Isogeny volcanoes: a computational perspective

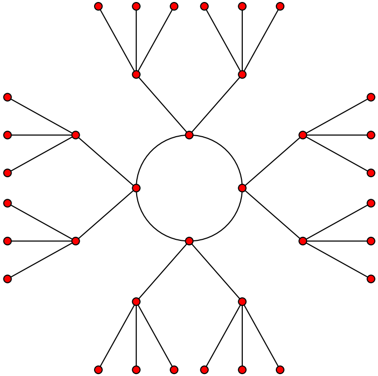
Andrew V. Sutherland

Massachusetts Institute of Technology

ANTS X — July 9, 2012

A volcano

A volcano



ℓ-volcanoes

For a prime ℓ, an ℓ-*volcano* is a connected undirected graph whose vertices are partitioned into levels $V_0, \ldots, V_d$.

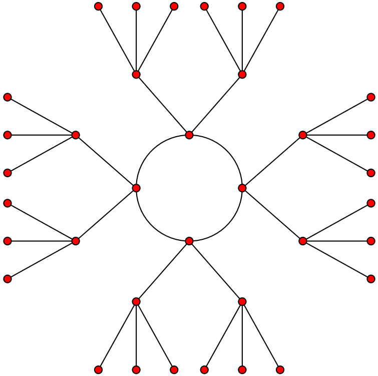
1. The subgraph on V_0 (the *surface*) is a connected regular graph of degree $0, 1$, or 2.

2. For $i > 0$, each $v \in V_i$ has exactly one neighbor in V_{i-1}. All edges not on the surface arise in this manner.

3. For $i < d$, each $v \in V_i$ has degree ℓ+1.

We allow self-loops and multi-edges in our graphs, but this can happen only on the surface of an ℓ-volcano.

A 3-volcano of depth 2



Elliptic curves

An elliptic curve E/k is a smooth projective curve of genus 1 with a distinguished k-rational point 0.

For any field extension k'/k, the set of k'-rational points $E(k')$ forms an abelian group with identity element 0.

When the characteristic of k is not 2 or 3 (which we assume for convenience) we may define E with an equation of the form

$$y^2 = x^3 + Ax + B,$$

where $A, B \in k$.

j-invariants

The $\bar{k}$-isomorphism classes of elliptic curves E/k are in bijection with the field k. For $E\colon\ y^2 = x^3 + Ax + B$, the *$j$-invariant* of E is

$$j(E) = j(A,B) = 1728\frac{4A^3}{4A^3 + 27B^2} \in k.$$

The j-invariants $j(0,B) = 0$ and $j(A,0) = 1728$ are special.
They correspond to elliptic curves with extra automorphisms.

For $j_0 \not\in \{0, 1728\}$, we have $j_0 = j(A,B)$, where

$$A = 3j_0(1728 - j_0) \qquad \text{and} \qquad B = 2j_0(1728 - j_0)^2.$$

Note that $j(E_1) = j(E_2)$ does not necessarily imply that E_1 and E_2 are isomorphic over k, but they must be isomorphic over $\bar{k}$.

ℓ-isogenies

An *isogeny* $\phi\colon E_1 \to E_2$ is a morphism of elliptic curves,
a rational map that fixes the point 0.

It induces a group homomorphism $\phi\colon E_1(\bar{k}) \to E_2(\bar{k})$.
If ϕ is nonzero then it has a finite kernel.
Every finite subgroup of $E_1(\bar{k})$ is the kernel of an isogeny.

ℓ-isogenies

An *isogeny* $\phi\colon E_1 \to E_2$ is a morphism of elliptic curves,
a rational map that fixes the point 0.

It induces a group homomorphism $\phi\colon E_1(\bar{k}) \to E_2(\bar{k})$.
If ϕ is nonzero then it has a finite kernel.
Every finite subgroup of $E_1(\bar{k})$ is the kernel of an isogeny.

The *degree* of an isogeny is its degree as a rational map.
For a nonzero *separable* isogeny, $\deg\phi = |\ker\phi|$.

We are interested in isogenies of prime degree $\ell \neq \operatorname{char} k$,
which are necessarily separable isogenies with cyclic kernels.

The *dual isogeny* $\hat{\phi}\colon E_2 \to E_1$ has the same degree ℓ as ϕ, and

$$\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [\ell]$$

is the *multiplication-by-ℓ* map.

The ℓ-torsion subgroup

For $\ell \neq \mathrm{char}(k)$, the ℓ-*torsion subgroup*

$$E[\ell] = \{P \in E(\bar{k}) : \ell P = 0\}$$

is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and thus contains $\ell + 1$ cyclic subgroups of order ℓ, each of which is the kernel of an ℓ-isogeny.

These ℓ-isogenies are not necessarily defined over k.

An ℓ-isogeny is defined over k (and has image defined over k) if and only if its kernel is Galois-invariant.

The number of Galois-invariant order-ℓ subgroups of $E[\ell]$ is either $0, 1, 2$, or $\ell + 1$.

The modular equation

Let $j\colon \mathbb{H} \to \mathbb{C}$ be the classical modular function.

For any $\tau \in \mathbb{H}$, the values $j(\tau)$ and $j(\ell\tau)$ are the j-invariants of elliptic curves over $\mathbb{C}$ that are ℓ-isogenous.

The minimal polynomial $\Phi_\ell(Y)$ of the function $j(\ell z)$ over $\mathbb{C}(j)$ has coefficients that are actually integer polynomials of $j(z)$.

Replacing $j(z)$ with X yields the *modular polynomial* $\Phi_\ell \in \mathbb{Z}[X, Y]$ that parameterizes pairs of ℓ-isogenous elliptic curves $E/\mathbb{C}$:

$$\Phi_\ell\big(j(E_1), j(E_2)\big) = 0 \quad \Longleftrightarrow \quad j(E_1) \text{ and } j(E_2) \text{ are } \ell\text{-isogenous.}$$

This moduli interpretation remains valid over any field of characteristic not ℓ.

$\Phi_\ell(X, Y) = 0$ is a defining equation for the affine modular curve $Y_0(\ell) = \Gamma_0(\ell)\backslash\mathbb{H}$.

The graph of ℓ-isogenies

Definition
The *ℓ-isogeny graph* $G_\ell(k)$ has vertex set $\{j(E) : E/k\} = k$
and edges (j_1, j_2) for each root $j_2 \in k$ of $\Phi_\ell(j_1, Y)$ (with multiplicity).

Except for $j \in \{0, 1728\}$, the in-degree of each vertex of G_ℓ is equal to its out-degree. Thus G_ℓ is a bi-directed graph on $k \backslash \{0, 1728\}$, which we may regard as an undirected graph.

Note that we have an infinite family of graphs $G_\ell(k)$ with vertex set k, one for each prime $\ell \neq \mathrm{char}(k)$.

Ordinary and supersingular curves

For an elliptic curve E/k with $\operatorname{char}(k) = p$ we have

$$E[p] \simeq \begin{cases} \mathbb{Z}/p\mathbb{Z} & (\textit{ordinary}), \\ \{0\} & (\textit{supersingular}). \end{cases}$$

For isogenous elliptic curves $E_1 \sim E_2$, either both are ordinary or both are supersingular. Thus the each isogeny graph G_ℓ decomposes into ordinary and supersingular components.

This has cryptographic applications; see [Charles-Lauter-Goren 2008], for example.

Ordinary and supersingular curves

For an elliptic curve E/k with $\mathrm{char}(k) = p$ we have

$$E[p] \simeq \begin{cases} \mathbb{Z}/p\mathbb{Z} & (\textit{ordinary}), \\ \{0\} & (\textit{supersingular}). \end{cases}$$

For isogenous elliptic curves $E_1 \sim E_2$, either both are ordinary or both are supersingular. Thus the each isogeny graph G_ℓ decomposes into ordinary and supersingular components.

Every supersingular curve is defined over $\mathbb{F}_{p^2}$. Thus the supersingular components of $G_\ell(\mathbb{F}_{p^2})$ are regular graphs of degree $\ell + 1$.

In fact, $G_\ell(\mathbb{F}_{p^2})$ has just one supersingular component, and it is a *Ramanujan graph* [Pizer 1990].

This has cryptographic applications; see [Charles-Lauter-Goren 2008], for example.

Endomorphism rings

Isogenies from an elliptic curve E to itself are *endomorphisms*.
They form a ring $\mathrm{End}(E)$ under composition and point addition.

We always have $\mathbb{Z} \subseteq \mathrm{End}(E)$, due to scalar multiplication maps.
If $\mathbb{Z} \subsetneq \mathrm{End}(E)$, then E has *complex multiplication* (CM).

For an elliptic curve E with complex multiplication:

$$\mathrm{End}(E) \simeq \begin{cases} \text{order in an imaginary quadratic field} & \text{(ordinary)}, \\ \text{order in a quaternion algebra} & \text{(supersingular)}. \end{cases}$$

Every elliptic curve over a finite field $\mathbb{F}_q$ has CM, since if E is ordinary then the *Frobenius endomorphism* $\pi_E(x, y) = (x^q, y^q)$ does not lie in $\mathbb{Z}$.

