac{k_v[\theta]}{\theta^2 - f(a_0, a_1)} \text{ where } t = [a_0 : a_1] \in \mathbb{P}^1(k_v) = \mathbb{P}^1(\mathscr{O}_v).$$

(note this is $k_v \times k_v$ if $f(a_0, a_1)$ is a square). Consider only $v \in \Omega_k$ such that $f \in \mathscr{O}_v[t_0, t_1]$ and $2\operatorname{disc}(f) \in \mathscr{O}_v^\times$. Hence, f will remain separable mod v, so we really have a hyperelliptic curve over $\mathscr{O}_v$.

- If $f(a_0, a_1) \not\equiv 0 \bmod v$, then $\mathbf{k}(C_t)/k_v$ is unramified.

  Furthermore, it is split/trivial if and only if $f(a_0, a_1) \bmod v \in (\mathbb{F}_v^\times)^2$. If $\#\mathbb{F}_v \gg 0$, then $f(a_0, a_1)$ will take on both square and non-square values.

  Remark 1.4.9. If $\Pi\colon \mathcal{C} \to \mathbb{P}^1_{\mathscr{O}_v}$ is étale over $\operatorname{Spec} \mathscr{O}_v \xrightarrow{t} \mathbb{P}^1_{\mathscr{O}_v}$, then $\mathbf{k}(C_t)/k_v$ is unramified and the iso. class is determined by its special fiber. ∘

- If $\{f(t_0, t_1) \bmod v\} \subset \mathbb{P}^1_{\mathbb{F}_v}$ has no roots, then $\mathbf{k}(C_t) \otimes_k k_v/k_v$ is unramified.

- Now assume $f(a_0, a_1) \equiv 0 \mod v$. WLOG assume $[a_0 : a_1] \equiv [0 : 1] \bmod v$. Then, $f(t_0, t_1) \equiv t_0 g(t_0, t_1) \bmod v$, where $g \in \mathbb{F}_v[t_0, t_1] \setminus \langle t_0 \rangle$.

  By Hensel, lift factorization $f(t_0, t_1) = \ell(t_0, t_1)\widetilde{g}(t_0, t_1)$ over k_v. Change coordinates to get

  $$f(t_0, t_1) = t_0 \widetilde{g}(t_0, t_1) = t_0\left(u t_1^{2t+1} + t_0 h(t_0, t_1)\right).$$

  Choose $a_0 \in \mathscr{O}_v$ with $v(a_0) = 1$. Then,

  $$f(a_0, 1) = a_0(u + a_0 h(a_1, 1)) \equiv a_0 u \bmod \mathfrak{m}_v^2.$$

  By varying $a_0 \in \mathfrak{m}_v \setminus \mathfrak{m}_v^2$, we obtain all (both) quadratic ramified extensions.

  Remark 1.4.10. Here, we actually used the presentation of the curve. ∘

△

Question 1.4.11 (Audience, paraphrased)**.** *What happens at 2?*

Answer. It'll be harder and the answer will look different.

For a curve over a number field, we say that $\delta(C/k) \supset \operatorname{ind}(C)\mathbb{N} \cap \mathbb{N}_{\geq 2g+1}$. An analogous thing holds for finite fields, but this fails for curves over local fields.

Warning 1.4.12 (see Creutz–Viray, "degree sets of curves over henselian fields")**.** There exists curves over local fields such that, e.g.,

$$\{\deg x : x \in C\} = 2\mathbb{N} \cup 3\mathbb{N}.$$

In particular, can't get a point of prime degree for any prime bigger than 3, even though it has index 1. •

Such curves will have very bad reduction. This sort of answer doesn't occur over number fields, so you run into situations where you have very different answers. ⋆

Proposition 1.4.13 (Balcik, Chan, Liu, Viray)**.** *Let $\mathcal{C} \xrightarrow{\pi} \mathbb{P}^1_{\mathscr{O}_v}$ be a finite, flat morphism with good reduction. Let $\overline{x} \in \mathcal{C}$ be a closed point where the map is ramified and set $\overline{t} = \pi(\overline{x})$. Then,*

$$\mathscr{O}_{\mathscr{C}, \overline{x}} \simeq \mathscr{O}_{\mathbb{P}^1, \overline{t}}[\beta] \text{ where } \beta \text{ has minimal polynomial of the form } \widetilde{f}^e + p_0 u.$$

Remark 1.4.14. Compare to the hyperelliptic equation

$$y^2 + t_0\Big(-ut_1^{2g+1} - t_0 h(t_0, t_1)\Big)\,. \qquad \circ$$

Remark 1.4.15. Above, $\deg(\widetilde{f})$ is the ratio $\deg(\overline{x})/\deg(\overline{t})$. Furthermore, if $\deg \widetilde{f} = 1$, they can prove that you obtain all ramified extensions of degree e. If $\deg \widetilde{f} > 1$, there can be obstructions to getting all ramified extensions (but they can say how many of them you get). $\circ$

Proposition 1.4.16 (Meta Theorem, BCLV)**.** *Let $C \xrightarrow{\pi} \mathbb{P}^1$ be a degree d map. If $v \in \Omega_k$ with $\#\mathbb{F}_v \gg 0$ and let L/k_v be an extension which is "compatible with the geometry of π," then there exists a $t \in \mathbb{P}^1(k)$ such that $\mathbf{k}(C_t) \otimes_k k_v$ contains a maximal subfield isomorphic to L.*

Remark 1.4.17 (Dèbes, Ghazi; Beckmann)**.** Unramified case already follows from work on the unramified Grunewald problem $\circ$

Theorem 1.4.18 (BCLV)**.** *Let $C \xrightarrow{\pi} \mathbb{P}^1$ be a cyclic cover of degree d such that all ramifications points have ramification index d. Then, for all $v \in \Omega_v$ with $\#\mathbb{F}_v \gg 0$, all $f \mid d$, and all totally ramified degree d extensions L/k_v:*

- *$\exists t \in \mathbb{P}^1(k)$ such that $\mathbf{k}(C_t)$ has d/f places above v, each with inertia degree f.*
- *$\exists t \in \mathbb{P}^1(k)$ such that $\mathbf{k}(C_t) \otimes_k k_v \simeq L \iff \mathbb{P}^1(\mathbb{F}_v)$ contains a branch point.*

Theorem 1.4.19 (BCLV)**.** *Let $C \xrightarrow{\pi} \mathbb{P}^1$ be a degree d map whose Galois closure is an S_d-extension and such that all branch points have a unique ramification above w/ ram. index 2, then:*
for all $v \in \Omega_k$ with $\#\mathbb{F}_v \gg 0$ and all partitions $(f_i) | - d$

- *$\exists t \in \mathbb{P}^1(k)$ s.t. $\mathbf{k}(C_t)$ is unramified at v with inertia degrees (f_i)*
- *$\exists t \in \mathbb{P}^1(k)$ such that $\mathbf{k}(C_t)$ is ramified at $v \iff \mathbb{P}^1(\mathbb{F}_v)$ contains a branch point.*
- *Furthermore, for any $t \in \mathbb{P}^1(k)$, there is at most one $w \mid v$ that is ramified and it has $e(w/v) = 2$.*

Warning 1.4.20. The tricky case (excluded in previous two theorems) is when there is an $x \in C$ such that $\deg x > \deg \pi(x)$ and $e(x/\pi(x)) > 1$. •

1.4.2 Further Directions

(1) Classification of curves with a fixed minimum density degree.

See Harris–Silverman, Abramovich–Harris, Kadets–Vogt

(2) Geometric restrictions from low degree parameterized points.

(3) Galois-theoretic properties in $\mathbb{P}^1$- and AV-parameterizations.

See [Khawaja–Siksek]

(4) Uniform bounds for the number of isolated points.

(5) Variation of residue fields in AV-parametrizations.

2 Anthony Várilly–Alvarado (Rice University): Vojta's Conjectures: Motivation and Applications

2.1 Lecture 1 (11/4)

Note 3. I'm sitting too far up to read the blackboard easily, so this'll be fun...

Vojta's conjecture if very appealing, but the statement is a bit technical. We'll state it in the third lecture. We'll do heights today and some complex analysis tomorrow. Algebraic geometry will finally enter the picture on Wednesday.

"If you haven't seen heights before, today is a very important day in your life."

2.1.1 Heights: Roth's Theorem

Setup 2.1.1. Let $K/\mathbb{Q}$ be a number field, $\mathscr{O}_K$ its ring of integers. We write Ω_K for its set of places and $\Omega_\infty \subset \Omega_K$ for the archimedean ones. Given a place $v \in \Omega_K$, we write K_v for the corresponding completion and $\|\cdot\|_v$ for the corresponding norm (not an absolute value in the complex case):

- If $K_v = \mathbb{R}$, then $v = \sigma\colon K \hookrightarrow \mathbb{R}$ and $\|\alpha\|_v = |\sigma(\alpha)|$.
- If $K_v = \mathbb{C}$, then $v = (\sigma, \overline{\sigma}) : K \hookrightarrow \mathbb{C}$ and we take $\|\alpha\|_v = \langle\sigma(\alpha)\rangle^2$.
- If K_v is non-archimedean, then $v = \mathfrak{p} \subset \mathscr{O}_K$ and we take

$$\|\alpha\|_v \coloneqq (\mathscr{O}_K : \mathfrak{p})^{-\operatorname{ord}_\mathfrak{p}(\alpha)} = p^{-f \operatorname{ord}_\mathfrak{p}(x)},$$

  where $\mathfrak{p} \mid p$ and $f \coloneqq [(\mathscr{O}_K/\mathfrak{p}) : \mathbb{F}_p]$ is the `inertia degree`.

Theorem 2.1.2 (`product formula`)**.**

$$\prod_{v \in \Omega_K} \|x\|_v = 1 \text{ for } x \in K^\times.$$

(note: in practice, if you can compute that the LHS is < 1, then this proves that $x = 0$).

Let $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$ with $x_i \in K$. We define the `relative exponential height` of P to be

$$H_K(P) \coloneqq \prod_v \max\{\|x_0\|_v, \ldots, \|x_n\|_v\}.$$

Note this is well-defined by the product formula.

