A generalization to Elkies's Theorem on infinitely many supersingular primes

Wanlin Li, Centre de Recherches Mathématiques
joint with Elena Mantovan, Rachel Pries and Yunqing Tang

VaNTAGe series 10 , Nov 9, 2021

Elkies's theorem

Theorem (Elkies, 1987)

For every elliptic curve $E/\mathbb{Q}$, there exist infinitely many primes at which the reduction of E is supersingular.

Remarks:

1. If E is not CM, then at 100% of primes, its reduction is ordinary. Heuristically, we expect $\sim X^{1/2-o(1)}$ supersingular primes $\leq X$.

2. Elkies (1989) generalized the theorem to a large set of number fields.

3. Analogous results for certain abelian surfaces with quaternionic multiplication were obtained by Jao (2003), Sadykov (2004), and Baba-Grananth (2008).

A generalization to Elkies's theorem

Theorem (L.–Mantovan–Pries–Tang, In preparation)

Let $C : y^5 = x(x-1)(x-t)$ *be a smooth projective curve satisfying:*

- $j_C := \frac{(t^2-t+1)^3}{t^2(t-1)^2} \in \mathbb{Q} \cap [0, \frac{27}{4}]$*;*
- *the reduction of* C *at* 5 *is singular;*

then there exist infinitely many primes at which the reduction of $\mathrm{Jac}(C)$ *is "supersingular".*

Here "supersingular" means the p-divisible group over $\overline{\mathbb{F}}_p$,

$$\mathrm{Jac}(C)[p^\infty] \sim \begin{cases} \mathrm{ord}^2 \oplus \mathrm{ss}^2, p \equiv 1 \bmod 5; \\ \mathrm{ss}^4, p \equiv 2, 3, 4 \bmod 5; \end{cases}$$

where ord is $E[p^\infty]$ for an ordinary elliptic curve and ss is $E[p^\infty]$ for a supersingular elliptic curve.

Newton locus

Given an abelian variety $A/\overline{\mathbb{F}}_p$, the isogeny class of the p-divisible group $A[p^\infty]$ is determined by its Newton polygon.

The set of symmetric Newton polygons of dimension g and height $2g$ form a poset and give a stratification of $\mathcal{A}_{g,\bar{\mathbb{F}}_p}$, where the largest locus is ordinary and the smallest locus is supersingular.

Consider the 1-dimensional family of curves $y^5 = x(x-1)(x-t)$ parameterized by $t \in \overline{\mathbb{F}}_p, p \neq 5$.

There are two Newton strata on the Torelli image of this family:

one is open and dense, called μ-ordinary; the other consists of finitely many points, called basic or "supersingular".

Remarks

1. With Cantoral Farfán, Mantovan, Pries and Tang, we are working towards proving that for 100% of rational primes, the reduction of a non-CM $\mathrm{Jac}(C)$ is μ-ordinary.

   (Recall: for 100% of rational primes, the reduction of a non-CM $E/\mathbb{Q}$ is ordinary.)

2. We can extend the theorem to $j(t) \in \mathbb{Q}(\sqrt{5})$ with an extra local condition on C.

3. We are working on extending the theorem to more curves in this family (relaxing $j(t) \in [0, \frac{27}{4}]$ and C mod 5 being singular),

   and curves in several other superelliptic families
   (e.g. $y^7 = x(x-1)(x-t)$).

Parameterization of $y^5 = x(x-1)(x-t)$

Given a curve $C : y^5 = x(x-1)(x-t)$, the invariant

$$j_C := \frac{(t^2-t+1)^3}{t^2(t-1)^2}$$

uniquely determines its isomorphism class over $\overline{\mathbb{Q}}$.

So $j(t)$ is a parameter for the coarse moduli space $\mathcal{S} \simeq \mathbb{P}^1_{\mathbb{Q}}$ of the family.

