Multiplicative relations among differences of singular moduli

Vahagn Aslanyan

University of Manchester

Manchester Number Theory Seminar

28 November 2023

Joint work with S. Eterović and G. Fowler

Classical problems in Diophantine geometry

Some classical problems in Diophantine geometry seek to describe the sets of special points on algebraic curves. Let $C \subseteq \mathbb{C}^2$ be an irreducible curve.

- **Lang's problem.** Special point $= (\xi, \eta)$ where ξ and η are roots of unity. When does C contain infinitely many special points?

Theorem (Ihara, Serre, Tate)

C contains infinitely many speical points if and only if it is special, i.e. it is defined by an equation $x^m y^n = \rho$ where ρ is a root of unity.

- **André's theorem.** Special point $= (\xi, \eta)$ where ξ and η are singular moduli, i.e. j-invariants of CM elliptic curves.
  When does C contain infinitely many special points?

Theorem (André)

C contains infinitely many speical points if and only if it is special, i.e. it is defined by an equation of the form $x = \rho$ or $y = \rho$ or $\Phi_N(x, y) = 0$ where ρ is a singular modulus and Φ_N is the N-th modular polynomial.

Special points and varieties: exponential case

- A special point is a tuple all of whose coordinates are roots of unity. Equivalently, special points are torsion points in $\mathbb{G}_{\mathrm{m}}^n$. These are bi-algebraic for the function $e^{2\pi iz}$; they are the values of this function at rational points.
- A special variety is a torsion coset of an algebraic torus. It is defined by equations of the form $y_1^{m_1} \cdots y_n^{m_n} = \rho$ where ρ is a root of unity. These are bi-algebraic for the function $e^{2\pi iz}$; they are the images of $\mathbb{Q}$-affine subspaces of $\mathbb{G}_{\mathrm{a}}^n$ under this function.

Special points and varieties: modular case

- $j : \mathbb{H} \to \mathbb{C}$ is the modular j-function.
- For any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ we have $j(\gamma z) \equiv j(z)$.
- There is a collection $\Phi_N(X, Y)$ of modular polynomials such that for any $z, w \in \mathbb{H}$ we have

$$\exists g \in \mathrm{GL}_2^+(\mathbb{Q})(w = gz) \Leftrightarrow \exists N(\Phi_N(j(z), j(w)) = 0).$$

- Special points are tuples of singular moduli, i.e. the j-invariants of CM elliptic curves. A number $\sigma \in \mathbb{C}$ is special iff for some $N > 1$ it satisfies $\Phi_N(\sigma, \sigma) = 0$. These are bi-algebraic for j: singular moduli are the images of quadratic irrationals under j.
- Special varieties in $Y(1)^n$ (identified with $\mathbb{C}^n$) are defined by equations of the form $y_k = \sigma$ and $\Phi_N(y_k, y_l) = 0$ where σ is special. These are bi-algebraic for j: they are the images of geodesic subvarieties of $\mathbb{H}^n$, i.e. subsets cut out by equations $z_k = g_{k,l} z_l$ and $z_k = \tau$ with $g_{k,l} \in \mathrm{GL}_2^+(\mathbb{Q})$ and $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$.

Manin-Mumford and André-Oort

Theorem

If a variety V contains a Zariski dense set of special points then V is special.

When $V \subseteq \mathbb{G}_{\mathrm{m}}^n$, this is Manin-Mumford for algebraic tori (due to Raynaud and Hindry).

When $V \subseteq Y(1)^n$, this is André-Oort for products of modular curves (due to Pila).

Multiplicative relations among singular moduli

We now consider a Diophantine problem of mixed modular-multiplicative type.

Theorem (Pila-Tsimerman)

Let $n \in \mathbb{Z}_{>0}$. Then there exist only finitely many n-tuples $(\sigma_1, \ldots, \sigma_n)$ of pairwise distinct singular moduli for which there exist $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ such that

$$\prod_{i=1}^{n} \sigma_i^{a_i} = 1.$$

Theorem (Pila-Tsimerman)

Let $g_1, \ldots, g_k \in \mathrm{GL}_2^+(\mathbb{Q})$. If the functions $j(g_1 z), \ldots, j(g_n z)$ are pairwise distinct then they are multiplicatively independent modulo $\mathbb{C}$.

In view of the second result, the first theorem is implied by Zilber-Pink. Note that the second result does not formally follow from Ax-Schanuel.

Differences of singular moduli

Now we look at multiplicative relations among differences of singular moduli. Since 0 is a singular modulus, the set of differences of singular moduli contains all singular moduli.

These are "highly divisible" in the sense that they tend to have relatively small prime factors. For instance,

$$j\left(\frac{-1+\sqrt{163}i}{2}\right) - j\left(\frac{-1+\sqrt{67}i}{2}\right) = -2^{15}\cdot 3^7\cdot 5^3\cdot 7^2\cdot 13\cdot 139\cdot 331.$$

Gross and Zagier studied prime factorisations of differences of singular moduli.

The results we are going to look at fit in the general Zilber-Pink/unlikely intersections picture.

Fixed σ

Theorem (A.-Eterović-Fowler)

Let $n \in \mathbb{Z}_{>0}$. Let σ be a singular modulus. Then there exist only finitely many n-tuples $(\alpha_1, \ldots, \alpha_n)$ of pairwise distinct singular moduli such that $\sigma \notin \{\alpha_1, \ldots, \alpha_n\}$ and there exist $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ for which

$$\prod_{i=1}^{n} (\alpha_i - \sigma)^{a_i} = 1.$$

For $\sigma = 0$ this is a theorem of Pila and Tsimerman.
This follows from the following functional independence result.