Example 2.1.3. Take $K = \mathbb{Q}$ and $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\mathbb{Q})$ with $x_i \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$. Then,

$$H_\mathbb{Q}(P) = \max\{|x_0|, \ldots, |x_n|\}$$

(usual archimedean absolute value). E.g. $H_\mathbb{Q}([1 : 2]) = 2$ and $H_\mathbb{Q}([100 : 201]) = 201$. Note that $[100 : 201] = [1 : 201/100]$ which doesn't feel that different from $[1 : 2]$, but clearly the former is "more arithmetically complex/harder to write down"; heights capture this. △

Lemma 2.1.4. *If L/K is a finite extension and $P \in \mathbb{P}^n(K)$, then*

$$H_L(P) = H_K(P)^{[K:L]}.$$

The main point is that, for fixed $v \in \Omega_X$,

$$\sum_{w \in \Omega_L \,:\, w|v} [L_w : K_v] = [L : K].$$

Definition 2.1.5. We define the absolute exponential height of $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ to be

$$H(P) \coloneqq H_K(P)^{1/[K:\mathbb{Q}]}$$

for any finite $K/\mathbb{Q}$ such that $P \in \mathbb{P}^n(K)$. ◇

We also define logarithmic heights:

$$h_K(P) \coloneqq \log H_K(P) \text{ and } h(P) \coloneqq \log H(P).$$

Can think of $h(P)$ as measuring the number of bits used to record the coordinates of P. For a number $x \in K$, we define its height to be

$$h(x) \coloneqq h([x:1]) = \sum_{v \in \Omega_K} \log \max\{\|x\|_v, 1\} = \sum_{v \in \Omega_K} \log^+ \|x\|_v \text{ where } \log^+(a) = \log \max\{a, 1\} = \max\{\log a, 0\}.$$

Theorem 2.1.6 (Northcott Finiteness)**.** *Fix $B \in \mathbb{R}_{>0}$ and an integer $d \in \mathbb{Z}_{\geq 1}$. Then,*

$$\#\left\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \colon H(P) \leq B \text{ and } \deg P \leq d\right\} < \infty.$$

2.1.2 Diophantine Approximation

Theorem 2.1.7 (Dirichlet 1842)**.** *Take $x \in \mathbb{R} \setminus \mathbb{Q}$. Then, there are infinitely many rational approximations $p/q \in \mathbb{Q}$ such that*

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{q^2}.$$

Contrast this with the following.

Theorem 2.1.8 (Liouville 1844)**.** *For $\alpha \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$ and any $\varepsilon > 0$, there are only finitely many rational numbers $p, q \in \mathbb{Q}$ such that*

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{q^{d+\varepsilon}} \text{ where } d = \deg x.$$

Taking α to be a quadratic number, this shows that Dirichlet's result is optimal in general. However, for larger degree numbers, there are improvements. Improvements to $q^{d+\varepsilon}$:

- Thue (19??): $q^{\frac{1}{2}d+1+\varepsilon}$
- Siegel (1921): $q^{2\sqrt{d}+\varepsilon}$
- Gelfond/Dyson (1947): $q^{\sqrt{2d}+\varepsilon}$
- Roth (1955): $q^{2+\varepsilon}$

Now, Dirichlet's theorem says that Roth's theorem can't be improved.

Example 2.1.9. Consider the equation $x^3 - 7y^3 = 19$. We'll prove that this has finitely many $\mathbb{Z}$-solutions.

If $|x|$ (or $|y|$) is large, then $x/y \approx \sqrt[3]{7}$. This is where Roth comes in. One can check that (use difference of cubes)

$$\left|\frac{x}{y} - \sqrt[3]{7}\right| = \left|\frac{19/y^3}{(x/y)^2 + (x/y)\sqrt[3]{7} + \sqrt[3]{49}}\right| = \left|\frac{19}{y(x^2 + xy\sqrt[3]{7} + y^2\sqrt[3]{49})}\right| \ll \frac{1}{y^3}.$$

Thus, Roth (with $\varepsilon = 1$) implies that there are only f.many possibilities for $x/y \in \mathbb{Q}$. △

Let's mention a generalization of Roth.

Theorem 2.1.10. *Let K be a number field, S a finite set of places (may assume $S \supset \Omega_\infty$ if you want), fix some $\alpha \in \overline{\mathbb{Q}}$, some $\varepsilon > 0$, and some $C > 0$. Then, there are only f.many $x \in K$ such that*

$$\prod_{v \in S} \min\{1, \|x - \alpha\|_v\} \leq \frac{C}{H_K(x)^{2+\varepsilon}}. \tag{2.1}$$

Let's rewrite this in a way that'll be closer to the complex analysis we'll see tomorrow. First take logs of (2.1).

$$\begin{aligned}
\sum_{v \in S} \log \min\{1, \|x - \alpha\|_v\} &\leq \log C - (2+\varepsilon) h_K(x) \\
-\sum_{v \in S} \log \min\{1, \|x - \alpha\|_v\} &\geq -\log C + (2+\varepsilon) h_K(x) \\
\sum_{v \in S} \max\left\{0, \log \left\|\frac{1}{x-\alpha}\right\|_v\right\} &\geq (2+\varepsilon) h_K(x) - \log C \\
\frac{1}{[K:\mathbb{Q}]} \sum_{v \in S} \log^+ \left\|\frac{1}{x-\alpha}\right\|_v &\geq (2+\varepsilon) h(x) - \frac{\log C}{[K:\mathbb{Q}]}
\end{aligned}$$

Theorem 2.1.11. *Let K be a number field, $S \subset \Omega_K$ a finite set of places, $\alpha \in K$, $\varepsilon > 0$, and $C \in \mathbb{R}$. Then, for all but f.many $x \in K$, we have*

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v \in S} \log^+ \left\|\frac{1}{x-\alpha}\right\|_v \leq (2+\varepsilon) h(x) + C.$$

Tomorrow we'll look at some complex analysis and establish a dictionary between one variable complex analysis and number fields. We'll see two main theorems of Nevalinna theory. Using our dictionary to translate these to number fields, we'll recover the above theorem. The translate of its statement in higher dimensions outputs Vojta's conjecture.

2.2 Lecture 2 (11/5): One variable Nevanlinna Theory

"I've spent 16 years in a department very heavily populated by analysis, so I haven't taught any analysis of any kind. This is probably something that I shouldn't do unsupervised, but here we go."

Goal. Study the distribution of values of a meromorphic function $f \colon \mathbb{C} = \overline{\mathbb{C}} \coloneqq \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$.

Remark 2.2.1. If f is a polynomial, then $f(z) = a$ has $\deg f$ many solutions (counted w/ multiplicity). What if $f(z)$ is a transcendental function? ◦

Example 2.2.2. $f(z) = e^z$. Then, $e^z = a$ has infinitely many solutions if $a \neq 0, \infty$ and no solutions otherwise. △

We want to count, but once you run into infinitys, you have to be a little careful. Let's try truncating to something like a disc of radius r.

Definition 2.2.3. Let $f\colon \mathbb{C} \to \overline{\mathbb{C}}$ meromorphic. Fix $r > 0$ and $a \in \mathbb{C}$. The counting function of f is

$$n_f(r, a) \coloneqq \#\text{zeros of } f(z0 = a \text{ in } |z| < r \text{ (with multiplicity)}.$$

Furthermore, $n_f(0, a)$ is the multiplicity of $f(z) = a$ at $z = 0$. Furthermore, $n_f(r, \infty)$ is the number of poles of $f(z)$ in $|z| < r$ (w/ multiplicity). ◇

Recall 2.2.4 (argument principle)**.** The difference between zeros and poles is computed by the integral of a logarithmic derivative of $f - a$. More precisely,

$$n_f(r, a) - n_f(r, \infty) = \frac{1}{2\pi i} \int_{|z|=r} \frac{f'(z)}{f(z) - a} \mathrm{d}z. \tag{2.2}$$

⊙

Exercise. Use Cauchy–Riemann (in the form $\partial f/\partial r = (1/ir)\partial f/\partial\theta$) to show that the RHS of (2.2) is equal to

$$\frac{r}{2\pi} \frac{\partial}{\partial r} \int_{-\pi}^{\pi} \log \left| f\left(re^{i\theta}\right) - a \right| \mathrm{d}\theta.$$

Assumption. We'll assume that $f(0) \neq a, \infty$ throughout. This isn't strictly necessary, but simplifies things for us.

Note (divide by t and integrate to get the second line)

I can't make out what's in the second line

$$n_f(t, a) - n_f(t, \infty) = \frac{t}{2\pi} \frac{\partial}{\partial t} \int_{-\infty}^{\infty} \log \left| f(te^{i\theta}) - a \right| \mathrm{d}\theta$$
$$\int_0^r n_f(t, a) \frac{\mathrm{d}t}{t} - \int_0^r n_f(t, \infty) \frac{\mathrm{d}t}{t} = \frac{1}{2\pi} \int_{-\pi}^{\pi} \log \left| f(te^{i\theta}) + \ldots \right|$$

Notation 2.2.5. $N_f(r, a) = \int_0^r n_f(t, a) \frac{\mathrm{d}t}{t}$ is called an integrated counting function.

Now use $\log |x| = \log^+ |x| - \log^+ |1/x|$ to see that the RHS above is equal to

$$\frac{1}{2\pi} \int_{-\pi}^{\pi} \log^+ \left| f(re^{i\theta}) - a \right| \mathrm{d}\theta - \frac{1}{2\pi} \log^+ \frac{1}{|f(re^{i\theta}) - a|} \mathrm{d}\theta + O(1)$$

as $r \to \infty$. Use this to define the proximity function of f:

$$m_f(r, \infty) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \log^+ \left| f(re^{i\theta}) \right| \mathrm{d}\theta$$
$$m_f(r, a) \coloneqq m_{\frac{1}{f-a}}(r, \infty) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \log^+ \frac{1}{|f(re^{i\theta}) - a|} \mathrm{d}\theta.$$

Note that mass of the integral $m_f(r, a)$ is concentrated around the values on the circle where $f(z) \approx a$.

Remark 2.2.6. Informally,

- most contributions to this $m_f(r, a)$ come from z on the circle $|z| = r$ such that $f(z)$ is close to a (i.e. $|f(z) - a|$ is small).
- $m_f(r, a)$ is the "average proximity of $f(z)$ to a on the circle of radius r."

