The DLP on Elliptic Curves with the same order

Marios Magioladitis

University of Duisburg-Essen, IEM

January 15, 2008

Aim of the talk

Theorem of Tate

Let E and E' be two elliptic curves over $\mathbb{F}_q$.

$$E \text{ and } E' \text{ are isogenous } \Leftrightarrow |E| = |E'|.$$

Main question

Consider E, E' isogenous elliptic curves.

$$DLP(E) \stackrel{?}{=} DLP(E')$$

Answer

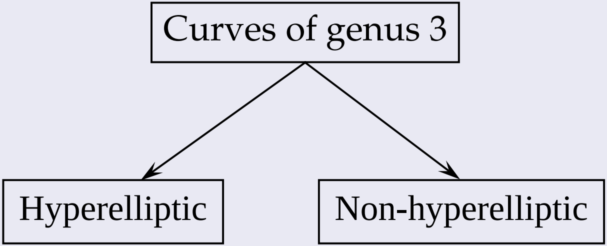
Yes*

- Generalized Riemann hypothesis ✓
- The same endomorphism ring (*technical*) ✓

Question: Can we extend it for curves of genus 2?
Answer: Hopefully, yes!

For genus > 1 we have to work with Jacobians.

Question: Can we extend it for curves of genus 3?
Answer: No :(



Curves of genus 3

1. DLP in hyperelliptic case: $\tilde{O}(q^{4/3})$ group operations (Gaudry, Thomé, Thériault, Diem)
2. DLP in non-hyperelliptic case: $\tilde{O}(q)$ group operations (Diem's index calculus algorithm)
3. $\exists$ "many" (at least 18.78%) hyperelliptic curves of genus 3 with an explicit isogeny of small degree of their Jacobian to a Jacobian of a non-hyperelliptic curve. (Smith)

DLP is random reducible

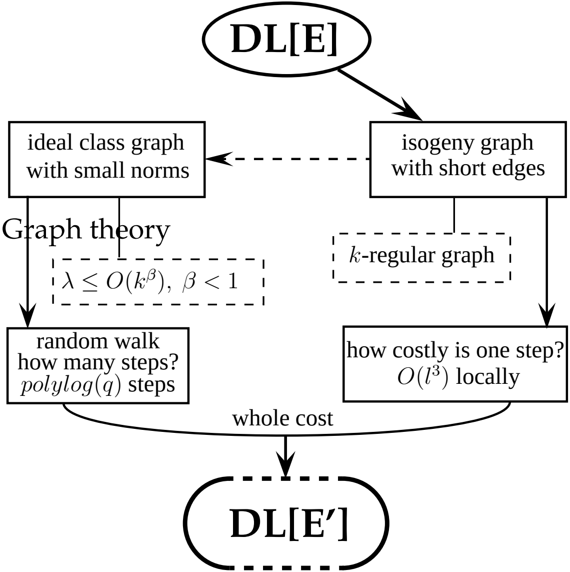
Let E and E' be two isogenous elliptic curves over $\mathbb{F}_q$.

$$E \text{ and } E' \text{ belong to the same level } \Leftrightarrow \mathrm{End}\,(\mathrm{E}) = \mathrm{End}\,(\mathrm{E}').$$

Corollary *(Assuming GRH)*

The DLP on elliptic curves is random reducible.
Given any algorithm A that solves DLP on some fixed positive proportion of curves in a fixed level, then DLP can probabilistically solved on any given curve in the same level with *polylog(q)* expected queries to A with random inputs.

Sketch of the proof



Number and type of isogenies $E \longrightarrow E'$ of degree ℓ

Kohel (1996)

Case	Type	Subcase	Type
$\ell \nmid c_E$	$1 + \left(\frac{D}{\ell}\right) \rightarrow$	$\ell \nmid c_\pi$	
		$\ell \mid c_\pi$	$\ell - \left(\frac{D}{\ell}\right) \downarrow$
$\ell \mid c_E$	$1 \uparrow$	$\ell \nmid \frac{c_\pi}{c_E}$	
		$\ell \mid \frac{c_\pi}{c_E}$	$\ell \downarrow$

1. $\downarrow$ $[\mathrm{End}\,(\mathrm{E}) : \mathrm{End}\,(\mathrm{E}')] = \ell$
2. $\uparrow$ $[\mathrm{End}\,(\mathrm{E}') : \mathrm{End}\,(\mathrm{E})] = \ell$
3. $\rightarrow$ $\mathrm{End}\,(\mathrm{E}) = \mathrm{End}\,(\mathrm{E}')$

A standard result from graph theory

Proposition

Let $\mathcal{G}$ be a k-regular graph with h vertices. Suppose that the eigenvalue λ of any non-constant eigenvector satisfies the bound $|\lambda| \leq c$ for some $c < k$. Let S be any subset of the vertices of $\mathcal{G}$, and x be any vertex in $\mathcal{G}$. Then a random walk of any length at least $\frac{\log 2h/|S|^{1/2}}{\log k/c}$ starting from x will land in S with probability at least $\frac{|S|}{2h}$.

Main result

Theorem (*Assuming GRH*)

Let E be an elliptic curve of order N over $\mathbb{F}_q$. There exists a polynomial $P(x)$, independent of N and q, s.t. for $P(\log q)$, the isogeny graph $\mathcal{G}$ on each level is a nearly Ramanujan graph and any random walk on $\mathcal{G}$ will reach a subset of size h with probability at least $\frac{h}{2|\mathcal{G}|}$ after polylog(q) steps.