On the evaluation of modular polynomials

Andrew V. Sutherland

Massachusetts Institute of Technology

ECC 2012

http://arxiv.org/abs/1202.3985
http://arxiv.org/abs/1208.5370

A brief journey through space-time...

Space and time

In a universe with n dimensions, the amount of data that can be stored within a distance r of the CPU is $O(r^n)$.

An algorithm with space complexity S is at an average distance $\Omega(S^{1/n})$ from its data. The speed of light is bounded by a constant, thus the time to read or write a bit located at a distance r is $\Omega(r)$.

Conclusion: space complexity $S \implies$ time complexity $\Omega(S^{1+1/n})$.

Space and time

In a universe with n dimensions, the amount of data that can be stored within a distance r of the CPU is $O(r^n)$.

An algorithm with space complexity S is at an average distance $\Omega(S^{1/n})$ from its data. The speed of light is bounded by a constant, thus the time to read or write a bit located at a distance r is $\Omega(r)$.

Conclusion: space complexity $S \implies$ time complexity $\Omega(S^{1+1/n})$.

The RAM model permits algorithms with quasi-linear space and time complexity, but these complexities cannot be realized in practice.

If we are given an algorithm whose theoretical space and time complexity are quasi-linear, reducing the space complexity will speed up the real-world running time of the algorithm, often dramatically.

Isogenies of elliptic curves

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

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

The induced homomorphism $\phi\colon E_1(\bar{k}) \to E_2(\bar{k})$ has a finite kernel. Conversely, 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 nonzero *separable* isogenies, $\deg \phi = |\ker \phi|$.

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

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 $j \notin \{0, 1728\}$, we have $j = j(A,B)$, where

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

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

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 $E_\tau/\mathbb{C}$ and $E_{\ell\tau}/\mathbb{C}$ that are ℓ-isogenous.

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

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 whose characteristic is not equal to ℓ.

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

Isogenies make hard problems easier

Isogenies play a key role in many applications:

- The Schoof-Elkies-Atkin (SEA) point-counting algorithm.
- Computing the endomorphism ring of an elliptic curve.
- The elliptic curve discrete logarithm problem (?).
- Computing Hilbert class polynomials $H_D(X)$.
- Computing modular polynomials.

Isogenies make hard problems easier

Isogenies play a key role in many applications:

- The Schoof-Elkies-Atkin (SEA) point-counting algorithm.
- Computing the endomorphism ring of an elliptic curve.
- The elliptic curve discrete logarithm problem (?).
- Computing Hilbert class polynomials $H_D(X)$.
- Computing modular polynomials.

Modular polynomials $\Phi_\ell(X, Y)$ are used in all of these applications.

Given an elliptic curve E/F, the roots of the univariate polynomial

$$\phi_\ell(Y) = \Phi_\ell(j(E), Y) \in F[Y]$$

that lie in F are precisely the j-invariants of the elliptic curves $\tilde{E}/F$ that are ℓ-isogenous to E.

Modular polynomials are very large...

$\Phi_\ell \in \mathbb{Z}[X, Y]$ is symmetric, with degree $\ell + 1$ in both X and Y.
Asymptotically, its size is $O(\ell^3 \log \ell)$ bits.

ℓ	coefficients	largest	average	total
127	8258	7.5kb	5.3kb	5.5MB
251	31880	16kb	12kb	48MB
503	127262	36kb	27kb	431MB
1009	510557	78kb	60kb	3.9GB
2003	2009012	166kb	132kb	33GB
3001	4507505	259kb	208kb	117GB
4001	8010005	356kb	287kb	287GB
5003	12522512	454kb	369kb	577GB
10007	50085038	968kb	774kb	4.8TB

Size of $\Phi_\ell(X, Y)$

. . . but instantiated modular polynomials are not.

For an elliptic curve E over a finite field $\mathbb{F}_q$, the size of the instantiated polynomial $\phi_\ell(Y) = \Phi_\ell(j(E), Y)$ is only $O(\ell \log q)$ bits.

Even if q is quite large, say 4096 bits, for $\ell = 10007$ the size of $\phi_\ell(Y)$ is just 5MB, which is almost a million times smaller than $\Phi_\ell(X, Y)$.

. . . but instantiated modular polynomials are not.

For an elliptic curve E over a finite field $\mathbb{F}_q$, the size of the instantiated polynomial $\phi_\ell(Y) = \Phi_\ell(j(E), Y)$ is only $O(\ell \log q)$ bits.

Even if q is quite large, say 4096 bits, for $\ell = 10007$ the size of $\phi_\ell(Y)$ is just 5MB, which is almost a million times smaller than $\Phi_\ell(X, Y)$.

A quote from the former elliptic curve point-counting world record holder (at 2500 decimal digits):

"Despite this progress, computing modular polynomials remains the stumbling block for new point counting records. Clearly, to circumvent the memory problems, one would need an algorithm that directly obtains the polynomial specialised in one variable."

INRIA Project TANC, 2007

Results

Let $E/\mathbb{F}_q$ be an elliptic curve and let $\ell < q$ be a prime $(\ell \neq \text{char } \mathbb{F}_q)$.

Theorem

Under the generalized Riemann hypothesis (GRH), one can compute the instantiated modular polynomial $\Phi_\ell(j(E), Y)$ using $O(\ell \log q)$ space in time quasi-linear in the size of Φ_ℓ (quasi-cubic in ℓ).

Results

Let $E/\mathbb{F}_q$ be an elliptic curve and let $\ell < q$ be a prime $(\ell \neq \operatorname{char} \mathbb{F}_q)$.

Theorem
Under the generalized Riemann hypothesis (GRH), one can compute the instantiated modular polynomial $\Phi_\ell(j(E), Y)$ using $O(\ell \log q)$ space in time quasi-linear in the size of Φ_ℓ (quasi-cubic in ℓ).

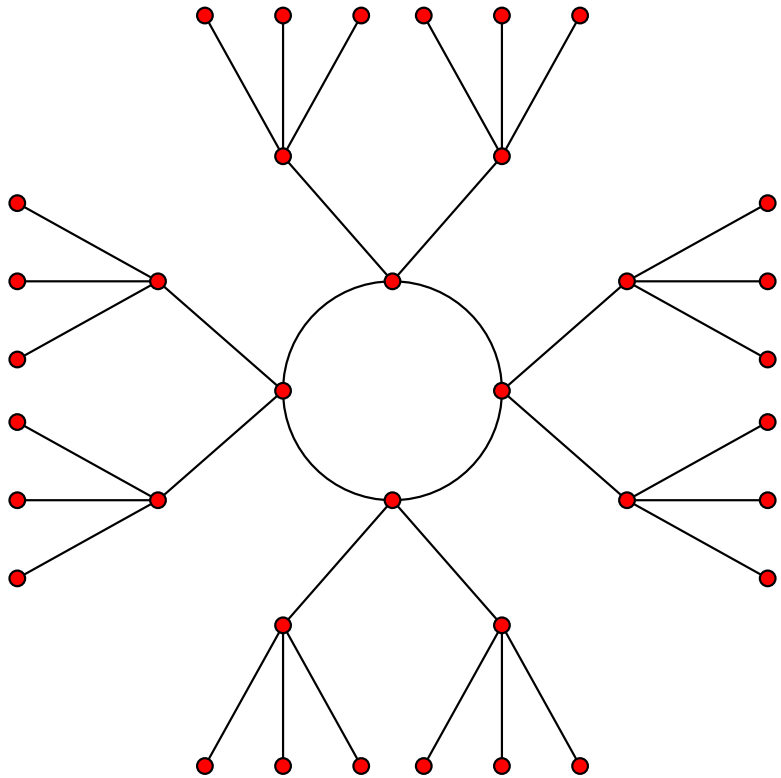
Applying this to SEA, we can compute $\#E(\mathbb{F}_q)$ in $\tilde{O}(n^4)$ time and $O(n^2 \log n)$ space $(n = \log q)$, under standard heuristic assumptions. Previously, the SEA algorithm required $\Omega(n^3 \log n)$ space (or $\Omega(n^4)$ if precomputed modular polynomials are used).

This has led to a new elliptic curve point-counting record modulo a 5011-digit prime (and improvements in the range of practical interest).

The new results also yield improved space complexity bounds (and better performance) for many other algorithms that use isogenies.