○

Exercise. Use $\log^+|x \pm y| \leq \log^+|x| + \log^+|y| + 2$ $(x, y \in \mathbb{R})$ to show that $m_f(r, \infty) = m_{f-a}(r, \infty) + O(1)$ as $r \to \infty$. This let's us rewrite Jensen as

$$\begin{aligned} & N_f(r, a) - N_f(r, \infty) = m_{f-a}(r, \infty) - m_f(r, a) + O(1) \\ \implies & N_f(r, \infty) + m_f(r, \infty) = N_f(r, a) + m_f(r, a) + O(1) \end{aligned}$$

Remark 2.2.7. The constants in the $O(1)$ depend on f, a (but only weakly on a). ∘

Definition 2.2.8. We define the characteristic function of f to be

$$T_f(r) \coloneqq N_f(r, \infty) + m_f(r, \infty).$$

Vojta calls this the height of f. ◇

Slogan. Solving $f(z) = a$ is independent*ish* of a.

Theorem 2.2.9 (First Main Theorem of Nevanlinna)**.** *Let $f \colon \mathbb{C} \to \overline{\mathbb{C}}$ be meromorphic. Then,*

$$T_f(r) = N_f(r, a) + m_f(r, a) + O_{a,f}(1) \text{ as } r \to \infty$$

for any $a \in \mathbb{C}$.

Example 2.2.10. Take $f(a) = z^d$. Then, $T_f(r) = d \log r$ (so can think of characteristic function as a replacement for the idea of the degree of a polynomial). More generally, if f is rational, then $T_f(r) = O(\log r)$. △

Warning 2.2.11. If you try to compute the RHS of Theorem 2.2.9 by hand, you'll probably get stuck (even for something like $f(z) = e^z$ and $a = 1$). •

Keep in mind that N_f should "count the number of zeros of $f(z) = a$ on the circle $|z| = r$" and m_f should "measure the proximity of $f(z)$ to a along the circle $|z| = r$."

Exercise. For $f(z) = e^z$, $T_f(r) = r/\pi$.

Theorem 2.2.12 (Second Main Theorem of Nevanlinna)**.** *Let $f \colon \mathbb{C} \to \overline{\mathbb{C}}$ be meromorphic. Fix $a_1, \ldots, a_n \in \mathbb{C}$ distinct. Then,*

$$\sum_{i=1}^{n} m_f(r, a_i) \leq_{exc} 2T_f(r) + O(\log^+ T_f(r)) - o(\log r) \text{ as } r \to \infty,$$

where $\leq_{exc}$ means this inequality holds for $r > 0$ outside a set of finite Lebesgue measure.

Corollary 2.2.13.

$$\sum_{i=1}^{n} m_f(r, a_i) \leq_{exc} (2 + \varepsilon) T_f(r) + C$$

for any $\varepsilon > 0$ and $C \in \mathbb{R}$.

(Compare this Roth's theorem Theorem 2.1.11).

2.2.1 Vojta's Vision

Let K be a number field and let $S \subset \Omega_K$ be a finite set of places. Assume $S \supset \Omega_\infty$. Vojta suggests Table 1.

Complex World	Number theory world
$f\colon \mathbb{C} \to \overline{\mathbb{C}}$ meromorphic	infinite subset of K
$f\|_{D(r)}$, $D(r)$ = disc of radius r	$x \in K$
angle θ	$v \in \Omega_K$ (maybe $v \in S$)
$\left\|f(re^{i\theta})\right\|$	$\|x\|_v$
$\operatorname{ord}_z(f)$	$\operatorname{ord}_v(x)$
$\log \frac{r}{\|z\|}$	$\log(\mathscr{O}_K : \mathfrak{p})$ (for this for $v \notin S$)
$m_f(r,a) = \frac{1}{2\pi}\int_{-\pi}^{\pi} \log^+ \frac{1}{\|f(re^{i\theta}) - a\|} \mathrm{d}\theta$	$m_S(x,a) = \sum_{v\in S} \log^+ \left\|\frac{1}{x-a}\right\|_v$
$m_f(r,\infty) = \frac{1}{2\pi}\int_{-\pi}^{\pi} \log^+ \left\|f(re^{i\theta})\right\| \mathrm{d}\theta$	$m_S(x) = \sum_{v\in S} \log^+ \|x\|_v$

Table 1: Vojta's dictionary

Apply Table 1 to Corollary 2.2.13. You get

$$\sum_{v\in S} \log^+ \left\|\frac{1}{x-a}\right\|_v \le (2+\varepsilon)h_K(x) + C$$

with the "missing set of finite Lebesgue measure" is not "for all but finitely many x."

Remark 2.2.14. Applying the dictionary to Theorem 2.2.12 gives a statement of Roth's theorem w/ more precise error term. This is still open. ∘

Tomorrow, we'll review dictionary and add some more lines.

2.3 Lecture 3 (11/6)

Note 4. My laptop will die before the end of the lecture. Sorry

Let's first finish our table.

Complex World	Number theory world
$f\colon \mathbb{C} \to \overline{\mathbb{C}}$ meromorphic	infinite subset of K
$f\|_{D(r)}$, $D(r)$ = disc of radius r	$x \in K$
angle θ	$v \in S$
$\left\|f(re^{i\theta})\right\|$	$\|x\|_v$
$\operatorname{ord}_z(f)$	$\operatorname{ord}_v(x)$
$\log \frac{r}{\|z\|}$	$\log(\mathscr{O}_K : \mathfrak{p})$ (this for $v \notin S$)
$m_f(r,a) = \frac{1}{2\pi}\int_{-\pi}^{\pi} \log^+ \frac{1}{\|f(re^{i\theta}) - a\|} \mathrm{d}\theta$	$m_S(x,a) = \sum_{v\in S} \log^+ \left\|\frac{1}{x-a}\right\|_v$
$m_f(r,\infty) = \frac{1}{2\pi}\int_{-\pi}^{\pi} \log^+ \left\|f(re^{i\theta})\right\| \mathrm{d}\theta$	$m_S(x) = \sum_{v\in S} \log^+ \|x\|_v$
$N_f(r,a) = \int_0^r n_f(t,a)\frac{\mathrm{d}t}{t} = \sum_{\|z\|<r} \operatorname{ord}_z^+(f-a)\cdot \log\frac{r}{\|z\|}$	$N_S(x,a) = \sum_{v\notin S} \operatorname{ord}_v^+(x-a)\log(\mathscr{O}_K : \mathfrak{p}) = \sum_{v\notin S} \log^+ \left\|\frac{1}{x-a}\right\|_v$
$T_f(r) = N_f(r,\infty) + m_f(r,\infty)$	$h_K(x) = \sum_{v\notin S} \|x\|_v + \sum_{v\in S} \|x\|_v$

Table 2: Vojta's dictionary (v2). Think places on boundary are those in S and places inside the disc are those not in S.

Recall 2.3.1 (Theorem 2.2.9)**.** $T_f(r) = N_f(r,a) + m_f(r,a) + O(1)$ as $r \to \infty$. ⊙

The translation of this into number theory is

$$h_K(x) = \sum_{v \notin S} \log^+ \left\| \frac{1}{x-a} \right\|_v + \sum_{v \in S} \log^+ \left\| \frac{1}{x-a} \right\|_v + O(1),$$

i.e.

Lemma 2.3.2 (exercise)**.** $h_K(a) = h_K(x-a) + O(1)$.

What's the higher-dimensional story look like?

Recall 2.3.3. In 1D, for $f\colon \mathbb{C} \to \mathbb{P}^1(\mathbb{C})$, fixed $a \in \mathbb{C}$ and then looked at how close f got to a. Note that a is a divisor on $\mathbb{P}^1_{\mathbb{C}}$. ⊙

Now, let X be a smooth, projective $\mathbb{C}$-variety of dimension n. Let $D \subset X$ be a (reduced) normal crossings divisor. Consider maps $f\colon \mathbb{C}^n \to X$ which are `nondegenerate` (i.e. Jacobian determinant $\neq 0$). Can define analogous counting/proximity/etc. functions, but we won't spell out their definitions in detail.

- $N_f(D, r)$ – counting function

  Measures the "mass of values" of f that land in the divisor $D \subset X$ in a ball of radius r in $\mathbb{C}^n$. Something like (φ^{n-1} a volume form)

  $$\int_0^r \left(\int_{f^* D \cap B(t)} \varphi^{n-1} \right) \frac{\mathrm{d}t}{t}$$

  Note 5. 9% battery power...

- Given a metrized line bundle L on X, get characteristic function $T_L(r)$ which measures "mass of values" of f that either land in L (e.g. some associated divisor) or get close to it in a ball of radius r in $\mathbb{C}^n$.

Theorem 2.3.4 (Stoll '72, Carlson–Griffiths '73)**.** *If $\delta > 0$ and A an ample divisor on X, then*

$$N_f(D, r) \geq T_{K_X + D}(x) - \delta T_A(x) + \underbrace{N_1(r)}_{\text{more on this tomorrow}}$$

for $r > 0$ outside a set of finite Lebesgue measure.

We now need to extend our table.

Complex World	Number theory world
$f\colon \mathbb{C}^n \to X$ nondegenerate	$R \subset X(K)$ Zariski dense
$T_L(r)$	$h_L(P)$
$N_f(D, r)$	$N_S(D, P)$

Table 3: Vojta's dictionary in higher dimensions

Note 6. 4% battery (while writing table)...

2.4 Lecture 4 (11/7)

Conjecture 2.4.1 (`Vojta 2.1`)**.** *Let K be a number field, $\Omega_\infty \subset S \subset \Omega_K$ finite, X a nice K-variety,*

on sideboard at beginning of lecture

$D \subset X$ a normal crossings divisor, H a big line bundle on X, $\delta \in \mathbb{R}_{\geq 0}$, and $r \in \mathbb{Z}_{>0}$.

