An inverse problem for isogeny volcanoes

LFANT Seminar

Henry Bambury

DGA, DIENS, Équipe Inria CASCADE

11th of April 2023

Disclaimer

- Joint work with Francesco Campagna [1] and Fabien Pazuki [2]
- Talk based on https://arxiv.org/abs/2210.01086
- I am now a PhD student in lattice-based crypto

[1] Leibniz Universität Hannover
[2] Københavns Universitet

Outline of the talk

- Introduction to isogeny graphs in the *easiest* setting
- The connected components: Volcano exploration
- Solving the inverse problem

Isogeny graphs: (brief) history and applications

Original work

- David Kohel's PhD thesis (1996)

A computational tool

- Computing endomorphism rings
- Computing modular/Hilbert class polynomials
- Point counting

In cryptography

- First proposal by Couveignes (1997)
- Post-Quantum attempts: SIDH, CSIDH, etc

Defining vertices: j-invariants

j-invariants

Let $E/\mathbb{F}_p : y^2 = x^3 + ax + b$ be an elliptic curve, the j-invariant of E is

$$j(E) = j(a, b) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

- p possible j-invariants, all are reached.
- Encompass classes of $\overline{\mathbb{F}}_p$-isomorphisms $(x, y) \mapsto (u^2 x, u^3 y)$.
- $j = 0$ and $j = 1728$ (in $\mathbb{F}_p$) are special.

Defining edges: isogenies

Isogenies

An isogeny is a non-constant homomorphism $\varphi : E \to E'$.
It is surjective and has finite kernel $C = \ker\varphi$.
The degree of φ is $\deg\varphi = \#C$.

- An isogeny φ is defined over $\mathbb{F}_p$ if $\ker\varphi$ is stable by Galois action.
- In this talk, isogenies are equivalent up to their kernel.
- Small degree isogenies are easy to compute.

Ordinary vs supersingular

Endomorphism ring

Let $E/\mathbb{F}_p$ be an elliptic curve, and k a field. Then the endomorphism ring $\mathrm{End}_k(E)$ is the ring of all k-rational isogenies from E to itself.

- When $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ is an order in an imaginary quadratic field, E and $j(E)$ are called ordinary .
- The rest is supersingular.
- Over $\mathbb{F}_p$, we have $O(\sqrt{p})$ supersingular j-invariants.
- Every $\overline{\mathbb{F}}_p$-isogeny between ordinary curves with $j \neq 0, 1728$ has an equivalent $\mathbb{F}_p$-isogeny .

Quick reminder: imaginary quadratic orders

Orders are subrings of the ring of integers.

Maximal order

In $K = \mathbb{Q}(\sqrt{-D})$,
$\mathcal{O}_K = \mathbb{Z}[\sqrt{-D}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{-D}}{2}\right]$.

Quadratic orders

Orders in $K = \mathbb{Q}(\sqrt{-D})$ are of the form $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ with $f \in \mathbb{Z}_{>0}$ (think lattices).

- We have a correspondence between negative integers $\equiv 0, 1 \mod 4$ and orders.
- $f = [\mathcal{O}_K : \mathcal{O}]$ is called the conductor of $\mathcal{O}$.
- $\mathrm{Disc}(\mathcal{O}) = f^2 \, \mathrm{Disc}(\mathcal{O}_K)$.
- We define $\mathrm{Cl}(\mathcal{O})$ as usual.
- Class number notation: $h(\mathcal{O}) = \# \, \mathrm{Cl}(\mathcal{O})$.

So what is the isogeny graph??

- $p > 3$ is a *large* prime.
- $\ell \neq p$ is a *small* prime.

Isogeny graph

The ordinary ℓ-isogeny graph $\mathcal{G}_\ell(\mathbb{F}_p)$ has set of vertices all ordinary j-invariants in $\mathbb{F}_p$ and edges all $\mathbb{F}_p$-rational ℓ-isogenies.

- Up to isomorphism of curves, up to equivalence of isogeny.
- $\mathcal{G}_\ell(\mathbb{F}_p)$ can be seen as undirected outside of $j = 0, 1728$.
- Possible self-loops, double edges and double self-loops.
- Roots of $\Phi_\ell(X, Y)$ with multiplicity.