A volcano

A volcano



ℓ-volcanoes

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

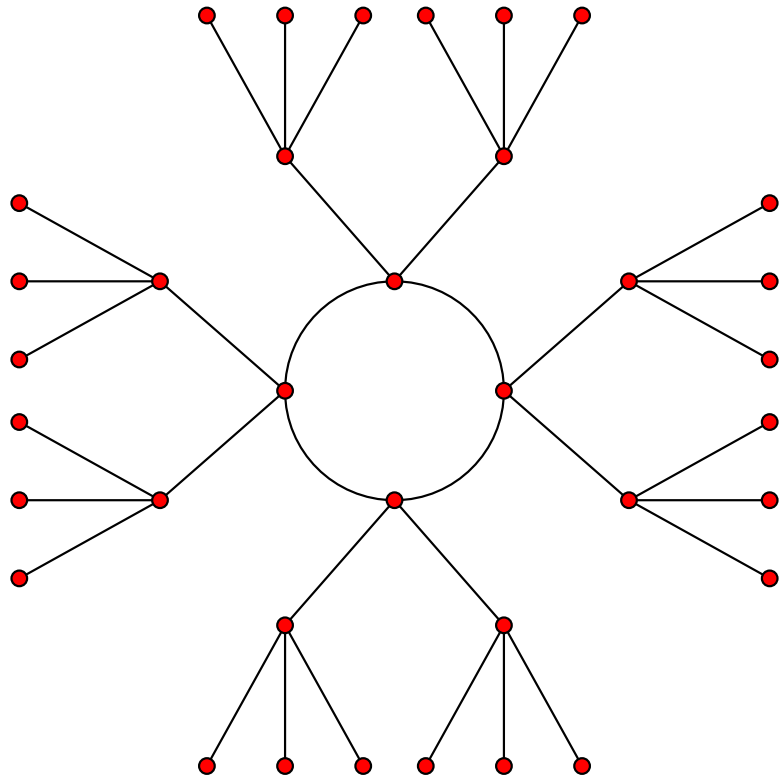
1. The subgraph on V_0 (the *surface*) is a connected regular graph of degree $0, 1$, or 2.

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, but this can happen only on the surface.

A 3-volcano of depth 2



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.

It consists of *ordinary* and *supersingular* components.

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

An elliptic curve E over a field of characteristic $p > 0$ is supersingular iff $E[p] = \{0\}$.

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:

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

In characteristic $p > 0$, every elliptic curve has CM, since the p-power Frobenius endomorphism $(x, y) \mapsto (x^p, y^p)$ 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 CM by an imaginary quadratic order $\mathcal{O}$.

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 $\varphi_{\mathfrak{a}} : E \to E'$ 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].

Isogeny volcanoes

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 $D = \mathrm{disc}(\mathcal{O}_0)$.*

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

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

The term *volcano* is due to Fouquet and Morain (ANTS V).
See `http://arxiv.org/abs/1208.5370` for more on isogeny volcanoes.

Modular polynomials via isogeny volcanoes [BLS]

Given an odd prime ℓ, we may compute $\Phi_\ell(X,Y)$ as follows:

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 $\Phi_\ell(X,Y) \bmod p$ as follows:
   a. Compute $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ using $H_D(X) \bmod p$.
   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 $O(\ell^3 \log^{3+\epsilon} \ell)$ using $O(\ell^3 \log \ell)$ space (or $O(\ell^2 \log q)$ space to compute $\Phi_\ell \bmod q$).

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].

Explicit Chinese Remainder Theorem

Suppose $c \equiv c_i \bmod p_i$ for k distinct primes p_i. Then

$$c \equiv \sum c_i a_i M_i \bmod M,$$

where $M = \prod p_i$, $M_i = M/p_i$ and $a_i = 1/M_i \bmod p_i$.
If $M > 2|c|$, we can recover $c \in \mathbb{Z}$.

With $M > 4|c|$, the explicit CRT computes $c \bmod q$ directly via

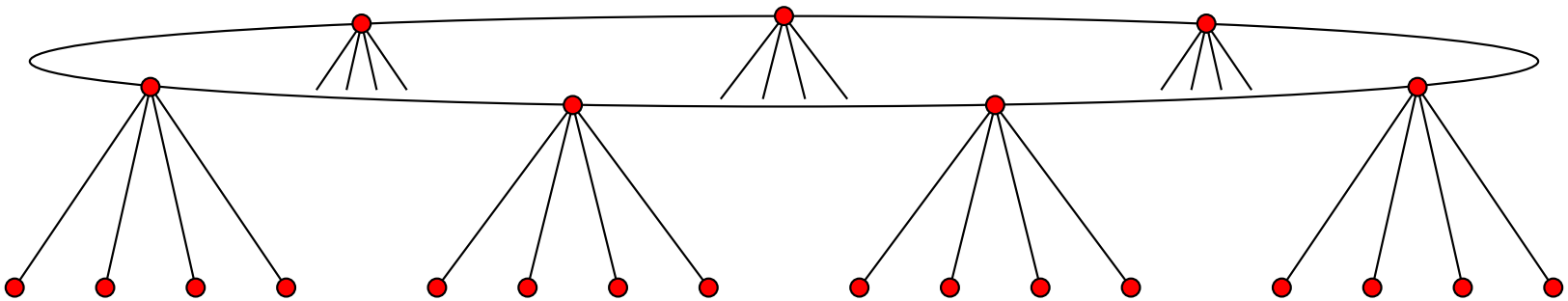
$$c = \left(\sum c_i a_i M_i - rM\right) \bmod q,$$

where $r = \mathrm{rnd}(\sum a_i c_i / p_i)$ is computed using $O(\log k)$ bits of precision.

Using an online algorithm, this can be applied to N coefficients c in parallel, using $O(\log M + k \log q + N(\log q + \log k)) \approx O(N \log q)$ space.

Montgomery-Silverman 1990, Bernstein 1995, S 2011.

Mapping a volcano



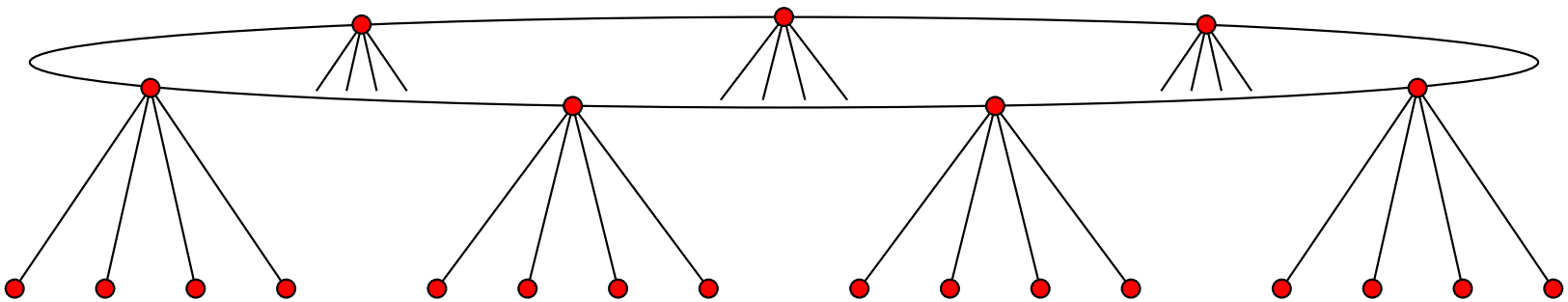
Mapping a volcano

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

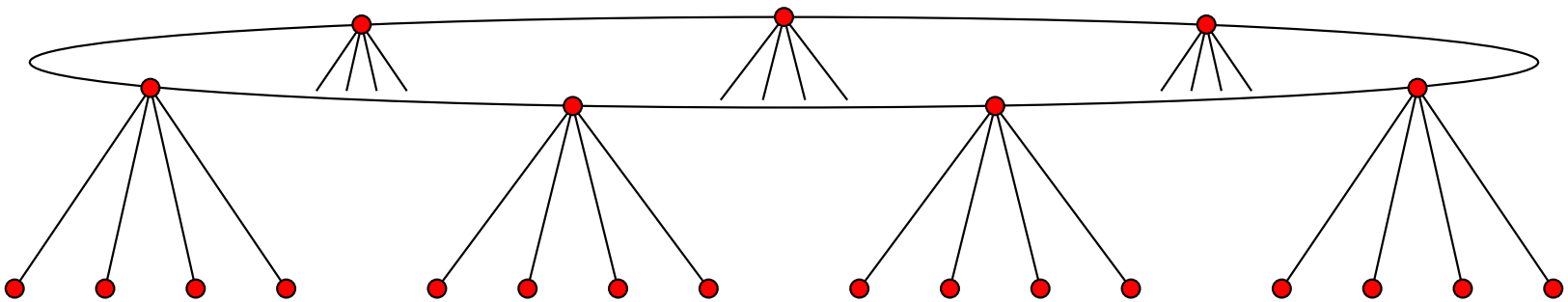
$\ell = 5, \quad p = 4451, \quad D = -151$