Then, there is a proper Zariski closed subset $Z = Z(K, S, X, D, H, \delta, r) \subsetneq X$ such that, for all $P \in X(\overline{\mathbb{Q}}) \setminus Z$ with $[\kappa(P) : K] \leq r$,

$$N_S^{(1)}(D, P) + d_K(\kappa(P)) \geq h_{K_X + D}(P) - \delta h_H(P) - O(1).$$

Remark 2.4.2. If you don't truncate (i.e. replace $N_S^{(1)}(D, P)$ with $N_S(D, P)$), call the above statement Vojta 2.0. There is a Vojta 3.0, but we won't get to it. ∘

2.4.1 Loose end from heights

Let X be a smooth projective variety over a number field K. Let $\mathscr{L} \in \operatorname{Pic} X$ be a base point free line, so we get $\varphi_{\mathscr{L}} \colon X \to \mathbb{P}^n$. We defined a height function $h_{\mathscr{L}} \colon X(\overline{\mathbb{Q}}) \to \mathbb{R}$ (up to $O(1)$) via $h_{\mathscr{L}}(P) = h(\varphi_{\mathscr{L}}(P)) + O(1)$.

Notation 2.4.3. $h_D \coloneqq h_{\mathscr{O}_X(D)}$.

Example 2.4.4. If D is an ample (resp. big[2]) divisor, L/K is finite, and $B > 0$, then the set

$$\{P \in X(L) : h_D(P) \leq B\}$$

is finite (resp. not Zariski dense). △

2.4.2 Vojta for algebraic points, with truncation

Let X be a nice variety over a number field K, and let $\Omega_\infty \subset S \subset \Omega_K$ be finite. Let $D = \sum_i D_i$ be our (reduced) normal crossings divisor.

Choose a model $(\mathcal{X}, \mathcal{D})$ of (X, D). Let's assume $\mathcal{X}/\mathscr{O}_{K,S}$ is smooth and proper and that $\mathcal{D} = \sum_i \mathcal{D}_i$ s.t. (X, D) is the generic fiber of $(\mathcal{X}, \mathcal{D}_i)$.

Say $P \in X(\overline{\mathbb{Q}})$ with residue field $L = \kappa(P)$. Spread this out to a point $P \in \mathcal{X}(\mathscr{O}_{L,T})$ ($T = \{w : w \mid v \text{ for some } v \in S\}$).

Notation 2.4.5. We define

$$n_q(\mathcal{D}_i, P) \coloneqq \text{colength of pullback of } \mathcal{D}_i \text{ along } P_q \colon \operatorname{Spec}(\mathscr{O}_{L,T})_q \to \mathcal{X},$$

i.e. $P_q^*(I_{\mathcal{D}_i}) = \mathfrak{m}_q^{n_q(\mathcal{D}_i, P)}$. Then define

$$n_q(D, P) = \sum_i n_q(\mathcal{D}_i, P).$$

This depends on choice of model, but only by "bounded amount."

Definition 2.4.6. We define the counting function

$$N_S(D, P) \coloneqq \frac{1}{[L : K]} \sum_{\mathfrak{q} \in \operatorname{Spec} \mathscr{O}_{L,T}} n_{\mathfrak{q}}(D, P) \cdot \log(\mathscr{O}_L : \mathfrak{q}),$$

[2] Think: D big $\iff nD = A + E$ for some $n \geq 1$, some ample A, and some effective E

along with the truncated counting function

$$N_S^{(1)}(D,P) \coloneqq \frac{1}{[L:K]} \sum_{\substack{\mathfrak{q} \in \operatorname{Spec} \mathscr{O}_{L,T} \\ n_q(D,P)>0}} \log(\mathscr{O}_L : \mathfrak{q}). \qquad \diamond$$

To understand the statement of Conjecture 2.4.1, we'll also need logarithmic discriminants.

Definition 2.4.7. For L/K a finite extension, its logarithmic discriminant is

$$d_K(L) \coloneqq \frac{1}{[L:K]} \log \operatorname{Disc} \mathscr{O}_L - \log \operatorname{Disc} \mathscr{O}_K = \frac{1}{[L:K]} \deg \Omega_{\mathscr{O}_L/\mathscr{O}_K}. \qquad \diamond$$

Remark 2.4.8. Conjecture 2.4.1 is a statement from 1998, appearing in an IMRN paper called "a more generalized abc conjecture". ∘

Remark 2.4.9 (see discussion around Conjecture 2.4.1)**.** Vojta 1.0 = Vojta 2.0 with $r = 1$. ∘

Theorem 2.4.10 (Vojta, 1998)**.** *Vojta 2.1* $\iff$ *Vojta 2.0.*

We are interested in Vojta 2.1 with $r = 1$ (this is *stronger* than Vojta 1.0).

2.4.3 Vojta $\implies$ abc*

Conjecture 2.4.11 (abc conjecture Masser–Osterlé ca. '85)**.** *For all $\varepsilon > 0$, there exists some $C > 0$ such that for all $a, b, c \in \mathbb{Z}$ with*

$$a + b + c = 0 \quad \textit{and} \quad \gcd(a,b,c) = 1,$$

we have

$$\max\{|a|, |b|, |c|\} \leq C \prod_{p \mid abc} p^{1+\varepsilon}.$$

"If you look at the LHS, this immediately just smells like a height."

Proposition 2.4.12. *Vojta 2.1 (Conjecture 2.4.1) with $r = 1$ implies abc (Conjecture 2.4.11) with possibly f.many exceptions.*

Proof. Set $K = \mathbb{Q}$ and $S = \{\infty\}$. Let (a,b,c) be a triple as in Conjecture 2.4.11. This gives a point $P = [a,b,c] \in \mathbb{P}^2(\mathbb{Q})$ lying on the line $L = \{x_0 + x_1 + x_2 = 0\} \simeq \mathbb{P}^1$. Since $\gcd(a,b,c) = 1$, we have $h(P) = \log \max\{|a|, |b|, |c|\}$. Consider the coordinate lines

$$L_0 = \{x_0 = 0\}, \quad L_1 = \{x_1 = 0\}, \quad \text{and} \quad L_2 = \{x_2 = 0\}.$$

Observe: P, considered as a curve in $\mathbb{P}^2_{\mathbb{Z}}$, meets the divisor L_0 (resp. L_1, L_2) at $p \iff p \mid a$ (resp. $p \mid b, p \mid c$). Thus, for $D' = L_0 + L_1 + L_2 \subset \mathbb{P}^2_{\mathbb{Q}}$, we have

$$N_S^{(1)}(D', P) = \sum_{p \mid abc} \log p.$$

Recall 2.4.13. We are aiming to prove Conjecture 2.4.11, i.e. that

$$\log \max\{|a|, |b|, |c|\} \leq \log C + (1+\varepsilon) \sum_{p \mid abc} \log p$$

for all $\varepsilon > 0$ and some $C = C(\varepsilon) > 0$. In the current context, this is equivalent to

$$h(P) \leq (1+\varepsilon)N_S^{(1)}(D', P) + O_\varepsilon(1) \iff N_S^{(1)}(D', P) \geq (1-\delta)h(P) - O_\delta(1) \text{ for } \delta = \frac{\varepsilon}{\varepsilon+1}.$$

This is looking a whole lot like Conjecture 2.4.1 (and also we see why we'll want to apply it on $\mathbb{P}^1$ instead of $\mathbb{P}^2$; $K_{\mathbb{P}^2}$ is too negative). ⊙

Apply Vojta 2.1 (Conjecture 2.4.1) with $K = \mathbb{Q}$, $S = \{\infty\}$, $X = L \simeq \mathbb{P}^1$ and $D = D'|_X = 3$ points on X. Hence, $\mathscr{O}_X(D) \simeq \mathscr{O}_{\mathbb{P}^1}(3)$ and $\mathscr{O}_X(K_X) \simeq \mathscr{O}_{\mathbb{P}^1}(-2)$, so $\mathscr{O}_X(K_X + D) \simeq \mathscr{O}_{\mathbb{P}^1}(1)$ so $h_{K_X+D} = h + O(1)$. Take $H = \mathscr{O}_{\mathbb{P}^1}(1)$, $\delta = \varepsilon/(\varepsilon+1) > 0$ and $r = 1$. With these choices, Conjecture 2.4.1 spits out

$$N_S^{(1)}(D, P) + 0 \geq h_{\mathscr{O}(1)}(P) - \delta h_{\mathscr{O}(1)}(P) - O(1) = (1-\delta)h(P) - O(1)$$

for all but f.many $P \in \mathbb{P}^1(\mathbb{Q})$. All that remains is to check (exercise) that $N_S^{(1)}(D', P) = N_S^{(1)}(D, P)$. ■

Remark 2.4.14. By increasing C, you sees that abc w/ f.many exceptions is equivalent to abc. ∘

3 Damaris Schindler (Universität Göttingen): Counting techniques for rational points

3.1 Lecture 1 (11/5)

We'll talk today and tomorrow about the circle method. Sounds like lectures geared towards those of us who haven't seen analytic methods in point counting before (which is good for me).

Motivation. Counting rational points of bounded height on a hypersurface $X \subset \mathbb{P}^n_{\mathbb{Q}}$. Can also tackle such problems over more general number fields or function fields, but this is an intro, so we'll stick to $\mathbb{Q}$.

Example 3.1.1. Say $X\colon F(x_0,\dots,x_n) = 0$ with $F \in \mathbb{Z}[x_0,\dots,x_n]$ homogeneous. Recall that given $\underline{x} = (x_0,\dots,x_n) \in \mathbb{Z}^{n+1}$ with $\gcd(x_0,\dots,x_n) = 1$, we consider the height function (viewing $\underline{x}$ as a point in projective space)

$$H(\underline{x}) \coloneqq \max_{0\le i\le n} |x_i|\,.$$

This should be the only height we need in this course. Now, we want to count

$$\#\{x \in X(\mathbb{Q})\colon H(x) \le P\} = \frac{1}{2}\#\left\{(x_1,\dots,x_n)\,\middle|\,\begin{array}{c}\gcd(x_1,\dots,x_n)=1, |x_i|\le P\\ \text{and } F(x_1,\dots,x_n)=0\end{array}\right\}$$

(factor of $1/2$ because two such representatives, $\pm\underline{x}$). We'd like an asymptotic formula for such a count. △

Remark 3.1.2. The circle method will require many variables compared to the degree. This automatically puts us in the realm of Fano varieties. ∘

Notation 3.1.3. For $\alpha \in \mathbb{R}$, we set $e(\alpha) \coloneqq e^{2\pi i\alpha}$.