Pictures!

Structure: Frobenius, trace and cordilleras

Structure: Frobenius, trace and cordilleras

The Frobenius equation

Let π be the Frobenius endomorphism associated to $E/\mathbb{F}_p$ where $j(E) \neq 0, 1728$ and $K = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then

$$4p - t^2 = -f^2 \,\mathrm{Disc}(\mathcal{O}_K)$$

where $t = \mathrm{Tr}(\pi)$ and $f = [\mathcal{O}_K : \mathbb{Z}[\pi]]$.

- $j(E) \neq 0, 1728$ means $\mathrm{Disc}(K) < -4$ and $\#\,\mathrm{Aut}(E) = 2$: the equation in red has at most one solution $(t, f) \in \mathbb{N}^2$.
- In fact $t = p + 1 - \#E$: we have $|t| \leq \lfloor 2\sqrt{p} \rfloor$.
- Isogenies preserve $\#E$.
- Same Frobenius $\iff$ same $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ $\iff$ same trace up to sign $\iff$ isogenous up to equivalence.

Structure: Frobenius, trace and cordilleras

Cordillera

The *t-cordillera*[a] of $\mathcal{G}_\ell(\mathbb{F}_p)$ is the subgraph induced by the following set of vertices:

$$\mathcal{V}_t = \{j(E) : E/\mathbb{F}_p \text{ and } p + 1 - \#E(\mathbb{F}_p) = \pm t\}.$$

[a] Terminology credit: Miret, Sadornil, Tena, Tomàs and Valls (2007)

- 1 positive $t \iff$ 1 imaginary quadratic field (*).
- All $\mathcal{O} = \mathrm{End}_{\mathbb{F}_p}(E)$ for $E/\mathbb{F}_p$ such that $j(E) \in \mathcal{V}_t$ satisfy

$$\mathbb{Z}[\pi_t] \subseteq \mathcal{O} \subseteq \mathcal{O}_K.$$

- All *ordinary* traces live in $[\![1, \lfloor 2\sqrt{p} \rfloor]\!]$.
- There can be no edges between cordilleras (*).
- Over $\mathbb{F}_p$, no cordillera is empty (Waterhouse 1969).

Structure: Horizontal vs Vertical isogenies

Lemma

Let $\varphi : E_1 \to E_2$ be an ℓ-isogeny. Then

$$[\mathcal{O}_1 : \mathcal{O}_2] = \frac{1}{\ell}, 1, \text{ or } \ell.$$

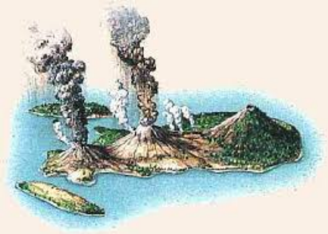
- φ increases $\mathcal{O}$: vertical ascending.
- φ decreases $\mathcal{O}$: vertical descending.
- φ leaves $\mathcal{O}$ unchanged: horizontal.

$$\mathbb{Z}[\pi] \subseteq \mathbb{Z} + m\ell^d \mathcal{O}_K \subset \mathbb{Z} + m\ell^{d-1}\mathcal{O}_K \subset \ldots \subset \mathbb{Z} + m\mathcal{O}_K \subseteq \mathcal{O}_K$$

Structure: Volcano Belts

Belts

We partition cordilleras into belts: subgraphs in which all orders have conductors of the form $m\ell^k$, where m is coprime to ℓ.



$$\mathbb{Z}[\pi] \subseteq \mathbb{Z} + m\ell^d \mathcal{O}_K \subset \mathbb{Z} + m\ell^{d-1}\mathcal{O}_K \subset \ldots \subset \mathbb{Z} + m\mathcal{O}_K \subseteq \mathcal{O}_K$$

In a given cordillera,

$$\{\text{belts}\} \longleftrightarrow \{\text{divisors of the conductor of } \mathbb{Z}[\pi] \text{ coprime to } \ell\}$$

Structure: Levels and ascending isogenies

Levels

A vertex of $\mathcal{G}_\ell(\mathbb{F}_p)$ with order $\mathbb{Z} + m\ell^k\mathcal{O}_K$ lies at level k if $(\ell, m) = 1$. If $\mathbb{Z}[\pi] = \mathbb{Z} + f\mathcal{O}_K$ then $d = v_\ell(f)$ is called the depth.

