A LOCAL-GLOBAL PRINCIPLE FOR ISOGENIES BETWEEN ELLIPTIC CURVES OVER NUMBER FIELDS

Samuele Anni

Universiteit Leiden - Université Bordeaux 1

Grenoble, 28th Journées Arithmétiques;
4th July 2013
### 1 Preliminaries and introduction
- Local-to-global principles
- Local-to-global principle for elliptic curves: TORSION
- Local-to-global principle for elliptic curves: ISOGENIES

### 2 Exceptional pairs

### 3 New results

### 4 Finiteness result
Local-global problems: from knowledge about local structures to knowledge about global structures.
**Local-global problems**: from knowledge about local structures to knowledge about global structures.

In this context: from $p$-adic information global information. For example:
Local-global problems: from knowledge about local structures to knowledge about global structures.

In this context: from $p$-adic information global information. For example:

Local-to-global principles for quadratic forms.
Local-global problems: from knowledge about local structures to knowledge about global structures.

In this context: from $p$-adic information global information. For example:

**Local-to-global principles for quadratic forms.**

**Theorem of Hasse-Minkowski**

Two quadratic forms with coefficients in $\mathbb{Q}$ which are equivalent over $\mathbb{Q}_p$ for all prime numbers $p$ and over $\mathbb{R}$ are equivalent over $\mathbb{Q}$. 
Local-to-global principle for elliptic curves: TORSION

Let $\ell$ be a prime. Katz in 1981 studied the local-global principle for $\ell$-torsion for elliptic curves.

**Theorem (Katz)**

Let $E$ be an elliptic curve over a number field $K$. If $E$ has non-trivial $\ell$-torsion locally at a set of primes with density one then $E$ is $K$-isogenous to an elliptic curve which has non-trivial $\ell$-torsion over $K$.

He proved this by reducing the problem to a purely group-theoretic statement.
Local-to-global principle for elliptic curves: TORSION

Let $\ell$ be a prime. Katz in 1981 studied the local-global principle for $\ell$-torsion for elliptic curves.
Local-to-global principle for elliptic curves: TORSION

Let $\ell$ be a prime. Katz in 1981 studied the local-global principle for $\ell$-torsion for elliptic curves.

**Theorem (Katz)**

Let $E$ be an elliptic curve over a number field $K$. If $E$ has non-trivial $\ell$-torsion locally at a set of primes with density one then $E$ is $K$-isogenous to an elliptic curve which has non-trivial $\ell$-torsion over $K$. 
Local-to-global principle for elliptic curves: TORSION

Let $\ell$ be a prime. Katz in 1981 studied the local-global principle for $\ell$-torsion for elliptic curves.

**Theorem (Katz)**

Let $E$ be an elliptic curve over a number field $K$. If $E$ has non-trivial $\ell$-torsion locally at a set of primes with density one then $E$ is $K$-isogenous to an elliptic curve which has non-trivial $\ell$-torsion over $K$.

He proved this by reducing the problem to a purely group-theoretic statement.
Local-to-global principle for elliptic curves: ISOGENIES

**Definition**

Let $E$ be an elliptic curve defined on a number field $K$, and let $\ell$ be a prime number. If $\mathfrak{p}$ is a prime of $K$ where $E$ has good reduction, $\mathfrak{p}$ not dividing $\ell$, we say that $E$ admits an $\ell$-isogeny **locally** at $\mathfrak{p}$ if the Néron model of $E$ over the ring of integer of $K_\mathfrak{p}$ admits an $\ell$-isogeny.
Local-to-global principle for elliptic curves: ISOGENIES

**Definition**

Let $E$ be an elliptic curve defined on a number field $K$, and let $\ell$ be a prime number. If $\mathfrak{p}$ is a prime of $K$ where $E$ has good reduction, $\mathfrak{p}$ not dividing $\ell$, we say that $E$ admits an $\ell$-isogeny **locally** at $\mathfrak{p}$ if the Néron model of $E$ over the ring of integer of $K_{\mathfrak{p}}$ admits an $\ell$-isogeny.

If $E$ admits an $\ell$-isogeny over $K$, then $E$ necessarily admits an $\ell$-isogeny locally at every prime of good reduction. The converse statement has been recently studied by Sutherland (arxiv, November 2011).
**Question**

Let $E$ be an elliptic curve defined over a number field $K$, and let $\ell$ be a prime number, if $E$ admits an $\ell$-isogeny locally at a set of primes with density one then does $E$ admit an $\ell$-isogeny over $K$?
**Question**

Let $E$ be an elliptic curve defined over a number field $K$, and let $\ell$ be a prime number, if $E$ admits an $\ell$-isogeny locally at a set of primes with density one then does $E$ admit an $\ell$-isogeny over $K$?