Example 3.1.4. Consider a diagonal hypersurface $x_1^k + \cdots + x_s^k = x_{s+1}^k + \cdots + x_{2s}^k$. Let's ignore the gcd condition for now (to trick to handling it using 'Mobius inversion'). Define

$$N(P) \coloneqq \#\left\{(x_1,\dots,x_{2s})\,\middle|\,\begin{array}{c}|x_i|\le P \text{ and}\\ x_1^k+\cdots+x_s^k = x_{s+1}^k+\cdots+x_{2s}^k\end{array}\right\}.$$

Recall the goal is understand $N(P)$ as $P \to \infty$. We'll translate this into Fourier theory. Define

$$T(\alpha) \coloneqq \sum_{|x|\le P} e(\alpha x^k).$$

Need an indicator function for when an integer is 0 or not. Many such, but we'll use

$$\int_0^1 e(\alpha n)\mathrm{d}\alpha = \begin{cases}1 & \text{if } n = 0\\ 0 & \text{otherwise.}\end{cases}$$

Compute

$$\begin{aligned}\int_0^1 |T(\alpha)|^{2s}\,\mathrm{d}\alpha &= \int_0^1 T(\alpha)^s T(-\alpha)^s \mathrm{d}\alpha\\ &= \sum_{|x_1|\le P}\cdots\sum_{|x_{2s}|\le P}\int_0^1 e\big(\alpha(x_1^k+\cdots+x_s^k-x_{s+1}^k-\cdots-x_{2s}^k)\big)\,\mathrm{d}\alpha\\ &= \#\left\{x_1,\dots,x_{2s}\in\mathbb{Z} \mid |x_i|\le P \text{ and } x_1^k+\cdots+x_s^k-(x_{s+1}^k+\cdots+x_{2s}^k)=0\right\}\end{aligned}$$

$$= N(P).$$

The hope is that we can now understand this exponential sum. What should we expect the answer to be? △

3.1.1 Heuristics for the growth of $N(P)$

We'll discuss two such heuristics, one from Diophantine side and one from Fourier side.

Diophantine Vaguely assume things behave "randomly". Consider the map

$$\varphi\colon \{(x_1,\dots,x_{2s}) \mid |x_i| \le P\} \longmapsto x_1^k + \cdots + x_s^k - (x_{s+1}^k + \cdots + x_{2s}^k).$$

Note this lands in $[-2sP^k,\dots,2sP^k]$. Suppose for now that the images are equidistributed (among integers in this range), so the probability we hit zero is roughly P^{2s}/P^k, i.e. $N(P) \approx P^{2s-k}$.

Fourier For a second heuristic, recall $N(P) = \int_0^1 |T(\alpha)|^{2s}\,\mathrm{d}\alpha$, where $T(\alpha) = \sum_{|x|\le P} e(\alpha x^k)$. Note that, for $\alpha = 0$ and $P \in \mathbb{N}$, we have $T(0) = 2P+1$. What about for α close to zero?

If $|\alpha| \le c_0 P^{-k}$ for sufficiently small constant c_0, then for each term: $\left|e(\alpha x^k) - 1\right| \le \frac{1}{100}$ (when $|x| \le P$). For such α, we get $|T(\alpha)| \gg P$ (larger than a constant times P). So, from the region

$$\int_{|\alpha| \ll P^{-k}} |T(\alpha)|^{2s}\,\mathrm{d}\alpha,$$

we expect a contribution of size roughly P^{2s-k}.

You could try to do a similar thing around $\alpha = \frac{1}{2}, \frac{1}{3}, \dots$ (rationals with small denominator). For a more generic value of α, one could expect the terms $e(\alpha x^k)$ to be randomly distributed along the unit circle $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. This would lead to the expectation that $T(\alpha) \sim P^{1/2}$ ('square root cancellation').[3] Hence,

$$\int_{\text{generic } \alpha} |T(\alpha)|^{2s}\,\mathrm{d}\alpha \approx P^s.$$

Above should be error term, so we want $2s - k > s$, i.e. $s > k$.

Remark 3.1.5. Only expect to prove this asymptotic if $s > k$. This is called the square root barrier. In order to be Fano, only need $2s > k$, so Manin's conjecture kicks in earlier. There are some (but few?) cases known where we can push beyond this square root barrier. ∘

Let's try and discuss this 'generic α' bit a little more precisely.

3.1.2 Weyl's inequality and Hua's inequality

Recall

$$N(P) = \int_0^1 |T(\alpha)|^{2s}\,\mathrm{d}\alpha \text{ where } T(\alpha) = \sum_{|x|\le P} e(\alpha x^k).$$

[3] Some mention of the central limit theorem that I did not catch.

Lemma 3.1.6 (Weyl's inequality)**.** *Let $\varepsilon > 0$. Assume that there are coprime integers $a \in \mathbb{Z}$, $q \in \mathbb{N}$ such that*[4] $|\alpha - a/q| \le 1/q^2$*. Then,*

$$|T(\alpha)| \ll P^{1+\varepsilon}\left(P^{-1/\mathcal{K}} + q^{-1/\mathcal{K}} + \left(\frac{P^k}{q}\right)^{-1/\mathcal{K}}\right),$$

where $\mathcal{K} = 2^{k-1}$.

Remark 3.1.7. The trivial upper bound is $|T(\alpha)| \ll P$, so we get savings once q is large than a small power of P. For $P \le q \le P^{k-1}$, we obtain

$$|T(\alpha)| \ll P^{1-1/\mathcal{K}+\varepsilon}.$$

Note this saving will be $2s$ times as big since we really compute with $|T(\alpha)|^{2s}$. This is one reason why circle method requires a large number of variables. ∘

Example 3.1.8. Let q be prime and $k = 2$. Set $\alpha = 1/q$ and $P = q$. Then,

$$T\left(\frac{1}{q}\right) = \sum_{x=-q}^{q} e\left(\frac{x^2}{q}\right) = 1 + 2\sum_{x=1}^{q} e\left(\frac{x^2}{q}\right).$$

Note that we have a quadratic Gauss sum above. It has absolute value around $q^{1/2}$. Hence, by bounding the Gauss sum, $|T(1/q)| \le 2\sqrt{q} + 1$.

What does Weyl give? Lemma 3.1.6 shows that

$$\left|T\left(\frac{1}{q}\right)\right| \ll q^{1+\varepsilon-1/2} = q^{1/2+\varepsilon}$$

which is pretty good. △

Let's see a bit about the idea of the proof of Lemma 3.1.6.

We can bound linear exponential sums, because these are geometric sums.

$$\sum_{|x|\le P} e(\alpha x) \ll \min\left(P, \|\alpha\|^{-1}\right) \quad \text{where } \|\alpha\| \coloneqq \min_{m\in\mathbb{Z}} |\alpha - m|$$

(note: $\|\alpha\|$ is the *distance from α to the nearest integer*).

Example 3.1.9 (Weyl differencing for $k = 2$)**.** Now consider

$$|T(\alpha)|^2 = \left|\sum_{|x|\le P} e(\alpha x^2)\right|^2 = \sum_{|x|\le P}\sum_{|y|\le P} e\left(\alpha(x^2 - y^2)\right).$$

Substitute $x = y + h$, so

$$|T(\alpha)|^2 = \sum_{|y|\le P}\sum_{h:\ |y+h|\le P} e\left(\alpha((y+h)^2 - y^2)\right).$$

Above, $(y+h)^2 - y^2 = 2hy + h^2$ is linear in y. Change the order of summation:

Maybe I copied this down incorrectly. If this note is still here, I haven't yet double checked this.

[4] Alway's possible by Dirichlet's lemma Theorem 2.1.7

$$|T(\alpha)|^2 \leq \sum_h \left| \sum_{|y|\leq P \text{ and } |h+y|\leq P} e(\alpha \cdot 2hy) \right| \qquad \triangle$$

3.2 Lecture 2 (11/6)

Let's try to pick up were we left off. We discussed the counting function

$$N(P) = \#\left\{x_1, \ldots, x_{2s} \in \mathbb{Z} \mid |x_i| \leq P \text{ and } x_1^k + \cdots + x_s^k = x_{s+1}^k + \cdots + x_{2s}^k\right\}.$$

We re-expressed this as a Fourier integral over an exponential sum:

$$N(P) = \int_0^1 |T(\alpha)|^{2s} \, \mathrm{d}\alpha \text{ where } T(\alpha) = \sum_{|x|\leq P} e(\alpha x^k). \tag{3.1}$$

We realize that $T(\alpha)$ is big near $\alpha = 0$ and used this to predict an asymptotic of the shape cP^{2s-k} for some $c > 0$. For 'generic' α (say, not close to a rational number), we said we expect some square-root cancellation. These observations will be made more precise via the introduction of major/minor arcs.

3.2.1 Major and minor arcs

Assume $k \geq 2$ and introduce a fixed parameter $\delta > 0$.

For integers $1 \leq a \leq q$ with $\gcd(a, q) = 1$ (we'll consider the fraction a/q), set

$$\mathfrak{M}_{a,q} = \left\{\alpha \in \mathbb{R} : \left|\alpha - \frac{a}{q}\right| < P^{-k+\delta}\right\}.$$

The major arcs consist of the union

$$\mathfrak{M} = \bigcup_{q \leq P^\delta} \bigcup_{\substack{a=1 \\ \gcd(a,q)=1}}^{q} \mathfrak{M}_{a,q}$$

of these $\mathfrak{M}_{a,q}$ for fractions with 'small' denominator. Note that $\mathfrak{M}$ has relatively small volume (something like $P^{-k+3\delta}$), but we expect them to give the main contribution to our integral (3.1). The minor arcs are the complement

$$\mathfrak{m} = [0, 1] \setminus \mathfrak{M}.$$

Lemma 3.2.1. *If $2s \geq 2^k + 1$, then there exists some $\delta' > 0$ such that*

$$\int_{\mathfrak{m}} |T(\alpha)|^{2s} \, \mathrm{d}\alpha \ll P^{2s-k-\delta'}$$

Note this is smaller than the expected main term (P^{2s-k}), so it says the minor acts go into the error term. We need three ingredients to prove this.

