Pro-p criterion of good reduction of punctured elliptic curves

Wojciech Porowski

University of Nottingham

June/July 2021

Notation

p - a prime number, assume $p \geq 5$,
K - a finite field extension of $\mathbb{Q}_p$,
$G_K = \mathrm{Gal}(K^{\mathrm{alg}}/K)$ - the absolute Galois group of K,
E - an elliptic curve over K,
$O \in E(K)$ - the origin of the elliptic curve E,
$X = E \setminus \{O\}$ - a hyperbolic curve over K obtained from E by removing the origin,
$\pi_1(X)$ - the étale fundamental group of X,
$\pi_1(X_{K^{\mathrm{alg}}})$ - the geometric fundamental group of X.

Pro-p fundamental groups

Δ_X - maximal pro-p quotient of $\pi_1(X_{K^{\mathrm{alg}}})$,
Π_X - maximal geometrically pro-p fundamental group, i.e., we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(X_{K^{\mathrm{alg}}}) & \longrightarrow & \pi_1(X) & \longrightarrow & G_K & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \Delta_X & \longrightarrow & \Pi_X & \longrightarrow & G_K & \longrightarrow & 1. \end{array}$$

Note that the relative Grothendieck Conjecture holds for maximal geometrically pro-p fundamental groups (for hyperbolic curves over K).

Problem

The starting point of today's talk is the following problem.

Question

Given the topological group Π_X, is it possible to determine the reduction type of the elliptic curve E over K?

Using the terminology introduced in previous talks, this is a question in absolute mono-anabelian geometry.
Similar question has been already considered by Y. Hoshi in the case of proper hyperbolic curves.

Main Result

In this talk we will sketch a proof of the following theorem:

Theorem (P.)

Assume that $p \geq 5$ and that E has a nontrivial K-rational p-torsion point. Then, the reduction type of E over K can be determined group theoretically from the topological group Π_X.

During the talk we will also explain the necessity these two additional assumptions.

Plan

Here is a brief plan of the proof.

- First we look only at the action of Galois group on the Tate module of E. This will be enough to determine the potential reduction type of E (i.e., after a finite extension). Then we will reduce our problem to the case of an elliptic curve with potentially good supersingular reduction.
- Second part deals only with the above case. Here we use mono-anabelian methods introduced by S. Mochizuki, together with some facts from the theory of elliptic curves.

Tate Module of E

$T_p(E)$ - p-adic Tate module of E, $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$,
It is known that the subgroup $\Delta_X \subset \Pi_X$ can be characterized group theoretically.
Thus we may construct the short exact sequence

$$1 \to \Delta_X \to \Pi_X \to \Pi_X/\Delta_X \to 1,$$

as well as the representation

$$G_K \cong \Pi_X/\Delta_X \curvearrowright \Delta_X^{\mathrm{ab}} \cong T_p(E).$$

Problems with G_K

But cannot we simply finish here by saying that E has good reduction iff the above representation is crystalline?
The problem comes from the fact that in the absolute setting the quotient Π_X/Δ_X and the Galois group G_K are not equipped with a fixed isomorphism.
Moreover, the notion of a crystalline representation is not group theoretic (unlike, for example, unramified representations).
In the following we will simply write $G_K = \Pi_X/\Delta_X$, thus the group G_K should be considered up to an automorphism.

Galois Action on the Tate Module

Let $I_K \subset G_K$ be the inertia subgroup.
Denote $\mu_n \subset K^{\text{alg}}$ - roots of unity of order n; $\mathbb{Z}_p(1) = \varprojlim \mu_{p^n}$
Recall some facts about the p-adic representation $V_p(E)$.
If E is a Tate curve, then we have

$$1 \to \mathbb{Q}_p(1) \to V_p(E) \to \mathbb{Q}_p \to 1.$$

If E has good ordinary reduction, then

$$1 \to \mathbb{Q}_p(\chi^{-1})(1) \to V_p(E) \to \mathbb{Q}_p(\chi) \to 1,$$

where χ is some unramified character.
Finally, if E has good supersingular reduction then there are no nontrivial I_K-equivariant homomorphisms $V_p(E) \to \mathbb{Q}_p$.

Potential type of reduction

Going back to the representation $G_K \curvearrowright \Delta_X^{\mathrm{ab}} \otimes \mathbb{Q}_p \cong V_p(E)$.
Pick L/K finite extension such that E has semi-stable reduction over L. (this can be done group theoretically).
Then E has bad reduction over L iff $\exists$ a surjection $V_p(E) \twoheadrightarrow \mathbb{Q}_p$.
Moreover, if E has good reduction over L we may distinguish ordinary and supersingular ones.