Horizontal and vertical isogenies

Let $\varphi\colon E_1 \to E_2$ by an ℓ-isogeny of ordinary elliptic curves with CM.
Let $\mathrm{End}(E_1) \simeq \mathcal{O}_1 = [1, \tau_1]$ and $\mathrm{End}(E_2) \simeq \mathcal{O}_2 = [1, \tau_2]$.

Then $\ell\tau_2 \in \mathcal{O}_1$ and $\ell\tau_1 \in \mathcal{O}_2$.

Thus one of the following holds:

- $\mathcal{O}_1 = \mathcal{O}_2$, in which case φ is *horizontal*;
- $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$, in which case φ is *descending*;
- $[\mathcal{O}_2 : \mathcal{O}_1] = \ell$, in which case φ is *ascending*.

In the latter two cases we say that φ is a *vertical* isogeny.

The theory of complex multiplication

Let E/k have $\mathrm{End}(E) \simeq \mathcal{O} \subset K = \mathbb{Q}(\sqrt{D})$, with $D = \operatorname{disc} K$.

For each invertible $\mathcal{O}$-ideal $\mathfrak{a}$, the $\mathfrak{a}$-torsion subgroup

$$E[\mathfrak{a}] = \{P \in E(\bar{k}) : \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\}$$

is the kernel of an isogeny $\varphi_{\mathfrak{a}} \colon E \to E'$ of degree $N(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$.
We necessarily have $\mathrm{End}(E) \simeq \mathrm{End}(E')$, so $\varphi_{\mathfrak{a}}$ is **horizontal**.

If $\mathfrak{a}$ is principal, then $E' \simeq E$. This induces a $\mathrm{cl}(\mathcal{O})$-action on the set.

$$\mathrm{Ell}_{\mathcal{O}}(k) = \{j(E) : E/k \text{ with } \mathrm{End}(E) \simeq \mathcal{O}\}.$$

This action is faithful and transitive; thus $\mathrm{Ell}_{\mathcal{O}}(k)$ is a principal homogeneous space, a *torsor*, for $\mathrm{cl}(\mathcal{O})$.

One can decompose horizontal isogenies of large prime degree into an equivalent sequence of isogenies of small prime degrees, which makes them **easy to compute**; see [Bröker-Charles-Lauter 2008, Jao-Souhkarev ANTS IX].

Horizontal isogenies

Every horizontal ℓ-isogeny arises from the action of an invertible $\mathcal{O}$-ideal $\mathfrak{l}$ of norm ℓ.

If $\ell \mid [\mathcal{O}_K : \mathcal{O}]$, no such $\mathfrak{l}$ exists; if $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$, then there are

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

such ℓ-isogenies.

In the split case, $(\ell) = \mathfrak{l} \cdot \bar{\mathfrak{l}}$, and the $\mathfrak{l}$-orbits partition $\mathrm{Ell}_{\mathcal{O}}(k)$ into cycles corresponding to the cosets of $\langle [\mathfrak{l}] \rangle$ in $\mathrm{cl}(\mathcal{O})$.

Vertical isogenies

Let $\mathcal{O}$ be an imaginary quadratic order with discriminant $D_\mathcal{O} < -4$, and let $\mathcal{O}' = \mathbb{Z} + \ell\mathcal{O}$ be the order of index ℓ in $\mathcal{O}$.

The map that sends each invertible $\mathcal{O}'$-ideal $\mathfrak{a}$ to the (invertible) $\mathcal{O}$-ideal $\mathfrak{a}\mathcal{O}$ preserves norms and induces a surjective homomorphism

$$\phi\colon\ \mathrm{cl}(\mathcal{O}') \to \mathrm{cl}(\mathcal{O})$$

compatible with the class group actions on $\mathrm{Ell}_\mathcal{O}(k)$ and $\mathrm{Ell}_{\mathcal{O}'}(k)$.

It follows that each $j(E') \in \mathrm{Ell}_{\mathcal{O}'}(k)$ has a unique ℓ-isogenous "parent" $j(E)$ in $\mathrm{Ell}_\mathcal{O}(k)$, and every vertical isogeny must arise in this way.

The "children" of $j(E)$ correspond to a coset of the kernel of ϕ, which is a cyclic of order $\ell - \left(\frac{D_\mathcal{O}}{\ell}\right)$, generated by the class of an invertible $\mathcal{O}'$-ideal with norm ℓ^2.

Ordinary elliptic curves over finite fields

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with *trace of Frobenius*

$$t = \operatorname{tr}\pi_E = q + 1 - \#E(\mathbb{F}_q).$$

Then $\pi_E^2 - t\pi_E + q = 0$ and we have the *norm equation*

$$4q = t^2 - v^2 D,$$

where D is the (fundamental) discriminant of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{t^2 - 4q}) \simeq \operatorname{End}(E) \otimes \mathbb{Q}$ and $v = [\mathcal{O}_K : \mathbb{Z}[\pi_E]]$. We have

$$\mathbb{Z}[\pi_E] \subseteq \operatorname{End}(E) \subseteq \mathcal{O}_K.$$

Thus $[\mathcal{O}_K : \operatorname{End}(E)]$ divides v; this holds for any E with trace t.
If we define $\operatorname{Ell}_t(\mathbb{F}_q) = \{j(E) : E/\mathbb{F}_q \text{ with } \operatorname{tr}\pi_E = t\}$, then

$$\operatorname{Ell}_t(\mathbb{F}_q) = \bigcup_{\mathbb{Z}[\pi_E] \subseteq \mathcal{O} \subseteq \mathcal{O}_K} \operatorname{Ell}_{\mathcal{O}}(\mathbb{F}_q).$$

The main theorem

Theorem (Kohel)

Let V be an ordinary connected component of $G_\ell(\mathbb{F}_q)$ that does not contain $0, 1728$. Then V is an ℓ-volcano in which the following hold:

(i) *Vertices in level V_i all have the same endomorphism ring $\mathcal{O}_i$.*

(ii) $\ell \nmid [\mathcal{O}_K : \mathcal{O}_0]$, *and* $[\mathcal{O}_i : \mathcal{O}_{i+1}] = \ell$.

(iii) *The subgraph on V_0 has degree $1 + (\frac{D}{\ell})$, where $D = \operatorname{disc}(\mathcal{O}_0)$.*

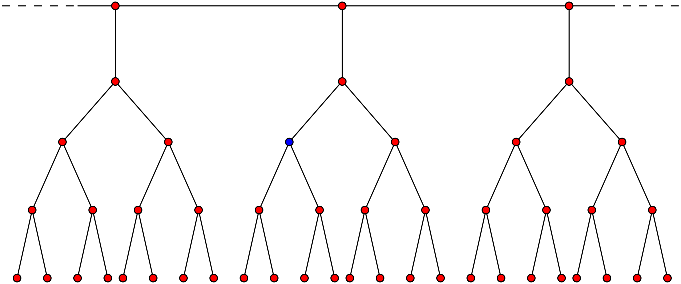
(iv) *If $(\frac{D}{\ell}) \geq 0$ then $|V_0|$ is the order of $[\mathfrak{l}]$ in $\operatorname{cl}(\mathcal{O}_0)$.*

(v) *The depth of V is $\operatorname{ord}_\ell(v)$, where $4q = t^2 - v^2 D$.*

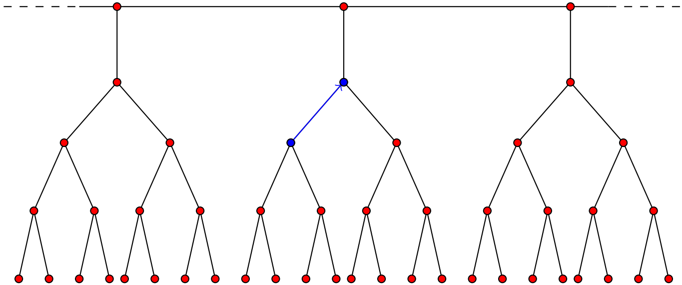
The term *volcano* is due to Fouquet and Morain (ANTS V).

