LINFOOT TALK — MODEL THEORETIC NUMBER THEORY

Question to keep the braying crowd occupied: Suppose $n^t \in \mathbb{Z}$ for every $n \in \mathbb{N}$. What can be said about t?

1. Number theory

Number theory is often concerned with relationships between numbers. This often takes the form of asking how many solutions there are to some algebraic equations up to a certain size. For example:

Conjecture 1 (Manin's conjecture)**.** *Let V be the intersection of r hypersurfaces of degree d in $\mathbb{P}^n$. Then there is a Zariski open subset U of V and a constant c_1 depending on V and our notion of "size" such that the number of elements in $U \cap \mathbb{P}^n(\mathbb{Q})$ up to size T is*

$$c_1 T^{n+1-rd} (\log T)^{c_2(v)} (1 + o(1))$$

as $T \to \infty$.

2. Counting problems

Manin's conjecture is a typical counting problem.

Let $X \subset \mathbb{R}^n$ and $H : \mathbb{Q} \to \mathbb{R}_{>0}$ be a meaningful function to measure size. Let

$$N(X, T) = \#\{\vec{x} \in X(\mathbb{Q}^n) \,:\, H(x_i) \leqslant T\}.$$

The counting problem is to understand this function N.

Ostensibly it depends on X, H, and T, but really the choice of H doesn't make much difference as long as we're not purposefully oafish. We'll use $H(a/b) = \max\{|a|, |b|\}$ for $\mathrm{hcf}(a, b) = 1$.

So, for example, if $\mathcal{P}$ is the set of primes then

$$N(\mathcal{P}, T) \cong \frac{T}{\log T}.$$

Or if we let

$$X_n = \{(x, y, z) \in \mathbb{R}^3 \,:\, x^n + y^n = z^n,\, xyz \neq 0\},$$

then

$$N(X_n, T) = 0$$

for $n \geqslant 3$ while $N(X_2, T)$ isn't known exactly, determining it is Gauss's circle problem.

In 1989 Enrico Bombieri and Jonathan Pila introduced some novel techniques for the counting problem when X is an irreducible algebraic curve or the graph

of a transcendental analytic function $f : [0,1] \to \mathbb{R}$. Buried in their paper is the following useful result.

Theorem 2. *Let $\phi : (0,1)^\ell \to (0,1)^n$ be a C^k function with*

$$|\partial^\alpha \phi(x)| = \left| \frac{\partial^{|\alpha|}}{\partial x_1^{\alpha_1} \cdots \partial x_\ell^{\alpha_\ell}} \phi(x) \right| \leqslant 1$$

for $|\alpha| \leqslant k$, and let $X = \mathrm{im}(\phi)$. Then $X(\mathbb{Q}, T)$ is contained in the intersection of X with $\ll_{\varepsilon, X} T^\varepsilon$ algebraic hypersurfaces of degree $d(\varepsilon)$ with $d(\varepsilon) \to \infty$ as $\varepsilon \to 0$.

So a common technique is to reparametrise sets by functions like this. Obviously this result is no good in the algebraic case. But if $f : [0,1] \to \mathbb{R}$ is transcendental and analytic, for example, then these intersections are just points and B–P showed there are $c(d) = c(\varepsilon)$ of them. So if X is the graph of such an f then

$$N(X, T) \ll_{\varepsilon, X} T^\varepsilon.$$

The next step is when $f : [0,1]^2 \to \mathbb{R}$, but now there's a problem. The function f can be transcendental but still contain algebraic curves which unduly boost the value of $N(X, T)$. The solution is to omit them. Let

$$X^{\mathrm{alg}} = \bigcup_{\substack{U \subseteq X \\ U \text{ semi-alg.} \\ \dim(U) \geqslant 1}} U,$$

and $X^{\mathrm{trans}} = X \backslash X^{\mathrm{alg}}$. In higher dimensions it makes sense to estimate $N(X^{\mathrm{trans}}, T)$. This is analogous to counting points in a Zariski open subset in Manin's conjecture.

In 2003 JP published his proof of the two-dimensional case.

Theorem 3. *Let $f : [0,1]^2 \to \mathbb{R}$ be transcendental and analytic and $\varepsilon > 0$, and let X be the graph of f. Then*

$$N(X^{trans}, T) \ll_{\varepsilon, X} T^\varepsilon.$$

The basic idea of the proof is the same: intersect X with T^ε hypersurfaces. This gives T^ε curves in $\mathbb{R}^3$ which can be projected down to $\mathbb{R}^2$ to apply the earlier case. But these curves depend on T and without sufficient uniformity the whole thing goes to pot.