Reduction to good supersingular case

To check if good ordinary reduction descends from L to K we use the following nontrivial results from p-adic Hodge Theory:

- Every two dimensional p-adic representation V fitting in the following s.e.s
$$1 \to \mathbb{Q}_p(\chi^{-1})(1) \to V \to \mathbb{Q}_p(\chi) \to 1$$
is semistable (here χ is an unramified character).
- If $V_p(E)$ is semistable then E has semistable reduction.

Then, since (for elliptic curves) semistable + potentially good $\Rightarrow$ good, we may solve the potentially good ordinary case.
Therefore, from now on we assume that E has potentially good supersingular reduction.

Decomposition group of a cusp

Temporarily X - a hyperbolic curve over K.
Cusp $=$ geometric point lying on the boundary of X.
Fix a decomposition group D of a K-rational cusp c, $D \subset \Pi_X$.
We have a short exact sequence:

$$1 \to I \to D \to G_K \to 1.$$

where $I = D \cap \Delta_X$ is an inertia group.
We have $I \cong \mathbb{Z}_p(1)$ as G_K-modules, canonically.

Cuspidal sections

A section s of the surjection $D \twoheadrightarrow G_K$ is called cuspidal.
We consider cuspidal sections up to conjugation by I.
The set of cuspidal sections is a torsor over $H^1(G_K, I)$.
Define $\widehat{K^*} = \varprojlim_{n\in\mathbb{N}} K^*/(K^*)^{p^n}$ (only powers of p).
By Kummer theory $\widehat{K^*} = H^1(G_K, \mathbb{Z}_p(1)) \cong H^1(G_K, I)$.
One can identify cuspidal sections with cohomology classes in $H^1(D, I)$ whose restriction to I

$$H^1(D, I) \to H^1(I, I) = \mathrm{Hom}(I, I)$$

is the identity.

Discrete sections

R_c - completion of the local ring at the cusp c; $\mathfrak{m}_c$ - maximal ideal, $T_c^\vee = \mathfrak{m}_c/\mathfrak{m}_c^2$ - cotangent space at c.
For nonzero $\omega \in T_c^\vee$, choice of compatible system of p-power roots determines a section of the surjection $D \twoheadrightarrow G_K$.
We obtain a map of sets:

$$T_c^\vee \setminus \{0\} \longrightarrow \{\text{cuspidal sections}\}$$

Sections in the image are called discrete sections, they form a torsor over a group $K^{*\mu} = K^*/\{\text{roots of unity of order prime to } p\}$ (we have $K^{*\mu} \hookrightarrow \widehat{K^*}$).

Integral sections

Suppose now that E has good reduction over K.
Let $\mathcal{O}_K$ - the valuation ring of K, $U_K \subset \mathcal{O}_K^*$ - group of (principal) units.
Smooth model defines an $\mathcal{O}_K$-structure on the K-vector space $T_c^\vee$, i.e., a free $\mathcal{O}_K$-module $T_{\mathcal{O}_K}^\vee$ of rank 1 s.t. $T_{\mathcal{O}_K}^\vee \otimes K = T_c^\vee$.
Discrete sections coming from generators of this $\mathcal{O}_K$-module are called integral.
The set of integral sections is a torsor over the group U_K.

Remark

Note that the notion of discrete/integral section is not, a priori, group theoretic.

Valuation of the discriminant

How do we use these sections to find the reduction type of E?
Let L/K a field extension s. t. E has good reduction over L.
Write D_L for the preimage of $G_L \subset G_K$ under $D \twoheadrightarrow G_K$.
Consider the following diagram:

$$\begin{array}{ccc} D_L & \underset{}{\overset{s_L}{\rightleftarrows}} & G_L \\ \downarrow & & \downarrow \\ D & \underset{s_K}{\rightleftarrows} & G_K. \end{array}$$

Lemma

There exists a discrete section s_K which restricts to an integral section s_L over L if and only if the valuation $v_K(\Delta)$ of the minimal discriminant Δ of E over K is divisible by 12.

Sketch of the proof

Write $T := T_K^\vee$, $T_L = T \otimes L$.
Fix a minimal Weierstrass equation for E over K with discriminant Δ

$$y^2 + a_1xy + a_3y = x^3 + a_4x^2 + a_2x + a_6,$$

and similarly for E_L with the prime symbol (e.g. x', y', Δ').
Functions $z = x/y$ and $z' = x'/y'$ are uniformizers at O, write t and t' for the corresponding cotangent vectors ($t \in T, t' \in T_L$).
Hence they define discrete sections; moreover, t' defines an integral section since E has good reduction over L.
Thus, the first statement in the lemma is equivalent to the existence of $a \in K^*$ and $b \in \mathcal{O}_L^*$ such that $at = bt'$ (equality in T_L).