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

General requirements

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

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



Mapping a volcano

Example

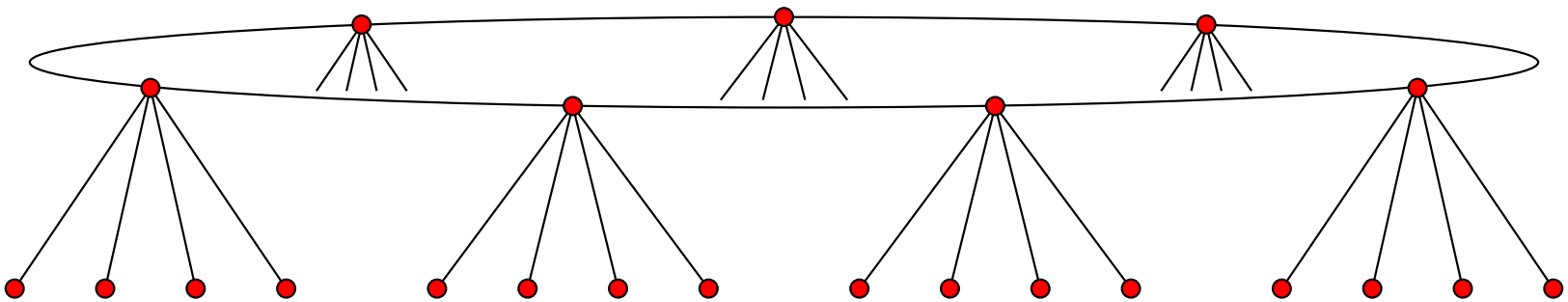
$\ell = 5, \quad p = 4451, \quad D = -151$

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

General requirements

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

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



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

Mapping a volcano

Example

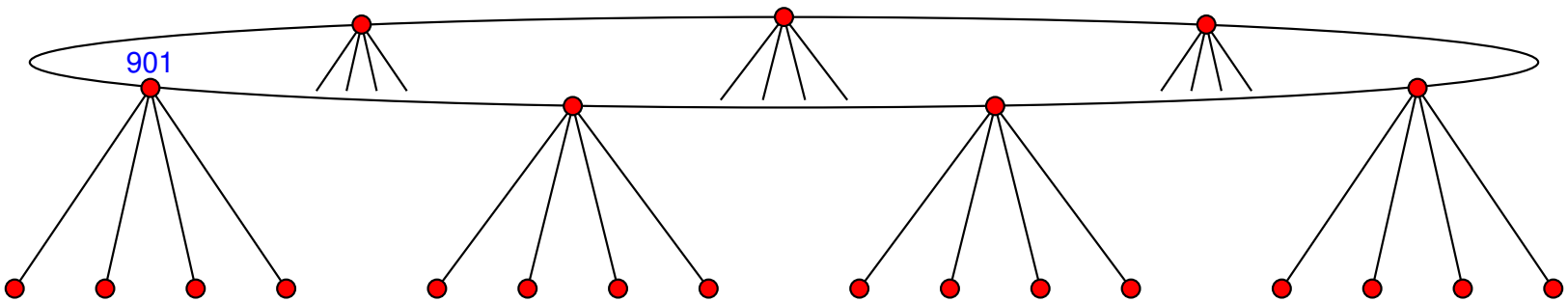
$\ell = 5, \quad p = 4451, \quad D = -151$

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

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

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

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

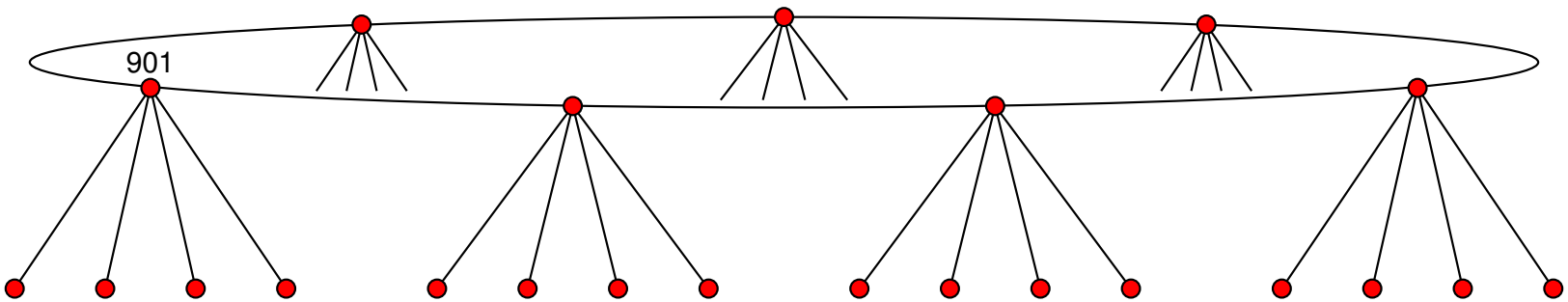
$\ell_0 = 2$

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

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

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

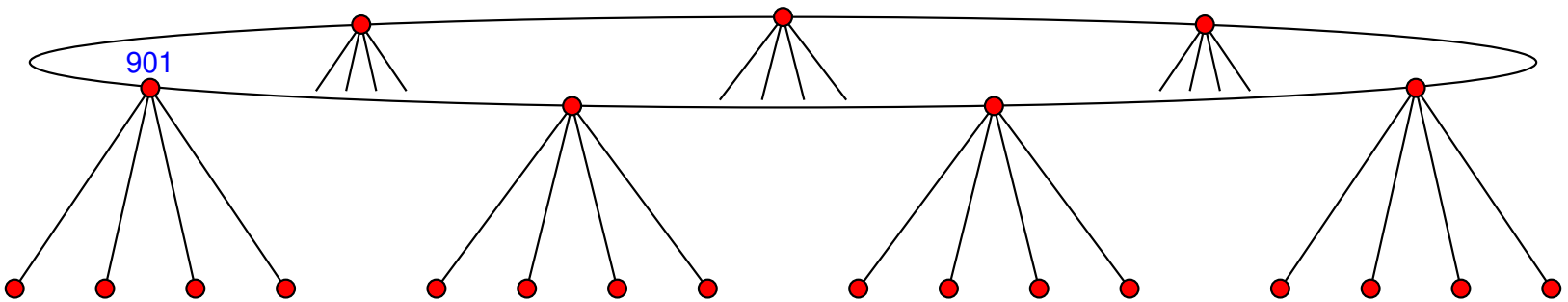
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

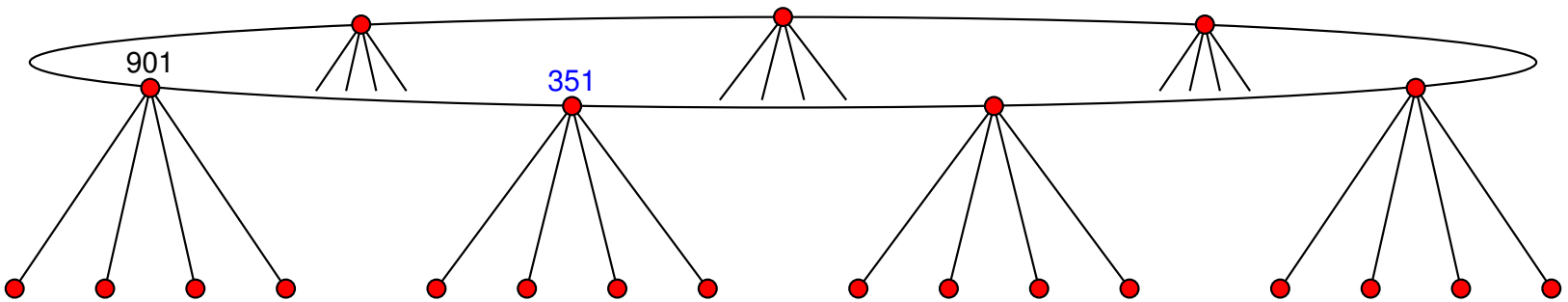
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