Applications

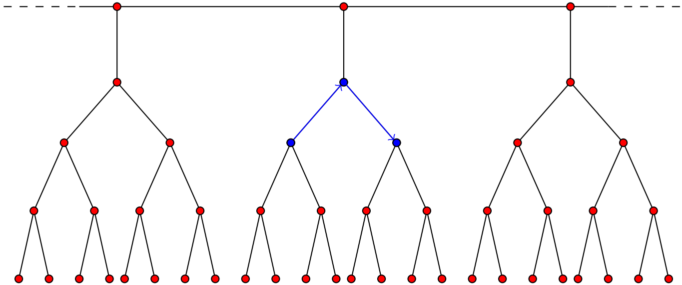
Finding the floor



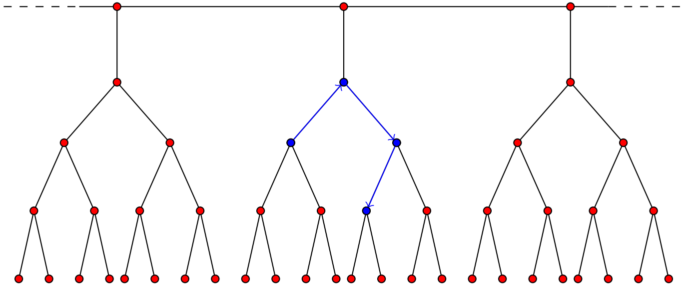
Finding the floor



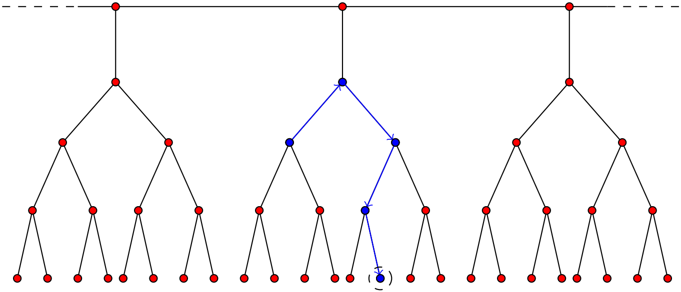
Finding the floor



Finding the floor

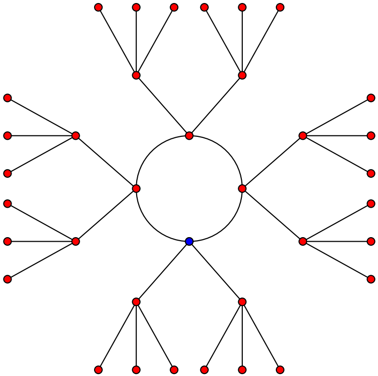


Finding the floor

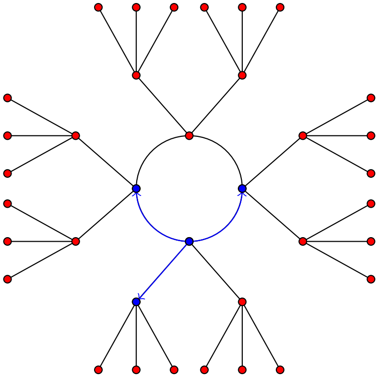


Curves on the floor necessarily have cyclic rational ℓ-torsion. This is useful, for example, when constructing Edwards curves with the CM method [Morain 2009].

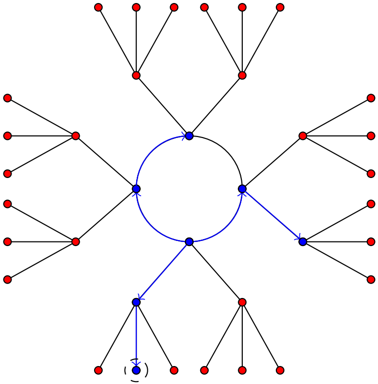
Finding a shortest path to the floor



Finding a shortest path to the floor



Finding a shortest path to the floor



We now know that we are 2 levels above the floor.

Application: identifying supersingular curves

The equation $4q = t^2 - v^2D$ implies that each ordinary component of $G_\ell(\mathbb{F}_q)$ is an ℓ-volcano of depth less than $\log_\ell \sqrt{4q}$.

Given $j(E) \in \mathbb{F}_{p^2}$, if we cannot find a shortest path to the floor in $G_2(\mathbb{F}_{p^2})$ within $\lceil \log_2 p \rceil$ steps, then E **must be supersingular**.

Conversely, if E is supersingular, our attempt to find the floor must fail, since every vertex in the supersingular component has degree $\ell + 1$.

See [S 2012] for details.

Application: identifying supersingular curves

The equation $4q = t^2 - v^2D$ implies that each ordinary component of $G_\ell(\mathbb{F}_q)$ is an ℓ-volcano of depth less than $\log_\ell \sqrt{4q}$.

Given $j(E) \in \mathbb{F}_{p^2}$, if we cannot find a shortest path to the floor in $G_2(\mathbb{F}_{p^2})$ within $\lceil \log_2 p \rceil$ steps, then E **must be supersingular**.

Conversely, if E is supersingular, our attempt to find the floor must fail, since every vertex in the supersingular component has degree $\ell + 1$.

This yields a (probabilistic) algorithm to determine supersingularity in $\tilde{O}(n^3)$ time, where $n = \log p$, improving the $\tilde{O}(n^4)$ complexity of the best previously known algorithms.

Moreover, the expected running time on a random elliptic curve is $\tilde{O}(n^2)$, matching the complexity of the best *Monte Carlo* algorithms, and faster in practice.

See [S 2012] for details.

Application: computing endomorphism rings

Given an ordinary elliptic curve $E/\mathbb{F}_q$, if we compute the Frobenius trace t and put $4q = t^2 - v^2 D$, we can determine $\mathcal{O} \simeq \mathrm{End}(E)$ by determining $u = [\mathcal{O}_K : \mathcal{O}]$, which must divide v.

It suffices to determine the level of $j(E)$ in its ℓ-volcano for $\ell | v$.

Problem: when ℓ is large it is not feasible to compute Φ_ℓ, nor is it feasible to directly compute a **vertical** ℓ-isogeny.

See [Bisson-S 2011] and [Bisson 2011] for more details.

Application: computing endomorphism rings

Given an ordinary elliptic curve $E/\mathbb{F}_q$, if we compute the Frobenius trace t and put $4q = t^2 - v^2 D$, we can determine $\mathcal{O} \simeq \mathrm{End}(E)$ by determining $u = [\mathcal{O}_K : \mathcal{O}]$, which must divide v.

It suffices to determine the level of $j(E)$ in its ℓ-volcano for $\ell | v$.

Problem: when ℓ is large it is not feasible to compute Φ_ℓ, nor is it feasible to directly compute a **vertical** ℓ-isogeny.

Solution: we may determine the primes $\ell | u$ by finding *smooth relations* that hold in $\mathrm{cl}((v/\ell)^2 D)$ but not in $\mathrm{cl}(\ell^2 D)$ and evaluating the corresponding **horizontal** isogenies (and similarly for ℓ^e)

This yields a probabilistic algorithm to compute $\mathrm{End}(E)$ with subexponential expected running time $L[1/2, \sqrt{3}/2]$, under GRH..

See [Bisson-S 2011] and [Bisson 2011] for more details.

Example

Let $q = 2^{320} + 261$ and suppose $\operatorname{tr} \pi_E = t$, where
$t = 2306414344576213633891236434392671392737040459558$.

Then $4q = t^2 - v^2 D$, where $D = -147759$ and $v = 2^2 p_1 p_2$ with

$$\begin{aligned} p_1 &= 16447689059735824784039, \\ p_2 &= 71003976975490059472571. \end{aligned}$$

For $D_1 = 2^4 p_2^2 D$, and $D_1' = p_1^2 D$, the relation

$$\{\mathfrak{p}_5, \mathfrak{p}_{19}^2, \bar{\mathfrak{p}}_{23}^{210}, \mathfrak{p}_{29}, \mathfrak{p}_{31}, \bar{\mathfrak{p}}_{41}^{145}, \mathfrak{p}_{139}, \bar{\mathfrak{p}}_{149}, \mathfrak{p}_{167}, \bar{\mathfrak{p}}_{191}, \bar{\mathfrak{p}}_{251}^6, \mathfrak{p}_{269}, \bar{\mathfrak{p}}_{587}^7, \bar{\mathfrak{p}}_{643}\}$$

holds in $\mathrm{cl}(D_1)$ but not in $\mathrm{cl}(D_1')$ ($\mathfrak{p}_\ell$ is an ideal of norm ℓ).
For $D_2 = 2^4 p_1^2 D$, and $D_2' = p_2^2 D$, the relation

$$\{\mathfrak{p}_{11}, \bar{\mathfrak{p}}_{13}^{576}, \mathfrak{p}_{23}^2, \bar{\mathfrak{p}}_{41}, \bar{\mathfrak{p}}_{47}, \mathfrak{p}_{83}, \mathfrak{p}_{101}, \bar{\mathfrak{p}}_{197}^{28}, \bar{\mathfrak{p}}_{307}^3, \mathfrak{p}_{317}, \bar{\mathfrak{p}}_{419}, \mathfrak{p}_{911}\}$$

holds in $\mathrm{cl}(D_2)$ but not in $\mathrm{cl}(D_2')$.

Constructing elliptic curves with the CM method

Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D.
The *Hilbert class polynomial* $H_D \in \mathbb{Z}[X]$ is defined by

$$H_D(X) = \prod_{j \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})} (X - j).$$

Equivalently, it is the minimal polynomial of $j(\mathcal{O})$ over $K = \mathbb{Q}(\sqrt{D})$.
The field $K_{\mathcal{O}} = K(j(\mathcal{O}))$ is the *ring class field* for $\mathcal{O}$.

One can also construct supersingular curves with Hilbert class polynomials; see [Bröker 2008].