Lemma 3.2.2 (Dirichlet's lemma)**.** *Let $\alpha \in \mathbb{R}$, $Y \in \mathbb{R}_{>0}$. Then, there exists $q \in \mathbb{N}, a \in \mathbb{Z}$ with $1 \leq q \leq Y$ and $\gcd(a, q) = 1$ such that*

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qY}.$$

Theorem 3.2.3 (Weyl's inequality). *If $|\alpha - a/q| < 1/q^2$, then*

$$|T(\alpha)| \ll P^{1+\varepsilon}\left(P^{-1} + q^{-1} + \left(\frac{P^k}{q}\right)^{-1}\right)^{\frac{1}{2^{k-1}}}$$

Theorem 3.2.4 (Hua's inequality).

$$\int_0^1 |T(\alpha)|^{2^k}\,\mathrm{d}\alpha \ll P^{2^k-k+\varepsilon}$$

(think of this as an averaged form of Weyl's inequality)

Remark 3.2.5. Note that

$$\int_0^1 |T(\alpha)|^{2^k} = \#\left\{x_1,\dots,x_{2^k} \in \mathbb{Z} : |x_i| \le P \text{ and } x_1^k + \cdots + x_{2^{k-1}}^k = x_{2^{k-1}+1}^k + \cdots + x_{2^k}^k\right\}.$$

∘

Proof of Lemma 3.2.1. We want to bound the integral over minor arcs, assuming $2s \ge 2^k + 1$.

$$\begin{aligned}\int_{\mathfrak{m}} |T(\alpha)|^{2s}\,\mathrm{d}\alpha &\ll \sup_{\alpha\in\mathfrak{m}} |T(\alpha)|^{2s-2^k} \cdot \int_0^1 |T(\alpha)|^{2^k}\,\mathrm{d}\alpha \\ &\ll \sup_{\alpha\in\mathfrak{m}} |T(\alpha)|^{2s-2^k} \cdot P^{2^k-k+\varepsilon} \qquad \text{Theorem 3.2.4}\end{aligned}$$

Now, for $\alpha \in \mathfrak{m}$, apply Lemma 3.2.2 with $Y = P^{k-\delta}$ to find $1 \le a \le q$ coprime such that

$$\left|\alpha - \frac{a}{q}\right| \le \frac{1}{q}P^{-k+\delta}.$$

If q was small, we'd be in the major arcs. Since $q\alpha \in \mathfrak{m}$, we conclude that $q > P^\delta$. Now apply Weyl's inequality Lemma 3.1.6 to deduce that

$$|T(\alpha)| \ll P^{1+\varepsilon}P^{-\frac{\delta}{2^{k-1}}}.$$

Thus,

TODO: Double check the exponents

$$\int_{\mathfrak{m}} |T(\alpha)|^{2s}\,\mathrm{d}\alpha \ll \left(P^{1-\frac{\delta}{2^{k-1}}}\right)^{s-2^k} \cdot P^{2^k-k+\varepsilon} \ll P^{2s+\varepsilon-\delta'} \text{ where } \delta' = \delta\cdot 2^{k-1}.$$ ■

What about the Major arcs?

Example 3.2.6. Say $\alpha = a/q$ is a rational number. Then (note the exponential only depends on x mod q below),

$$T\left(\frac{a}{q}\right) = \sum_{x=-P}^{P} e\left(\frac{a}{q}x^k\right) \sim \frac{2P}{q}\sum_{y=1}^{q} e\left(\frac{a}{q}y^k\right)$$

and this looks handlable (it's similar to a Gauss sum?). △

For $\alpha = \frac{a}{q} + \beta \in \mathfrak{M}_{a,q}$ (so β small and $q \le P^\delta$), can do something similar

$$T\left(\frac{a}{q}+\beta\right) = \sum_{x=-P}^{P} e\left(\left(\frac{a}{q}+\beta\right)x^k\right) = \sum_{y=1}^{q} \sum_{z:|y+zq|\le P} e\left(\left(\frac{a}{q}+\beta\right)(y+zq)^k\right) = \sum_{y=1}^{q} e\left(\frac{a}{q}y^k\right) \sum_{z:|y+zq|\le P} e\big(\beta(y+zq)^k\big).$$

If $\beta = 0$, would get something like P/q in the second factor (adding up a bunch of 1's). In reality, compare the second factor with a corresponding integral to deduce that (think: $u = y + zq$)

$$T\left(\frac{a}{q}+\beta\right) \sim \sum_{y=1}^{q} e\left(\frac{a}{q}y^k\right) \cdot \frac{1}{q} \int_{-P}^{P} e\big(\beta u^k\big)\,\mathrm{d}u.$$

We want to put all this together to compute the integral over the major arcs.

$$\begin{aligned}\int_{\mathfrak{M}} |T(\alpha)|^{2s}\,\mathrm{d}\alpha &\sim \sum_{q\le P^\delta} \sum_{\substack{a=1\\ \gcd(a,q)=1}}^{q} \int_{|\beta|<P^{-k+\delta}} \left|T\left(\frac{a}{q}+\beta\right)\right|^{2k} \mathrm{d}\beta \\ &\sim \sum_{q\le P^\delta} \sum_{\substack{a=1\\ \gcd(a,q)=1}}^{q} \left|\frac{1}{q}\sum_{y=1}^{q} e\left(\frac{a}{q}y^k\right)\right|^{2s} \int_{|\beta|<P^{-k+\delta}} \left|\int_{-P}^{P} e\big(\beta u^k\big)\,\mathrm{d}u\right|^{2s} \mathrm{d}\beta.\end{aligned}$$

This splits into two parts (the sum of a's and q's, and the integral over β): the arithmetic (finite prime) and integral (infinite prime) parts. It turn's out the finite part absolutely converges even if you let q run from 1 to ∞. The finite part,

$$\sum_{q=1}^{\infty} \sum_{\substack{a=1\\ \gcd(a,q)=1}}^{q} \left|\frac{1}{q}\sum_{y=1}^{q} e\left(\frac{a}{q}y^k\right)\right|^{2s} = \mathfrak{S}$$

is called a `singular series` and the infinite part

$$\int_{|\beta|<P^{-k+\delta}} \left|\int_{-P}^{P} e\big(\beta u^k\big)\,\mathrm{d}u\right|^{2s} \mathrm{d}\beta$$

is called a `singular integral`. This piece will have size roughly $P^{2s-k}\cdot\gamma$ (probably won't have time to derive this here).

Combining major and minor arcs gives that

$$N(P) = \mathfrak{S}\gamma P^{2s-k} + O\Big(P^{2s-k-\delta'}\Big),$$

so we get the leading constant coming separately from finite and infinite places. Can think of this as an analytic local-global principle. One can show that

$$\mathfrak{S} = \prod_{p \text{ prime}} \sigma_p \text{ where } \sigma_p = \lim_{J\to\infty} \sum_{j=0}^{J} \sum_{\substack{a=1\\ p\nmid a}}^{p^j} \left|p^{-j}\sum_{y=1}^{p^j} e\left(\frac{a}{p^j}y^k\right)\right|^{2s}. \tag{3.2}$$

This of σ_p as a p-adic analogue of the integral of $|T(\alpha)|^{2s}$. By analogy, should expect this to be related

to a count of points mod p. Note

$$p^{-J}\sum_{y=1}^{p^J} e\left(\frac{aP^{J-j}}{p^J}y^k\right) = p^{-j}\sum_{y=1}^{p^j} e\left(\frac{a}{p^j}y^k\right),$$

so we can make all these inner sums (in (3.2)) have the same length. Thus,

$$\sigma_p = \lim_{J\to\infty} p^{-2sJ}\sum_{Y_1=1}^{p^J}\cdots\sum_{Y_{2s}=1}^{p^J} e\left(\frac{a}{p^J}\left(Y_1^k+\cdots+Y_s^k-Y_{s+1}^k-\cdots-Y_{2s}^k\right)\right)$$

Now use that

$$\sum_{a=1}^{q} e\left(\frac{am}{q}\right) = \begin{cases} 0 & \text{if } q\nmid m \\ q & \text{otherwise.}\end{cases}$$

Thus,

$$\sigma_p = \lim_{J\to\infty} p^{-J(2s-1)}\#\left\{y_1,\dots,y_{2s} \bmod p^J : y_1^k+\cdots+y_s^k \equiv y_{s+1}^k+\cdots+y_{2s}^k \bmod P^J\right\}.$$

Note we expect p^{2sJ-J} solutions (if things are random), so we use this as our normalization. This also shows that σ_p (and so $\mathfrak{S}$) is positive.

3.2.2 Vinogradov

Recall that the above discussion required $2s \geq 2^k+1$, so need many many variables. Can cut this down these days using Vinogradov's mean value theorem.

Let

$$J_s^k(P) = \#\left\{x_1,\dots,x_{2s}\in\mathbb{Z} : 1\leq x_i\leq P \text{ and } \sum_{i=1}^{s} x_i^j = \sum_{i=s+1}^{2s} x_i^j \text{ for all } 1\leq j\leq k\right\}.$$

This set is invariant under dilation (scale by fix number) and translation (add 1 to each variable).

Theorem 3.2.7 (Vinogradov's mean value theorem)**.** $J_s^k \ll \left(P^{2k-\frac{k(k+1)}{2}}+P^s\right)P^{\varepsilon}$

(note $k(k+1)/2 = 1+2+\cdots+k$ is the sum of the degrees of the equations).

Remark 3.2.8. The P^s summand comes from trivial solutions (e.g. $x_i = x_{i+s}$ for all $1\leq i\leq s$). ∘

To make use of this, consider

$$f(\underline{\alpha}) = \sum_{x=1}^{p} e\left(\alpha_1 x+\alpha_2 x^2+\cdots+\alpha_k x^k\right),$$

and observe that

$$\int_{[0,1]^k} |f(\underline{\alpha})|^{2s}\,\mathrm{d}\alpha = J_s^k(P).$$

Introduce parameters

$$J_s^k(P,h_1,\dots,h_{k-1}) = \#\left\{1\leq x_i\leq P, i=1,\dots,2s, \sum_{i=1}^{s} x_i^j - \sum_{i=s+1}^{2s} x_i^j = h_j, 1\leq j\leq k\right\}.$$

This is equal to

$$\int_{[0,1]^k} |f(\underline{\alpha})|^{2s} e(-\alpha_1 h_1 - \cdots - \alpha_k h_k)\, \mathrm{d}\alpha$$

whose absolute value is at most

$$\int_{[0,1]^k} |f(\underline{\alpha})|^{2s}\, \mathrm{d}\alpha = J_s^k(P, \underline{0}).$$

Finally,

$$\int_0^1 |T(\alpha)|^{2s}\, \mathrm{d}\alpha = \sum_{h_1} \cdots \sum_{h_{k-1}} J_s^k(P, h_1, \ldots, h_{k-1}, 0) \ll PP^2 \ldots P^{k-1} P^{2s-k(k+1)/2+\varepsilon} \ll P^{2s-k+\delta},$$

so can get down to something like $2s > k^2$ for the number of variables.