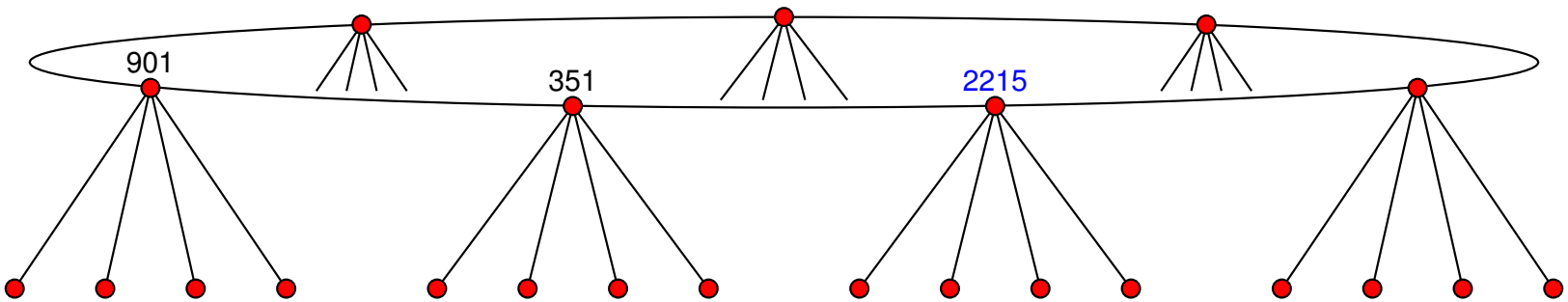
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

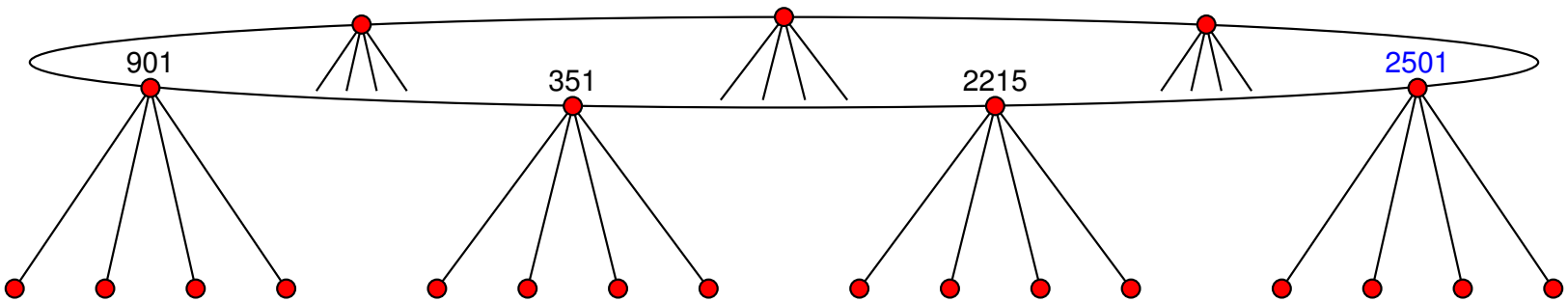
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

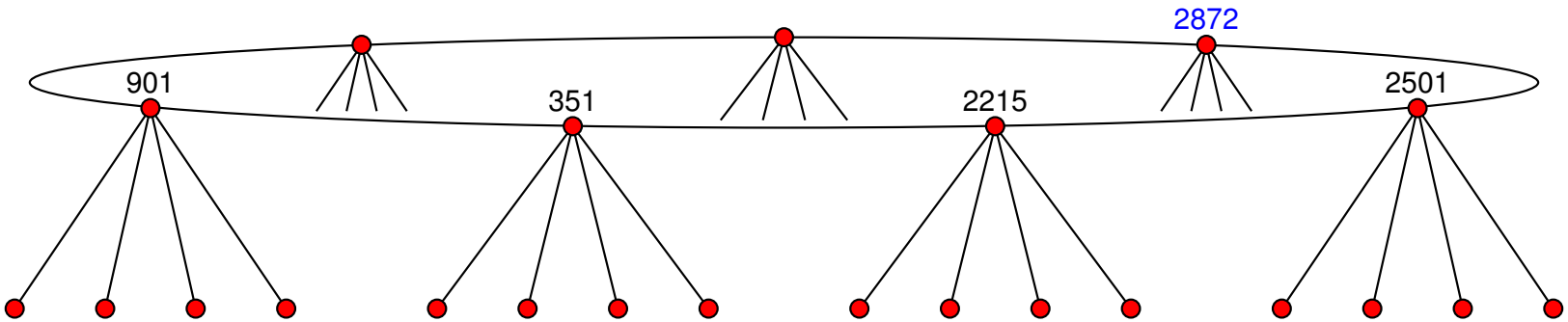
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

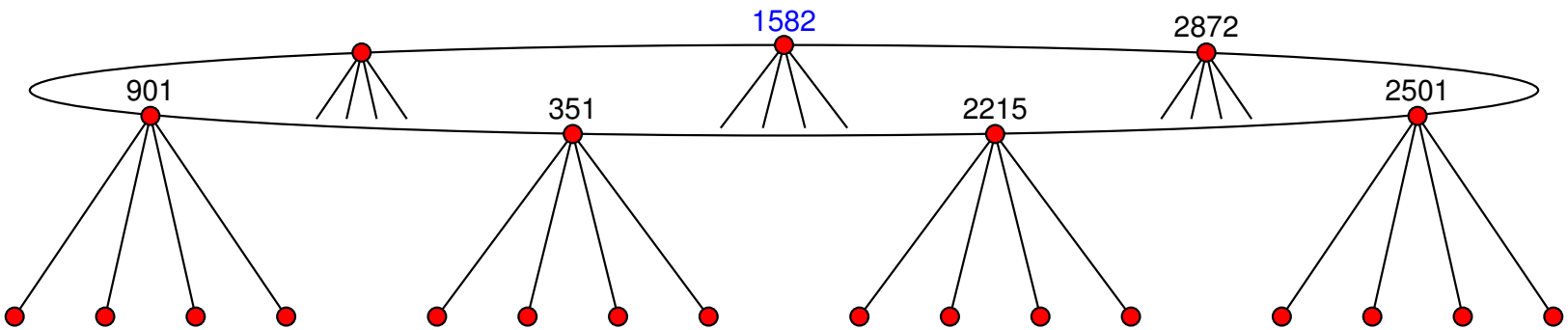
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

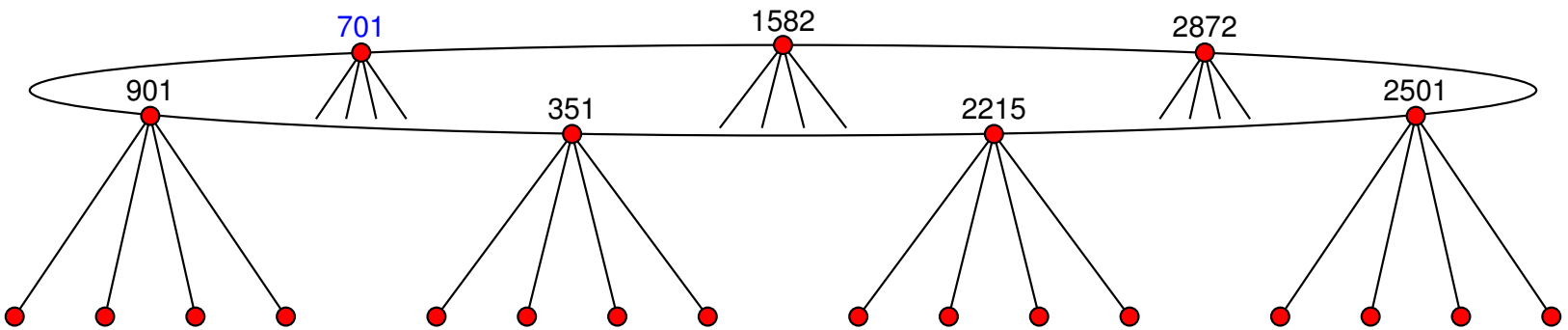
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

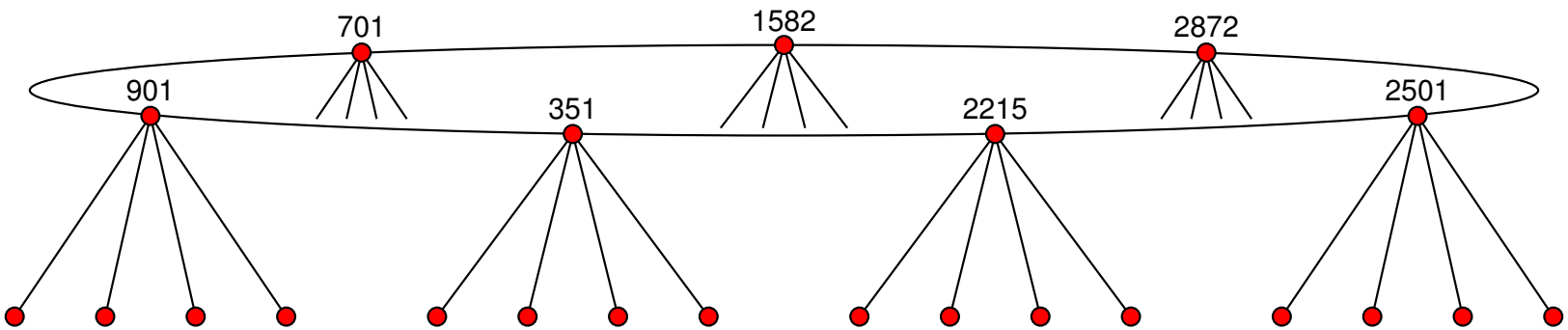
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