Constructing elliptic curves with the CM method

Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D.
The *Hilbert class polynomial* $H_D \in \mathbb{Z}[X]$ is defined by

$$H_D(X) = \prod_{j \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})} (X - j).$$

Equivalently, it is the minimal polynomial of $j(\mathcal{O})$ over $K = \mathbb{Q}(\sqrt{D})$.
The field $K_{\mathcal{O}} = K(j(\mathcal{O}))$ is the *ring class field* for $\mathcal{O}$.

If q splits completely in $K_{\mathcal{O}}$, then $H_D(X)$ splits completely in $\mathbb{F}_q[X]$, and every root of H_D is the j-invariant of an elliptic curve $E/\mathbb{F}_q$ with $N = q + 1 - t$ points, where $4q = t^2 - v^2 D$.

Every ordinary elliptic curve $E/\mathbb{F}_q$ can be constructed in this way, but computing H_D becomes quite difficult as $|D|$ grows.

The size of H_D is $O(|D| \log |D|)$ bits, exponential in $\log q$.

One can also construct supersingular curves with Hilbert class polynomials; see [Bröker 2008].

Application: computing Hilbert class polynomials

The CRT approach to computing $H_D(X)$, as described in [Belding-Bröker-Enge-Lauter ANTX VIII] and [S 2011].

1. Select a sufficiently large set of primes of the form $4p = t^2 - v^2 D$.
2. For each prime p, compute $H_D \bmod p$ as follows:
   a. Generate random curves $E/\mathbb{F}_p$ until $\#E = p + 1 - t$.
   b. Use volcano climbing to find $E' \sim E$ with $\mathrm{End}(E') \simeq \mathcal{O}$.
   c. Enumerate $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ by applying the $\mathrm{cl}(\mathcal{O})$-action to $j(E')$.
   d. Compute $\prod_{j \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)}(X - j) = H_D(X) \bmod p$.
3. Use the CRT to recover H_D over $\mathbb{Z}$ (or mod q via the explicit CRT).

Under the GRH, the expected running time is $O(|D| \log^{5+\epsilon} |D|)$, quasi-linear in the size of H_D.

One can similarly compute other types of class polynomials [Enge-S ANTS IX].

Using a polycyclic presentation

For $D = -79447$, $\mathrm{cl}(D)$ is cyclic of order $h(D) = 100$.
It is generated by the class of an ideal $\mathfrak{a}_{19}$ with norm 19.

Using a polycyclic presentation

For $D = -79447$, $\mathrm{cl}(D)$ is cyclic of order $h(D) = 100$.
It is generated by the class of an ideal $\mathfrak{a}_{19}$ with norm 19.

But $\mathrm{cl}(D)$ is also generated by the classes of ideals $\mathfrak{a}_2$ and $\mathfrak{a}_{13}$ with norms 2 and 13. The classes $[\mathfrak{a}_2]$ and $[\mathfrak{a}_{13}]$ have orders 20 and 50 and thus are not independent in $\mathrm{cl}(\mathcal{O})$, in fact $[\mathfrak{a}_{13}]^5 = [\mathfrak{a}_2]^{18}$.

Nevertheless, every element of $\mathrm{cl}(D)$ can uniquely represented as

$$[\mathfrak{a}_2]^{e_2}[\mathfrak{a}_{13}]^{e_{13}},$$

with $0 \le e_2 < 20$ and $0 \le e_{13} < 5$.

In general, any sequence of generators for a finite abelian group G determines a *polycyclic presentation* for G.

Using a polycyclic presentation

For $D = -79447$, $\mathrm{cl}(D)$ is cyclic of order $h(D) = 100$.
It is generated by the class of an ideal $\mathfrak{a}_{19}$ with norm 19.

But $\mathrm{cl}(D)$ is also generated by the classes of ideals $\mathfrak{a}_2$ and $\mathfrak{a}_{13}$ with norms 2 and 13. The classes $[\mathfrak{a}_2]$ and $[\mathfrak{a}_{13}]$ have orders 20 and 50 and thus are not independent in $\mathrm{cl}(\mathcal{O})$, in fact $[\mathfrak{a}_{13}]^5 = [\mathfrak{a}_2]^{18}$.

Nevertheless, every element of $\mathrm{cl}(D)$ can uniquely represented as

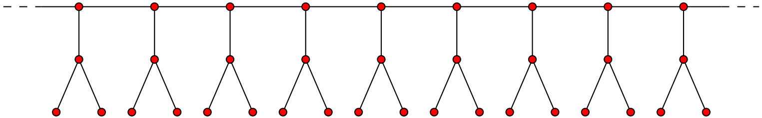
$$[\mathfrak{a}_2]^{e_2}[\mathfrak{a}_{13}]^{e_{13}},$$

with $0 \le e_2 < 20$ and $0 \le e_{13} < 5$.

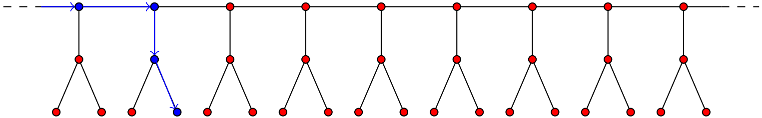
In general, any sequence of generators for a finite abelian group G determines a *polycyclic presentation* for G.

Using the polycyclic presentation $([\mathfrak{a}_2], [\mathfrak{a}_{13}])$ to enumerate $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ is **100 times faster** than using $([\mathfrak{a}_{19}])$.

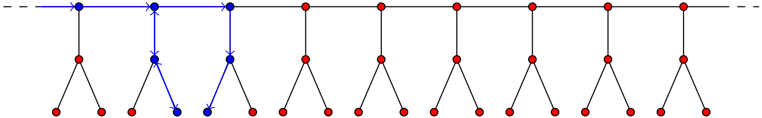
Running the rim



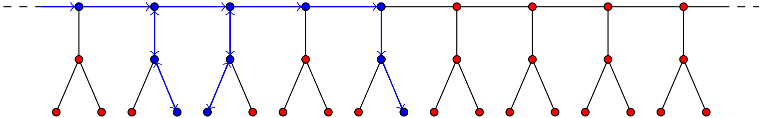
Running the rim



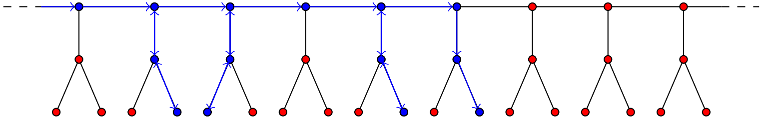
Running the rim



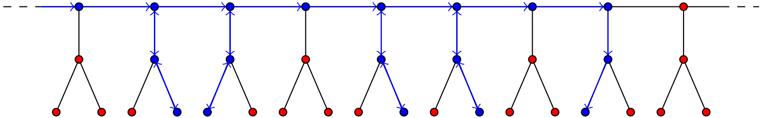
Running the rim



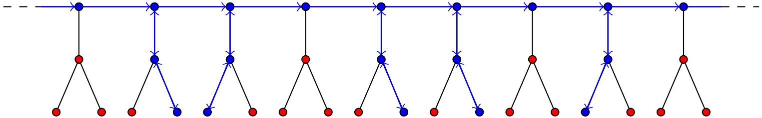
Running the rim



Running the rim



Running the rim



For particularly deep volcanoes, one may prefer to use a pairing-based approach; see [Ionica-Joux ANTS IX].

Computational results

The CRT method has been used to compute $H_D(X)$ with $|D| > 10^{13}$, and using alternative class polynomials, with $|D| > 10^{15}$ (for comparison, the previous record was $|D| \approx 10^{10}$).

When $\mathrm{cl}(\mathcal{O})$ is composite (almost always the case), one can accelerate the CM method by decomposing the ring class field [Hanrot-Morain 2001, Enge-Morain 2003].

Combining this idea with the CRT approach has made CM constructions with $|D| > 10^{16}$ possible [S 2012].

Application: computing modular polynomials

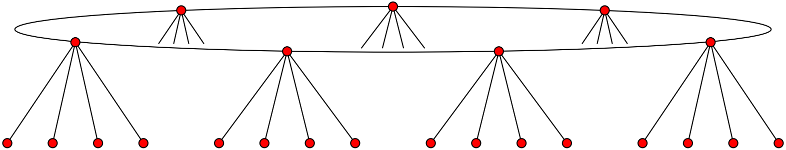
We can also use a CRT approach to compute $\Phi_\ell(X,Y)$ [Bröker-Lauter-S 2012].

1. Select a sufficiently large set of primes of the form $4p = t^2 - \ell^2 v^2 D$ with $\ell \nmid v$, $p \equiv 1 \bmod \ell$, and $h(D) > \ell + 1$.
2. For each prime p, compute $\Phi_\ell \bmod p$ as follows:
   a. Compute $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ using $H_D \bmod p$.
   b. Map the ℓ-volcanoes intersecting $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ (without using Φ_ℓ).
   c. Interpolate $\Phi_\ell(X,Y) \bmod p$.
3. Use the CRT to recover Φ_ℓ over $\mathbb{Z}$ (or mod q via the explicit CRT).