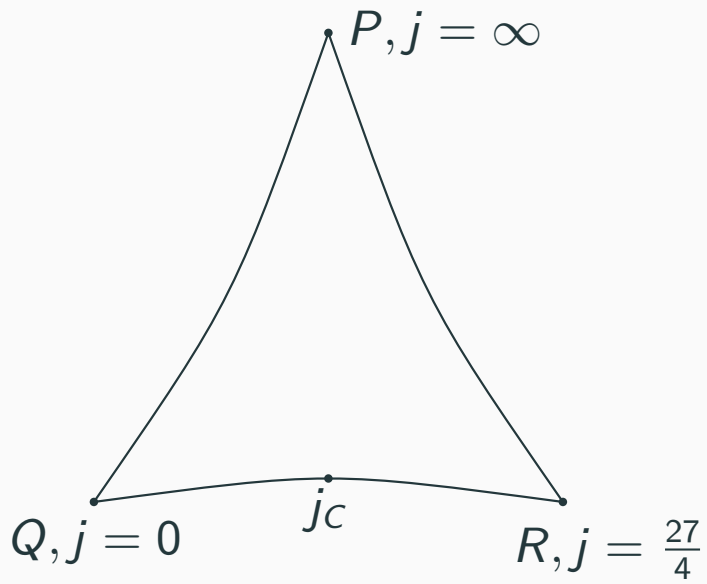
In the theorem, having $j(t) \in \mathbb{Q}$ means the field of moduli for C is $\mathbb{Q}$.

Geometry of $\mathcal{S}(\mathbb{C})$

Over $\mathbb{Q}(\zeta_5)$, $C : y^5 = x(x-1)(x-t)$ admits an automorphism

$$(x, y) \mapsto (x, \zeta_5 y).$$

This induce $\mathbb{Q}(\zeta_5) \hookrightarrow \mathrm{End}^0_{\mathbb{Q}}(\mathrm{Jac}(C))$ and $\mathcal{S} \hookrightarrow \mathrm{Sh}(\mathbb{Q}(\zeta_5))$, a compact Shimura curve with reflex field $\mathbb{Q}(\zeta_5)$.



We get $\mathcal{S}(\mathbb{C}) \simeq \Delta(2, 3, 10) \setminus \mathbb{H}$. Its fundamental domain is two copies of the hyperbolic triangle with vertices $j = 0, \frac{27}{4}, \infty$.

Newton strata for $\mathcal{S}(\overline{\mathbb{F}}_p)$

For any $p \neq 5$, $\mathcal{S}$ has good reduction at p and $\mathcal{S}_{\overline{\mathbb{F}}_p} \simeq \mathbb{P}^1_{\overline{\mathbb{F}}_p}$ has two Newton loci, μ-ordinary and basic ("supersingular").

The μ-ordinary locus is open and dense and the "supersingular" locus is 0-dim consisting of finitely many points.

There is only one Newton locus for $\mathcal{S}_{\overline{\mathbb{F}}_5}$ and it is supersingular.

strategy of proof

Goal: "Catch" primes p s.t. $(C \bmod p) \in$ "supersingular" locus of $\mathcal{S}_{\overline{\mathbb{F}}_p}$.

Call this set of primes $\mathcal{T}$.

Strategy: Construct curves $C_1, C_2, \cdots$ and define sets

$$T_i = \{p \mid C \simeq C_i \bmod p\}$$

such that

1. For each i, $T_i \cap \mathcal{T} \neq \emptyset$;
2. For any $p \in T_i \cap T_j \Rightarrow p \notin \mathcal{T}$;
3. For each i, $(C_i \bmod 5)$ is smooth.

A sketch of proof

Given C and a finite set $\mathcal{S}$ of primes, construct a "supersingular" $p \notin S$.

1. For totally positive prime element $\lambda \in \mathbb{Q}(\sqrt{5})$, construct CM curves C_λ. Moreover, $\mathrm{Jac}(C_\lambda)$ admits "supersingular" reduction at $\mathfrak{p}$ where

$$\left(\frac{-\lambda}{\mathfrak{p}}\right) \neq 1, \ \mathfrak{p} \text{ a prime of } \mathbb{Q}(\sqrt{5});$$

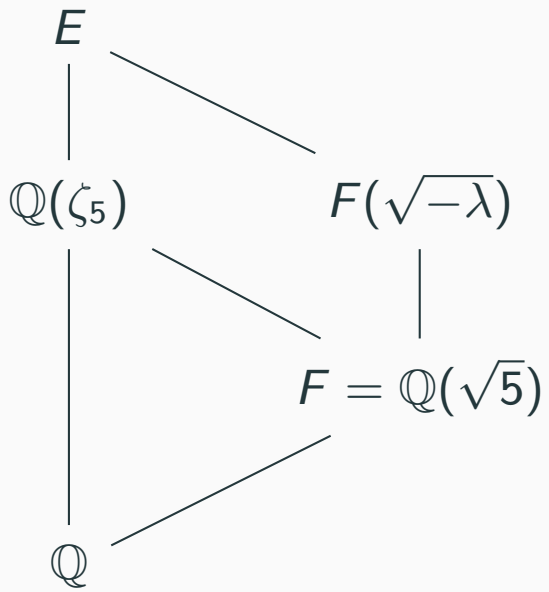
2. Define $P_\lambda(x) \in \mathbb{Q}(\sqrt{5})[x]$ such that $v_\mathfrak{p}(P_\lambda(j_C)) > 0$ implies $(C \simeq C_\lambda \bmod \mathfrak{p})$.
3. By deformation theory, the numerator and denominator of $(j_C - \frac{27}{4})P_\lambda(j_C)$ are $\equiv \square \bmod \lambda$.
   (or a similar statement with a change of coordinate holds)
4. Find congruence conditions on λ which imply $P_\lambda(x)$ having a unique real root (for each $\mathbb{Q}(\sqrt{5}) \hookrightarrow \mathbb{R}$).

