Unlikely Intersections and applications to Diophantine problems

L. CAPUANO - Politecnico di Torino

In the last lecture we saw how the proof of relative Manin-Mumford conj. for curves work applying Pila-Wilkie's theorem.

QUESTION: How do we go from Manin-Mumford to Zilber-Pink?

Take $C = \mathbb{P}^1 \setminus \{0, 1, \infty\}$ and $\mathcal{E}_\lambda \to C$ the family of elliptic curves in Legendre form

$$yz^2 = x(x-z)(x-\lambda z)$$

Thm (Barroero-C. '16)
Take three sections $P_1(\lambda), P_2(\lambda), P_3(\lambda) : C \to \mathcal{E}_\lambda$; assume that they are linearly independent; then $\exists$ at most finitely many $\lambda_0 \in C$ s.t. $\exists\, \underline{a}, \underline{b} \in \mathbb{Z}^3$ lin. indep. s.t.

$$\begin{cases} \sum_{i=1}^{3} a_i P_i(\lambda_0) = O_{\lambda_0} \\ \sum_{i=1}^{3} b_i P_i(\lambda_0) = O_{\lambda_0} \end{cases}$$

I want to sketch what is the point counting result that has to be applied in this case.
Take $P_1(\lambda), P_2(\lambda), P_3(\lambda) : \mathcal{C} \longrightarrow \mathcal{E}_\lambda$;

Now we want to count $\lambda_0 \in \mathbb{P}^1 \setminus \{0,1,\infty\}$ such that
$$\begin{cases} a_1 P_1\lambda_0 + a_2 P_2\lambda_0 + a_3 P_3\lambda_0 = O_{\lambda_0} \\ b_1 P_1\lambda_0 + b_2 P_2\lambda_0 + b_3 P_3\lambda_0 = O_{\lambda_0} \end{cases}$$

$\Rightarrow$ Take again
$$\exp : \mathbb{C}/L_\lambda \longrightarrow \mathcal{E}_\lambda$$
where $L_\lambda = \langle \omega_1, \omega_2 \rangle$ ↑ generators of the period lattice

and z_i elliptic logarithms of P_i; now
$$\sum_{i=1}^{3} a_i P_i(\lambda_0) = O_{\lambda_0} \iff \sum_{i=1}^{3} a_i z_i(\lambda_0) \in L_{\lambda_0}$$

If we write
$$P_i(\lambda) = u_{i1}\omega_1 + u_{i2}\omega_2 \quad \text{with } u_{ij} : D_{\lambda_0} \to \mathbb{R}$$

and we consider the map
$$\Theta : D_{\lambda_0} \longrightarrow \mathbb{R}^6$$
$$\lambda \longmapsto (u_{11}, u_{12}, u_{21}, u_{22}, u_{31}, u_{32})$$
We call again
$$S = \Theta(D_\lambda) \subseteq \mathbb{R}^6$$ SUBANALYTIC SURFACE

then we are interested in counting points in S satisfying a linear system of relations

$$\circledast \begin{cases} a_1 u_{11} + a_2 u_{12} + a_3 u_{13} = c_1 \\ a_1 u_{21} + a_2 u_{22} + a_3 u_{23} = c_2 \\ b_1 u_{11} + b_2 u_{12} + b_3 u_{13} = c_3 \\ b_1 u_{21} + b_2 u_{12} + b_3 u_{13} = c_4 \end{cases} \quad \text{for some } c_i \in \mathbb{Z}$$

CLAIM: Want to count points in S satisfying $\circledast$ with $\max\{|a_i|, |b_j|, |c_k|\} \leq T$.

We can translate this problem in counting "semi-rational points" in definable families, i.e. points with only "some" of the points which are rational of bounded height. This can be done applying a thm of Habegger-Pila

If we now look at $\mathbb{R}^{10} \times S \subseteq \mathbb{R}^{16}$, we denote by

$$W = \{(a_i, b_j, c_k, u_{ij}) \in \mathbb{R}^{10} \times S \mid \circledast \text{ holds}\}$$

in $\mathbb{R}^{10} \times \mathbb{R}^6$ this is a definable family in $\mathbb{R}_{an}$.

Denote by

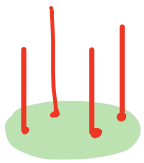
$$\tilde{W}(Q,T) = \{ \underline{w} \in W \mid \text{the first 10 coord. are rationals of height bounded by } T \}$$

Consider π_1 and π_2 the projections:

$$\mathbb{R}^{10} \times S \supseteq W \xrightarrow{\pi_1} \mathbb{R}^{10}$$

$$\pi_2 \downarrow$$

$$\mathbb{R}^6$$



Habegger-Pila's thm tells that:

- either

$$\#\{\text{points is } S \mid \circledast \text{ holds with } |a_i|, |b_j|, |c_k| \leq T\} = \#\pi_2(\tilde{W}(Q,T)) \leq c_\varepsilon T^\varepsilon$$

- or there is a semi-algebraic arc γ in $\pi_1(W)$ such that $\pi_2(\pi_1^{-1}(\gamma))$ is non constant.

