Local-Global Principle of Elliptic Curves

Angelos Koutsianas

Department of Mathematics
Aristotle University of Thessaloniki

Department of Mathematics
Xavier University of Louisiana
29 October, 2024

joint with
Stevan Gajović and Jeroen Hanselman

Local-Global Principle

"Description": Let V be a system of Diophantine equations with coefficients over a number field K. The system V has a solution over K if and only if it has a solution modulo $\mathfrak{p}$ for all primes (finite and infinite).

Example

Question: Find the integer solutions of the equation $y^2 = 3x^3 + 2$?

Local-Global Principle

"Description": Let V be a system of Diophantine equations with coefficients over a number field K. The system V has a solution over K if and only if it has a solution modulo $\mathfrak{p}$ for all primes (finite and infinite).

Example

Question: Find the integer solutions of the equation $y^2 = 3x^3 + 2$?

Solution: It is enough to consider the equation modulo 3.

Local-Global Principle

Example (Legendre)

The quadratic form $ax^2 + by^2 + cz^2 = 0$ has an integer solution if and only if the system

$$\begin{aligned} u^2 &\equiv -bc \pmod{|a|} \\ v^2 &\equiv -ac \pmod{|b|} \\ w^2 &\equiv -ab \pmod{|c|}. \end{aligned}$$

Local-Global Principle

Example (Legendre)

The quadratic form $ax^2 + by^2 + cz^2 = 0$ has an integer solution if and only if the system

$$\begin{aligned} u^2 &\equiv -bc \pmod{|a|} \\ v^2 &\equiv -ac \pmod{|b|} \\ w^2 &\equiv -ab \pmod{|c|}. \end{aligned}$$

Example (Selmer)

The equation

$$3x^3 + 4y^3 + 5z^3 = 0$$

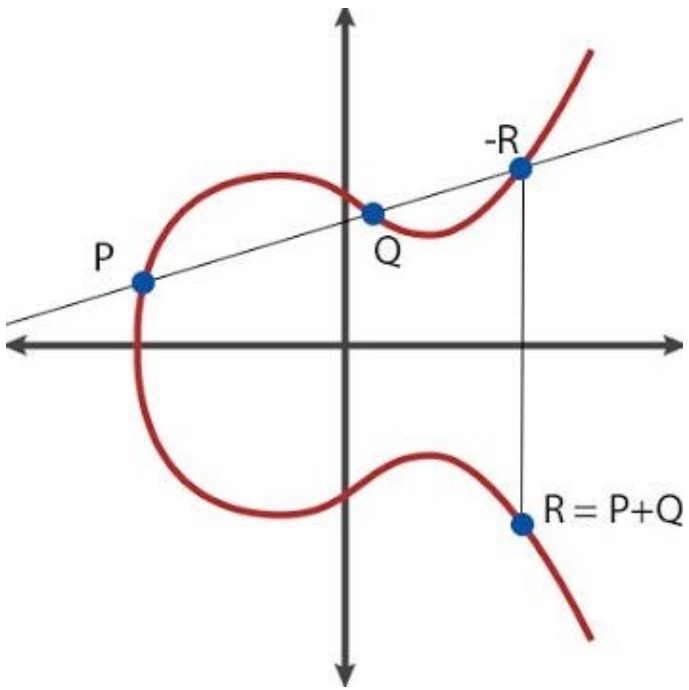
has a solution over $\mathbb{R}$ and modulo p for all primes but it does **not** have an integer solution.

Elliptic Curves

Let K be a field. Then an elliptic curve E/K is a non-singular curve of the form

$$E: \ y^2 = x^3 + Ax + B, \quad A, B \in K.$$

We can give a group structure on E.



Elliptic Curves Isogeny

Let $E,\ E'$ two elliptic curves over K. A homomorphisms $\phi:\ E \to E'$ with $\ker(\phi) < \infty$ is called an **isogeny**.

Definition

We say that E **admits a K-rational ℓ-isogeny** if there exists ϕ as above such that $\#\ker(\phi) = \ell$ and $\ker(\phi)$ is stable under the action of G_K.