**Theorem (Sutherland)**

Let $E$ be an elliptic curve defined over a number field $K$ and let $\ell$ be a prime number. Assume $\sqrt{\left(\frac{-1}{\ell}\right) \ell \notin K}$, and suppose $E/K$ admits an $\ell$-isogeny locally at a set of primes with density one. Then $E$ admits an $\ell$-isogeny over a quadratic extension of $K$. Moreover, if $\ell \equiv 1 \mod 4$ or $\ell < 7$, $E$ admits an $\ell$-isogeny defined over $K$. 
1 Preliminaries and introduction

2 Exceptional pairs

3 New results

4 Finiteness result
**Definition**

Let $K$ be a number field, let $E$ be an elliptic curve over $K$ and $\ell$ a prime number, a pair $(\ell, j(E))$ is said to be **exceptional** for $K$ if $E/K$ admits an $\ell$-isogeny locally everywhere but not over $K$.
Definition

Let $K$ be a number field, let $E$ be an elliptic curve over $K$ and $\ell$ a prime number, a pair $(\ell, j(E))$ is said to be exceptional for $K$ if $E/K$ admits an $\ell$-isogeny locally everywhere but not over $K$.

Sutherland proved the following result:
Definition

Let $K$ be a number field, let $E$ be an elliptic curve over $K$ and $\ell$ a prime number, a pair $(\ell, j(E))$ is said to be exceptional for $K$ if $E/K$ admits an $\ell$-isogeny locally everywhere but not over $K$.

Sutherland proved the following result:

Theorem (Sutherland)

The pair $(7, 2268945/128)$ is the only exceptional pair for $\mathbb{Q}$.
Theorem (Sutherland)

Let $E$ be an elliptic curve defined over a number field $K$ and let $\ell$ be a prime number. Assume $\sqrt{\left( \frac{-1}{\ell} \right) \ell} \not\in K$, and suppose $E/K$ admits an $\ell$-isogeny locally at a set of primes with density one. Then $E$ admits an $\ell$-isogeny over a quadratic extension of $K$. Moreover, if $\ell \equiv 1 \mod 4$ or $\ell < 7$, $E$ admits an $\ell$-isogeny defined over $K$. 
Let $E$ be an elliptic curve defined over a number field $K$, then on the $\ell$-torsion points of $E[\ell](\overline{Q})$ there is a $\text{Gal}(\overline{Q}/K)$-action. Then there exist a Galois representation $\rho_{E,\ell}$:
Let $E$ be an elliptic curve defined over a number field $K$, then on the $\ell$-torsion points of $E[\ell](\overline{\mathbb{Q}})$ there is a $\text{Gal}(\overline{\mathbb{Q}}/K)$-action. Then there exist a Galois representation $\rho_{E,\ell}$:

$$\text{Gal}(\overline{\mathbb{Q}}/K) \xrightarrow{\rho_{E,\ell}} \text{Aut}(E[\ell]) \cong \text{GL}_2(\mathbb{F}_\ell).$$
Let $E$ be an elliptic curve defined over a number field $K$, then on the $\ell$-torsion points of $E[\ell](\overline{\mathbb{Q}})$ there is a $\text{Gal}(\overline{\mathbb{Q}}/K)$-action. Then there exist a Galois representation $\rho_{E,\ell}$:

$$\text{Gal}(\overline{\mathbb{Q}}/K) \xrightarrow{\rho_{E,\ell}} \text{Aut}(E[\ell]) \cong \text{GL}_2(\mathbb{F}_\ell).$$

**Remark**

Let $(\ell, j(E))$ be an exceptional pair for the number field $K$ and let $G = \rho_{E,\ell}(\text{Gal}(\overline{\mathbb{Q}}/K))$. Then $G$ is a subgroup of $\text{GL}_2(\mathbb{F}_\ell)$ such that $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$. 
Given an elliptic curve $E$, defined over a number field $K$, the compatibility between $\rho_{E,\ell}$ and the Weil pairing on $E[\ell]$ implies that:

\[
\zeta_{\ell} \text{ is in } K \quad \text{if and only if} \quad G \text{ is contained in } \text{SL}_2(F_{\ell}) \text{ if and only if } H, \text{ the projective image of } G, \text{ is contained in } \text{SL}_2(F_{\ell})/\{\pm 1\} \text{ if and only if } \sqrt{\ell} \text{ belongs to } K.
\]

Remark: The solution to the local-global principle about $\ell$-isogenies over $K$ depends on $\sqrt{\ell} \text{ belonging to } K$. 