An ℓ-cordillera and its belts have a unique depth (*).

Lemma

Let $E/\mathbb{F}_p$ with $\mathrm{End}(E) = \mathbb{Z} + v\mathcal{O}_K$, where $\ell | v$. Then there exists a vertical ascending ℓ-isogeny from $j(E)$.

Structure: How many curves at a given level?

Lemma

Let $\mathcal{O}$ be an order of discriminant D in $K = \mathbb{Q}(\sqrt{t^2 - 4p})$ where $|t| \in [\![1, \lfloor 2\sqrt{p} \rfloor]\!]$. If $\mathbb{Z}[\pi] \subset \mathcal{O}$ Then the set $\mathrm{Ell}_{F_p}(\mathcal{O})$ of j-invariants with endomorphism ring $\mathcal{O}$ has cardinality $h(\mathcal{O}) = \# \mathrm{Cl}(\mathcal{O})$.

- These can be seen as roots mod p of the Hilbert class polynomial $H_D(X)$.
- Summing over all belts we can decompose p as a sum of class numbers.

Lemma

$$h(\mathcal{O}') = h(\mathcal{O}) \left(\ell - \left(\frac{\mathrm{Disc}(\mathcal{O})}{\ell} \right) \right) \quad \textit{if } [\mathcal{O}' : \mathcal{O}] = \ell$$

.

CM action and Horizontal isogenies

Lemma

- *If* $\varphi : E \to E'$ *is a horizontal* ℓ*-isogeny, there exists an integral invertible* $\mathcal{O}$*-ideal* $\mathfrak{L}$ *of norm* ℓ *such that* $E' \cong E/E[\mathfrak{L}]$.
- *Reciprocally, invertible ideals* $\mathfrak{L}$ *of norm* ℓ *give rise to* ℓ*-isogenies* $\varphi : E \to E/E[\mathfrak{L}]$.

- This is the degree ℓ part of the free and transitive group action of $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{Ell}_{\mathbb{F}_p}(\mathcal{O})$.
- Now we only need to look at ideals!

Structure: Horizontal isogenies

Corollary

There are exactly $1 + \left(\frac{\mathrm{Disc}(\mathcal{O})}{\ell}\right)$ *horizontal edges from a vertex with endomorphism ring* $\mathcal{O}$*.*

- No horizontal isogenies outside of level 0!
- The level 0 only connected components are called craters.
- Otherwise the number only depends on the cordillera:

$$1 + \left(\frac{D(\mathcal{O}_K)}{\ell}\right) = \begin{cases} 0 & \text{if } \ell \text{ is inert in } K, \\ 1 & \text{if } \ell \text{ is ramified in } K, \\ 2 & \text{if } \ell \text{ splits in } K, \end{cases}$$

Structure: The crater

Structure: The crater

1. ℓ is inert in K
2. $\ell = \mathfrak{L}^2$, $\mathfrak{L}$ principal
3. $\ell = \mathfrak{L}\overline{\mathfrak{L}}$, $\mathfrak{L}$ principal
4. $\ell = \mathfrak{L}^2$, $\mathfrak{L}$ non principal
5. $\ell = \mathfrak{L}\overline{\mathfrak{L}}$, $[\mathfrak{L}]$ of order $n > 1$ in $\mathrm{Cl}(\mathcal{O})$

All craters in a given belt are the same, as cosets of the CM action.

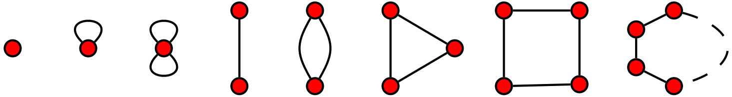


Figure: All possible craters.