Suppose K is a number field and E/K. It is easy to show that when E admits a K-rational ℓ-isogeny then $\tilde{E}/\mathbb{F}_{\mathfrak{p}}$ also admits an $\mathbb{F}_{\mathfrak{p}}$-rational ℓ-isogeny for almost all primes $\mathfrak{p}$ in K, where $\tilde{E}/\mathbb{F}_{\mathfrak{p}}$ is the reduction curve of E at $\mathfrak{p}$.

Local-Global Isogeny Property

Question

When $\tilde{E}/\mathbb{F}_{\mathfrak{p}}$ admits an $\mathbb{F}_{\mathfrak{p}}$-rational ℓ-isogeny for almost all primes $\mathfrak{p}$ in K, does E admit a K-rational ℓ-isogeny?

Local-Global Isogeny Property

In 2012, Sutherland shows that the answer is usually "yes", but there are pairs $(E/K, \ell)$ for which that answer is "no". In particular, the answer depends only on the j-invariant of E and the prime ℓ.

Definition

A pair (j_0, ℓ) with $j_0 \in K$ is called *exceptional for* K is there exists E/K with $j(E) = j_0$ and the answer to the above question is "no". Such a prime ℓ is called an *exceptional prime for* K.

Let ℓ an integer prime with $(\ell, \mathrm{char}(K)) = 1$. We denote by $E[\ell]$ the points of E with order ℓ. We can show that

$$E[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2 .$$

For $\sigma \in G_K$, the absolute Galois group of K, and $P \in E[\ell]$ it holds that $P^\sigma \in E[\ell]$. Therefore, we get a representation

$$\bar{\rho}_{E,\ell} : \ G_K \to \mathrm{GL}_2(\mathbb{F}_\ell),$$

which is the action of G_K on $E[\ell]$.

Conditions on Exceptional Primes

We can give necessary conditions on exceptional primes. Let $\ell^* = \left(\frac{-1}{\ell}\right)\ell$. Let $G_{E,\ell} = \bar{\rho}_{E,\ell}(G_K)$ and $H_{E,\ell} = \mathbb{P}(G_{E,\ell})$.

Theorem (Sutherland, 2012)

Let K with $\sqrt{\ell^*} \notin K$. If (j_0, ℓ) is exceptional pair for K, then for the elliptic curve E/K with $j(E) = j_0$ holds:

1. *Then $H_{E,\ell} \simeq D_{2n}$, where $n > 1$ is an odd divisor of $(\ell - 1)/2$,*
2. *$\ell \equiv 3 \pmod 4$,*
3. *The group $G_{E,\ell}$ is contained in the normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$,*
4. *E obtains a rational ℓ-isogeny over $K(\sqrt{\ell^*})$.*

Conditions on Exceptional Primes

Theorem (Banwait-Cremona, 2014)

Let K with $\sqrt{\ell^*} \in K$. If (j_0, ℓ) is exceptional pair for K, then for the elliptic curve E/K with $j(E) = j_0$ holds:

1. $H_{E,\ell} \simeq A_4$ *and* $\ell \equiv 1 \pmod{12}$,
2. $H_{E,\ell} \simeq S_4$ *and* $\ell \equiv 1 \pmod{24}$,
3. $H_{E,\ell} \simeq A_5$ *and* $\ell \equiv 1 \pmod{60}$,
4. $H_{E,\ell} \simeq D_{2n}$ *and* $\ell \equiv 1 \pmod{4}$, *where* $n > 1$ *is a divisor of* $(\ell - 1)/2$, *and* $G_{E,\ell}$ *lies in a normaliser of a split Cartan subgroup of* $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Exceptional Primes over $\mathbb{Q}$

Using the above theorem Sutherland proves that the only exceptional pair when $K = \mathbb{Q}$ is $(\frac{2268945}{128}, 7)$. In particular, the elliptic curve

$$y^2 = x^3 - 138915x - 18932130,$$

admits a 7-isogeny at every prime p of good reduction (and over $\mathbb{R}$) but it does not admit a 7-isogeny over $\mathbb{Q}$.

Exceptional Primes over Number Fields

We can search for exceptional primes in the following directions:

1. Either we fix K and try to find all exceptional primes ℓ for K, or
2. we fix ℓ and search if ℓ is exceptional in a "suitable" (infinite) family of number fields K.