A sketch of proof

5. λ can be chosen such that primes above p split if $p \in \mathcal{S} - \{5\}$ or $v_p(j_C - \frac{27}{4}) \neq 0$ and C_λ is smooth at 5 (WLOG,assume $5 \in \mathcal{S}$).
6. From analyzing quadratic forms over $\mathbb{Q}(\sqrt{5})$ and applying Hecke's equidistribution theorem simultaneously for the two embeddings $\lambda \hookrightarrow \mathbb{R}$, we obtain the existence of λ satisfying the desired congruence conditions and $\frac{1+\sqrt{5}}{2}(j_C - \frac{27}{4})P_\lambda(j_C)$ is totally positive.
7. From
$$\left(\frac{(j_C - \frac{27}{4})P_\lambda(j_C)}{\lambda}\right) \neq -1, \text{ and } \left(\frac{\frac{1+\sqrt{5}}{2}}{\lambda}\right) = -1,$$
we conclude that there exists a totally positive prime element $\pi_\mathfrak{p}$ with $v_\mathfrak{p}(P_\lambda(j_C)) > 0$ such that
$$\left(\frac{\pi_\mathfrak{p}}{\lambda}\right) = \left(\frac{-\lambda}{\pi_\mathfrak{p}}\right) \neq 1$$
Thus, we get a "supersingular" prime for C outside of $\mathcal{S}$.

CM cycles and its reduction

$\dim \mathrm{Jac}(C) = 4$; $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$. Let $\lambda \in O_F$ be a totally positive prime, then E is a CM field with $[E : \mathbb{Q}] = 8$. Consider $\mathrm{Jac}(C_\lambda)$ with CM by O_E.



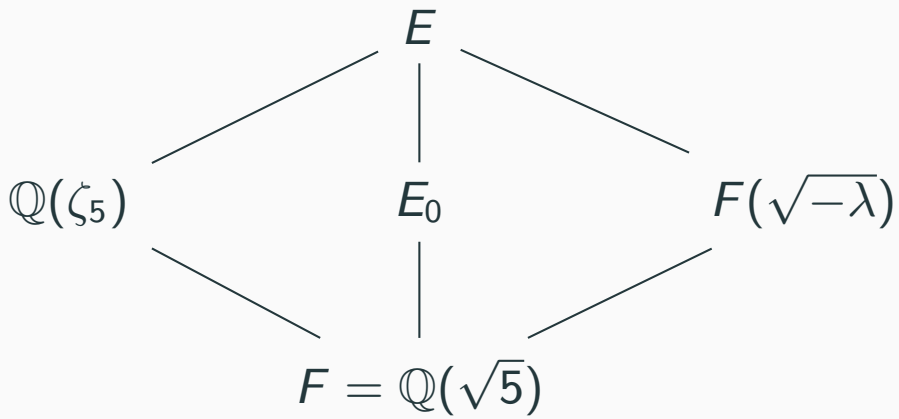
There is a unique (primitive) CM type compatible with the signature.

By Shimura–Taniyama formula, if a prime $\mathscr{P}$ lies above $\mathfrak{p} \subset F$ non-split in $F(-\lambda)/F$, then the reduction of $\mathrm{Jac}(C_\lambda)$ at $\mathscr{P}$ is "supersingular".

Real CM points: uniqueness

A real CM point C_λ corresponds to a principally polarized abelian variety with CM by O_E and isomorphic to its complex conjugate.

From CM theory, it is given by a pair $(\mathfrak{a}, \xi)$ where $\mathfrak{a}$ is an ideal class of E fixed by complex conjugation and $\xi \in E$ induces a principal polarization.