Under the GRH, the expected running time is $O(\ell^3 \log^{3+\epsilon} \ell)$, quasi-linear in the size of Φ_ℓ.

We can similarly compute modular polynomials for other modular functions.
One can also use a CRT approach to compute Φ_N for composite N [Ono-S in prog].

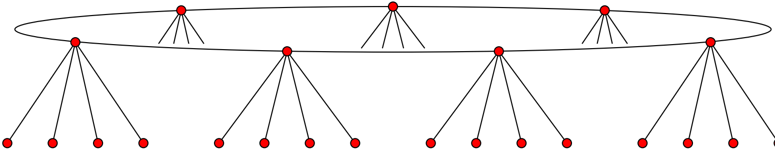
Mapping a volcano



Mapping a volcano

Example
$\ell \;= 5, \quad p = 4451, \quad D = -151$

General requirements
$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$



Mapping a volcano

Example

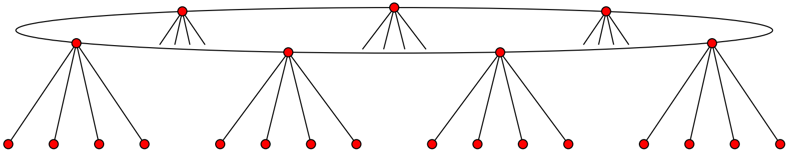
$\ell = 5, \quad p = 4451, \quad D = -151$

$t = 52, \quad v = 2, \quad h(D) = 7$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

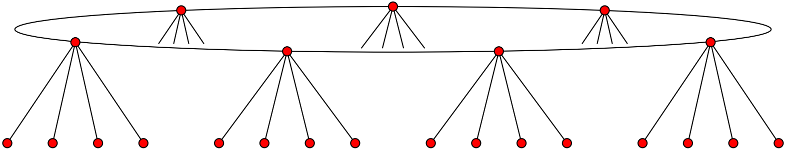
$\ell \nmid v, \quad \left(\frac{D}{\ell}\right) = 1, \quad h(D) \geq \ell + 2$



Mapping a volcano

Example
$\ell \;= 5, \quad p = 4451, \quad D = -151$
$t \;= 52, \quad v = 2, \quad h(D) = 7$

General requirements
$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$
$\ell \nmid v, \quad \left(\frac{D}{\ell}\right) = 1, \quad h(D) \geq \ell + 2$



1. Find a root of $H_D(X)$

Mapping a volcano

Example

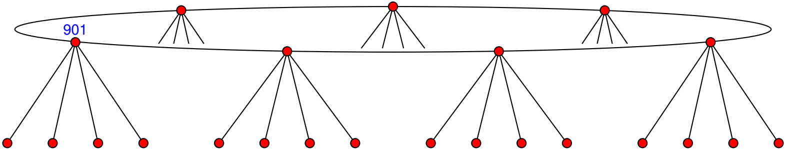
$\ell = 5, \quad p = 4451, \quad D = -151$

$t = 52, \quad v = 2, \quad h(D) = 7$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$



1. Find a root of $H_D(X)$: 901

Mapping a volcano

Example

$\ell = 5, \quad p = 4451, \quad D = -151$

$t = 52, \quad v = 2, \quad h(D) = 7$

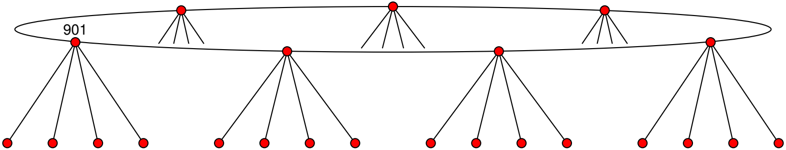
$\ell_0 = 2$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \ (\frac{D}{\ell_0}) = 1$



2. Enumerate surface using the action of α_{ℓ_0}

Mapping a volcano

Example

$\ell = 5, \quad p = 4451, \quad D = -151$

$t = 52, \quad v = 2, \quad h(D) = 7$

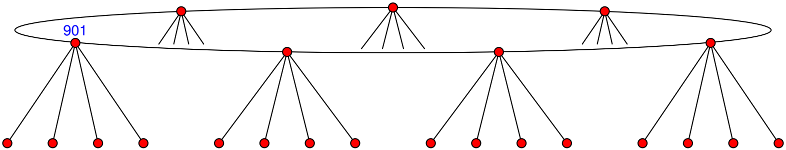
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \ (\frac{D}{\ell_0}) = 1, \ \alpha_\ell = \alpha_{\ell_0}^k$



2. Enumerate surface using the action of α_{ℓ_0}

$901 \xrightarrow{2} 1582 \xrightarrow{2} 2501 \xrightarrow{2} 351 \xrightarrow{2} 701 \xrightarrow{2} 2872 \xrightarrow{2} 2215 \xrightarrow{2}$

Mapping a volcano

Example

$\ell \;= 5, \quad p = 4451, \quad D = -151$

$t \;= 52, \quad v = 2, \quad h(D) = 7$

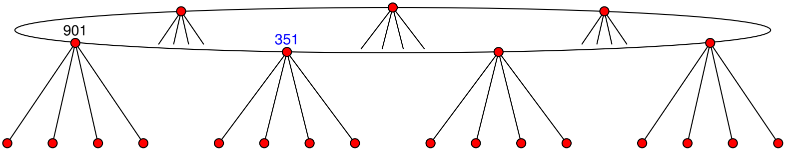
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \; (\frac{D}{\ell_0}) = 1, \; \alpha_\ell = \alpha_{\ell_0}^k$



2. Enumerate surface using the action of α_{ℓ_0}

$901 \xrightarrow{2} 1582 \xrightarrow{2} 2501 \xrightarrow{2} 351 \xrightarrow{2} 701 \xrightarrow{2} 2872 \xrightarrow{2} 2215 \xrightarrow{2}$

Mapping a volcano

Example

$\ell \;= 5, \quad p = 4451, \quad D = -151$

$t \;= 52, \quad v = 2, \quad h(D) = 7$

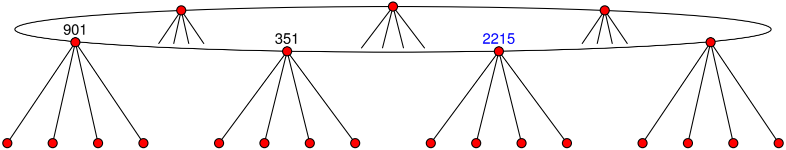
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \ (\frac{D}{\ell_0}) = 1, \ \alpha_\ell = \alpha_{\ell_0}^k$



2. Enumerate surface using the action of α_{ℓ_0}

$901 \xrightarrow{2} 1582 \xrightarrow{2} 2501 \xrightarrow{2} 351 \xrightarrow{2} 701 \xrightarrow{2} 2872 \xrightarrow{2} 2215 \xrightarrow{2}$

Mapping a volcano

Example

$\ell = 5, \quad p = 4451, \quad D = -151$

$t = 52, \quad v = 2, \quad h(D) = 7$

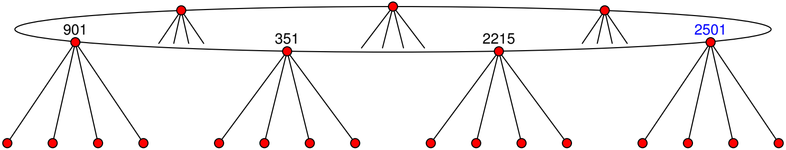
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \ (\frac{D}{\ell_0}) = 1, \ \alpha_\ell = \alpha_{\ell_0}^k$



2. Enumerate surface using the action of α_{ℓ_0}

$901 \xrightarrow{2} 1582 \xrightarrow{2} 2501 \xrightarrow{2} 351 \xrightarrow{2} 701 \xrightarrow{2} 2872 \xrightarrow{2} 2215 \xrightarrow{2}$

Mapping a volcano

Example

$\ell \ = 5, \quad p = 4451, \quad D = -151$

$t \ = 52, \quad v = 2, \quad h(D) = 7$

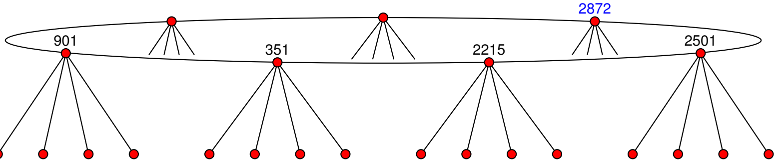
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \ (\frac{D}{\ell_0}) = 1, \ \alpha_\ell = \alpha_{\ell_0}^k$



2. Enumerate surface using the action of α_{ℓ_0}

$901 \xrightarrow{2} 1582 \xrightarrow{2} 2501 \xrightarrow{2} 351 \xrightarrow{2} 701 \xrightarrow{2} 2872 \xrightarrow{2} 2215 \xrightarrow{2}$

