The ABCs of Diophantine Geometry

Paul Vojta

University of California, Berkeley

and

The Fields Institute

This semester's Thematic Program at the Fields Institute is titled:

"Arithmetic Geometry, Hyperbolic Geometry, and Related Topics"

- Arithmetic (Diophantine) Geometry
- Hyperbolic Geometry (Nevanlinna Theory)
- Arakelov Theory

Some Diophantine Equations

A diophantine equation is a system of polynomial equations in which the solutions are assumed to lie in $\mathbb{Q}$ or $\mathbb{Z}$ (or some more general rings).

Equation		Solutions
$x^3 + y^3 = 1\,,$	$x, y \in \mathbb{Q}$	$\{(1,0),(0,1)\}$
$3x^3 + 4y^3 = 5\,,$	$x, y \in \mathbb{Q}$	$\emptyset$ (Selmer)
$y^2 + y = x^3 - x\,,$	$x, y \in \mathbb{Q}$	Infinitely many

All of these are cubics in two variables, and all will give a Riemann surface of genus 1 (minus one or two points) if you graph them in $\mathbb{C}^2$ (allowing $x, y \in \mathbb{C}$).

In each case there is a number field k (i.e., an extension field $k \supseteq \mathbb{Q}$ with $[k : \mathbb{Q}]$ finite) for which the equation has infinitely many solutions with $x, y \in k$.

Question. *Given a system of polynomial equations in n variables with coefficients in $\overline{\mathbb{Q}}$. Assume that the graph of solutions in $\mathbb{C}^n$ is a compact connected Riemann surface, minus finitely many points. Does there exist a number field k over which this system has infinitely many solutions?*

Genus	Answer
$0,\ 1$	Yes
≥ 2	No (Faltings)

Question. *Let X be a compact connected Riemann surface. Does there exist a non-constant holomorphic function $f\colon \mathbb{C} \to X$?*

Genus	Answer
$0,\ 1$	Yes
≥ 2	No (Picard)

Given a number field k, let $\mathscr{O}_k$ denote the integral closure of $\mathbb{Z}$ in k. It is called the ring of integers of k.

Question. *Given a system of polynomial equations in n variables with coefficients in $\overline{\mathbb{Q}}$. Assume that the graph of solutions in $\mathbb{C}^n$ is a compact connected Riemann surface, minus s points. Does there exist a number field k such that this system has infinitely many solutions in $\mathscr{O}_k^n$?*

$x^2 - 2y^2 = 1$: yes ($k = \mathbb{Q}$, Pell) $\qquad 9x^2 - 18y^2 = 1$: no.
In each case the genus is 0 and $s = 2$.

For a finite set S of prime numbers, let $\mathbb{Z}[1/S] = \mathbb{Z}[1/p : p \in S]$. (This is the set of rational numbers that can be written as a fraction whose denominator is a product of powers of primes in S.) For a number field k and S as above, let $\mathscr{O}_{k,S}$ denote the integral closure of $\mathbb{Z}[1/S]$ in k.

Question. *Given a system of polynomial equations in n variables with coefficients in $\overline{\mathbb{Q}}$. Assume that the graph of solutions in $\mathbb{C}^n$ is a compact connected Riemann surface, minus s points. Does there exist a number field k and a set S (as above) such that this system has infinitely many solutions in $\mathscr{O}_{k,S}^n$?*

Genus	s	Answer
0	≤ 2	Yes
0	> 2	No (Siegel)
1	0	Yes
1	> 0	No (Siegel)
≥ 2	≥ 0	No (Siegel & Faltings)

Question. *Let X be a compact connected Riemann surface. Does there exist a non-constant holomorphic function $f\colon \mathbb{C} \to X$ whose image omits (at least) s points?*

Genus	s	Answer
0	≤ 2	Yes
0	> 2	No (Picard)
1	0	Yes
1	> 0	No (Picard)
≥ 2	≥ 0	No (Picard)

(If g is the genus, then the answer is yes if and only if $2g - 2 + s \leq 0$.)

What is going on here?