This would give an algebraic rel. between the elliptic logarithms z_1, z_2, z_3 and this is again a contraddiction because of a thm of Bertrand.

$$\Rightarrow \quad \#\underset{\shortparallel}{\tilde{W}}(\mathcal{R},T) \leq c_\varepsilon T^{\varepsilon}$$

$\{$ points in S satisfying $\circledast$ with max coeff $\leq T\}$

To conclude, one has to relate T with the degree $[\mathbb{Q}(\lambda_0):\mathbb{Q}]$, and this can be done applying a thm of Masser + other diophantine ingredients.

Let me end this first lecture by mentioning that we also obtained a statement for split semiabelian varieties (combining Barroero-C. and the pf of Zilber-Pink for curves in $\tilde{\mathbb{G}}_m^n$ using o-minimality obtained in my PhD thesis.

For simplicity I give the statement for $\mathcal{E}_\lambda^n \times \mathbb{G}_m^r$:

Thm (Barroero-C. '17)

Let $P_1,\dots,P_n : \mathcal{C} \longrightarrow \mathcal{E}_\lambda$ be n sections and let $f_1,\dots,f_r$ be r rational functions.
Assume that no rel of the form $\sum a_i P_i = 0$ and no mult. relation of the form $\prod f_i^{m_i} = 1$ holds identically on $\mathcal{C}$.

Then, $\exists$ at most 0 finitely many $\lambda_0 \in \mathcal{C}$ s.t. $\exists\ \underline{a} \in \mathbb{Z}^n$, $\underline{m} \in \mathbb{Z}^r$ not both zero such that

$$\begin{cases} \sum a_i P_i(\lambda_0) = 0 \ \lambda_0 & \text{on } \mathcal{E}^n_{\lambda_0} \times \mathbb{G}^r_{am} \\ \sum f_i(\lambda_0)^{m_i} = 1 \end{cases}$$

In the last part of the minicourse, I want to speak about recent applications to the function field version of a conjecture of Silverman on the greatest common divisor of divisibility sequences. (j.w. F. Barroero & A. Turchet)

Def: A sequence of integers $\{d_n\}_{n \in \mathbb{N}}$ is said to be a "DIVISIBILITY SEQUENCE" if

$$\forall\ m \mid n \implies d_n \mid d_n$$

"Independent divisibility sequences should have only a finite number of common factors."

Consider for $a \in \mathbb{Z}_{\geq 1}$ $\quad d_n = a^n - 1$

CONJ (Ailon-Rudnick) If a, b are mult. independent, then $\exists\ \infty$ many integers $k \geq 1$ s.t.

$$\gcd(a^k-1, b^k-1) = \gcd(a-1, b-1)$$

The polynomial analogue of this is known, and actually a stronger result holds:

Thm (AILON-RUDNICK '04) Let k field of char 0; $a, b \in k[t]$ mult. independent polynomials; then $\exists\, c_{a,b} \in k[t]$ s.t.

$$\gcd(a^n-1, b^n-1) \mid c_{a,b} \qquad \forall n \geq 1$$

and

$$\gcd(a^n-1, b^n-1) = \gcd(a-1, b-1) \text{ for } \infty \text{ many } n \geq 1.$$

Notice that geometrically the sequence a^n-1 comes from alg. subgroups of $\mathbb{G}_m$ or rk 0. One can define other divisibility sequences coming from other algebraic groups.

- **Elliptic divisibility sequences**

$E/\mathbb{Q}$ elliptic curve: any non-zero rational point $P \in E(\mathbb{Q})$ can be written as

$$P = (x_P, y_P) = \left(\frac{A_P}{D_P^2}, \frac{B_P}{D_P^3}\right) \qquad \text{with } \gcd(A_P, D_P) = 1,\ \gcd(B_P, D_P) = 1$$

If P is not a TORSION POINT $\Rightarrow$
$\{D_{nP}\}$ is a DIVISIBILITY SEQUENCE

In this case Silverman proposed the analogous conjecture of Ailon-Rudnick:

CONJ (SILVERMAN) Assume P_1, P_2 are two LIN. INDEP. points (i.e. no rel of the form $a_1P_1 + a_2P_2 = O$ holds with $a_i \in \mathrm{End}(E)$). Then $\exists\, \infty$ many $n \geq 1$ s.t.

$$\mathrm{GCD}(D_{nP_1}, D_{nP_2}) = \mathrm{GCD}(D_{P_1}, D_{P_2})$$

(more general conj. holds for general alg. groups)