Mapping a volcano

Example

$\ell \ = 5, \quad p = 4451, \quad D = -151$

$t \ = 52, \quad v = 2, \quad h(D) = 7$

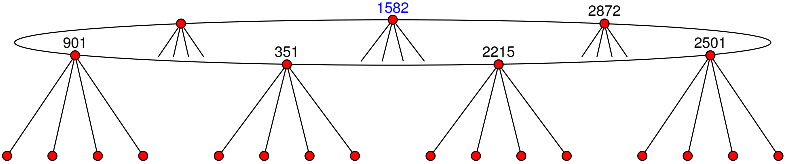
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \ (\frac{D}{\ell_0}) = 1, \ \alpha_\ell = \alpha_{\ell_0}^k$



2. Enumerate surface using the action of α_{ℓ_0}

$901 \xrightarrow{2} 1582 \xrightarrow{2} 2501 \xrightarrow{2} 351 \xrightarrow{2} 701 \xrightarrow{2} 2872 \xrightarrow{2} 2215 \xrightarrow{2}$

Mapping a volcano

Example

$\ell = 5, \quad p = 4451, \quad D = -151$

$t = 52, \quad v = 2, \quad h(D) = 7$

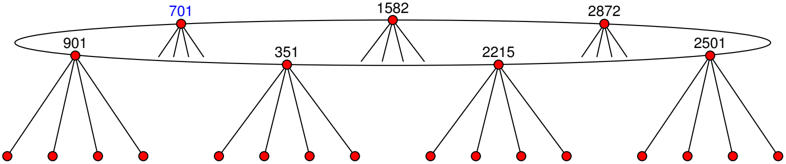
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \ (\frac{D}{\ell_0}) = 1, \ \alpha_\ell = \alpha_{\ell_0}^k$



2. Enumerate surface using the action of α_{ℓ_0}

$901 \xrightarrow{2} 1582 \xrightarrow{2} 2501 \xrightarrow{2} 351 \xrightarrow{2} 701 \xrightarrow{2} 2872 \xrightarrow{2} 2215 \xrightarrow{2}$

Mapping a volcano

Example

$\ell \ = 5, \quad p = 4451, \quad D = -151$

$t \ = 52, \quad v = 2, \quad h(D) = 7$

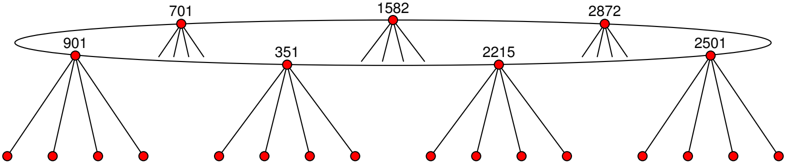
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \ (\frac{D}{\ell_0}) = 1, \ \alpha_\ell = \alpha_{\ell_0}^k$



3. Descend to the floor using Vélu’s formula

Mapping a volcano

Example

$\ell \;= 5, \quad p = 4451, \quad D = -151$

$t \;= 52, \quad v = 2, \quad h(D) = 7$

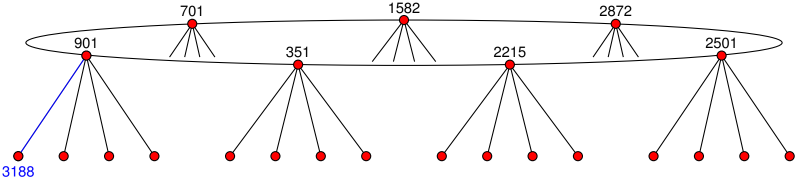
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \; (\frac{D}{\ell_0}) = 1, \; \alpha_\ell = \alpha_{\ell_0}^k$

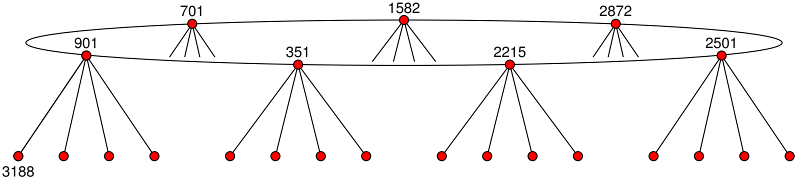


3. Descend to the floor using Vélu's formula: $901 \xrightarrow{5} 3188$

Mapping a volcano

Example
$\ell = 5, \quad p = 4451, \quad D = -151$
$t = 52, \quad v = 2, \quad h(D) = 7$
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements
$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$
$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$
$\ell_0 \neq \ell, \ (\frac{D}{\ell_0}) = 1, \ \alpha_\ell = \alpha_{\ell_0}^k$



4. Enumerate floor using the action of β_{ℓ_0}

Mapping a volcano

Example

$\ell \;= 5, \quad p = 4451, \quad D = -151$

$t \;= 52, \quad v = 2, \quad h(D) = 7$

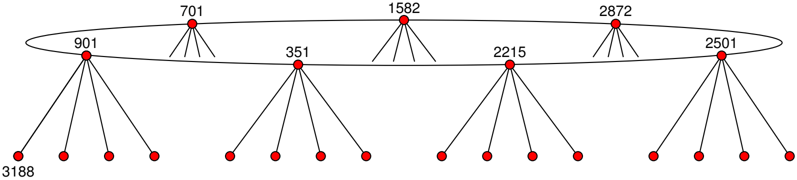
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \; (\frac{D}{\ell_0}) = 1, \; \alpha_\ell = \alpha_{\ell_0}^k, \; \beta_{\ell^2} = \beta_{\ell_0}^{k'}$



4. Enumerate floor using the action of β_{ℓ_0}

$$\begin{array}{l}
3188 \xrightarrow{2} 945 \xrightarrow{2} 3144 \xrightarrow{2} 3508 \xrightarrow{2} 2843 \xrightarrow{2} 1502 \xrightarrow{2} 676 \xrightarrow{2} \\
2970 \xrightarrow{2} 3497 \xrightarrow{2} 1180 \xrightarrow{2} 2464 \xrightarrow{2} 4221 \xrightarrow{2} 4228 \xrightarrow{2} 2434 \xrightarrow{2} \\
1478 \xrightarrow{2} 3244 \xrightarrow{2} 2255 \xrightarrow{2} 2976 \xrightarrow{2} 3345 \xrightarrow{2} 1064 \xrightarrow{2} 1868 \xrightarrow{2} \\
3328 \xrightarrow{2} 291 \xrightarrow{2} 3147 \xrightarrow{2} 2566 \xrightarrow{2} 4397 \xrightarrow{2} 2087 \xrightarrow{2} 3341 \xrightarrow{2}
\end{array}$$

Mapping a volcano

Example

$\ell = 5, \quad p = 4451, \quad D = -151$

$t = 52, \quad v = 2, \quad h(D) = 7$

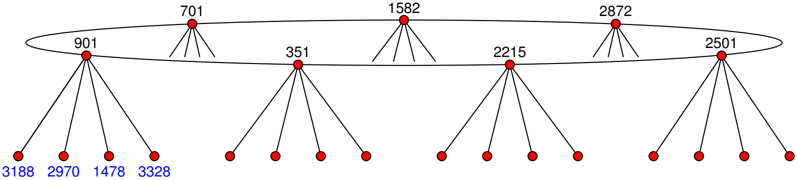
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell,\ (\frac{D}{\ell_0}) = 1,\ \alpha_\ell = \alpha_{\ell_0}^k,\ \beta_{\ell^2} = \beta_{\ell_0}^{k'}$



4. Enumerate floor using the action of β_{ℓ_0}

$$3188 \xrightarrow{2} 945 \xrightarrow{2} 3144 \xrightarrow{2} 3508 \xrightarrow{2} 2843 \xrightarrow{2} 1502 \xrightarrow{2} 676 \xrightarrow{2}$$
$$2970 \xrightarrow{2} 3497 \xrightarrow{2} 1180 \xrightarrow{2} 2464 \xrightarrow{2} 4221 \xrightarrow{2} 4228 \xrightarrow{2} 2434 \xrightarrow{2}$$
$$1478 \xrightarrow{2} 3244 \xrightarrow{2} 2255 \xrightarrow{2} 2976 \xrightarrow{2} 3345 \xrightarrow{2} 1064 \xrightarrow{2} 1868 \xrightarrow{2}$$
$$3328 \xrightarrow{2} 291 \xrightarrow{2} 3147 \xrightarrow{2} 2566 \xrightarrow{2} 4397 \xrightarrow{2} 2087 \xrightarrow{2} 3341 \xrightarrow{2}$$

Mapping a volcano

Example

$\ell = 5, \quad p = 4451, \quad D = -151$

$t = 52, \quad v = 2, \quad h(D) = 7$

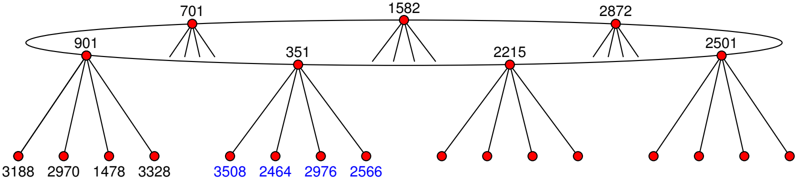
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \ (\frac{D}{\ell_0}) = 1, \ \alpha_\ell = \alpha_{\ell_0}^k, \ \beta_{\ell^2} = \beta_{\ell_0}^{k'}$