3.3 Lecture 3 (11/7): Sieves

Note 7. I get the impression I won't understand much of what happens in this lecture

She wrote up on overview of (especially the end of) yesterday. Maybe if I find the energy, I'll take a picture before it gets erased and later put it in these notes (maybe).

Update: I did not

3.3.1 Quick Review

On the global side, we started with

$$N(P) = \#\left\{|x_i| \le P, 1 \le i \le 2s, x_1^k + \cdots + x_s^k = x_{s+1}^k + \cdots + x_{2s}^k\right\}.$$

We expressed this in the Fourier side as

$$N(P) = \int_0^1 |T(\alpha)|^{2s}\, \mathrm{d}\alpha \text{ where } T(\alpha) = \sum_{|x| \le P} e(\alpha x^k).$$

We studied the minor arcs to put them in the error term. This was the source of needing many variables to apply the circle method. After getting rid of these, we're left with the major arcs. Near a rational number, we have

$$T\left(\frac{a}{q} + \beta\right) \sim \frac{1}{q} \sum_{y=1}^{q} e\left(\frac{a}{q} y^k\right) \int_{-P}^{P} e\big(\beta u^k\big)\, \mathrm{d}u,$$

which has the break up between finite and infinite places. In the end, one finds that

$$N(P) \sim \left(\prod_{p \le \infty} \sigma_p\right) P^{2s-k},$$

where

$$\sigma_p = \lim_{N \to \infty} p^{-N(2s-1)} \#\left\{x_1, \ldots, x_{2s} \bmod p^N : x_1^k + \cdots + x_s^k = x_{s+1}^k + \cdots + x_{2s}^k \bmod p^N\right\}$$

(and $\int_{-P}^{P} e(\beta u^k) \mathrm{d}u = \sigma_\infty P^{2s-k}$, I think?).

Remark 3.3.1. If you have sufficiently many local solutions mod p^N, then can prove that $\prod \sigma_p > 0$ and therefore there must be a global solution. Thus, this gives an "analytic Hasse principle". ∘

3.3.2 Sieves

To start with some motivation, let's discuss norm form equations.

Let $K/\mathbb{Q}$ be a number field, $d = [K : \mathbb{Q}]$. Choose a $\mathbb{Q}$-basis $\omega_1, \dots, \omega_d$. Consider the norm form

$$N(x_1, \dots, x_d) = \mathrm{N}_{K/\mathbb{Q}}(x_1\omega_1 + \cdots + x_d\omega_d) \in \mathbb{Q}[x_1, \dots, x_d]_{\deg = d}.$$

Let $f(t) \in \mathbb{Z}[t]$ be another polynomial and consider the affine variety

$$N(x_1, \dots, x_d) = f(t) \neq 0.$$

Conjecturally, the Brauer–Manin obstruction is the only one for such varieties. There's much more one could say here, but let's move on for now.

Example 3.3.2. $K = \mathbb{Q}(i)$ and $X(x_1, x_2) = x_1^2 + x_2^2$. Let's homogeneous f, so consider $f(a/b) = b^{-\deg f} f(a, b)$. We want to solve $b^{-\deg f} f(a, b) = \square + \square$ with a, b both integers. Maybe first try to find $a, b \in \mathbb{Z}$ such that $b, f(a, b) > 0$ and so that $bf(a, b)$ is composed of primes which are $\equiv 1 \bmod 4$. This is the sort of thing sieves help with. △

Formulation of a sieve problem Let $x \in \mathbb{R}_{>0}$ and choose some $\mathcal{A} = (a_n)_{n<x}$ with $a_n \in \mathbb{R}_{\geq 0}$ always. Let $\mathcal{P}$ be a set of prime numbers (these will be the primes we want to remove). For $z > 0$ (the sifting level), we set

$$\mathcal{P}(z) = \prod_{\substack{p \in \mathcal{P} \\ p < z}} p.$$

Goal. Understand the sifting function

$$S(\mathcal{A}, z) \coloneqq \sum_{\substack{n \leq x \\ \gcd(n, P(z)) = 1}} a_n.$$

Example 3.3.3 (Eratosthenes, up to spelling)**.** Set $a_n = 1$ for all n, $z = \sqrt{x}$, and $\mathcal{P}$ the set of *all* prime numbers. Then,

$$S(\mathcal{A}, z) = \sum_{\substack{n \leq x \\ \gcd\left(n, \prod_{p<z} p\right)}} 1 = \#\left\{p : \sqrt{x} \leq p \leq x\right\} = \pi(x) + O(\sqrt{x}).$$ △

Example 3.3.4 (Example 3.3.2)**.** Choose some $N \in \mathbb{N}$. Set

$$a_n = \sum_{\substack{n = bf(a,b) \\ (a,b) \in \mathbb{Z}^2 \cap [0,N]^2}} 1 = \#(a, b) \in \mathbb{Z}^2 \cap [0, N]^2 : bf(a, b) = n.$$

Note that $bf(a, b) \ll N^{\deg f + 1}$, so we'll set $x \sim N^{\deg f + 1}$. Just for concreteness, suppose f is a cubic, so $\deg f + 1 = 4$. Set $\mathcal{P} = \{\text{prime } p \equiv 3 \bmod 4\}$. We would like to show that $S(\mathcal{A}, z) > 0$ for $z \sim N^3$ (because a prime dividing b or $f(a, b)$ will have size $\ll \max(N, N^3)$) and N sufficiently large. △

As an indicator function for $\gcd(n, P(z)) = 1$, we use the Mobius function. Note (exercise)

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Here, the Mobius function is

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n \text{ is a product of } r \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

Thus,

$$S(\mathcal{A}, z) = \sum_{n \le x} a_n \sum_{d \mid \gcd(P(z), n)} \mu(d) = \sum_{d \mid P(z)} \mu(d) \sum_{\substack{n \le x \\ d \mid n}} a_n$$

(can think of end result as inclusion-exclusion principle). For $d \in \mathbb{N}$, we write

$$A_d(x) = \sum_{\substack{n \le x \\ d \mid n}} a_n \text{ and } A(x) = a_1(x) = \sum_{n \le x} a_n,$$

so $S(\mathcal{A}, z) = \sum_{d \mid P(z)} \mu(d) A_d(x)$. Note we expect $A_d(x)$ to be a proportion of $A(x)$ typically (what's the probability something in our sequence is divisible by d?)

Example 3.3.5 (Example 3.3.3)**.** In this example, we have $A_d(x) = \sum_{n \le x \text{ and } n \equiv 0 \bmod d} 1 = \lfloor x/d \rfloor \sim x/d$. △

Assumption (soft)**.** We often assume that there is some $X(x) \in \mathbb{R}$, a function $g \colon \mathbb{N} \to \mathbb{R}$ and a function $r_d(x)$ ($d \in \mathbb{N}$, $x \in \mathbb{R}$) such that

$$A_d(x) = g(d)X(x) + r_d(x)$$

($r_d(x)$ should be an error term).

If we substitute $A_d(x) \sim g(d)X$, we would get

$$S(\mathcal{A}, z) \sim \sum_{d \mid P(z)} \mu(d) g(d) X = X \sum_{d \mid P(z)} \mu(d) g(d).$$

Assume further that g is multiplicative, so we get an Euler product

$$S(\mathcal{A}, z) \sim X \prod_{\substack{p \in \mathcal{P} \\ p < z}} (1 - g(p)).$$

Example 3.3.6 (Example 3.3.3)**.** Recall $a_n = 1$, $z = \sqrt{x}$, $\mathcal{P} = \{\text{all primes}\}$. Furthermore, $S(\mathcal{A}, z) = \pi(x) + O(\sqrt{x})$ and $A_d(x) = x/d + O(1)$. Hence, $g(p) = 1/p$ and $|r_d(x)| \le 1$. Then,

$$S(\mathcal{A}, z) = x \prod_{p < \sqrt{x}} \left(1 - \frac{1}{p}\right) + \sum_{d \mid P(z)} \mu(d) r_d(x).$$

By Merten's (up to spelling) theorem, $\prod_{p<z}(1 - 1/p) \sim e^{-\gamma}/\log z$, so $S(\mathcal{A}, z) \sim 2e^{-\gamma} \frac{x}{\log x} + \text{error terms}$. This is unfortunate because we expect/know the main term should have to be a constant of 1 out front. What's gone wrong?

Can think that the even of being divisible by p is not independent as you vary p. Imagine you have $p_1, p_2, p_3 \sim \sqrt{x}$. Then a number of size x being divisible by p_1, p_2 and/or p_3 are not independent events (if it's divisible by p_1, p_2 it certainly can't be divisible by p_3 or else it'd be too big).

From another perspective, $P(z)$ has too many divisors, so the 'error term' will be too big. △

Definition 3.3.7. We call a sequence $(\lambda^{\pm}(d))_{d|P(z)}$ (or defined for all d if you like) a `upper/lower bound sieve` if

$$\sum_{d|n} \lambda^{-}(d) \leq \sum_{d|n} \mu(d) \leq \sum_{d|n} \lambda^{+}(d).$$

◇

With such a thing, one gets

$$\sum_{d|P(z)} \lambda^{-}(z) A_d(x) \leq S(\mathcal{A}, z) \leq \sum_{d|P(z)} \lambda^{+}(d) A_d(x).$$

Remark 3.3.8. If $\lambda^{+}(d) = 0$ for $d > D$, then you'd get something like

$$S(\mathcal{A}, z) = \sum_{d|P(z)} \lambda^{+}(d) g(d) X + \sum_{d \leq D} |r_d(x)|,$$

so only have to worry about error terms for small d. ◦

Example 3.3.9 (Example 3.3.3)**.** Can try something like $\lambda^{-}(d) = \mu(d)$ if d divisible by at most one prime (and 0 otherwise). See exercise session. △

3.4 Lecture 4 (11/8): Methods from additive combinatorics

Note 8. The bottom half the board is low-key blocked by a sea of backs of heads...