JP managed this, but the general case looked pretty intractable. Which was where Alex Wilkie and model theory entered.

3. o-minimal structures

Model theory is a branch of mathematical logic. As Tony Blair might say, model theory is too large a subject to describe with a single soundbite, but it is the study of mathematical structures by studying what is true in those structures.

I like to think of model theory as an extension of the way we learn about groups at school. We don't do that by learning everything there is to learn about the Klein-4 group, and then in the following year take an advanced course where we

learn there are also other groups. But this is almost how we learn analysis, treating the reals as the only place it happens.

Model theory strips away these preconceptions and looks at whole classes of structures as single objects, studying whether the truth of a statement in one structure can be carried over to the others in its class. As a subject it thrives on generalities, but this works to its advantage. Once you've shown that the truth of a statement carries from one structure to another, you can prove theorems where ever it is simplest, and get the same theorem for free in the other structures.

Amongst the structures which contain something like $\mathbb{R}$ there is a particularly well behaved class, the o-minimal structures.

If R is a field with ordering $<$ then an o-minimal structure on R can be thought of as a family $(S_n)_{n\in\mathbb{N}^+}$ such that:

(1) S_n is a boolean algebra of subsets of R^n;
(2) if $A \in S_n$ then $R \times A$ and $A \times R$ are in S_{n+1};
(3) $\{(x, y) \in R^2 : x < y\} \in S_2$;
(4) $\{\vec{x} \in R^n : x_1 = x_n\} \in S_n$ for each n;
(5) if $\pi : R^{n+1} \to R^n$ is the projection map on the first n coordinates and $A \in S_{n+1}$ then $\pi(A) \in S_n$; and
(6) S_1 consists of all finite unions of singletons and (possibly unbounded) intervals in R.

If these conditions look like someone pulled them out of their hat then it's because they are geometric equivalents of the natural first-order logic operations, where the definition is very natural and very simple. Elements of S_n are called definable sets.

The paradigm example of an o-minimal structure is the collection of all semi-algebraic sets – sets given by polynomial equations and inequalities. The fact that $\pi(A)$ is semi-algebraic if A is was proved independently by logician Alfred Tarski and algebraic geometer Abraham Seidenberg.

Another example is the collection of all bounded subanalytic sets. These start with bounded semi-analytic sets, those defined locally by real power series, then allow projections down. Now condition (5) is free, but showing the complement of a subanalytic set is subanalytic is not easy. This was accomplished by Andrei Gabrielov. The sets that Pila got his T^ε bound for are definable in this structure.

A final example is the structure $\mathbb{R}_{\exp}$. This starts with "semi-exponential" sets given by exponential polynomial equations and inequalities, and then allowing projections. Alex Wilkie proved this collection is closed under taking complements and Khovanskiĭ showed semi-exponential sets have finitely many connected components, thus giving us (6).

In 2006 Pila and Wilkie proved the following:

Theorem 4 (Pila–Wilkie)**.** *Let $X \subset \mathbb{R}^n$ be a definable set in some o-minimal structure and $\varepsilon > 0$. Then*

$$N(X^{trans}, T) \ll_{\varepsilon, X} T^\varepsilon.$$

Using this, various new proofs of problems in the Manin–Mumford circle have been given, including the first unconditional proof of a bunch of cases of the André–Oort conjecture by JP.

The Pila–Wilkie theorem applies to Diophantine geometry. It can't really be improved in general because the Bombieri–Pila result is essentially best possible. But Wilkie conjectured an improvement of a more transcendental number theoretic nature.

Conjecture 5 (Wilkie's conjecture)**.** *Let $X \subset \mathbb{R}^n$ be a definable set in $\mathbb{R}_{\exp}$. There are constants $c_1(X)$ and $c_2(X)$ such that for all $T \geqslant e$,*

$$N(X^{trans}, T) \leqslant c_1(X)(\log T)^{c_2(X)}.$$

Known cases:

- $\dim(X) = 1$ (B., Jones–Thomas).
- $X \subset \mathbb{R}^3$ provided X can be nicely reparametrised (Jones–Thomas). In particular...
- $\{(x, y, z) \in \mathbb{R}^3 : (\log x)^a (\log y)^b (\log z)^c = 1\}$ for any $a, b, c \in \mathbb{Q}$ (B.).