Samuele Anni

A local-global principle for isogenies over number fields
Given an elliptic curve $E$, defined over a number field $K$, the compatibility between $\rho_{E,\ell}$ and the Weil pairing on $E[\ell]$ implies that:

$$\zeta_{\ell} \text{ is in } K \iff G \text{ is contained in } SL_2(F_{\ell});$$

$$H, \text{ the projective image of } G, \text{ is contained in } SL_2(F_{\ell})/\{\pm 1\} \iff \sqrt{(-1)_{\ell}} \ell \text{ is in } K.$$  

Remark: The solution to the local-global principle about $\ell$-isogenies over $K$ depends on $\sqrt{(-1)_{\ell}} \ell$ belonging to $K$. 
Given an elliptic curve $E$, defined over a number field $K$, the compatibility between $\rho_{E,\ell}$ and the Weil pairing on $E[\ell]$ implies that:

- $\zeta_\ell$ is in $K$ if and only if $G$ is contained in $SL_2(\mathbb{F}_\ell)$;
Given an elliptic curve $E$, defined over a number field $K$, the compatibility between $\rho_{E,\ell}$ and the Weil pairing on $E[\ell]$ implies that:

- $\zeta_\ell$ is in $K$ if and only if $G$ is contained in $\text{SL}_2(\mathbb{F}_\ell)$;
- $H$, the projective image of $G$, is contained in $\text{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$ if and only if $\sqrt{(\frac{-1}{\ell})} \ell$ is in $K$.
Given an elliptic curve $E$, defined over a number field $K$, the compatibility between $\rho_{E,\ell}$ and the Weil pairing on $E[\ell]$ implies that:

- $\zeta_{\ell}$ is in $K$ if and only if $G$ is contained in $\text{SL}_2(\mathbb{F}_{\ell})$;
- $H$, the projective image of $G$, is contained in $\text{SL}_2(\mathbb{F}_{\ell})/\{\pm 1\}$ if and only if $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ is in $K$.

**Remark**

The solution to the local-global principle about $\ell$-isogenies over $K$ depends on $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ belonging to $K$. 
1 Preliminaries and introduction

2 Exceptional pairs

3 New results
   - First case
   - Second case

4 Finiteness result
Let us assume that $\sqrt{\left(\frac{-1}{\ell}\right)} \ell \notin K$. 
Let us assume that $\sqrt{\left(\frac{-1}{\ell}\right)} \notin K$.

**Lemma (Sutherland)**

Let $G$ be a subgroup of $\text{GL}_2(\mathbb{F}_\ell)$ whose image $H$ in $\text{PGL}_2(\mathbb{F}_\ell)$ is not contained in $\text{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. Suppose $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$.

Then $\ell \equiv 3 \mod 4$ and the following holds:

1. $H$ is dihedral of order $2n$, where $n > 1$ is an odd divisor of $(\ell - 1)/2$;
2. $G$ is properly contained in the normalizer of a split Cartan subgroup;
3. $\mathbb{P}^1(\mathbb{F}_\ell)/G$ contains an orbit of size 2.
Proposition (A.)

Let \((\ell, j(E))\) be an exceptional pair for the number field \(K\) with \(\sqrt{(-1/\ell) \ell}\) not belonging to \(K\). Then \(E\) admits an \(\ell\)-isogeny over \(K(\sqrt{-\ell})\) (and actually, two such isogenies).
Main Theorem (A.)

Let $(\ell, j(E))$ be an exceptional pair for the number field $K$ of degree $d$ over $\mathbb{Q}$, such that $\sqrt{\left(\frac{-1}{\ell}\right)} \ell \notin K$. Then

Remark

This theorem implies the result obtained by Sutherland in the case $K = \mathbb{Q}$.

This theorem is proved studying the Galois representation $\rho_{E,\ell}$.
Main Theorem (A.)

Let \((\ell, j(E))\) be an exceptional pair for the number field \(K\) of degree \(d\) over \(\mathbb{Q}\), such that \(\sqrt{\left(\frac{-1}{\ell}\right)} \ell \not\in K\). Then \(\ell \equiv 3 \text{ mod } 4\) and

\[ 7 \leq \ell \leq 6d+1. \]
Main Theorem (A.)