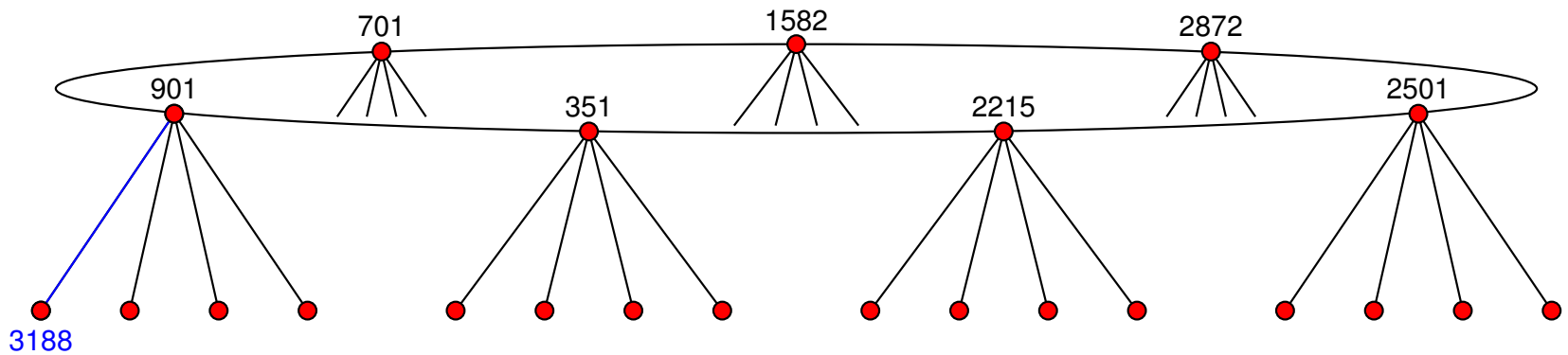
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

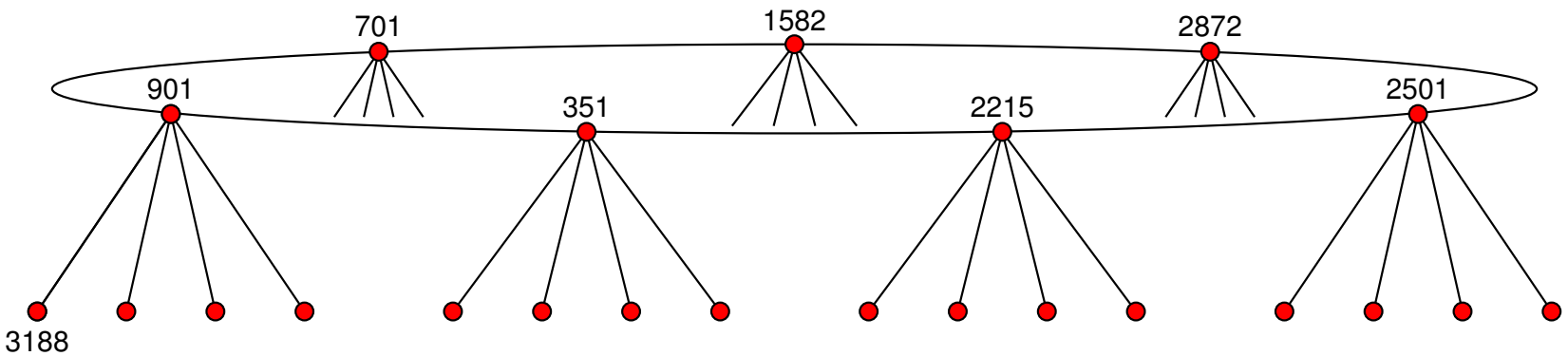
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

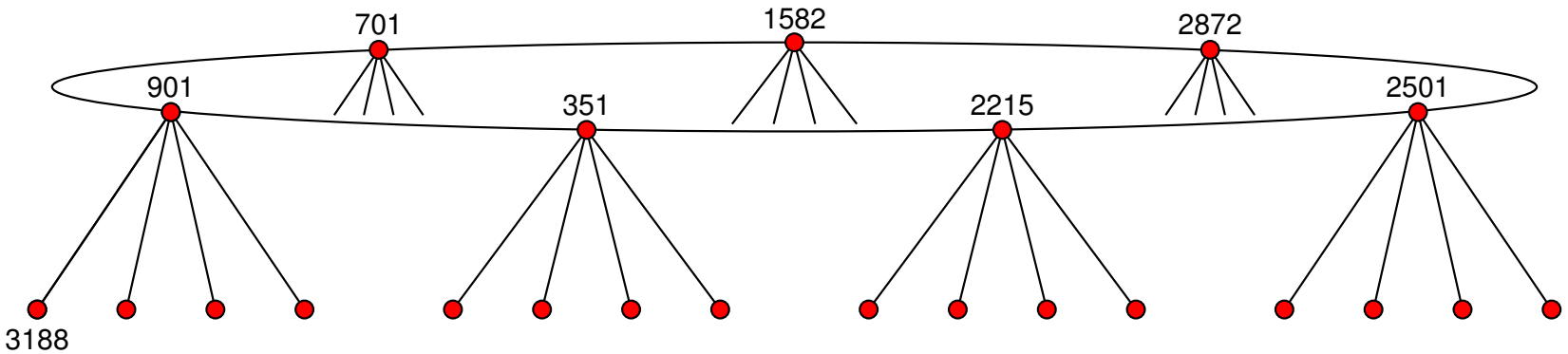
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

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

Mapping a volcano

Example

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

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

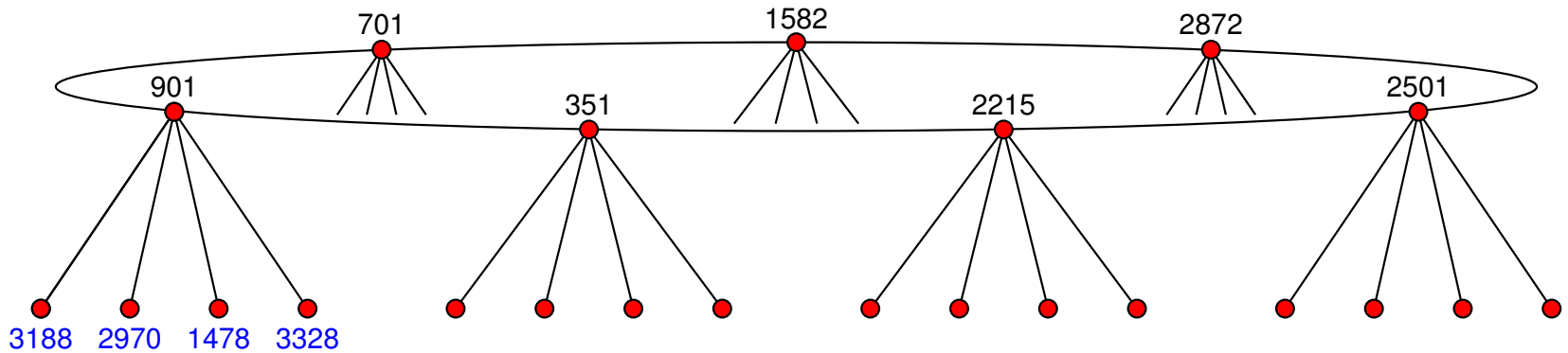
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

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

Mapping a volcano

Example

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

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

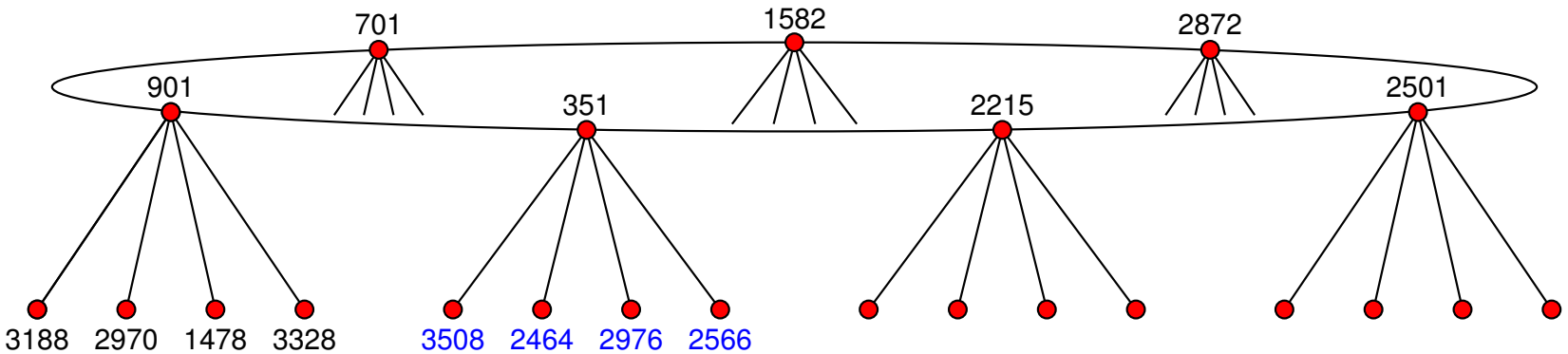
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