Nevanlinna Theory

Nevanlinna theory is part (most) of value distribution theory of holomorphic functions

Consider the function e^z. It has no zeroes or poles, so as a map $\mathbb{C} \to \mathbb{P}^1(\mathbb{C})$ it omits the values 0 and ∞.

Theorem (Picard). *There is no non-constant holomorphic function $\mathbb{C} \to \mathbb{P}^1(\mathbb{C})$ omitting three or more values.*

[draw $\exp^{-1}(2)$]

Note that $\exp^{-1}(w) = \begin{cases} \{\log w + 2\pi i n : n \in \mathbb{Z}\} & w \in \mathbb{C} \setminus \{0\}, \\ \emptyset & w = 0, \infty \end{cases}$

$\therefore\ \#\{z \in \mathbb{C} : e^z = w$ and $|z| \le r\} = \begin{cases} \frac{r}{\pi} + O_w(1) & w \in \mathbb{C} \setminus \{0\}, \\ 0 & w = 0, \infty \end{cases}$

From now on assume $f(0) \ne 0, \infty$.
Let $\log^+ x = \max\{0, \log x\}$. Also let $f \colon \mathbb{C} \to \mathbb{C}$ be meromorphic.

Definition. The proximity function is

$$m_f(r) = \int_0^{2\pi} \log^+ |f(re^{i\theta})| \frac{d\theta}{2\pi}, \qquad \text{and}$$

$$m_f(a, r) = m_{1/(f-a)}(r) = -\int_0^{2\pi} \log^- |f(re^{i\theta}) - a| \frac{d\theta}{2\pi} \qquad a \in \mathbb{C}.$$

Also let $m_f(\infty, r) = m_f(r)$.

Definition. The counting function is

$$N_f(r) = \sum_{|z|<r} \mathrm{ord}_z^+(1/f) \cdot \log \frac{r}{|z|}\ , \qquad \text{and}$$

$$N_f(a,r) = N_{1/(f-a)}(r) = \sum_{|z|<r} \mathrm{ord}_z^+(f-a) \cdot \log \frac{r}{|z|}\ .$$

Also let $N_f(\infty, r) = N_f(r)$.

Finally, we define the height function by

$$T_f(r) = m_f(r) + N_f(r)\ .$$

If $f(z) = e^z$ then $N_f(\infty, r) = 0$ and

$$m_f(\infty, r) = \int \log^+ e^{r\cos\theta} \frac{d\theta}{2\pi} = r \int_{-\pi/2}^{\pi/2} \cos\theta \frac{d\theta}{2\pi} = \frac{r}{\pi}\ .$$

Theorem (First Main Theorem (FMT)). *For all* $a \in \mathbb{C}$ *,*

$$m_f(a,r) + N_f(a,r) = T_f(r) + O_{f,a}(1)\ .$$

Since $m_f(a,r) \geq 0$, this gives an upper bound on $N_f(a,r)$.

Compare with Jensen's formula

$$\log|c_\lambda| = \int_0^{2\pi} \log|f(re^{i\theta})| \frac{d\theta}{2\pi} + N_f(\infty, r) - N_f(0, r) \,.$$

Theorem (Second Main Theorem (SMT)). *Let $a_1, \dots, a_q \in \mathbb{P}^1(\mathbb{C})$ be distinct. Then*

(*) $$\sum_{i=1}^{q} m_f(a_i, r) \le_{\text{exc}} 2\,T_f(r) + O(\log^+ T_f(r)) + o(\log r) \,,$$

where $O(\ )$ and $o(\ )$ depend only on f and $a_1, \dots, a_q$, and $\le_{\text{exc}}$ means that the inequality holds for all $r \in (0, \infty)$ outside of a set of finite Lebesgue measure.