4. A likely approach

The Pila–Wilkie proof relies on showing definable sets are the image of finitely many C^k maps with bounded derivatives up to order k. For Wilkie's conjecture we need C^∞ maps ϕ with

$$|\partial^\alpha \phi(\vec{x})| \leqslant \alpha!(A|\alpha|^C)^{|\alpha|}$$

for some A, C and for all $\alpha \in \mathbb{N}^\ell$.

That being said, that's not how the $\dim(X) = 1$ case is proved.

5. Sketch proof when $\dim(X) = 1$

Let $X \subset \mathbb{R}^n$, $\dim(X) = 1$. Can project down and use the maps $(x, y) \mapsto (\pm x^{\pm 1}, \pm y^{\pm 1})$ and a shed load of model theory to get X to be the graph of a smooth function $\phi : (0, 1) \to (0, 1)$.

There is a result that says $X(\mathbb{Q})$ lies on the intersection of X with $\ll (\log T)^c$ hypersurfaces of degree $\ll (\log T)^c$ if we can ensure $|\phi'| \leqslant 1$ and $\phi^{(j)}$ is either $\equiv 0$ or $\neq 0$ for $1 \leqslant j \leqslant\sim (\log T)^c$. So if we can split $(0, 1)$ into about $(\log T)^c$ subintervals where these criteria are met we're halfway there.

One last bit of model theory tells us that ϕ is implicitly exp-definable. So there are exponential polynomials $f_1, \ldots, f_m : \mathbb{R}^{m+1} \to \mathbb{R}$ and smooth functions $\phi = \phi_1, \phi_2, \ldots, \phi_m$ such that:

- $f_i(t, \phi_1(t), \ldots, \phi_m(t)) = 0$ for $1 \leqslant i \leqslant m$ and $t \in (0, 1)$;
- $\det \left(\frac{\partial f_i}{\partial y_j} \right)_{1 \leqslant i,j \leqslant m} \neq 0$.

Differentiating each f_i implicitly gives us m equations in the m unknowns ϕ_i', and we can solve this system because the matrix of coefficients in nonsingular. So we can find ϕ' (and inductively $\phi^{(j)}$) in terms of $\partial f_i/\partial y_j$.

Thanks to Khovanskiĭ, Gabrielov, and Vorobjov, we can bound the zeros of such expressions and so split $(0,1)$ into $(\log T)^c$ subintervals where aforementioned result holds.

A similar process lets us estimate the number of intersections of X with algebraic hypersurfaces of a given degree, and multiplying everything together we end up with

$$N(X^{\text{trans}}, T) \ll_X (\log T)^{11+6m}.$$

6. Transcendental application

Suppose we could get $N(X,T) \ll \log T$ for number fields $F \subset \mathbb{R}$, and then apply this to the set

$$X_\alpha = \{(x,y) \in \mathbb{R}^2 \,:\, y = x^\alpha\}$$

for irrational α.

Now suppose $(x_1,y_1),(x_2,y_2) \in X_\alpha$ with $x_i, y_i \in \overline{\mathbb{Q}}$ and x_1, x_2 multiplicatively independent. Let $F = \mathbb{Q}(x_i, y_i)$ then for $a_1, a_2 \in \mathbb{Z}$,

$$(x_1^{a_1}x_2^{a_2}, y_1^{a_1}y_2^{a_2}) \in X_\alpha \cap F^2$$

and if $(a_1,a_2) \neq (b_1,b_2)$ then the corresponding points in X_α will be different. taking all pairs a_1, a_2 with $|a_1| + |a_2| \leqslant \log T$ gives

$$N(X_\alpha, T) \gg (\log T)^2,$$

a contradiction. This implies...

Conjecture 6 (Four exponentials conjecture)**.** *Let $x_1, x_2 \in \mathbb{R}$ be $\mathbb{Q}$-linearly independent and $y_1, y_2 \in \mathbb{R}$ be $\mathbb{Q}$-linearly independent. Then at least one of*

$$e^{x_1y_1}, e^{x_1y_2}, e^{x_2y_1}, e^{x_2y_2}$$

is transcendental.

Assuming this to be true, now let $t \in \mathbb{R}$ be such that $2^t, 3^t \in \mathbb{Z}$. Apply the four-exponentials conjecture to the pairs $1, t$ and $\log 2, \log 3$. If t is irrational this would imply that one of

$$2, 3, 2^t, 3^t$$

was transcendental, but they're all integers. So $t \in \mathbb{Q}$. But if $t \in \mathbb{Q}$ and $2^t \in \mathbb{Z}$ then $t \in \mathbb{N}$.