Identifying supersingular elliptic curves

Andrew V. Sutherland

Massachusetts Institute of Technology

January 6, 2012

http://arxiv.org/abs/1107.1140

Supersingular elliptic curves

Let $\mathbb{F}_q$ be a finite field of characteristic p.

Recall that elliptic curves over finite fields come in two flavors: *ordinary* and *supersingular*.

ordinary	**supersingular**
$E[p] \cong \mathbb{Z}/p\mathbb{Z}$	$E[p]$ is trivial
$\#E(\mathbb{F}_q) \not\equiv 1 \bmod p$	$\#E(\mathbb{F}_q) \equiv 1 \bmod p$
$\mathrm{End}(E)$ is an order in an imaginary quadratic field	$\mathrm{End}(E)$ is an order in a quaternion algebra

Distribution of supersingular elliptic curves

Whether a curve E is supersingular or not depends only on its j-invariant $j(E)$, which identifies E up to isomorphism (over $\bar{\mathbb{F}}_q$).

If E is supersingular then $j(E) \in \mathbb{F}_{p^2}$, so we assume q is p or p^2.

There are $\frac{p}{12} + O(1)$ supersingular j-invariants in $\mathbb{F}_{p^2}$.
Of these, $O(h(-p)) = \tilde{O}(\sqrt{p})$ lie in $\mathbb{F}_p$.

In either case, the probability that a random elliptic curve $E/\mathbb{F}_q$ is supersingular is $\tilde{O}(1/\sqrt{q})$, which makes them very rare.

However, every elliptic curve over $\mathbb{Q}$ is supersingular modulo infinitely many primes p, by a theorem of Elkies.

Identifying supersingular elliptic curves

Problem: Given $E\colon y^2 = f(x) = x^3 + Ax + B$ defined over $\mathbb{F}_q$, determine whether E is ordinary or supersingular.

There is a fast Monte Carlo test that can prove E is ordinary.

Pick a random point P on $E(\mathbb{F}_q)$.
If $q = p$, test whether $(p+1)P \neq 0$.
If $q = p^2$, test whether $(p+1)P \neq 0$ and $(p-1)P \neq 0$.

If the tested condition holds, then E must be ordinary.
If E is in fact ordinary, each iteration of this test will succeed with probability $1 - O(1/\sqrt{q})$.

But this test can never **prove** that E supersingular.

Identifying supersingular elliptic curves

Problem: Given $E\colon y^2 = f(x) = x^3 + Ax + B$ defined over $\mathbb{F}_q$, determine whether E is ordinary or supersingular.

Solution 1: Compute the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$.
This takes time exponential in $n = \log p$.

Solution 2: Compute $\#E(\mathbb{F}_q)$ using Schoof's algorithm.
This takes $\tilde{O}(n^5)$ time.

Solution 3: Check that $\Phi_\ell(j(E), Y)$ splits completely in $\mathbb{F}_{p^2}$ for sufficiently many primes ℓ (similar to SEA).
This takes $\tilde{O}(n^4)$ expected time.

This talk: Use isogeny graphs.
This takes $\tilde{O}(n^3)$ expected time.

The graph of ℓ-isogenies

The classical modular polynomial $\Phi_\ell \in \mathbb{Z}[X, Y]$ parameterizes pairs of ℓ-isogenous elliptic curves in terms of their j-invariants.

Definition

The graph $G_\ell(\mathbb{F}_q)$ has vertex set $\mathbb{F}_q$ and for each $j_1 \in \mathbb{F}_q$ an edge (j_1, j_2) for each root $j_2 \in \mathbb{F}_q$ of $\Phi_\ell(j_1, Y)$, with multiplicity.

Isogenous curves have the same number of rational points. Thus the vertices in each connected component of $G_\ell(\mathbb{F}_q)$ are either all ordinary or all supersingular.

As abstract graphs, the ordinary and supersingular components of $G_\ell(\mathbb{F}_q)$ have distinctly different structures.

Supersingular components of $G_\ell(\mathbb{F}_{p^2})$

If j_1 is supersingular, then $\phi(Y) = \Phi_\ell(j_1, Y)$ splits completely in $\mathbb{F}_{p^2}$, since every supersingular j-invariant lies in $\mathbb{F}_{p^2}$.

Thus the supersingular vertices in $G_\ell(\mathbb{F}_{p^2})$ all have degree $\ell + 1$, and each supersingular component is an $(\ell + 1)$-regular graph.

There is in fact just one supersingular component (but we won't use this).

Ordinary components of $G_\ell(\mathbb{F}_q)$

Let E be an ordinary elliptic curve.
Then $\mathrm{End}(E) \cong \mathcal{O}$ with $\mathbb{Z}[\pi] \subset \mathcal{O} \subset \mathcal{O}_K$.

Here π is the Frobenius endomorphism and $K = \mathbb{Q}(\sqrt{D})$, where D is the fundamental imaginary quadratic discriminant satisfying

$$4q = \mathrm{tr}(\pi)^2 - v^2 D.$$

Each ordinary component of $G_\ell(\mathbb{F}_q)$ consists of levels $V_0, \ldots, V_d$.
The vertex $j(E)$ belongs to level V_i, where $i = \nu_\ell([\mathcal{O}_K : \mathcal{O}])$.