Structure: The volcano

Structure: Degree of the vertices

Lemma

Let $j(E) \in \mathbb{F}_p$ be an ordinary j-invariant. Then the number of vertices from $j(E)$ in $\mathcal{G}_\ell(\mathbb{F}_p)$ is one of $0, 1, 2$ or $\ell + 1$.

Proof

- $\hat{\varphi} \circ \varphi = [\ell] \implies \ker \varphi \subset \ker[\ell]$
- $\ell + 1$ size ℓ subgroups of $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$
- Defined over $\mathbb{F}_p \implies$ invariant under $\mathrm{Gal}(\mathbb{F}_p(E[\ell])/\mathbb{F}_p)$
- Fixing ≥ 3 $\mathbb{F}_\ell$-lines of $(\mathbb{Z}/\ell\mathbb{Z})^2$ fixes everything.

Structure: Volcanoes

Theorem (Kohel)

Connected components (*) of $\mathcal{G}_\ell(\mathbb{F}_p)$ are ℓ-volcanoes [a]: a cycle (crater) with isomorphic trees (lava flows) at each of its vertices. All vertices have arity $\ell + 1$, except for the leaves of the trees.

[a] Terminology credit: Fouquet, Morain

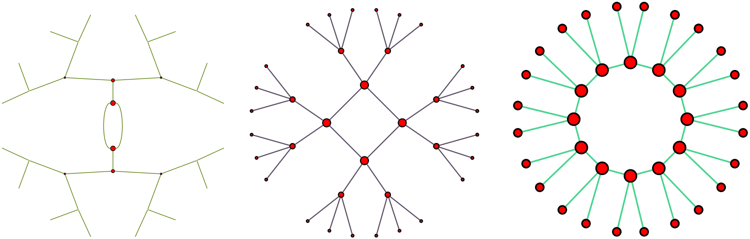


Figure: A 2-volcano and two 3-volcanoes

A zoo of possible connected components

Question: Suppose we are given an *abstract volcano* V[3]. Can we guarantee the existence of primes $p \neq \ell$ such that V is a connected component of $\mathcal{G}_\ell(\mathbb{F}_p)$?

[3] in the graph theoretic sense

A zoo of possible connected components

Question: Suppose we are given an *abstract volcano* V[3]. Can we guarantee the existence of primes $p \neq \ell$ such that V is a connected component of $\mathcal{G}_\ell(\mathbb{F}_p)$?

Crater only: $(V_0, \ell, 0)$

[3] in the graph theoretic sense

A zoo of possible connected components

Question: Suppose we are given an *abstract volcano* V[3]. Can we guarantee the existence of primes $p \neq \ell$ such that V is a connected component of $\mathcal{G}_\ell(\mathbb{F}_p)$?

Crater only: $(V_0, \ell, 0)$

Full volcano: (V_0, ℓ, d)

[3] in the graph theoretic sense

A zoo of possible connected components

Question: Suppose we are given an *abstract volcano* V[3]. Can we guarantee the existence of primes $p \neq \ell$ such that V is a connected component of $\mathcal{G}_\ell(\mathbb{F}_p)$?

Crater only: $(V_0, \ell, 0)$

Full volcano: (V_0, ℓ, d)

Replace $\mathbb{F}_p$ with $\mathbb{F}_{p^r}$

[3] in the graph theoretic sense

A very useful trick: depth is not a problem

Lemma

If we can find an order $\mathcal{O}$ *of an imaginary quadratic field* K *with* $\ell \nmid \mathrm{Disc}(\mathcal{O}) < -4$, *and a prime (integral ideal)* $\mathfrak{L}$ *above the (rational) odd prime* ℓ, *such that* $\mathfrak{L}$ *would generate a crater* V_0, *then for any* $d \geq 0$, *the volcano* (V_0, ℓ, d) *exists in infinitely many isogeny graphs* $\mathcal{G}_\ell(\mathbb{F}_p)$.

- *would generate* can be well defined.
- If $\ell = 2$ the result only holds for $d > 0$.
- What this means: in practice, don't worry about p or d.