Exceptional Primes over Number Fields

Theorem (Anni, 2014)

Let K a number field of degree d and discriminant Δ. Let $\ell_K := \max\{|\Delta|, 6d+1\}$. Then, if (j_0, ℓ) is an exceptional pair for K then it holds

1. $\ell \leq \ell_K$,
2. *There are finitely many exceptional pairs (j_0, ℓ) with $7 < \ell \leq \ell_K$.*

Conjecture (Banwait-Cremona, 2014)

11 is not an exceptional prime for any quadratic field.

Exceptional Primes over Number Fields

Theorem (Anni, 2014)

Let K a number field of degree d and discriminant Δ. Let $\ell_K := \max\{|\Delta|, 6d+1\}$. Then, if (j_0, ℓ) is an exceptional pair for K then it holds

1. $\ell \leq \ell_K$,
2. *There are finitely many exceptional pairs (j_0, ℓ) with $7 < \ell \leq \ell_K$.*

Conjecture (Banwait-Cremona, 2014)

11 *is not an exceptional prime for any quadratic field.*

Answer: It is enough to determine the quadratic points of the modular curves $X_{D_{10}}$.

Modular Curves

Let $G \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ with $\det(G) = \mathbb{F}_\ell^*$ and

$$\pi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{F}_\ell), \tag{1}$$

the natural projection. We denote by $\Gamma := \pi^{-1}(G \cap \mathrm{SL}_2(\mathbb{F}_\ell))$. We define the compact Riemann surface

$$X_G := (\mathbb{H} \cup \{i\infty\} \cup \mathbb{Q})/\Gamma,$$

where $\mathbb{H}$ is the Poincare upper half plane where the action of Γ is given by Möbius transformations. Then, X_G is a curve defined over $\mathbb{Q}$.

Moduli Interpretation

Becaus $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ the natural map $j : X_G \to X(1) \simeq \mathbb{P}^1$ is called the *j-map*. The curve X_G has the following moduli interpretation.

Moduli Interpretation

Every point $P \in X_G(K)$ corresponds to an elliptic curve E/K such that $j(P) = j(E)$ and $G_{E,\ell} \subset G$ and vice versa.

Why Quadratic Points on $X_{D_{10}}$?

Let $\ell = 11$ and K a quadratic field. By Sutherland's theorem we know that the exceptional pairs $(j_0, 11)$ correspond to curves E/K such that $H_{E,11} \simeq D_{10} \subset \mathrm{PGL}_2(\mathbb{F}_{11})$. Let G be the pullback of D_{10} in $\mathrm{GL}_2(\mathbb{F}_{11})$ and $X_{D_{10}} := X_G$.

Hence it is enough to compute the quadratic points of $X_{D_{10}}$.

Question

How do we compute the quadratic points on $X_{D_{10}}$?

Why Quadratic Points on $X_{D_{10}}$?

Let $\ell = 11$ and K a quadratic field. By Sutherland's theorem we know that the exceptional pairs $(j_0, 11)$ correspond to curves E/K such that $H_{E,11} \simeq D_{10} \subset \mathrm{PGL}_2(\mathbb{F}_{11})$. Let G be the pullback of D_{10} in $\mathrm{GL}_2(\mathbb{F}_{11})$ and $X_{D_{10}} := X_G$.

Hence it is enough to compute the quadratic points of $X_{D_{10}}$.

Question

How do we compute the quadratic points on $X_{D_{10}}$?

Answer: With the (symmetric) Chabauty method!

p-adic Numbers

Let p a prime. Then any $x \in \mathbb{Q}$ is written in the form $x = p^n \frac{a}{b}$ with $(ab, p) = 1$ and $n \in \mathbb{Z}$. We define the p-adic metric

$$|x| = p^{-n}.$$

The completion of $\mathbb{Q}$ with respect to the p-adic metric is called *the field of p-adic numbers* $\mathbb{Q}_p$. An element $x \in \mathbb{Q}_p$ is of the form

$$x = \sum_{i=-n_0}^{\infty} a_i p^i, \quad a_i \in \{0, \cdots, p-1\}, \ n_0 \in \mathbb{Z}.$$

We can do *p-adic analysis* in $\mathbb{Q}_p$.

p-adic Integration

Suppose X a smooth curve over $\mathbb{Q}$ of genus g and J its Jacobian. Let p be a prime of good reduction for X and $\tilde{X}$ the reduction of X modulo p. We also assume there exists $P_0 \in X(\mathbb{Q})$.