Note that ℓ^d divides v. Therefore

$$d < \log_\ell \sqrt{4q}.$$

ℓ-volcanoes

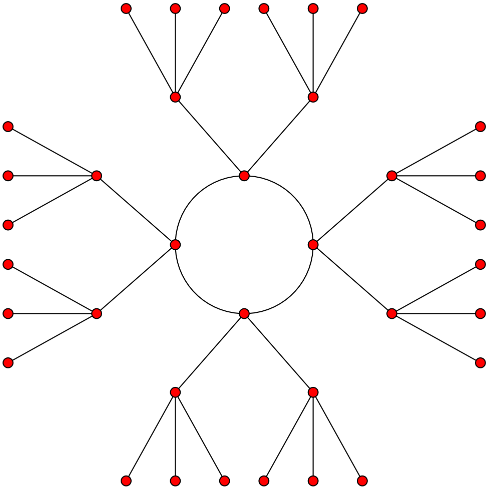
Vertices in level V_d have degree at most 2.
Vertices in level V_i with $i < d$ have degree $\ell + 1$.
Ordinary components are not $(\ell + 1)$-regular graphs.
They are ***ℓ-volcanoes***.

The vertices in level V_0 form a (possibly trivial) cycle.
All edges with origin in V_0 not in this cycle lead to V_1.

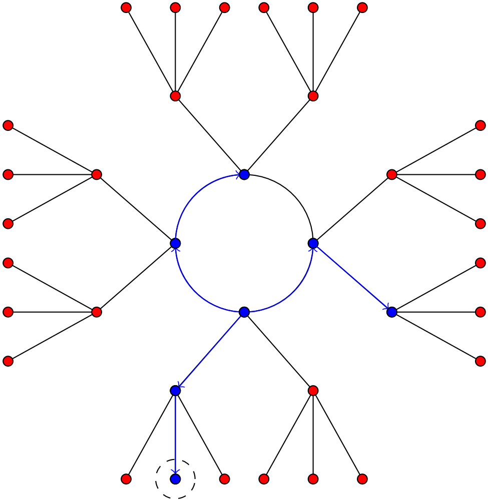
Vertices in level V_i with $i > 0$ have one edge up to V_{i-1},
all other edges (0 or ℓ of them) lead down to V_{i+1}.

Level V_0 is the *surface* and V_d is the *floor* (possibly $V_0 = V_d$).

A 3-volcano of depth 2



Finding a shortest path to the floor



Algorithm

Given an elliptic curve E over a field of characteristic p, determine whether E is ordinary or supersingular as follows:

1. If $j(E) \not\in \mathbb{F}_{p^2}$ then return **ordinary**.
2. If $p \le 3$ then return **supersingular** (resp. **ordinary**) if $j(E) = 0$ (resp. $j(E) \neq 0$).
3. Attempt to find 3 roots of $\Phi_2(j(E), Y)$ in $\mathbb{F}_{p^2}$.
   If this is not possible, return **ordinary**.
4. Walk 3 paths in parallel for up to $\lceil \log_2 p \rceil + 1$ steps.
   If any of these paths hits the floor, return **ordinary**.
5. Return **supersingular**.

$$\Phi_2(X, Y) = X^3 + Y^3 - X^2Y^2 + 1488(X^2Y + Y^2X) - 162000(X^2 + Y^2) + 40773375XY + 8748000000(X + Y) - 157464000000000.$$

Complexity analysis

Proposition

Let $n = \log p$.

- *We have a Las Vegas algorithm that runs in* $O(n^3 \log n \log\log n)$ *expected time, using* $O(n)$ *space.*
- *Given quadratic and cubic non-residues in* $\mathbb{F}_{p^2}$*, we have a deterministic algorithm:* $O(n^3 \log^2 n)$ *time and* $O(n)$ *space.*
- *For a random elliptic curve over* $\mathbb{F}_p$ *or* $\mathbb{F}_{p^2}$*, the average running time is* $O(n^2 \log n \log\log n)$*.*

The average complexity is the same as a single iteration of the Monte Carlo test, and has *better* constant factors.

Performance results (CPU milliseconds)

	ordinary				supersingular			
	Magma		**New**		Magma		**New**	
b	$\mathbb{F}_p$	$\mathbb{F}_{p^2}$	$\mathbb{F}_p$	$\mathbb{F}_{p^2}$	$\mathbb{F}_p$	$\mathbb{F}_{p^2}$	$\mathbb{F}_p$	$\mathbb{F}_{p^2}$
64	1	25	0.1	0.1	226	770	2	8
128	2	60	0.1	0.1	2010	9950	5	13
192	4	99	0.2	0.1	8060	41800	8	33
256	7	140	0.3	0.2	21700	148000	20	63
320	10	186	0.4	0.3	41500	313000	39	113
384	14	255	0.6	0.4	95300	531000	66	198
448	19	316	0.8	0.5	152000	789000	105	310
512	24	402	1.0	0.7	316000	2280000	164	488
576	30	484	1.3	0.9	447000	3350000	229	688
640	37	595	1.6	1.0	644000	4790000	316	945
704	46	706	2.0	1.2	847000	6330000	444	1330
768	55	790	2.4	1.5	1370000	8340000	591	1770
832	66	924	3.1	1.9	1850000	10300000	793	2410
896	78	1010	3.2	2.1	2420000	12600000	1010	3040
960	87	1180	4.0	2.5	3010000	16000000	1280	3820
1024	101	1400	4.8	3.1	5110000	35600000	1610	4880

Identifying supersingular elliptic curves

Andrew V. Sutherland

Massachusetts Institute of Technology

January 6, 2012

http://arxiv.org/abs/1107.1140