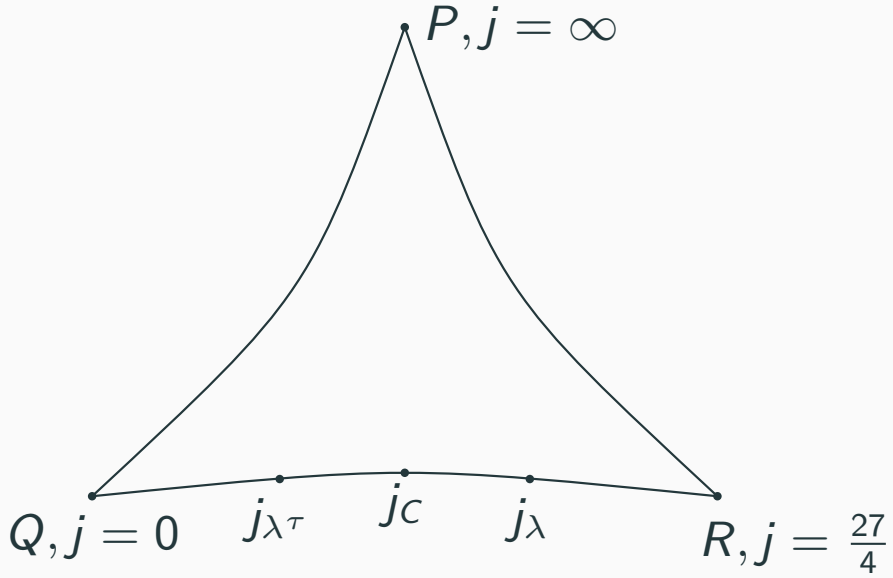
By analyzing the parity of the class number of E and the Hasse unit index $[N(\mathcal{U}_E) : \mathcal{U}_{E_0}^2]$, we give congruence conditions on λ which guarantees the number of real CM points being 1.

Real CM points: distribution

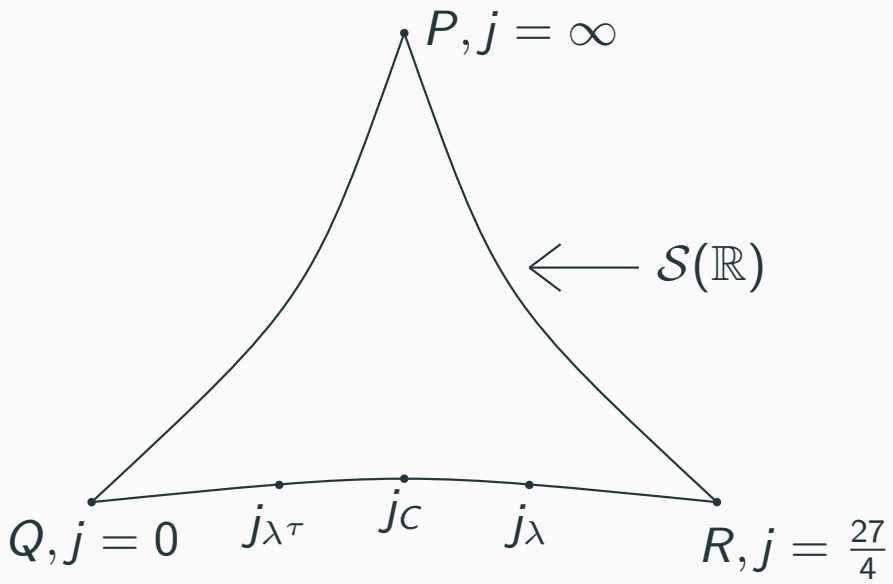
Denote the image of λ under two embeddings $\mathbb{Q}(\sqrt{5}) \hookrightarrow \mathbb{R}$ as λ, λ^τ.

Denote the unique real root for $P_\lambda(x)$ (resp. $P_{\lambda^\tau}(x)$) as j_λ (resp. j_{λ^τ}).

Want $\frac{1\pm\sqrt{5}}{2} P_\lambda(j_C)$ totally positive, i.e. $(j_C - j_\lambda)(j_C - j_{\lambda^\tau}) < 0$.



j_λ corresponds to $x, y \in O_F$ satisfying $\lambda = 3x^2 - (5+\sqrt{5})xy + \frac{5+\sqrt{5}}{2} y^2$.
Apply Hecke's equidistribution theorem to conclude $j_\lambda, j_{\lambda^\tau}$ dense on QR.



Thank you for your attention !