Sketch of the proof (2)

On the other hand, we have:

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t$$

for some $u \in L^*$ and $r, s, t \in L$. We know that $u^{12}\Delta = \Delta'$, which implies $12v(u) = -v(\Delta)$ (since Δ' is a unit).
Moreover, we check that $ut = t'$ therefore the equation $at = bt'$ is equivalent to $a = bu$, where $a \in K^*$ and $b \in \mathcal{O}_L^*$. But this is the same as $v(a) = v(u)$, i.e., $v(u) \in v(K^*)$. ■

Remark

When $p \geq 5$ (and E has pot. good reduction) we have $v_K(\Delta) < 12$ thus this lemma would prove the main theorem (assuming we can construct discrete and integral sections group theoretically).

Summary

We have just seen that constructing discrete and integral sections would prove the main theorem thanks to the previous lemma.
This construction is bit technical so we will only sketch the main points.
(1) Elliptic cuspidalization.
(2) Kummer classes of rational functions.
(3) Local heights of p-power torsion points.
(4) A *rigidity* isomorphism.

Elliptic cuspidalization

Recall that $X = E \setminus \{O\}$. Write $X_n \hookrightarrow X$ for the open subscheme obtained by removing p^n- torsion points from E.
The inclusion $X_n \hookrightarrow X$ induces surjection $\Pi_{X_n} \twoheadrightarrow \Pi_X$.
By applying elliptic cuspidalization one can reconstruct this extension from the topological group Π_X.
Idea of the construction:

$$\begin{array}{ccc} X_n & \hookrightarrow & E \\ \downarrow & & \downarrow n \\ X & \hookrightarrow & E, \end{array}$$

Kummer theory

Temporarily X - a hyperbolic curve over K. We have the Kummer map

$$\mathcal{O}(X)^* \to H^1(\Pi_X, \mathbb{Z}_p(1)).$$

Define

$$M_X = \mathrm{Hom}_{\mathbb{Z}_p}(H^2(\Delta_{\overline{X}}, \mathbb{Z}_p), \mathbb{Z}_p),$$

by Poincaré duality $M_X \cong \mathbb{Z}_p(1)$, canonically.
We may construct the following commutative diagram

$$\begin{array}{ccccc} K^* & \longrightarrow & \mathcal{O}(X)^* & \xrightarrow{div} & \bigoplus_{x \in cusps} \mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow \\ H^1(G_K, M_X) & \longrightarrow & H^1(\Pi_X, M_X) & \longrightarrow & \bigoplus_{x \in cusps} \mathbb{Z}_p. \end{array}$$

Sections vs Functions

By applying Kummer theory and elliptic cuspidalization we may construct cohomology classes of rational functions (inside $H^1(\Pi_U, M_X)$, where $U \hookrightarrow X$ is an open subscheme of X), whose divisors are supported on the set of p-power torsion points.
However, constant functions are replaced by $\widehat{K^*}$.
D, I - decomp. and inertia group of a fixed cusp c, f - uniformizer at c.
Restrict Kummer class of f to D:

$$H^1(D, I) \to H^1(I, I) = \mathrm{Hom}(I, I).$$

This produces a discrete section at the cusp c.
(The natural isom. $M_X \cong I$ is grp. theoretic)

Local Heights of p-torsion points

Suppose that E has good reduction over K. Fix a minimal Weierstrass equation of E:

$$y^2 + a_1xy + a_3y = x^3 + a_4x^2 + a_2x + a_6.$$

Recall the Néron-Tate local height function h. In our case we simply have $h(P) = -v(x(P))/2$.
Consider rational functions on E of the form $f = \lambda(x - x(P))$, where P - nonzero p-torsion point.
Function f has single zeroes at P and $-P$ and double pole at O.
Thus, the Kummer class of f may be constructed group theoretically.
Note that f is "close" to the function h.

Local Heights of p-torsion points (2)

Using functions similar to f we give a group theoretic computation of heights of p-power torsion points P. Here we need two facts:

- We have $v(x(P)) < 0$ and $v(x(P)) \to 0$ as $\mathrm{ord}(P) \to \infty$,
- Heights of p-torsion points are constrained by the shape of a Newton polygon of the power series determined by multiplication by p on the formal group of E (see [Serre]). Required part of the above polygon can be reconstructed from Π_X.

From the above one can construct the U_K-torsor of integral sections.

Rigidity isomorphism

Finally, there is a one technical point.
Discrete sections are obtained as a torsor over $H^1(G_K, I) \cong \widehat{K^*}$. However, the valuation map

$$H^1(G_K, I) \cong \widehat{K^*} \twoheadrightarrow \mathbb{Z}_p$$

is not (a priori) group theoretic (there is a $\mathbb{Z}_p^*$ indeterminacy). To fix this, we have to give a construction of a certain rigidity isomorphism; we achieve this again with the help of local heights.

References

Y. Hoshi - On the pro-p absolute anabelian geometry of proper hyperbolic curves,
S. Mochizuki - Galois sections in absolute anabelian geometry,
J. P. Serre - Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.

End of the talk

Thank you for your attention!