If $\Omega_{J_{\mathbb{Q}_p}}$ is the $\mathbb{Q}_p$-space of global 1-forms of J which has *dimension* g. Then due to Coleman there exists a pairing

$$\Omega_{J_{\mathbb{Q}_p}} \times J(\mathbb{Q}_p) \to \mathbb{Q}_p, \quad (\omega, D) \mapsto \int_0^D \omega,$$

which is bilinear and nondegenarate.

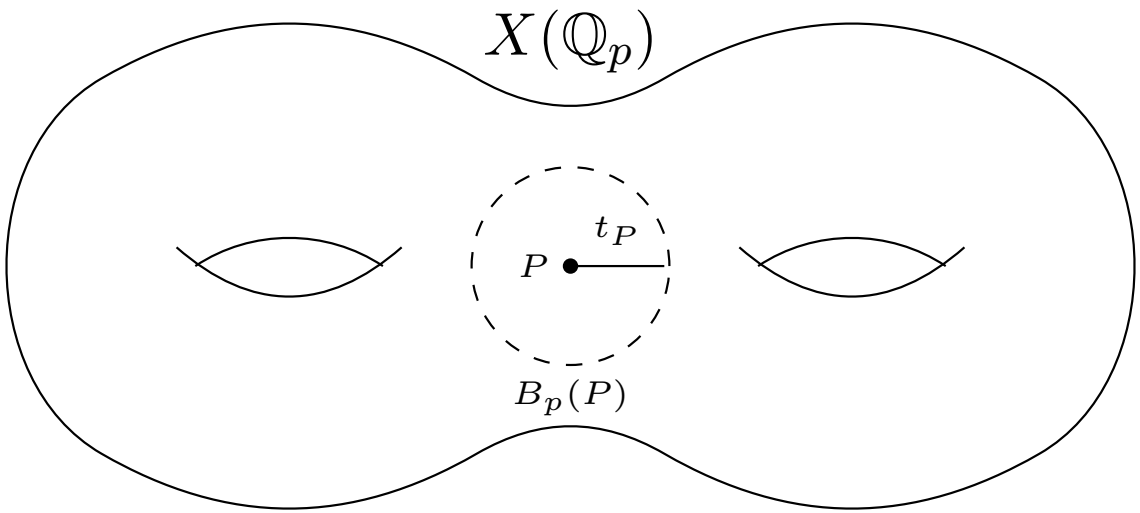
Residue Class

Let $P \in X(\mathbb{Q}_p)$ and $\tilde{P} \in \tilde{X}(\mathbb{F}_p)$ the reduction of P. The *residue class of* P is

$$B_p(P) := \{Q \in X(\mathbb{Q}_p) : \ \tilde{Q} = \tilde{P}\}.$$

Let t_P is a rational function on X that reduces to a uniformizer on $\tilde{X}$ at $\tilde{P}$. It holds

- t_P is a uniformizer at P and $\tilde{t}_{\tilde{P}}$ is a uniformizer at $\tilde{P}$.
- t_P defines a bijection $B_p(P) \to p\mathbb{Z}_p$ and $Q \mapsto t_P(Q)$. Moreover, $t_P(Q) = 0$ if and only if $P = Q$.



Integration on a Residue Class

Proposition

Let X, p, P, t_P as above and $\omega \in \Omega_{J_{\mathbb{Q}_p}}$. There exists a power series

$$\phi(x) = a_1 x + a_2 x^2 + a_3 x^3 + \cdots \in \mathbb{Q}_p[[x]],$$

such that

$$\int_0^{[Q-P]} \omega = \phi(z),$$

for all $Q \in B_p(P)$ and $z = t_P(Q)$.

Chabauty's Idea

Let $\text{rank}(J(\mathbb{Q})) = r$ with $r < g$ (*Chabauty condition*). Suppose $S \subset X(\mathbb{Q})$ a set of known points.