Corollary (Picard). *If $f\colon \mathbb{C} \to \mathbb{P}^1(\mathbb{C}) \setminus \{a_1, a_2, a_3\}$ is holomorphic with a_1, a_2, a_3 distinct, then f is constant.*

Proof. Since f never equals a_i, we have $N_f(a_i, r) = 0$, so the FMT gives $m_f(a_i, r) = T_f(r) + O(1)$. The left-hand side of (*) is therefore $3\,T_f(r) + O(1)$, so (*) becomes $T_f(r) \le_{\text{exc}} O(\log^+ T_f(r)) + o(\log r)$. But, if f is nonconstant then $T_f(r) \ge O(\log r)$, a contradiction. Therefore f is constant. $\square$

One can view the SMT as a lower bound on $N_f(a,r)$: the left-hand side of (*) is $q\,T_f(r) - \sum m_f(a_i,r)$, so (*) is equivalent to

$$\sum_{i=1}^{q} N_f(a_i,r) \ge_{\mathrm{exc}} (q-2)T_f(r) - O(\log^+ T_f(r)) - o(\log r)\ .$$

Advantages:

(1). $q-2 = \chi(\mathbb{P}^1 \setminus q$ points$)$,
(2). The left-hand side is independent of metrics; and
(3). One can phrase it using truncated counting functions (abc conjecture).

Number Theory

For a number field k, let M_k be its set of places. This is in one-to-one correspondence with the disjoint union

$$\{\text{nonzero primes in } \mathscr{O}_k\} \coprod \{\sigma\colon k \hookrightarrow \mathbb{R}\} \coprod \{\text{unordered pairs } (\sigma,\bar\sigma)\colon \sigma \ne \bar\sigma\colon k \hookrightarrow \mathbb{C}\}.$$

For $v \in M_k$ we define norms $\|\cdot\|_v$ by

$$\|x\| = \begin{cases} (\mathscr{O}_k : \mathfrak{p})^{-\operatorname{ord}_{\mathfrak{p}}(x)} & \text{if } v \nmid \infty,\ x \ne 0, \\ |\sigma(x)| & \text{if } v \text{ is real,} \\ |\sigma(x)|^2 & \text{if } v \text{ is complex.} \end{cases}$$

We then have a product formula $\prod_{v\in M_k} \|x\|_v = 1$ for all $x \in k$, $x \ne 0$.

Let S_∞ denote the set of archimedean (real or complex) places.

Let $S \supseteq S_\infty$ be a finite set of places of k; for $x \in k$ we then define

$$m_S(x) = m_S(\infty, x) = \sum_{v\in S} \log^+ \|x\|_v\ ,$$

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

$$N_S(x) = N_S(\infty, x) = \sum_{v \notin S} \log^+ \|x\|_v = \sum_{v \notin S} \mathrm{ord}_v^+ \left(\frac{1}{x}\right) \cdot \log(\mathscr{O}_k : \mathfrak{p}) \ ,$$

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

$$h_k(x) = m_S(x) + N_S(x) = \sum_{v \in M_k} \log^+ \|x\|_v = \log \prod_v \max\{1, \|x\|_v\} \ .$$

Corresponding to the FMT, we have

$$m_S(a, x) + N_S(a, x) = h_k\left(\frac{1}{x-a}\right) = h_k(x) + O_{a,k}(1) \ ,$$

a property of heights.

Theorem (Roth). *Let* k *and* S *be as above, and for all* $v \in S$ *let* $\alpha_v \in \overline{\mathbb{Q}}$. *Let* $\epsilon > 0$. *Then the inequality*

$$\prod_{v \in S} \min\{1, \|x - \alpha_v\|_v\} \le \frac{1}{H_k(x)^{2+\epsilon}} .$$

holds for only finitely many $x \in k$. *Here* $H_k(x) = \exp(h_k(x)) = \prod_v \max\{1, \|x\|_v\}$.

This is equivalent to the same statement with $\alpha_v \in k$ for all v (expand k). Equivalently, given k, S, ϵ, and $a_1, \dots, a_q \in k$, then the inequality

$$\prod_{i=1}^{q} \prod_{v \in S} \min\{1, \|x - a_i\|_v\} \le \frac{1}{H_k(x)^{2+\epsilon}}$$

holds for only finitely many $x \in k$.

Taking $-\log$ of both sides, and rearranging the logic, we then have that

$$\sum_{i=1}^{q} m_S(a_i, x) \le (2+\epsilon) h_k(x) + O(1)$$

for almost all $x \in k$.