Theorem

Let $g_1, \ldots, g_k \in \mathrm{GL}_2^+(\mathbb{Q})$ and let σ be a singular modulus. If the functions $j(g_1 z), \ldots, j(g_n z)$ are pairwise distinct then $j(g_1 z) - \sigma, \ldots, j(g_n z) - \sigma$ are multiplicatively independent modulo $\mathbb{C}$.

Here σ is fixed. What if we allow it to vary?

Multiplicative special curves

Definition

A function $f : \mathbb{H} \to \mathbb{C}$ is called a j-map if either it is of the from $j(gz)$ where $g \in \mathrm{GL}_2^+(\mathbb{Q})$ or is constantly equal to a singular modulus.

Definition

Let $n \in \mathbb{Z}_{>0}$. Let $f_1, \ldots, f_n, f$ be pairwise distinct j-maps, at least one of which is non-constant. The set $\{(f_1(z), \ldots, f_n(z), f(z)) : z \in \mathbb{H}\}$ is called a multiplicative special curve in $\mathbb{C}^{n+1}$ if there exist $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ such that, for all $z \in \mathbb{H}$,

$$\prod_{i=1}^{n} (f_i(z) - f(z))^{a_i} = 1.$$

- A multiplicative special curve is an algebraic curve.
- A multiplicative special curve gives rise to infinitely many multiplicative relations among differences of singular moduli.
- Modular polynomials give rise to multiplicative special curves, and these are the only such curves. For a given n, there are only finitely many of them.

Multiplicative special curves exist

Let $N \in \mathbb{Z}_{>0}$, let

$$C(N) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}) : ad = N, a > 0, 0 \leq b < d, \gcd(a, b, d) = 1 \right\}.$$

Then $\Phi_N(X, j(z)) = \prod_{g \in C(N)} (X - j(gz))$.

Let $F_N(X) := \Phi_N(X, X) = u \prod_k (X - \alpha_k)^{a_k}$.

We have

$$\prod_{g \in C(N)} (j(z) - j(gz)) = F_N(j(z)) = u \prod_k (j(z) - \alpha_k)^{a_k}.$$

Thus,

$$\prod_k (j(z) - \alpha_k)^{-a_k} \prod_{g \in C(N)} (j(z) - j(gz)) = u.$$

When leading coefficient u is ± 1 (e.g. N is non-square), this gives a multiplicative special curve.

Characterising multiplicative special curves

Theorem (A.-Eterović-Fowler)

Let $n \in \mathbb{Z}_{>0}$. Let $f_1, \dots, f_n, f$ be pairwise distinct j-maps, at least one of which is non-constant. Suppose that $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$ and $c \in \mathbb{C}^\times$ are such that

$$\prod_{i=1}^{n} (f_i(z) - f(z))^{a_i} = c \text{ for all } z.$$

Then, after a change of variables, $f(z) = j(z)$ and there exist $k \in \{1, \dots, n\}$, $N_1, \dots, N_k \in \mathbb{Z}_{>1}$ pairwise distinct, and $b_1, \dots, b_k \in \mathbb{Z} \setminus \{0\}$ such that

- $\{f_i : f_i \text{ is non-constant}\} = \{j(gz) : g \in C(N_i),\ i = 1, \dots, k\}$,
- $\prod_{f_i \neq const} (f_i(z) - f(z))^{a_i} = \prod_{i=1}^{k} \left(\prod_{g \in C(N_i)} (j(gz) - j(z)) \right)^{b_i}$,
- $\prod_{f_i = const} (f_i(z) - f(z))^{a_i} = c \prod_{i=1}^{k} F_{N_i}(j(z))^{-b_i}$.

Main results

Theorem (A.-Eterović-Fowler)

Let $n \in \mathbb{Z}_{>0}$. Then there are only finitely many multiplicative special curves in $\mathbb{C}^{n+1}$ and these may be determined effectively. If $n \leq 5$, then there are no multiplicative special curves in $\mathbb{C}^{n+1}$.

Theorem (A.-Eterović-Fowler)

Let $n \in \mathbb{Z}_{>0}$. Then there exist only finitely many $(n+1)$-tuples $(\alpha_1, \ldots, \alpha_n, \sigma)$ of pairwise distinct singular moduli $\alpha_1, \ldots, \alpha_n, \sigma$ such that $\prod_{i=1}^{n}(\alpha_i - \sigma)^{a_i} = 1$ for some $a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$ and $(\alpha_1, \ldots, \alpha_n, \sigma)$ does not belong to one of the finitely many multiplicative special curves in $\mathbb{C}^{n+1}$.

Corollary (A.-Eterović-Fowler)

Let $n \in \{1, \ldots, 5\}$. There exist only finitely many $(n+1)$-tuples $(\alpha_1, \ldots, \alpha_n, \sigma)$ of pairwise distinct singular moduli $\alpha_1, \ldots, \alpha_n, \sigma$ such that $\prod_{i=1}^{n}(\alpha_i - \sigma)^{a_i} = 1$ for some $a_1, \ldots, a_n \in \mathbb{Z}\setminus\{0\}$.