Goal

Prove that $S = X(\mathbb{Q})$.

Chabauty's Idea

Let $\text{rank}(J(\mathbb{Q})) = r$ with $r < g$ (*Chabauty condition*). Suppose $S \subset X(\mathbb{Q})$ a set of known points.

Goal

Prove that $S = X(\mathbb{Q})$.

Let $P \in S$ and $Q \in X(\mathbb{Q}) \cap B_p(P)$. Because $r < g$ there exists non-zero $\omega \in \Omega_{J_{\mathbb{Q}_p}}$ such that annihilates $J(\mathbb{Q})$. In other words, there exists ω such that

$$\phi(z) = \int_0^{[Q-P]} \omega = 0.$$

Hence, the only we have to do is to determine the zeros of $\phi(z)$.

Chabauty's Idea in Practice

In practice we prove that $X(\mathbb{Q}) \cap B_p(P) = \{P\}$ for every $P \in S$ and every $p \in T$ where T is a suitable finite set of primes.

Therefore it is enough to show that $X(\mathbb{Q}) \cap B_p(P) = \emptyset$ for all $P \in X(\mathbb{Q}_p) \setminus S$ and $p \in T$.

Chabauty's Idea in Practice

In practice we prove that $X(\mathbb{Q}) \cap B_p(P) = \{P\}$ for every $P \in S$ and every $p \in T$ where T is a suitable finite set of primes.

Therefore it is enough to show that $X(\mathbb{Q}) \cap B_p(P) = \emptyset$ for all $P \in X(\mathbb{Q}_p) \setminus S$ and $p \in T$.

But how?

Mordell-Weil Sieve

We can do it using the *Mordell-Weil Sieve*. The idea of the sieve is based on the following commutative diagram.

$$\begin{array}{ccc} X(\mathbb{Q}) & \xrightarrow{\pi} & J(\mathbb{Q}) \\ \downarrow{\scriptstyle red} & & \downarrow{\scriptstyle red} \\ \tilde{X}(\mathbb{F}_p) & \xrightarrow{\pi} & \tilde{J}(\mathbb{F}_p) \end{array}$$

We get $\pi(X(\mathbb{Q})) \subset W_p + L_p$ where W_p is a set of coset representatives of $\mathrm{red}^{-1}(\pi(\tilde{X}(\mathbb{F}_p)))$ and $L_p := \ker\Big(J(\mathbb{Q}) \to \tilde{J}(\mathbb{F}_p)\Big)$.

Let

$$W_T + L_T = \bigcap_{p \in T} (W_p + L_p),$$

where $L_T = \bigcap_{p \in T} L_p$ and W_T a finite subset of $J(\mathbb{Q})$. Obviously, $\pi(X(\mathbb{Q})) \in W_T + L_T$. If T is chosen carefully such that

$$\pi(S) + L_T = W_T + L_T \supset \pi(X(\mathbb{Q})),$$

$$L_T \subset \ker \left(J(\mathbb{Q}) \to \prod_{p \in T} \tilde{J}(\mathbb{F}_p) \right),$$

then we get $S = X(\mathbb{Q})$.

Symmetric Chabauty

Let $P \in X(K)$ where K is a quadratic field and $\bar{P} = P^\sigma$ where σ is a generator of $\mathrm{Gal}(K/\mathbb{Q})$.

Let $X^{(2)}$ the 2-nd symmetric power of X. The elements of $X^{(2)}(\mathbb{Q})$ corresponds to effective $\mathbb{Q}$-rational divisors on X of degree 2. In particular, $\{P, \bar{P}\}$ corresponds to an element of $X^{(2)}(\mathbb{Q})$ and vice versa.

Using the map $X^{(2)} \to J$, $\{P, \bar{P}\} \mapsto [P + \bar{P} - 2P_0]$ we can apply the Chabauty method at $X^{(2)}$ under the assumption that $r < g - 2$ due to the work of Siksek.