The Dictionary

Recall the definitions of the proximity function

$$m_f(r) = \int_0^{2\pi} \log^+ |f(re^{i\theta})| \frac{d\theta}{2\pi} \qquad \text{and} \qquad m_S(x) = \sum_{v\in S} \log^+ \|x\|_v$$

in Nevanlinna theory and number theory, respectively.

Also, the counting function is

$$N_f(r) = \sum_{|z|<r} \operatorname{ord}_z^+ \left(\frac{1}{f}\right) \cdot \log \frac{r}{|z|} \qquad \text{and} \qquad N_S(x) = \sum_{v\notin S} \operatorname{ord}_v^+ \left(\frac{1}{x}\right) \cdot \log(\mathscr{O}_k : \mathfrak{p})$$

in Nevanlinna theory and number theory, respectively.

We can see some similarities.

Nevanlinna Theory	Number Theory
$f\colon \mathbb{C} \to \mathbb{C}$, non-constant	$\{x\} \subseteq k$, infinite
r	x
θ	$v \in S$
$\lvert f(re^{i\theta})\rvert$	$\|x\|_v$, $v \in S$
$\operatorname{ord}_z f$	$\operatorname{ord}_v x$, $v \notin S$
$\log \frac{r}{\lvert z\rvert}$	$\log(\mathscr{O}_k : \mathfrak{p})$

Important:

- One holomorphic map corresponds to an infinite set of rational points.
- One rational point may correspond to $f\big|_{\bar{\mathbb{D}}_r}$.

Conjecture (Masser-Oesterlé "abc conjecture"). *For all $\epsilon > 0$ there is a constant C with the following property. All integers a, b, c satisfying $a + b + c = 0$ and $\gcd(a, b, c) = 1$ must satisfy the inequality*

$$\max\{|a|, |b|, |c|\} \le C \prod_{p|abc} p^{1+\epsilon} .$$

There is something in Nevanlinna theory which corresponds to this:

Definition. The truncated counting function in Nevanlinna theory is defined by

$$N_f^{(1)}(r) = N_f^{(1)}(\infty, r) = \sum_{|w|<r} \min\left\{1, \operatorname{ord}_w^+\left(\frac{1}{f}\right)\right\} \log \frac{r}{|w|}$$

and $N_f^{(1)}(a, r) = N_{1/(f-a)}^{(1)}(r)$ for $a \in \mathbb{C}$.

Theorem (Second Main Theorem with Truncated Counting Functions). *Let $a_1, \dots, a_q \in \mathbb{P}^1(\mathbb{C})$ be distinct. Then*

$$\sum_{i=1}^{q} N_f^{(1)}(a_i, r) \ge_{\text{exc}} (q-2)T_f(r) - O(\log^+ T_f(r)) - o(\log r) .$$

where $O(\ )$ and $o(\ )$ depend only on f and $a_1, \dots, a_q$.

In number theory, we have:

Definition. The truncated counting function in number theory is defined by

$$N_S^{(1)}(x) = N_S^{(1)}(\infty, x) = \sum_{v \notin S} \min\left\{1, \operatorname{ord}_v^+\left(\frac{1}{x}\right)\right\} \log(\mathscr{O}_k : \mathfrak{p})$$

and $N_S^{(1)}(a, x) = N_S^{(1)}(1/(x-a))$ for $a \in k$, $a \neq x$. Here, as usual, $\mathfrak{p}$ is the place of k corresponding to each place $v \notin S$.

Conjecture. *Let k be a number field, let $S \supseteq S_\infty$ be a finite set of places of k, let $a_1, \dots, a_q$ be elements of $k \cup \{\infty\}$, let $\epsilon > 0$, and let $c \in \mathbb{R}$. Then*

$$\sum_{i=1}^{q} N_S^{(1)}(a_i, x) \geq (q - 2 - \epsilon) h_k(x) + c$$

holds for all but finitely many $x \in k$.

When $k = \mathbb{Q}$, $S = \{\infty\}$, $q = 3$, and $\{a_1, a_2, a_3\} = \{0, 1, \infty\}$, this is the abc conjecture.