Let $(\ell, j(E))$ be an exceptional pair for the number field $K$ of degree $d$ over $\mathbb{Q}$, such that $\sqrt{(-1/\ell)} \notin K$. Then $\ell \equiv 3 \mod 4$ and

$$7 \leq \ell \leq 6d+1.$$ 

Remark

This theorem implies the result obtained by Sutherland in the case $K = \mathbb{Q}$. 
Main Theorem (A.)

Let $(\ell, j(E))$ be an exceptional pair for the number field $K$ of degree $d$ over $\mathbb{Q}$, such that $\sqrt{(-1/\ell)} \not\in K$. Then $\ell \equiv 3 \mod 4$ and

$$7 \leq \ell \leq 6d+1.$$ 

Remark

This theorem implies the result obtained by Sutherland in the case $K = \mathbb{Q}$.

This theorem is proved studying the Galois representation $\rho_{E,\ell}$. 
Let us assume that $\sqrt{\left(\frac{-1}{\ell}\right)} \ell \in K$. 

Let us assume that \( \sqrt{\left( \frac{-1}{\ell} \right)} \ell \in K \).

**Lemma (A.)**

Let \( G \) be a subgroup of \( \text{GL}_2(\mathbb{F}_\ell) \) whose image \( H \) in \( \text{PGL}_2(\mathbb{F}_\ell) \) is contained in \( \text{SL}_2(\mathbb{F}_\ell)/\{\pm 1\} \). Suppose \( |\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0 \) for all \( g \in G \) but \( |\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0 \). Then \( \ell \equiv 1 \mod 4 \) and one of the followings holds:

1. \( H \) is dihedral of order \( 2n \), where \( n \in \mathbb{Z}_{>1} \) is a divisor of \( \ell-1 \);
2. \( H \) is isomorphic to one of the following exceptional groups: \( A_4 \), \( S_4 \) or \( A_5 \).
Proposition (A.)

Let $E$ be an elliptic curve defined over a number field $K$ of degree $d$ over $\mathbb{Q}$ and let $\ell$ be a prime number. Let us suppose $\sqrt{\left(\frac{-1}{\ell}\right)} \ell \in K$. Suppose $E/K$ admits an $\ell$-isogeny locally at a set of primes with density one. Then:

1. if $\ell \equiv 3 \mod 4$ the elliptic curve $E$ admits a global $\ell$-isogeny over $K$;
2. if $\ell \equiv 1 \mod 4$ the elliptic curve $E$ admits an $\ell$-isogeny over $L$, finite extension of $K$, which can ramify only at primes dividing the conductor of $E$ and $\ell$.

Moreover, if $\ell \equiv -1 \mod 3$ or if $\ell \geq 60d+1$, then $E$ admits an $\ell$-isogeny over a quadratic extension $L$ of $K$. 
Proposition (A.)

Let \((\ell, j(E))\) be an exceptional pair for the number field \(K\) of degree \(d\) over \(\mathbb{Q}\) and discriminant \(\Delta\). Then

\[ \ell \leq \max \{ \Delta, 6d+1 \}. \]
**Question**

Let $K$ be a number field and let $\ell$ be a prime number, how many exceptional pairs $\langle \ell, j(E) \rangle$ do exist over $K$?
Proposition (A.)

Given a number field $K$:
**Proposition (A.)**

Given a number field $K$:

- if $\ell = 2, 3$ then there exists no exceptional pair;
Given a number field $K$:

- if $\ell = 2, 3$ then there exists no exceptional pair;
- there exist infinitely many exceptional pairs $(5,j(E))$ for the number field $K$ if and only if $\sqrt{5}$ belongs to $K;$
Proposition (A.)

Given a number field $K$:

- if $\ell = 2, 3$ then there exists no exceptional pair;
- there exist infinitely many exceptional pairs $(5, j(E))$ for the number field $K$ if and only if $\sqrt{5}$ belongs to $K$;
- if $\ell > 7$, then the number of exceptional pairs $(\ell, j(E))$ is finite.
Sketch of the Proof
Sketch of the Proof

- If $\ell = 2, 3$ then the result follows from the previous combinatorics.
Sketch of the Proof

- If $\ell = 2, 3$ then the result follows from the previous combinatorics.
- For $\ell \geq 5$ the result follows from counting rational points on modular curves.
Sketch of the Proof

- If $\ell = 2, 3$ then the result follows from the previous combinatorics.
- For $\ell \geq 5$ the result follows from counting rational points on modular curves.
Modular curves

Let $\ell \geq 5$ be a prime. The **modular curve** $X(\ell)$ is the compactified fine moduli space which classify, up to isomorphism, pairs $(E, \alpha)$, where $E$ is a generalized elliptic curve over a scheme $S$ over $\text{Spec}(\mathbb{Z}[1/\ell, \zeta_\ell])$ and $\alpha : (\mathbb{Z}/\ell\mathbb{Z})_S^2 \xrightarrow{\sim} E[\ell]$ is an isomorphism of group schemes over $S$ which is a full level $\ell$-structure.