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

Mapping a volcano

Example

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

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

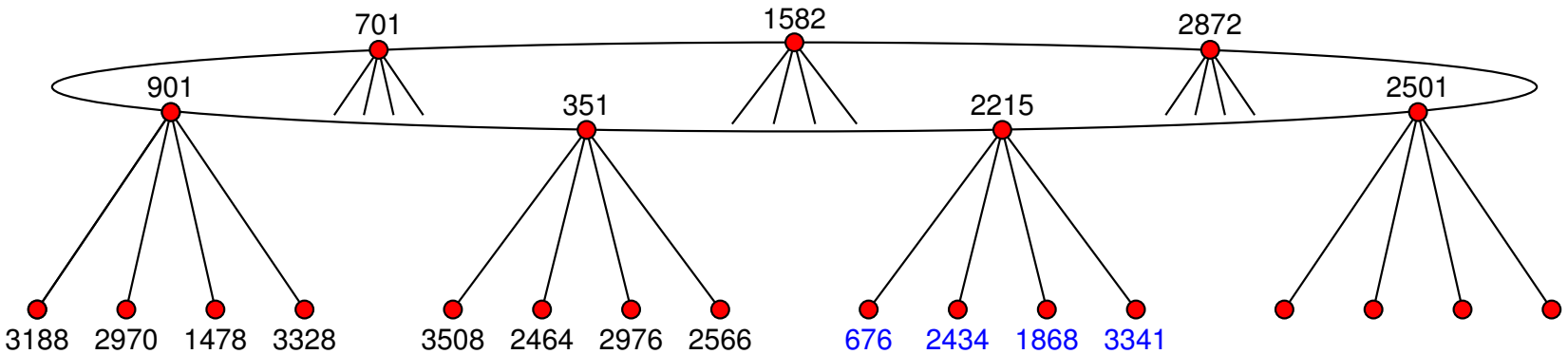
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

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

Mapping a volcano

Example

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

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

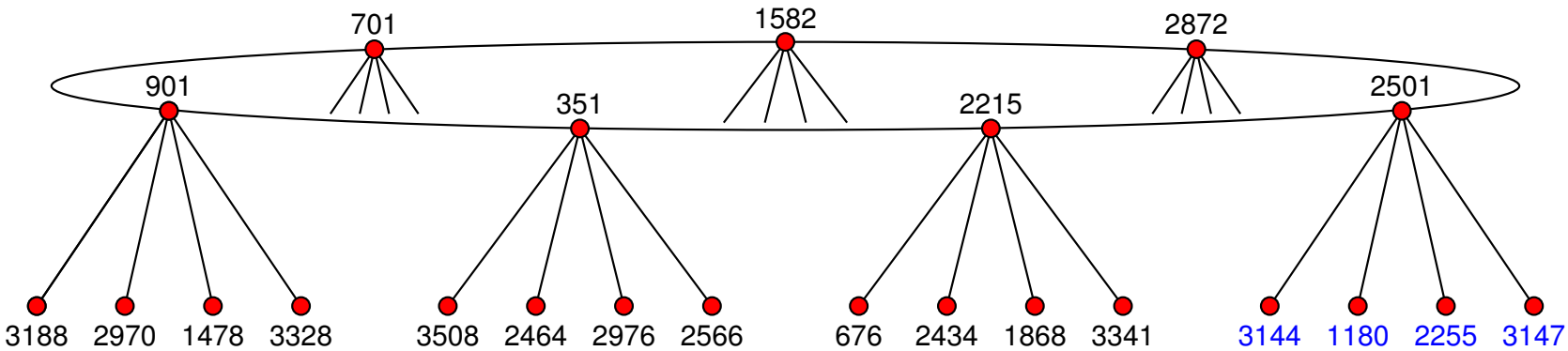
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

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

Mapping a volcano

Example

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

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

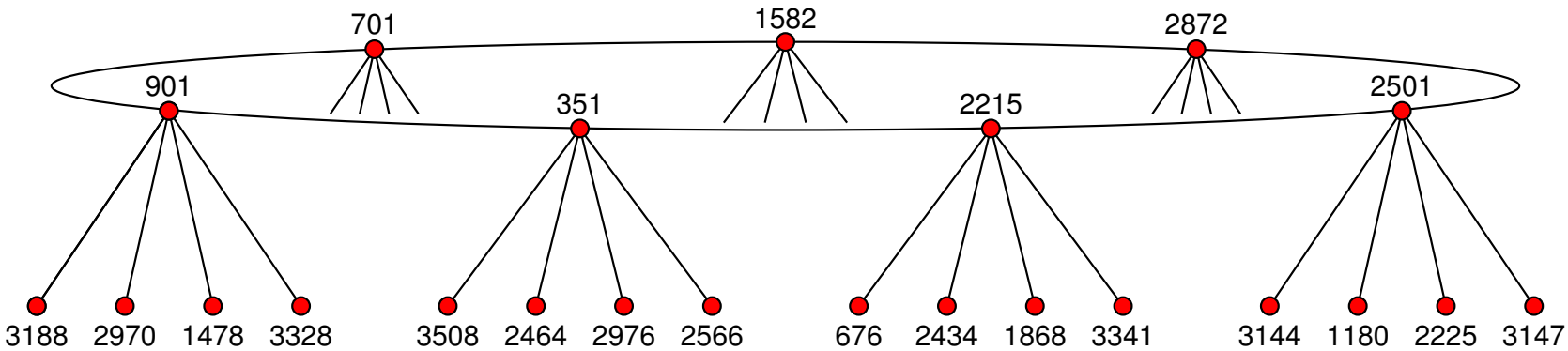
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

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

Mapping a volcano

Example

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

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

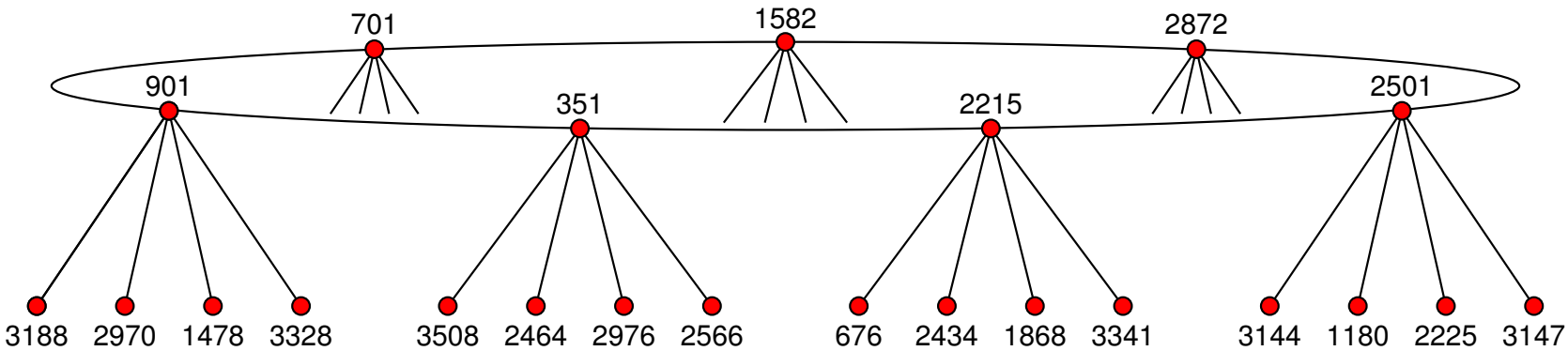
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