Making things geometrical

One can think of a finite set of points on a Riemann surface (or on an algebraic curve) as a divisor, which is reduced since the points are distinct. If D denotes such a divisor, then we can phrase the proximity, counting, and truncated counting functions in terms of divisors:

$$m_f(D,r) = \sum_{i=1}^{q} m_f(a_i,r)\,, \qquad \text{etc.}$$

Thus, we have:

Theorem (SMT for Riemann Surfaces with Truncated Counting Functions). *Let X be a compact connected Riemann surface, let D be an effective reduced divisor on X, let $\mathscr{K}$ be the canonical line sheaf on X, let $\mathscr{A}$ be an ample line sheaf on X, and let $f\colon \mathbb{C} \to X$ be a non-constant holomorphic function. Then*

$$N_f^{(1)}(D,r) \ge_{\text{exc}} T_{f,\mathscr{K}(D)}(r) - O(\log^+ T_{\mathscr{A},f}(r)) - o(\log r)\,.$$

Conjecture (Diophantine SMT with Truncated Counting Functions). *Let k and S be as usual, let X be a smooth projective curve over k, let D be an effective reduced divisor on X, let $\mathscr{K}$ be the canonical line sheaf on X, let $\mathscr{A}$ be an ample line sheaf on X, and let $\epsilon > 0$. Then, for all but finitely many $x \in X(k)$,*

$$N_S^{(1)}(D,x) \ge h_{k,\mathscr{K}(D)}(x) - \epsilon\, h_{k,\mathscr{A}}(x) + O(1)\,.$$

These then imply Picard's and Faltings' theorems when the genus is ≥ 2.

Finite ramified coverings and algebraic points

One can generalize the latter conjecture to deal with points over varying number fields of bounded degree over k. In Nevanlinna theory, this corresponds to replacing the domain $\mathbb{C}$ with a finite ramified covering of $\mathbb{C}$.

Theorem (SMT for Riemann Surfaces with Truncated Counting Functions and Finite Ramified Coverings). *Let X be a compact connected Riemann surface, let D be an effective reduced divisor on X, let $\mathscr{K}$ be the canonical line sheaf on X, let $\mathscr{A}$ be an ample line sheaf on X, let B be a connected Riemann surface, let $\pi\colon B \to \mathbb{C}$ be a proper surjective holomorphic map, and let $f\colon \mathbb{C} \to X$ be a non-constant holomorphic function. Then*

$$N_f^{(1)}(D,r) + N_{\mathrm{Ram}(\pi)}(r) \ge_{\mathrm{exc}} T_{f,\mathscr{K}(D)}(r) - O(\log^+ T_{\mathscr{A},f}(r)) - o(\log r)\ .$$

Here the additional term $N_{\mathrm{Ram}(\pi)}(r)$ is a counting function for ramification points of π.

Its counterpart in number theory is related to the discriminant:

$$d_k(x) = \frac{1}{[k(x):k]} \log |D_{k(x)}| \ .$$

Conjecture (Diophantine SMT with Truncated Counting Functions for Algebraic Points). *Let k and S be as usual, let $r \in \mathbb{Z}_{>0}$, let X be a smooth projective curve over k, let D be an effective reduced divisor on X, let $\mathscr{K}$ be the canonical line sheaf on X, let $\mathscr{A}$ be an ample line sheaf on X, and let $\epsilon > 0$. Then, for all but finitely many $x \in X(\bar{k})$ with $[k(x):k] \le r$,*

$$N_S^{(1)}(D,x) + d_k(x) \ge h_{k,\mathscr{K}(D)}(x) - \epsilon\, h_{k,\mathscr{A}}(x) + O(1) \ .$$

The conjecture when $\dim X > 1$

This conjecture has been posed also in higher dimensions, the only difference being that non-constant functions and infinite sets need to be replaced by Zariski-dense functions and sets, respectively.

And, both statements are conjectural.