The Modular Curve $X_{D_{10}}$

The modular curve $X_{D_{10}}$ has genus 6. By the work of Galbraith, Box and Assaf we can compute a non-singular model which is given by

$$
\begin{aligned}
&uw - 2vw + 2ux - 6vx + 2uy + 2vy + uz = 0,\\
&uw + vw + 2ux - 2vx + 2uy - 10vy - 5uz + 11vz = 0,\\
&-6u^2 + 6uv - 3v^2 + 11w^2 - 66wx + 11x^2 + 88wy - 110xy + 99y^2 + 44wz - 110xz = 0,\\
&6u^2 + 12uv + 12v^2 + 187wx + 22x^2 + 55wy - 44xy - 154y^2 + 66wz + 77xz + 121yz = 0,\\
&-9v^2 + 88w^2 - 11wx - 99x^2 - 77wy + 110xy - 11y^2 + 77wz - 297xz + 121yz = 0,\\
&-6u^2 - 12uv - 12v^2 + 33w^2 - 77wx + 66x^2 - 121wy - 132xy - 110y^2\\
&-44wz - 187xz + 121yz + 121z^2 = 0
\end{aligned}
$$

It holds that $\operatorname{rank}(J_{X_{D_{10}}}(\mathbb{Q})) = 1$.

The Modular Curve $X_{D_{10}}$

The curve $X_{D_{10}}$ is a degree 2 cover of the curve

$$C: \ y^2 + (x^3 + x^2 + x + 1)y = -2x^5 + 2x^4 - 3x^3 + 2x^2 - 2x,$$

under a map $\phi_{X_{D_{10}}} : X_{D_{10}} \to C$ that we can explicitly compute.

Note: It also holds $\text{rank}(J_C(\mathbb{Q})) = 1$. Moreover, $C \simeq X_0^+(121)$.

Proposition

We can prove that $C(\mathbb{Q}) = \{(1, -3), (1, -1), (0, -1), (0, 0), \pm\infty\}$.

Quadratic Points on $X_{D_{10}}$

In particular, the set

$$\begin{aligned} S = \{&(-3/4, 1/4, 0, \pm\frac{\sqrt{77}}{2}, 0, 1),\ (3/4, -5/4, 0, \pm\frac{\sqrt{77}}{2}, 0, 1) \\ &(1, 1, 1, \pm\sqrt{-11}, \pm\sqrt{-11}, 1),\ (-2/5, 2/5, 1/5, \pm\frac{\sqrt{209}}{5}, \mp\frac{\sqrt{209}}{5}, 1), \\ &(-1, 7, 5, \pm\sqrt{473}, \mp\sqrt{473}, 1), (-1/3, 0, -1/3, \pm\frac{\sqrt{22}}{3}, \pm\frac{\sqrt{22}}{3}, 1)\}, \end{aligned}$$

are quadratic points on $X_{D_{10}}$, all are pullbacks of $C(\mathbb{Q})$ under $\phi_{X_{D_{10}}}$.

Chabauty Method on $X^{(2)}_{D_{10}}$

We apply symmetric Chabauty for $p = 5, 7, 13, 17$ and we prove that the elements in S are the only elements in there residue classes modulo p of $X^{(2)}_{D_{10}}(\mathbb{Q}_p)$.

With the Mordell-Weil sieve we prove that S corresponds to the complete set of points on $X^{(2)}_{D_{10}}(\mathbb{Q})$.

The image of the points in S under the j-map is

$$J = [\infty, -3375, 8000, -884736, 16581375, -884736000].$$

The above values do not correspond to exceptional pairs over any quadratic field $K/\mathbb{Q}$.

Main Theorem

From the above we have given a positive answer in the conjecture of Banwait-Cremona.

Theorem (Gajović-Hanselman-K.)

11 *is not an exceptional prime for any quadratic field.*

Future Work

- Prove that 11 is not an exceptional prime for all cubic and quintic number fields.
- Consider exceptional pairs over cubic fields. The only possible primes primes are $\ell = 11$ and 19. We have to determine the cubic points on $X_{D_{10}}$ and $X_0^+(19^2)$. It holds that $g(X_0^+(19^2)) = 9$ and the rank of the Jacobian is 8 (big!).
- Compute quadratic and cubic points on the modular curves in the LMFDB database.

Thank you for your attention!!!