One can consider the function field analogue of this conjecture.
Take k number field, and take E an ell. curve $/k(t)$;

$$\forall\, P \in E(k(t)) \qquad x_P = \frac{A_P}{D_P^2} \quad \text{with } A_P, D_P \text{ coprime pol.}$$

Thm Let $P_1, P_2 \in E(k(t))$ independent points; then, $\exists D \in k[t]$ such that

$$\mathrm{GCD}(D_{nP_1}, D_{nP_2}) \mid D \qquad \forall n \geq 1.$$

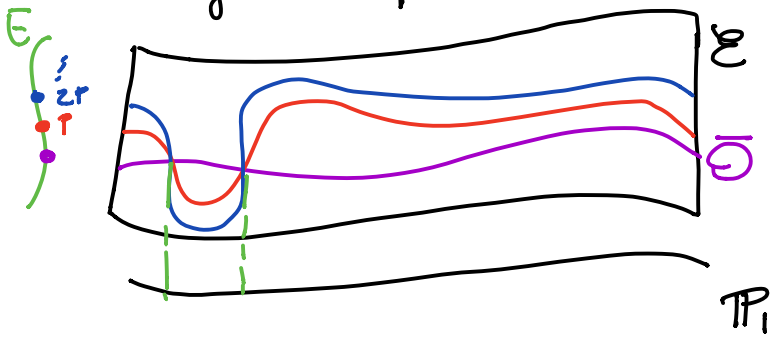
Moreover, $\exists \infty$ many $n \geq 1$ s.t.

$$GCD(D_{nP_1}, D_{nP_2}) = GCD(D_{P_1}, D_{P_2}).$$

proved by Silverman ($j(E)$ constant)
Ahioca-Hsia-Tucker in general.

GEOMETRIC POINT OF VIEW

E ell curve in Weierstrass form $/k(t)$
Take $\mathcal{E} \to \mathbb{P}^1$ elliptic surface
with generic fiber E



$P \in E(k(t)) \rightsquigarrow$ section $\sigma_P : \mathbb{P}^1 \to \mathcal{E}$
$O \in E(k(t)) \rightsquigarrow \bar{O} = \sigma_O(\mathbb{P}^1)$

Recall that we want to study $GCD(D_{nP_1}, D_{nP_2})$
where $x_{nP_i} = \frac{A_{nP_i}}{D^2_{nP_i}}$

Notice that $(t-\lambda) \mid D_P \iff \alpha \in \mathrm{supp}(\mathrm{div}_0 D_P)$,
i.e. $\sigma_P(\lambda) = O_\lambda$, and the order of vanishing is exactly the multiplicity of intersection between $\sigma_P(\mathbb{P}^1)$ and $\bar{O}$

In this case, notice that

$$\bigcup_{n\geq 1} \operatorname{Supp} \operatorname{GCD}(D_{nP_1}, D_{nP_2}) = \{\lambda \in \mathbb{P}^1 \text{ s.t. } \exists n \in \mathbb{N} : \sigma_{nP_1}(\lambda) = \sigma_{nP_2}(\lambda) = O_\lambda\}$$

$\Rightarrow$ finiteness by Relative-Manin Mumford

To have the result then one has to bound the $\operatorname{ord}_\lambda D_{nP}$ independently of n, but this can be done because either $\operatorname{ord}_\lambda D_{nP} = 0$ or $\operatorname{ord}_\lambda D_{nP} = \operatorname{ord}_\lambda D_P$.

One can further generalize by considering, instead of $\mathbb{P}^1$, a generic curve C and defining a suitable notion of GCD of DIVISORS on C
Moreover, we can take $\sigma_Q(\mathbb{P}^1)$ instead of $\bar{O}$

$\rightsquigarrow$ finiteness comes applying variants of the results of myself and F. Barroero.

$\rightsquigarrow$ very general result for abelian varieties.
I conclude with an example of the type of results we have :

Thm (Barbero - C. - Turchet '20)

Let $k = \overline{\mathbb{Q}}$ and let E be an elliptic curve over $k(t)$; take P, Q two points in $E(k(t))$ and $f, g \in k[t]$ two non constant polynomials.

(1) Assume P is non-TORSION; then $\exists\, c_1 \in k[t]$ such that

$$\gcd(D_{nP}, f^m - 1) \mid c_1 \qquad \forall\, n, m \geq 1$$

Moreover, $\gcd(D_{nP}, f^n - 1) = \gcd(D_P, f - 1)$ for all $n \in \mathbb{N}$ but finitely many arithmetic progressions.

(2) If no rel. of the form $nP = Q$ and $f^m = g$ hold + $j(E)$ non constant, then $\exists\, c_2 \in k[t]$ such that

$$\gcd(D_{nP-Q}, f^m - g) \mid c_2$$