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

Mapping a volcano

Example

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

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

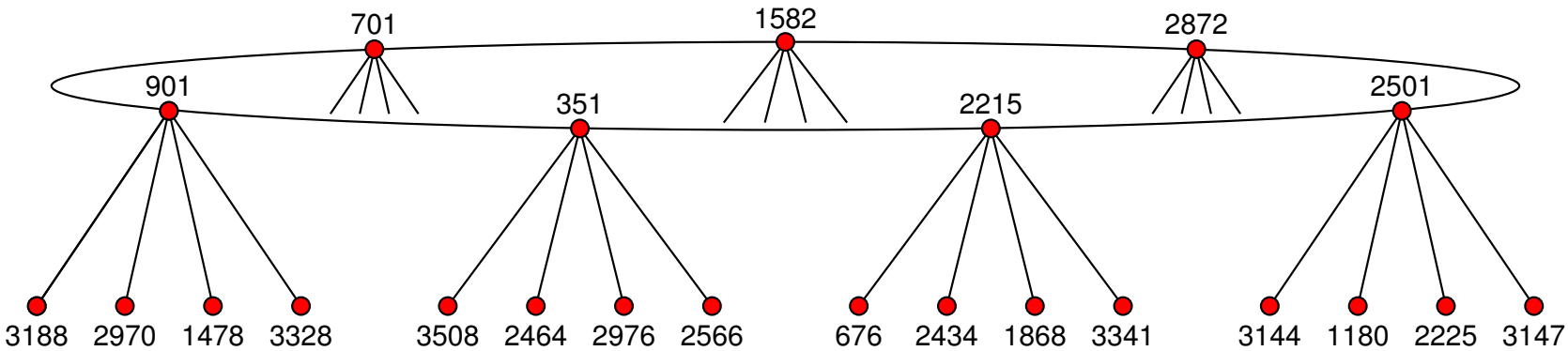
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

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

Mapping a volcano

Example

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

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

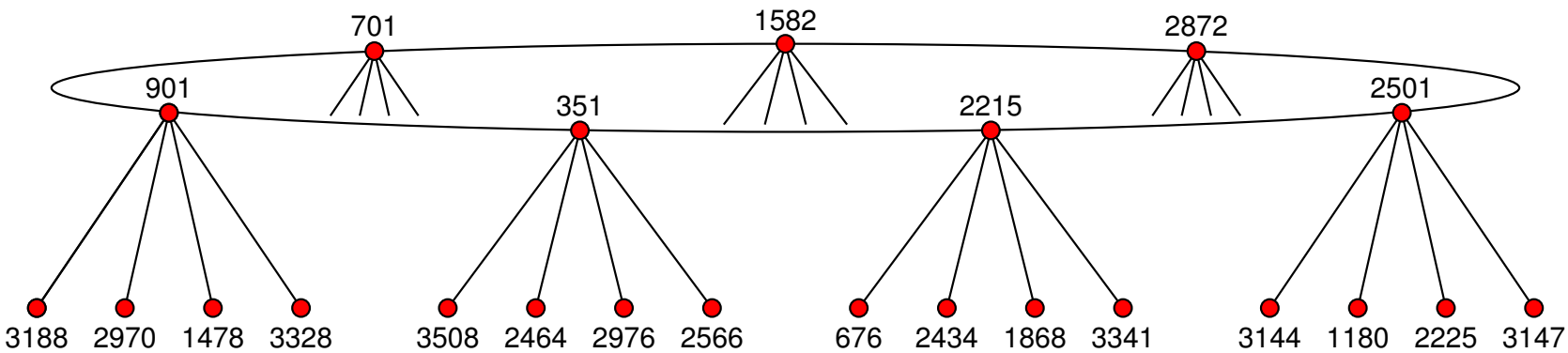
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

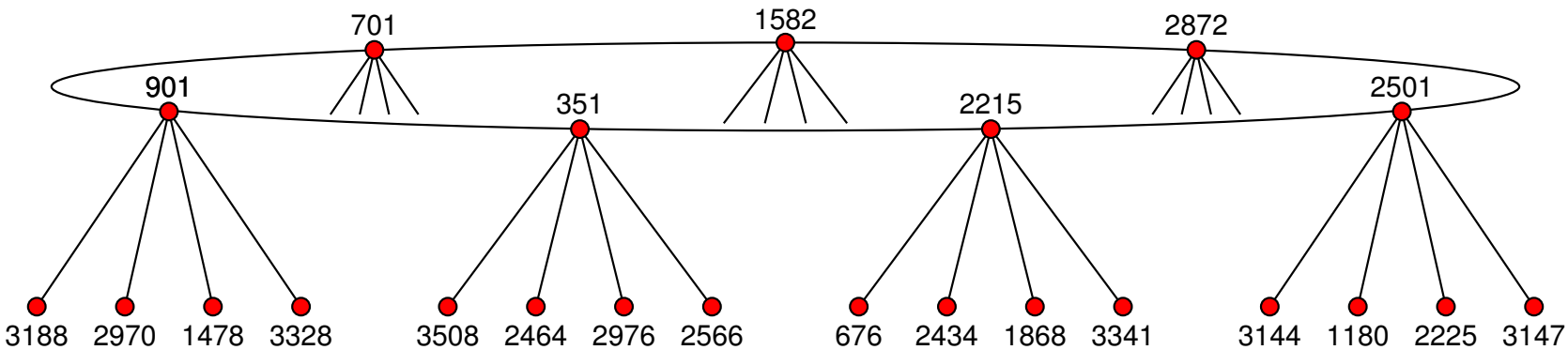
$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

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

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

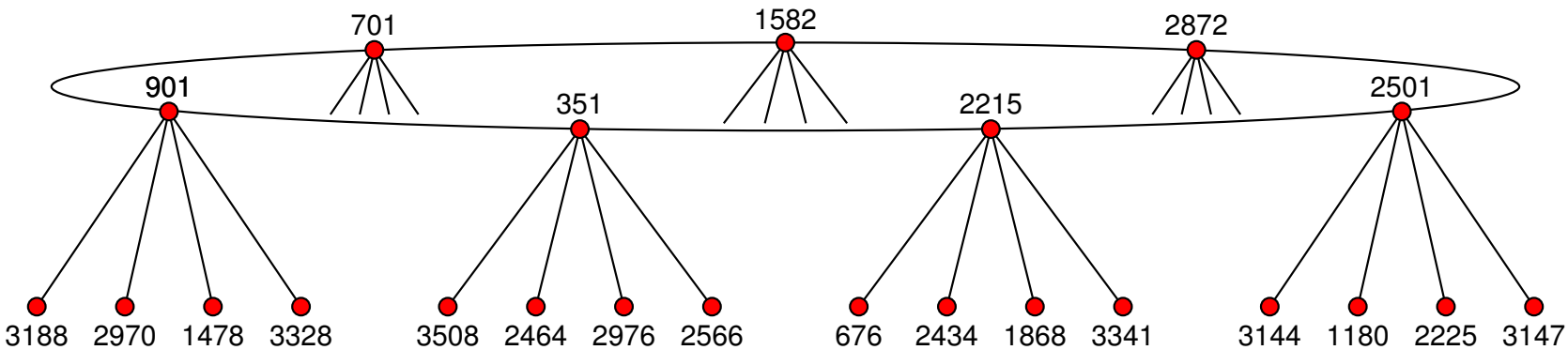


Interpolating $\Phi_\ell \bmod p$



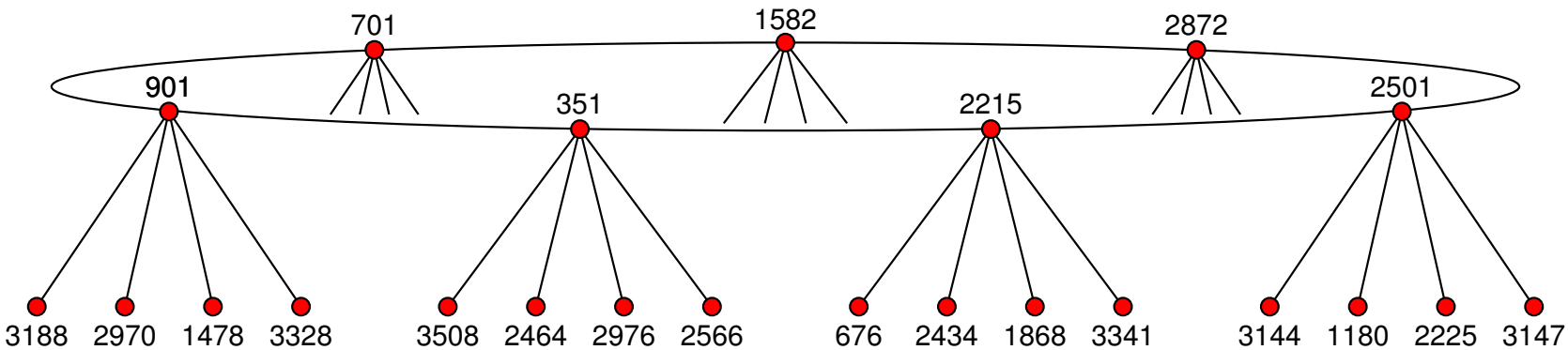
$$\Phi_5(X,\ 901) = (X - 701)(X - 351)(X - 3188)(X - 2970)(X - 1478)(X - 3328)$$
$$\Phi_5(X,\ 351) = (X - 901)(X - 2215)(X - 3508)(X - 2464)(X - 2976)(X - 2566)$$
$$\Phi_5(X, 2215) = (X - 351)(X - 2501)(X - 3341)(X - 1868)(X - 2434)(X - 676)$$
$$\Phi_5(X, 2501) = (X - 2215)(X - 2872)(X - 3147)(X - 2255)(X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

Interpolating $\Phi_\ell \bmod p$



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

Interpolating $\Phi_\ell \bmod p$



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

The Weber function

The Weber $\mathfrak{f}$-function is defined by

$$\mathfrak{f}(\tau) = \frac{\eta\big((\tau+1)/2\big)}{\zeta_{48}\eta(\tau)},$$

and satisfies $j(\tau) = (\mathfrak{f}(\tau)^{24} - 16)^3/\mathfrak{f}(\tau)^{24}$.