4. Enumerate floor using the action of β_{ℓ_0}

$$
\begin{array}{llllllll}
3188 \xrightarrow{2} 945 & \xrightarrow{2} 3144 & \xrightarrow{2} 3508 & \xrightarrow{2} 2843 & \xrightarrow{2} 1502 & \xrightarrow{2} 676 & \xrightarrow{2} \\
2970 \xrightarrow{2} 3497 & \xrightarrow{2} 1180 & \xrightarrow{2} 2464 & \xrightarrow{2} 4221 & \xrightarrow{2} 4228 & \xrightarrow{2} 2434 & \xrightarrow{2} \\
1478 \xrightarrow{2} 3244 & \xrightarrow{2} 2255 & \xrightarrow{2} 2976 & \xrightarrow{2} 3345 & \xrightarrow{2} 1064 & \xrightarrow{2} 1868 & \xrightarrow{2} \\
3328 \xrightarrow{2} 291 & \xrightarrow{2} 3147 & \xrightarrow{2} 2566 & \xrightarrow{2} 4397 & \xrightarrow{2} 2087 & \xrightarrow{2} 3341 & \xrightarrow{2}
\end{array}
$$

Mapping a volcano

Example

$\ell = 5, \quad p = 4451, \quad D = -151$

$t = 52, \quad v = 2, \quad h(D) = 7$

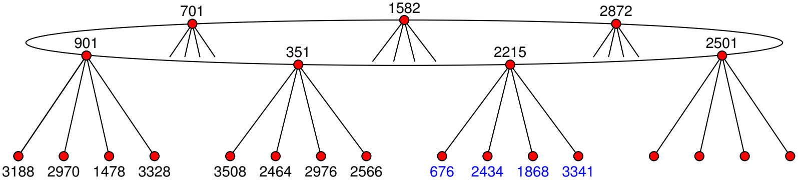
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \ (\frac{D}{\ell_0}) = 1, \ \alpha_\ell = \alpha_{\ell_0}^k, \ \beta_{\ell^2} = \beta_{\ell_0}^{k'}$



4. Enumerate floor using the action of β_{ℓ_0}

$$
\begin{array}{l}
3188 \xrightarrow{2} 945 \xrightarrow{2} 3144 \xrightarrow{2} 3508 \xrightarrow{2} 2843 \xrightarrow{2} 1502 \xrightarrow{2} {\color{blue}676} \xrightarrow{2} \\
2970 \xrightarrow{2} 3497 \xrightarrow{2} 1180 \xrightarrow{2} 2464 \xrightarrow{2} 4221 \xrightarrow{2} 4228 \xrightarrow{2} {\color{blue}2434} \xrightarrow{2} \\
1478 \xrightarrow{2} 3244 \xrightarrow{2} 2255 \xrightarrow{2} 2976 \xrightarrow{2} 3345 \xrightarrow{2} 1064 \xrightarrow{2} {\color{blue}1868} \xrightarrow{2} \\
3328 \xrightarrow{2} 291 \xrightarrow{2} 3147 \xrightarrow{2} 2566 \xrightarrow{2} 4397 \xrightarrow{2} 2087 \xrightarrow{2} {\color{blue}3341} \xrightarrow{2}
\end{array}
$$

Mapping a volcano

Example

$\ell = 5, \quad p = 4451, \quad D = -151$

$t = 52, \quad v = 2, \quad h(D) = 7$

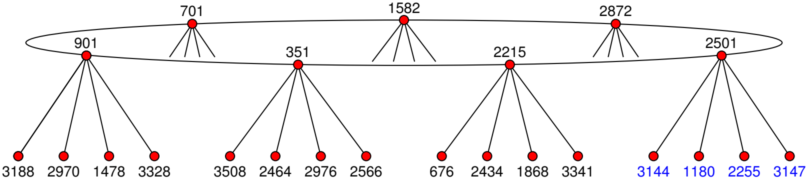
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \ (\frac{D}{\ell_0}) = 1, \ \alpha_\ell = \alpha_{\ell_0}^k, \ \beta_{\ell^2} = \beta_{\ell_0}^{k'}$



4. Enumerate floor using the action of β_{ℓ_0}

$$\begin{array}{lllllll}
3188 \xrightarrow{2} 945 & \xrightarrow{2} 3144 & \xrightarrow{2} 3508 & \xrightarrow{2} 2843 & \xrightarrow{2} 1502 & \xrightarrow{2} 676 & \xrightarrow{2} \\
2970 \xrightarrow{2} 3497 & \xrightarrow{2} 1180 & \xrightarrow{2} 2464 & \xrightarrow{2} 4221 & \xrightarrow{2} 4228 & \xrightarrow{2} 2434 & \xrightarrow{2} \\
1478 \xrightarrow{2} 3244 & \xrightarrow{2} 2255 & \xrightarrow{2} 2976 & \xrightarrow{2} 3345 & \xrightarrow{2} 1064 & \xrightarrow{2} 1868 & \xrightarrow{2} \\
3328 \xrightarrow{2} 291 & \xrightarrow{2} 3147 & \xrightarrow{2} 2566 & \xrightarrow{2} 4397 & \xrightarrow{2} 2087 & \xrightarrow{2} 3341 & \xrightarrow{2}
\end{array}$$

Mapping a volcano

Example

$\ell \;= 5, \quad p = 4451, \quad D = -151$

$t \;= 52, \quad v = 2, \quad h(D) = 7$

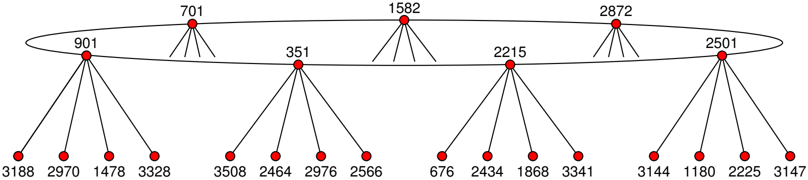
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \; (\frac{D}{\ell_0}) = 1, \; \alpha_\ell = \alpha_{\ell_0}^k, \; \beta_{\ell^2} = \beta_{\ell_0}^{k'}$



4. Enumerate floor using the action of β_{ℓ_0}

$$
\begin{array}{l}
3188 \xrightarrow{2} 945 \xrightarrow{2} 3144 \xrightarrow{2} 3508 \xrightarrow{2} 2843 \xrightarrow{2} \color{blue}{1502} \xrightarrow{2} 676 \xrightarrow{2} \\
2970 \xrightarrow{2} 3497 \xrightarrow{2} 1180 \xrightarrow{2} 2464 \xrightarrow{2} 4221 \xrightarrow{2} \color{blue}{4228} \xrightarrow{2} 2434 \xrightarrow{2} \\
1478 \xrightarrow{2} 3244 \xrightarrow{2} 2255 \xrightarrow{2} 2976 \xrightarrow{2} 3345 \xrightarrow{2} \color{blue}{1064} \xrightarrow{2} 1868 \xrightarrow{2} \\
3328 \xrightarrow{2} 291 \xrightarrow{2} 3147 \xrightarrow{2} 2566 \xrightarrow{2} 4397 \xrightarrow{2} \color{blue}{2087} \xrightarrow{2} 3341 \xrightarrow{2}
\end{array}
$$

Mapping a volcano

Example

$\ell \;= 5, \quad p = 4451, \quad D = -151$

$t \;= 52, \quad v = 2, \quad h(D) = 7$

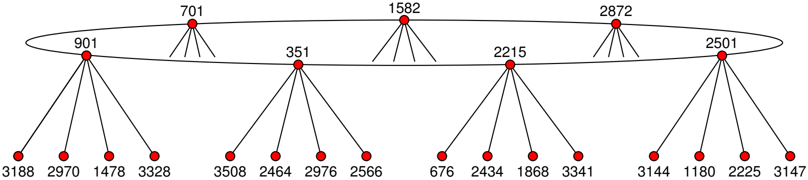
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell,\ (\frac{D}{\ell_0}) = 1,\ \alpha_\ell = \alpha_{\ell_0}^k,\ \beta_{\ell^2} = \beta_{\ell_0}^{k'}$



4. Enumerate floor using the action of β_{ℓ_0}

$$
\begin{array}{lllllllll}
3188 \xrightarrow{2} & {\color{blue}945} \xrightarrow{2} & 3144 \xrightarrow{2} & 3508 \xrightarrow{2} & 2843 \xrightarrow{2} & 1502 \xrightarrow{2} & 676 \xrightarrow{2} \\
2970 \xrightarrow{2} & {\color{blue}3497} \xrightarrow{2} & 1180 \xrightarrow{2} & 2464 \xrightarrow{2} & 4221 \xrightarrow{2} & 4228 \xrightarrow{2} & 2434 \xrightarrow{2} \\
1478 \xrightarrow{2} & {\color{blue}3244} \xrightarrow{2} & 2255 \xrightarrow{2} & 2976 \xrightarrow{2} & 3345 \xrightarrow{2} & 1064 \xrightarrow{2} & 1868 \xrightarrow{2} \\
3328 \xrightarrow{2} & {\color{blue}291} \xrightarrow{2} & 3147 \xrightarrow{2} & 2566 \xrightarrow{2} & 4397 \xrightarrow{2} & 2087 \xrightarrow{2} & 3341 \xrightarrow{2}
\end{array}
$$