A full level $\ell$-structure on a generalized elliptic curve $E$ over $S$ is a pair of points $(P_1, P_2)$, satisfying $P_1, P_2 \in E[\ell]$ and $e_\ell(P_1, P_2) = \zeta_\ell$ where $e_\ell$ is the Weil pairing on $E[\ell]$. 
In the case $\ell = 5$ the modular curve considered is

$$X_{V_4}(5) := G \backslash X(5),$$

where $G \subset GL_2(\mathbb{Z}/\ell\mathbb{Z})$ is the inverse image of $V_4 \subset PGL_2(\mathbb{Z}/\ell\mathbb{Z})$. 
In the case $\ell = 5$ the modular curve considered is

$$X_{V_4}(5) := G \backslash X(5),$$

where $G \subset GL_2(\mathbb{Z}/\ell\mathbb{Z})$ is the inverse image of $V_4 \subset PGL_2(\mathbb{Z}/\ell\mathbb{Z})$.

**Proposition**

Over $\text{Spec}(\mathbb{Q}(\sqrt{5}))$ the modular curve $X_{V_4}(5)$ is isomorphic to $\mathbb{P}^1$. 
For $\ell > 7$ the result follows applying Faltings’ Theorem.

In this case, an exceptional pair essentially (we are not considering exceptional subgroups) corresponds to a rational point of

$$X_{\text{split}}(\ell) := G \backslash X(\ell),$$

where $G$ is the normalizer of a split Cartan subgroup of $GL_2(\mathbb{F}_\ell)$. The curve $X_{\text{split}}(\ell)$ parametrizes elliptic curves endowed with a pair of independent cyclic $\ell$-isogenies.
The local-global principle for 7-isogenies leads us to a dichotomy between a finite and an infinite number of counterexamples according to the rank of a specific elliptic curve that we call the Elkies-Sutherland curve:

\[
y^2 = x^3 - 1715x + 33614
\]
The local-global principle for 7-isogenies leads us to a dichotomy between a finite and an infinite number of counterexamples according to the rank of a specific elliptic curve that we call the Elkies-Sutherland curve:

**Proposition (A.)**

If $\ell = 7$ then the number of exceptional pairs $(7, j(E))$ for a number field $K$, is finite or infinite, depending on the rank of the elliptic curve

$$E' : y^2 = x^3 - 1715x + 33614$$

being respectively $0$ or positive.
Examples for 7-isogenies:

For \( \mathbb{Q}(\sqrt{-23}) \) and \( \mathbb{Q}(i) \) there are \textbf{infinitely many} counterexamples to the local-global principle about 7-isogenies.

For any field in the following table there are \textbf{finitely many} counterexamples to the local-global principle about 7-isogenies:

\[
\begin{array}{ccc}
\mathbb{Q}(\sqrt{-14}) & \mathbb{Q}(\sqrt{-119}) & \mathbb{Q}(\sqrt{-210}) \\
\mathbb{Q}(\sqrt{-21}) & \mathbb{Q}(\sqrt{-133}) & \mathbb{Q}(\sqrt{-217}) \\
\mathbb{Q}(\sqrt{-35}) & \mathbb{Q}(\sqrt{-154}) & \mathbb{Q}(\sqrt{-231}) \\
\mathbb{Q}(\sqrt{-42}) & \mathbb{Q}(\sqrt{-161}) & \mathbb{Q}(\sqrt{-238}) \\
\mathbb{Q}(\sqrt{-91}) & \mathbb{Q}(\sqrt{-182}) & \mathbb{Q}(\sqrt{-259}) \\
\mathbb{Q}(\sqrt{-105}) & \mathbb{Q}(\sqrt{-203}) & \mathbb{Q}(\sqrt{-287})
\end{array}
\]
Further Directions

- Generalization for simple abelian varieties of dimension $d$ over $\mathbb{Q}$ which are principally polarized i.e. study of the subgroups of $\mathbb{P} \text{GSp}_{2d}(\mathbb{F}_\ell)$...
- Generalization for abelian varieties of GL$_2$-type;
- Generalization for isogenies of prime power degree;
- Generalization for isogenies of degree given by products of primes;
- ...
“Think Globally, Act Locally”
Patrick Geddes

Thanks!

Samuele Anni