Conjecture (Griffiths). *Let X be a smooth complex projective variety, let D be a normal crossings divisor on X, let $\mathscr{K}$ be the canonical line sheaf on X, let $\mathscr{A}$ be an ample line sheaf on X, let $\epsilon > 0$, let B be a connected Riemann surface, and let $\pi\colon B \to \mathbb{C}$ be a proper surjective holomorphic map. Then there is a proper Zariski-closed subset Z of X, depending only on X, D, $\mathscr{A}$, and ϵ, such that*

$$N_f^{(1)}(D,r) + N_{\mathrm{Ram}(\pi)}(r) \ge_{\mathrm{exc}} T_{\mathscr{K}(D),f}(r) - \epsilon\, T_{\mathscr{A},f}(r) - O(1)$$

holds for all holomorphic curves $f\colon B \to X$ whose image is not contained in Z.

Conjecture. *Let k and S be as usual, let X be a smooth projective variety over k, let D be a normal crossings divisor on X, let $\mathscr{K}$ be the canonical line sheaf on X, let $\mathscr{A}$ be an ample line sheaf on X, let $r \in \mathbb{Z}_{>0}$, and let $\epsilon > 0$. Then there is a proper Zariski-closed subset Z of X, depending only on X, D, $\mathscr{A}$, and ϵ, such that the inequality*

$$N_S^{(1)}(D,x) + d_k(x) \ge h_{\mathscr{K}(D),k}(x) - \epsilon\, h_{\mathscr{A},k}(x) - O(1)$$

holds for all $x \in (X \setminus Z)(\bar{k})$ with $[k(x):k] \le r$.

Many things imply abc

This latter conjecture implies the abc conjecture in a number of ways:

- If $k = \mathbb{Q}$, $r = 1$, and $X = \mathbb{P}^1$ (as noted already)
- Without truncated counting functions, with $\dim X = 1$ ("$1+\epsilon$ conjecture")
- Without truncated counting functions, with $r = 1$ (rational points)

The abc conjecture seems to be at the center of these types of conjectures.

A less sweeping conjecture

This conjecture is a bit less sweeping, being based on something in Nevanlinna theory that is actually proved.

If $\mathscr{E}$ is a vector sheaf on a scheme X, then we recall that

$$\mathbb{P}(\mathscr{E}) := \textbf{Proj} \bigoplus_{d \ge 0} S^d \mathscr{E} .$$

This is the space of hyperplanes in fibers of $\mathscr{E}$.

Theorem (McQuillan's "Tautological inequality"). *Let X be a nonsingular complex projective variety, let D be a normal crossings divisor on X, let $\mathscr{A}$ be an ample line sheaf on X, let $\pi\colon B \to \mathbb{C}$ be as usual, let $f\colon B \to X$ be a non-constant holomorphic map, and let $f'\colon B \to \mathbb{P}(\Omega_X(\log D))$ be its lifting. Then*

$$T_{\mathscr{O}(1),f'}(r) \le_{\text{exc}} N_f^{(1)}(D,r) + N_{\text{Ram}(\pi)}(r) + O(\log T_{\mathscr{A},f}(r) + \log r) .$$

Conjecture. *Let* k *and* S *be as usual, let* X *be a smooth projective variety over* k *with* $\dim X > 0$ *, let* D *be a normal crossings divisor on* X *, let* $r \in \mathbb{Z}_{>0}$ *, let* $\mathscr{A}$ *be an ample line sheaf on* X *, and let* $\epsilon > 0$ *. Then, for all* $x \in X(\bar{k})$ *with* $[k(x) : k] \le r$ *, there is a closed point* $x' \in \mathbb{P}(\Omega_{X/k}(\log D))$ *lying over* x *such that*

$$h_{\mathscr{O}(1),k}(x') \le N_S^{(1)}(D,x) + d_k(x) + \epsilon\, h_{\mathscr{A},k}(x) + O(1)\ .$$

Moreover, given a finite collection of rational maps $g_i \colon X \dashrightarrow W_i$ *to varieties* W_i *, there are finite sets* Σ_i *of closed points on* W_i *for each* i *with the following property. For each* x *as above,* x' *may be chosen so that, for each* i *, if* x *lies in the domain of* g_i *and if* $g_i(x) \notin \Sigma_i$ *, then* x' *lies in the domain of the induced rational map* $\mathbb{P}(\Omega_{X/k}) \dashrightarrow \mathbb{P}(\Omega_{W_i/k})$ *.*

This conjecture obviously deserves to be called the tautological conjecture.