Mapping a volcano

Example

$\ell = 5, \quad p = 4451, \quad D = -151$

$t = 52, \quad v = 2, \quad h(D) = 7$

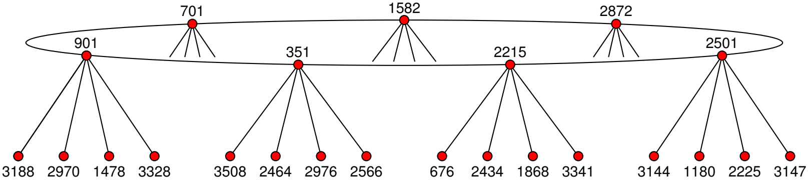
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \; (\frac{D}{\ell_0}) = 1, \; \alpha_\ell = \alpha_{\ell_0}^k, \; \beta_{\ell^2} = \beta_{\ell_0}^{k'}$



4. Enumerate floor using the action of β_{ℓ_0}

$$
\begin{array}{l}
3188 \xrightarrow{2} 945 \xrightarrow{2} 3144 \xrightarrow{2} 3508 \xrightarrow{2} 2843 \xrightarrow{2} 1502 \xrightarrow{2} 676 \xrightarrow{2} \\
2970 \xrightarrow{2} 3497 \xrightarrow{2} 1180 \xrightarrow{2} 2464 \xrightarrow{2} 4221 \xrightarrow{2} 4228 \xrightarrow{2} 2434 \xrightarrow{2} \\
1478 \xrightarrow{2} 3244 \xrightarrow{2} 2255 \xrightarrow{2} 2976 \xrightarrow{2} 3345 \xrightarrow{2} 1064 \xrightarrow{2} 1868 \xrightarrow{2} \\
3328 \xrightarrow{2} 291 \xrightarrow{2} 3147 \xrightarrow{2} 2566 \xrightarrow{2} 4397 \xrightarrow{2} 2087 \xrightarrow{2} 3341 \xrightarrow{2}
\end{array}
$$

Mapping a volcano

Example

$\ell \; = 5, \quad p = 4451, \quad D = -151$

$t \; = 52, \quad v = 2, \quad h(D) = 7$

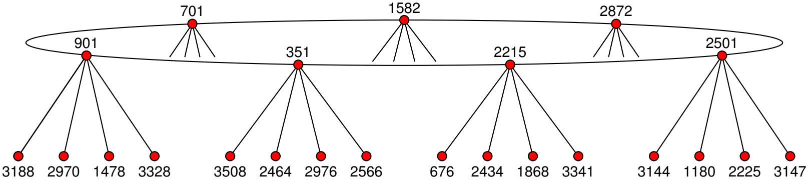
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

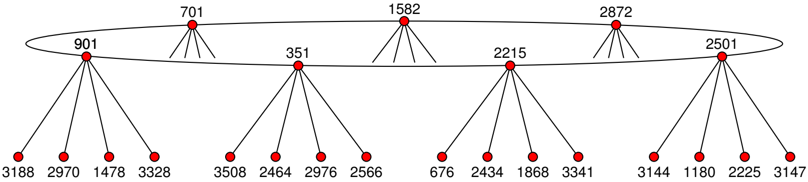
$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

$\ell \nmid v, \quad \left(\frac{D}{\ell}\right) = 1, \quad h(D) \geq \ell + 2$

$\ell_0 \neq \ell, \; \left(\frac{D}{\ell_0}\right) = 1, \; \alpha_\ell = \alpha_{\ell_0}^k, \; \beta_{\ell^2} = \beta_{\ell_0}^{k'}$

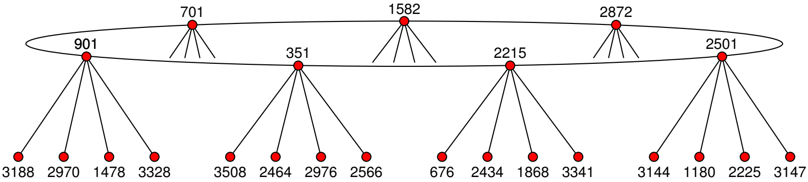


Interpolating $\Phi_\ell \bmod p$



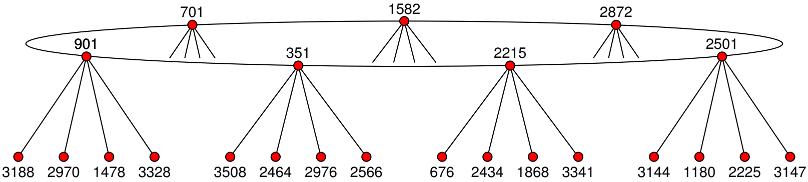
$$
\begin{aligned}
\Phi_5(X, 901) &= (X-701)(X-351)(X-3188)(X-2970)(X-1478)(X-3328)\\
\Phi_5(X, 351) &= (X-901)(X-2215)(X-3508)(X-2464)(X-2976)(X-2566)\\
\Phi_5(X, 2215) &= (X-351)(X-2501)(X-3341)(X-1868)(X-2434)(X-676)\\
\Phi_5(X, 2501) &= (X-2215)(X-2872)(X-3147)(X-2255)(X-1180)(X-3144)\\
\Phi_5(X, 2872) &= (X-2501)(X-1582)(X-1502)(X-4228)(X-1064)(X-2087)\\
\Phi_5(X, 1582) &= (X-2872)(X-701)(X-945)(X-3497)(X-3244)(X-291)\\
\Phi_5(X, 701) &= (X-1582)(X-901)(X-2843)(X-4221)(X-3345)(X-4397)
\end{aligned}
$$

Interpolating $\Phi_\ell \bmod p$



$$
\begin{aligned}
\Phi_5(X,\ 901) &= X^6 + 1337X^5 + 543X^4 + 497X^3 + 4391X^2 + 3144X + 3262\\
\Phi_5(X,\ 351) &= X^6 + 3174X^5 + 1789X^4 + 3373X^3 + 3972X^2 + 2932X + 4019\\
\Phi_5(X, 2215) &= X^6 + 2182X^5 + 512X^4 + 435X^3 + 2844X^2 + 2084X + 2709\\
\Phi_5(X, 2501) &= X^6 + 2991X^5 + 3075X^5 + 3918X^3 + 2241X^2 + 3755X + 1157\\
\Phi_5(X, 2872) &= X^6 + 389X^5 + 3292X^4 + 3909X^3 + 161X^2 + 1003X + 2091\\
\Phi_5(X, 1582) &= X^6 + 1803X^5 + 794X^4 + 3584X^3 + 225X^2 + 1530X + 1975\\
\Phi_5(X,\ 701) &= X^6 + 515X^5 + 1419X^4 + 941X^3 + 4145X^2 + 2722X + 2754
\end{aligned}
$$

Interpolating $\Phi_\ell \bmod p$



$$
\begin{aligned}
\Phi_5(X,Y) = X^6 + {} & (4450Y^5 + 3720Y^4 + 2433Y^3 + 3499Y^2 + 70Y + 3927)X^5 \\
& (3720Y^5 + 3683Y^4 + 2348Y^3 + 2808Y^2 + 3745Y + 233)X^4 \\
& (2433Y^5 + 2348Y^4 + 2028Y^3 + 2025Y^2 + 4006Y + 2211)X^3 \\
& (3499Y^5 + 2808Y^4 + 2025Y^3 + 4378Y^2 + 3886Y + 2050)X^2 \\
& (70Y^5 + 3745Y^4 + 4006Y^3 + 3886Y^2 + 905Y + 2091)X \\
& (Y^6 + 3927Y^5 + 233Y^4 + 2211Y^3 + 2050Y^2 + 2091Y + 2108)
\end{aligned}
$$

Computational results

Level records

1. **10009**: Φ_ℓ
2. **20011**: $\Phi_\ell \bmod q$
3. **60013**: $\Phi_\ell^{\mathfrak{f}}$

Speed records

1. **251**: Φ_ℓ in 28s $\Phi_\ell \bmod q$ in 4.8s (vs 688s)
2. **1009**: Φ_ℓ in 2830s $\Phi_\ell \bmod q$ in 265s (vs 107200s)
3. **1009**: $\Phi_\ell^{\mathfrak{f}}$ in 2.8s

Effective throughput when computing $\Phi_{1009} \bmod q$ is 100Mb/s.

Single core CPU times (AMD 3.0 GHz), using prime $q \approx 2^{256}$.
Polynomials $\Phi_\ell^{\mathfrak{f}}$ for $\ell < 5000$ available at `http://math.mit.edu/~drew`.