Motivation from yesterday: when does the Hasse principle hold for the affine variety

$$0 \neq f(t) = N(x_1, \ldots, x_d)?$$

Consider the special case where f is a product of linear factors.

Remark 3.4.1. We don't have a ton of time, so the main goal is to show how to reformulate this into a problem which can be attacked with some established machinery. ◦

After homogenizing, we can reduce to the following problem.

Let $\ell_1(\lambda, \mu), \ldots, \ell_n(\lambda, \mu) \in \mathbb{Z}[\lambda, \mu]$ for pairwise linearly independent linear forms. It would be nice if each ℓ_i were a linear form, so we search for $\lambda, \mu \in \mathbb{Z}^+$ such that

$$\ell_i(\lambda, \mu) = N(\underline{x}_i) \neq 0 \text{ for some } \underline{x}_i = (x_{i,1}, \ldots, x_{i,d}) \in \mathbb{Z}^d.$$

Let $K \subset \mathbb{R}^2$ be some 'nice' compact region (e.g. $K = [0,1]^2$). Define representation function

$R(n) = \#$representations of n as $N(\underline{x})$ where $x_1\omega_1 + \cdots + x_d\omega_d$ lies in some fundamental domain for the unit action.

We study the correlation function

$$N(T) = \sum_{(\lambda,\mu) \in \mathbb{Z}^2 \cap T \cdot K} \prod_{i=1}^{n} R(\ell_i(\lambda, \mu)) \text{ for } T \to \infty$$

(will count solutions to $\ell_1(\lambda, \mu) \ldots \ell_n(\lambda, \mu) = N(\underline{x})$ is some fundamental domain).

Remark 3.4.2. A 'similar' problem would be correlations of the von Mongoldt function $\Lambda(n)$ (recall: $\Lambda(p^k) = \log p$ and $\Lambda(n) = 0$ otherwise), e.g.,

$$\sum_{(\lambda,\mu)\in\mathbb{Z}^2\cap T\cdot K}\prod_{i=1}^{n}\Lambda(\lambda+(i-1)\mu)\,.$$

Note, $\lambda, \lambda+\mu, \lambda+2\mu$,... gives an arithmetic progression, so this studies weighted number of n-term arithmetic progressions in the primes. This is the sort of thing Green and Tao used in their 2008 work on arithmetic progressions in primes. ◦

Remark 3.4.3 (Browning, Matthieson 2016)**.** They extended Green-Tao's techniques to obtain asymptotics for $N(T)$ of the form

$$N(T) = \prod_{p\leq\infty} B_p \cdot T^2 + o(T^2).$$ ◦

To discuss the machinery, let's consider a more general set-up.

Setup 3.4.4. Choose $\psi_i\colon \mathbb{Z}^s \to \mathbb{Z}$ for $1 \leq i \leq n$ (s fixed but arbitrary. Previously, $s = 2$). Also consider affine linear forms $f_1, \dots, f_n\colon \mathbb{Z} \to \mathbb{R}$ and let $K \subset \mathbb{R}^2$ be a compact set.

Maybe want to study

$$\sum_{\underline{u}\in T\cdot K\cap\mathbb{Z}^s}\prod_{i=1}^{n} f_i(\psi_i(\underline{u}))$$

Definition 3.4.5. We say that the system $\underline{\psi} = (\psi_1, \dots, \psi_n)$ has `complexity` at most k if the following holds. For every $i \in \{1, \dots, n\}$ one can partition the functions $\{\psi_j : j \neq i\}$ into $k+1$ classes such that ψ_i is not contained in the affine linear span of any of these classes. ◇

Example 3.4.6. Take u_1, u_1+u_2, u_1+2u_2, 3 functions in 2 variables (also related to 3 term arithmetic progressions). This has complexity 1. △

Example 3.4.7. The system $u_1, u_1+u_2, \dots, u_1+(k+1)u_2$ has complexity k. Note if you have two forms in the same class, they'll span everything, so need $k+1$ classes. △

Example 3.4.8. The system u_1, u_1+2 has infinite complexity (i.e. Definition 3.4.5 holds for *no* k). So this sort of machinery won't work for twin primes (infinite complexity is out of reach). △

You should this of 'complexity 1' as the realm where the circle method applies. E.g. for three-term arithmetic progressions have 3 variables and 1 equation so circle might produce something like T^{3-1} in major arcs but only $T^{3/2}$ in the minor arcs. For a k-term arithmetic progression, can formulate it as a system of linear equations with $k+2$ variables and k equations (all numbers determined from first two), so get T^{k+2-k} is major arcs but square-root cancellation would have a $T^{(k+2)/2}$ showing up in the minor arcs, but $2 > (k+2)/2 \iff k = 1$.

Slogan. Complexity machinery is moving beyond the circle method.

Motivation. If all f_i were bounded, then correlations of the form

$$\sum_{\underline{u}\in\mathbb{Z}^s\cap T\cdot K}\prod_{i=1}^{n} f_i(\psi_i(\underline{u}))$$

are essentially controlled by Gowers norms of the f_i (if ψ_i has finite complexity).

First: move from $\mathbb{Z}$ to a finite group setting. Choose a prime $T' \in [CT, 2CT]$ with C sufficiently large. Define

$$\widetilde{f_i} \colon \frac{\mathbb{Z}}{T'\mathbb{Z}} \longrightarrow \mathbb{R}$$

via

$$\widetilde{f_i}(x) = \begin{cases} f_i(x) & \text{if } x \in \{1, \dots, T\} \\ 0 & \text{otherwise.} \end{cases}$$

This is supposed to not change the values showing up in the expression we're actually interested in controlling, but have the advantage of formally moving us to a finite group setting.

Definition 3.4.9 (Gowers norms)**.** Let $k \geq 0$. Set

$$\|f\|_{U^{k+1}(T')}^{2^{k+1}} := (T')^{-k-2} \sum_{x \in \mathbb{Z}/T'\mathbb{Z}} \sum_{\underline{h} \in (\mathbb{Z}/T'\mathbb{Z})^{k+1}} \prod_{\underline{\omega} \in \{0,1\}^{k+1}} f\left(x + \sum_{j=1}^{k+1} \omega_j h_j\right). \qquad \diamond$$

You're evaluating f at all the corners of a cube/parallelepiped and then averaging over all such cubes and all such sizes of cubes.

Warning 3.4.10. If f is complex-valued, you want to take $\overline{f}$ in the product whenever $\sum \omega_j \in 2\mathbb{Z}+1$. •

Remark 3.4.11. If f is bounded, then its norm is bounded as well. Also $\|f\|_{U^{k+1}(T')}$ (without the 2^{k+1}th power) scales linearly. ◦

Example 3.4.12 ($k = 1$)**.**

$$\begin{aligned} \|f\|_{U^2(T')}^4 &= (T')^{-3} \sum_{x, h_1, h_2} f(x)\overline{f}(xx + h_1)\overline{f}(x + h_2)f(x + h_1 + H_2) \\ &= (T')^{-3} \sum_{a+d=b+c} f(a)\overline{f}(b)\overline{f}(c)f(d) \end{aligned}$$

Consider Fourier transform

$$\widehat{f}(\xi) = (T')^{-1} \sum_{n \in \mathbb{Z}/T'\mathbb{Z}} f(n) e\left(\frac{\xi n}{T'}\right).$$

By orthogonality, one has

$$\|f\|_{U^2(T')}^4 = \sum_{\xi \in \mathbb{Z}/T'\mathbb{Z}} \left|\widehat{f}(\xi)\right|^4,$$

which is essentially just summing the Fourier coefficients of your function. △

Theorem 3.4.13 (generalized von Neumann Theorem)**.** *Assume that there exists a function $\nu \colon \mathbb{Z}/T'\mathbb{Z} \to \mathbb{R}_{>0}$, a pseudorandom measure, such that $|f_i(x)| \leq \nu(x)$ for all i, x. Let $\underline{\psi}$ be as before, of complexity k.*[5] *Assume that*

$$\|f_i\|_{U^{k=1}(T')} \leq \delta \text{ for some } i \text{ and } \delta > 0,$$

then

$$\sum_{\underline{u} \in T \cdot K \cap \mathbb{Z}^2} \prod_{i=1}^{n} f_i(\psi_i(\underline{u})) = o_\delta(T^s) + \kappa(\delta)T^s$$

with $\kappa(\delta) \to 0$ as $\delta \to 0$.

[5] We're sweeping something under the rug here

Example 3.4.14. Let $\mathcal{A} \subset \mathbb{Z}/T'\mathbb{Z}$ of size $\#\mathcal{A} \geq cT'$. Set $f(x) = f_i(x) = \mathbf{1}_{x\in\mathcal{A}} - \#\mathcal{A}/T'$ for all i (balanced indicator function; average $= 0$). Assume $\|f\|_{U^{n-1}(T')} \leq \delta$. Let $s = 2$ and $\psi_i(u_1, u_2) = u_1 + (i-1)u_2$ for $1 \leq i \leq n$ (an n-term AP). Our pseudorandom measure can be $\nu = 1$. Thus, von Neumann gives

$$\sum_{\underline{T}\in T\cdot K\cap\mathbb{Z}^2} \prod_{i=1}^{n} f_i(u_1 + (i-1)u_2) = o_\delta(T^2) + \kappa(\delta)T^2.$$

We'd like to know how often we find arithmetic progressions, i.e. to compute

$$\sum_{\underline{u}\in T\cdot K\cap\mathbb{Z}^2} \prod_{i=1}^{n} \left(f_i(u_1 + (i-1)u_2) + \frac{\#\mathcal{A}}{T'} \right) = \sum_{\underline{u}} \left(\frac{\#\mathcal{A}}{T'} \right)^n + \text{small stuff} \gg T^2. \qquad \triangle$$

4 List of Marginal Comments

Index