Depth is not a problem: sketch of proof

- We want $(t, f) \in \mathbb{N}^2$ and p such that

$$4p = t^2 - f^2 \operatorname{Disc}(\mathcal{O}),$$

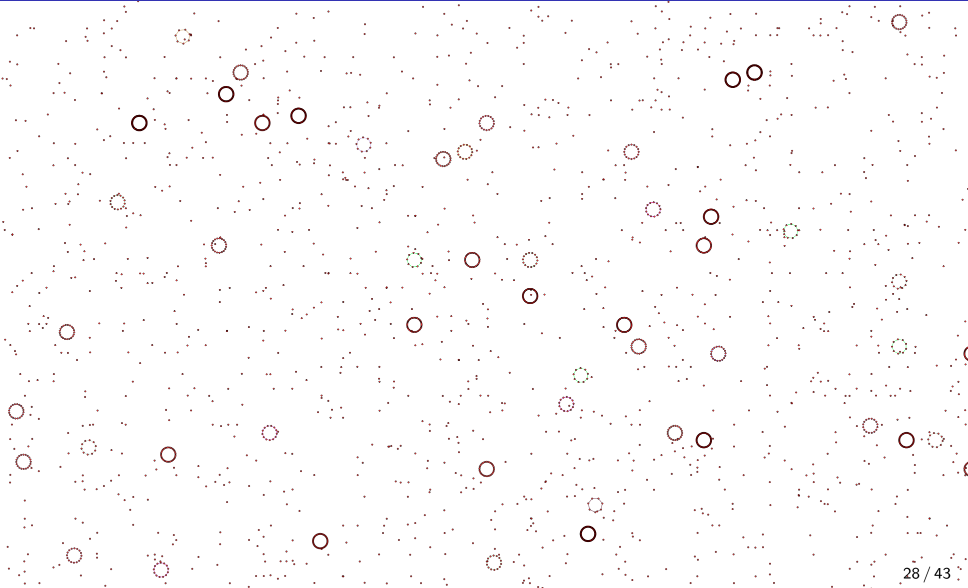
$t \neq 0$ and $v_\ell(f) = d$. This ensures $(V_0, \ell, d) \subset \mathcal{G}_\ell(\mathbb{F}_p)$.

- $p = x^2 + ny^2$ iff p splits completely in the ring class field of $\mathbb{Z}[\sqrt{-n}]$ (See Cox's eponymous book).
- Denote by H_k the ring class field of $\mathbb{Z}[\ell^k \sqrt{\operatorname{Disc}(\mathcal{O})}]$.

$$\begin{cases} H_d : & p = x^2 - \operatorname{Disc}(\mathcal{O})\ell^{2d}y^2 \\ H_{d+1} : & p = x^2 - \operatorname{Disc}(\mathcal{O})\ell^{2(d+1)}y^2 \end{cases}$$

- By Chebotarëv's theorem, there are infinitely many primes that split completely in H_d but not in H_{d+1}.

Intermission: funny behaviour?



Solving the weak inverse problem

Objective

Find infinitely many $p \neq \ell$ such that craters of size n are connected components in $\mathcal{G}_\ell(\mathbb{F}_p)$.

- Huge freedom on the choice of ℓ.
- Clear out all small craters by hand.
- Yamamoto (1970): we can construct an explicit imaginary quadratic field K such that $\mathrm{Disc}(\mathcal{O}_K) < -4$ and that has an element of order $n \geq 3$ in its class group $\mathrm{Cl}(\mathcal{O}_K)$.
- Cox (again!): the Dirichlet density of primes in a given quadratic imaginary class is strictly positive.
- Conclude with our previous Lemma.

Solving the inverse problem: easy craters

Objective

ℓ is now fixed. Find infinitely many $p \neq \ell$ such that volcanoes of shape (V_0, ℓ, d) are connected components in $\mathcal{G}_\ell(\mathbb{F}_p)$.

- Using our Lemma: forget about p and d , all we need is an imaginary quadratic field K in which ℓ has good behaviour.

Solving the inverse problem: easy craters

Objective

ℓ is now fixed. Find infinitely many $p \neq \ell$ such that volcanoes of shape (V_0, ℓ, d) are connected components in $\mathcal{G}_\ell(\mathbb{F}_p)$.

- Using our Lemma: forget about p and d , all we need is an imaginary quadratic field K in which ℓ has good behaviour.

Infinitely many K such that ℓ is inert (Dirichlet).

Figure: Crater type 1.

Solving the inverse problem: easy craters

Objective

ℓ is now fixed. Find infinitely many $p \neq \ell$ such that volcanoes of shape (V_0, ℓ, d) are connected components in $\mathcal{G}_\ell(\mathbb{F}_p)$.

- Using our Lemma: forget about p and d , all we need is an imaginary quadratic field K in which ℓ has good behaviour.

ℓ ramifies in a principal ideal of $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{-\ell})$. (*) for $\ell \leq 3$.

Figure: Crater type 2.

Solving the inverse problem: easy craters

Objective

ℓ is now fixed. Find infinitely many $p \neq \ell$ such that volcanoes of shape (V_0, ℓ, d) are connected components in $\mathcal{G}_\ell(\mathbb{F}_p)$.

- Using our Lemma: forget about p and d , all we need is an imaginary quadratic field K in which ℓ has good behaviour.

In $K = \mathbb{Q}(\sqrt{1-4\ell})$, $\alpha = \frac{1+\sqrt{1-4\ell}}{2}$ is integral of norm ℓ, who must split in $\mathcal{O}_K$ into two principal ideals.

Figure: Crater type 3.

Solving the inverse problem: easy craters

Objective

ℓ is now fixed. Find infinitely many $p \neq \ell$ such that volcanoes of shape (V_0, ℓ, d) are connected components in $\mathcal{G}_\ell(\mathbb{F}_p)$.

- Using our Lemma: forget about p and d , all we need is an imaginary quadratic field K in which ℓ has good behaviour.

Take $K = \mathbb{Q}(\sqrt{-\ell q})$ with a huge prime q. Then ℓ ramifies into a non-principal ideal, as its norm has to also be huge.

Figure: Crater type 4.

Solving the inverse problem: general craters

Objective

ℓ is now fixed. Find infinitely many $p \neq \ell$ such that volcanoes of shape (V_0, ℓ, d) are connected components in $\mathcal{G}_\ell(\mathbb{F}_p)$.

- Using our Lemma: forget about p and d , all we need is an imaginary quadratic field K in which ℓ has good behaviour.

Much harder! We want ℓ to split in two ideals whose class has prescribed order n in the ideal class group.

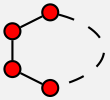


Figure: Crater type 5.

Solving the inverse problem: general craters

Theorem

The following properties hold.

1. *Let $n \neq 4$ be a positive integer and let $K = \mathbb{Q}(\sqrt{1 - 2^{n+2}})$. Then in $\mathcal{O}_K$ the prime 2 splits into two prime ideals whose corresponding classes in $\mathrm{Cl}(\mathcal{O}_K)$ have order n.*
2. *Let $K = \mathbb{Q}(\sqrt{-39})$. Then in $\mathcal{O}_K$ the prime 2 splits into two prime ideals whose corresponding classes in $\mathrm{Cl}(\mathcal{O}_K)$ have order 4.*
3. *Let $\ell \in \mathbb{Z}$ be an odd prime and let $n \in \mathbb{Z}_{>0}$. Define $K_1 := \mathbb{Q}(\sqrt{1 - \ell^n})$ and $K_2 := \mathbb{Q}(\sqrt{1 - 4\ell^n})$. Then either in $\mathcal{O}_{K_1}$ or in $\mathcal{O}_{K_2}$ the prime ℓ splits into two prime ideals whose corresponding classes in $\mathrm{Cl}(\mathcal{O}_{K_i})$ have order n.*

Solving the inverse problem: sketch of proof

- We work directly with diophantine equations.
- We use results from Nagell, Mahler and Pell.
- For example if $\ell = 2$, and $K = \mathbb{Q}(\sqrt{1-2^{n+2}})$ we write $\sqrt{1-2^{n+2}} = x\sqrt{-A}$ with A squarefree:

$$(\mathfrak{L}\overline{\mathfrak{L}})^n = 2^n = \frac{Ax^2+1}{4} = \frac{(1+x\sqrt{-A})}{2}\frac{(1-x\sqrt{-A})}{2}$$

- Now $\mathrm{ord}_{\mathrm{Cl}(\mathcal{O}_K)}(\mathfrak{L})|n$. Suppose it is $q < n$.
- If $q = 2$ expand and start cooking to get a contradiction except in one special case.
- If q is odd after clever manipulations we reach

$$U^2 - DV^2 = -A,$$

whose solutions are given by a theorem of Mahler. With a little more work we get a contradiction.

Solving the inverse problem: sketch of proof

- The case where ℓ is an odd prime is fun.
- Similar manipulations combined with an idea from Nagell yield the following:
- $K_1 = \mathbb{Q}(\sqrt{1-\ell^n})$ works when $\frac{\ell^{n/2}\pm 1}{2}$ is not a square.
- $K_2 = \mathbb{Q}(\sqrt{1-4\ell^n})$ works when $\ell^{n/2}$ is not the sum of two consecutive squares.
- Exercise: one condition has to be true!

Failing to solve the general inverse problem

Other fields

Almost everything we said on the structure of $\mathcal{G}_\ell(\mathbb{F}_p)$ transfers to $\mathcal{G}_\ell(\mathbb{F}_{p^r})$ for $r > 1$. Not true for the inverse problem!

Figure: The abstract volcano induced by $(2\text{-cycle}, 2, 1)$.

Proposition

The above volcano is an impossibility in any $\mathcal{G}_2(\mathbb{F}_{p^2})$.

Summary

In this talk:

- We defined the ordinary isogeny graph $\mathcal{G}_\ell(\mathbb{F}_p)$.
- We proved that its connected components look like volcanoes.
- We solved the inverse volcano problem over $\mathbb{F}_p$: every volcano exists in some $\mathcal{G}_\ell(\mathbb{F}_p)$.

Other directions:

- Inverse problem over $\mathbb{F}_{p^r}$.
- Given a volcano, which is the smallest field in which it lives?
- Better statistics on volcanoes.
- Faster algorithms to generate $\mathcal{G}_\ell(\mathbb{F}_p)$.
- A supersingular inverse problem?
- How many ℓ do you need to fully connect a cordillera?

Conclusion

Thank you![4]

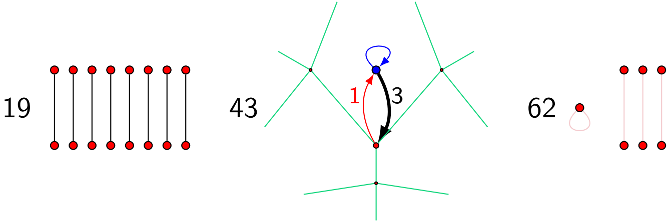


Figure: The 19/43/62-cordilleras in $\mathcal{G}_3(\mathbb{F}_{1009})$.

[4] If you want an illustration of any $\mathcal{G}_\ell(\mathbb{F}_p)$, feel free to send me an email!

References I

D.A. Cox.
Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication.
John Wiley & Sons, Inc., Hoboken, NJ, USA, April 1997.

M. Fouquet and F. Morain.
Isogeny volcanoes and the sea algorithm.
In C. Fieker and D.R. Kohel, editors, *Algorithmic Number Theory*, pages 276–291, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.

D. Kohel.
Endomorphism rings of elliptic curves over finite fields.
PhD thesis, University of California at Berkeley, 1996.

References II

J. Miret, D. Sadornil, J. Tena, R. Tomàs, and M. Valls.
Isogeny cordillera algorithm to obtain cryptographically good elliptic curves.
In *ACSW*, 2007.

T. Nagell.
Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns.
Nova Acta Soc. Sci. Upsaliensis (4), 16(2):38, 1955.

Y. Yamamoto.
On unramified Galois extensions of quadratic number fields.
Osaka Math. J., 7:57–76, 1970.

Illustration credits

- Volcanoes and Isogeny graphs are generated by myself using SageMath-Pari/GP-C++ and tikzit.
- The rest of the illustrations are stock pictures from Vilhelm Gunnarsson/Getty Images, Andy Krakovski/Istock and Reddit.