The coefficients of $\Phi_\ell^{\mathfrak{f}}$ are roughly 72 times smaller.
This means we need 72 times fewer primes.

The polynomial $\Phi_\ell^{\mathfrak{f}}$ is roughly 24 times sparser.
This means we need 24 times fewer interpolation points.

Overall, we get nearly a **1728-fold speedup** using $\Phi_\ell^{\mathfrak{f}}$.

Modular polynomials for $\ell = 11$

Classical:

$$X^{12} + Y^{12} - X^{11}Y^{11} + 8184X^{11}Y^{10} - 28278756X^{11}Y^9 + 53686822816X^{11}Y^8$$
$$- 61058988656490X^{11}Y^7 + 4257039313564171 2X^{11}Y^6 - 178995262728830 48X^{11}Y^5$$
$$+ 429783723877492846752 0X^{11}Y^4 - 529134841844639613861795X^{11}Y^3 + 272098116580566458155226 00X^{11}Y^2$$
$$- 37464200635670139351581761 2X^{11}Y + 29647090235524057528320000 0X^{11}$$

. . . 8 pages omitted . . .

$$+ 39242334509452765490869646240872004909952472337067462708993642064267017406194168673924546560 00 \ldots 000$$

Atkin:

$$X^{12} - X^{11}Y + 744X^{11} + 196680X^{10} + 187X^9Y + 21354080X^9 + 506X^8Y + 830467440X^8$$
$$- 11440X^7Y + 16875327744X^7 - 57442X^6Y + 208564958976X^6 + 184184X^5Y + 1678582287360X^5$$
$$+ 1675784X^4Y + 9031525113600X^4 + 1867712X^3Y + 32349979904000X^3 - 8252640X^2Y + 74246810880000X^2$$
$$- 19849600XY + 98997734400000X + Y^2 - 8720000Y + 58411072000000$$

Weber:

$$X^{12} + Y^{12} - X^{11}Y^{11} + 11X^9Y^9 - 44X^7Y^7 + 88X^5Y^5 - 88X^3Y^3 + 32XY$$

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`.

Computing $\phi_\ell(Y)$ with the CRT (naïve approach)

Strategy: lift $j(E)$ from $\mathbb{F}_q$ to $\mathbb{Z}$, compute $\Phi_\ell(X, Y) \bmod p$ and evaluate

$$\phi_\ell(Y) = \Phi_\ell(j(E), Y) \bmod p$$

for sufficiently many primes p. Obtain $\phi_\ell \bmod q$ via the explicit CRT.

Uses $O(\ell^2 \log^{3+\epsilon} p)$ expected time for each p, and $O(\ell^2 \log p)$ space.

Computing $\phi_\ell(Y)$ with the CRT (naïve approach)

Strategy: lift $j(E)$ from $\mathbb{F}_q$ to $\mathbb{Z}$, compute $\Phi_\ell(X, Y) \bmod p$ and evaluate

$$\phi_\ell(Y) = \Phi_\ell(j(E), Y) \bmod p$$

for sufficiently many primes p. Obtain $\phi_\ell \bmod q$ via the explicit CRT.

Uses $O(\ell^2 \log^{3+\epsilon} p)$ expected time for each p, and $O(\ell^2 \log p)$ space.

However, "sufficiently many" is now $O(\ell n)$, where $n = \log q$.
Total expected time is $O(\ell^3 n \log^{3+\epsilon} \ell)$, using $O(\ell n + \ell^2 \log \ell)$ space.

This approach is **not very useful**:

- If n is large (e.g. $n \approx \ell$), it takes way too long (quartic in ℓ).
- It n is small (e.g. $n \approx \log \ell$), it doesn't save any space.

Computing $\phi_\ell(Y)$ with the CRT (Algorithm 1)

Strategy: lift $j(E), j(E)^2, j(E)^3, \ldots, j(E)^{\ell+1}$ from $\mathbb{F}_q$ to $\mathbb{Z}$ and compute

$$\phi_\ell(Y) = \sum c_{ik} j(E)^i Y^k \bmod p$$

for sufficiently many primes p, where $\Phi_\ell = \sum c_{ik} X^i Y^k$.
Obtain $\phi_\ell \bmod q$ via the explicit CRT.

Computing $\phi_\ell(Y)$ with the CRT (Algorithm 1)

Strategy: lift $j(E), j(E)^2, j(E)^3, \ldots, j(E)^{\ell+1}$ from $\mathbb{F}_q$ to $\mathbb{Z}$ and compute

$$\phi_\ell(Y) = \sum c_{ik} j(E)^i Y^k \bmod p$$

for sufficiently many primes p, where $\Phi_\ell = \sum c_{ik} X^i Y^k$.
Obtain $\phi_\ell \bmod q$ via the explicit CRT.

Now "sufficiently many" is $O(\ell + n)$.

For $n = O(\ell \log \ell)$, uses $O(\ell^3 \log^{3+\epsilon} \ell)$ expected time
and $O(\ell^2 \log \ell)$ space (under GRH).

For $n = \Omega(\ell \log \ell)$, the space bound is optimal.

This algorithm can also evaluate the partial derivatives of Φ_ℓ needed to construct normalized equations for $\tilde{E}$ (important for SEA).

Computing $\phi_\ell(Y)$ with the CRT (Algorithm 2)

Strategy: lift $j(E)$ from $\mathbb{F}_q$ to $\mathbb{Z}$ and for sufficiently many primes p compute $\phi_\ell \bmod p$ as follows:

1. For each of $\ell+2$ j-invariants y_i, compute $z_i = \prod_k (j(E) - j_k)$, where the j_k range over $\ell+1$ neighbors of y_i in $G_\ell(\mathbb{F}_p)$.
2. Interpolate $\phi_\ell(Y) \in \mathbb{F}_p$ as the unique polynomial of degree $\ell+1$ for which $\phi_\ell(y_i) = z_i$.

Obtain $\phi_\ell \bmod q$ via the explicit CRT.

Computing $\phi_\ell(Y)$ with the CRT (Algorithm 2)

Strategy: lift $j(E)$ from $\mathbb{F}_q$ to $\mathbb{Z}$ and for sufficiently many primes p compute $\phi_\ell \bmod p$ as follows:

1. For each of $\ell+2$ j-invariants y_i, compute $z_i = \prod_k (j(E) - j_k)$, where the j_k range over $\ell+1$ neighbors of y_i in $G_\ell(\mathbb{F}_p)$.
2. Interpolate $\phi_\ell(Y) \in \mathbb{F}_p$ as the unique polynomial of degree $\ell+1$ for which $\phi_\ell(y_i) = z_i$.

Obtain $\phi_\ell \bmod q$ via the explicit CRT.

For $n = O(\ell^c)$, uses $O(\ell^3(n + \log \ell)\log^{1+\epsilon} \ell)$ expected time and $O(\ell n + \ell \log \ell)$ space (under GRH).

For $n = O(\log^{2-\epsilon} q)$ the algorithm is faster than computing Φ_ℓ.
For $n = \Omega(\log \ell)$ the space bound is optimal.

If n is $\Omega(\log^2 \ell)$ and $O(\ell \log \ell)$, one can use a hybrid approach.
This yields an optimal space bound for all $q > \ell$.

Genus 1 point counting in large characteristic

Algorithms to compute $\#E(\mathbb{F}_q) = q + 1 - t$.

Algorithm	Time	Space
Totally naive	$O(e^{2n+\epsilon})$	$O(n)$
Slightly less naive	$O(e^{n+\epsilon})$	$O(n)$
Baby-step giant-step	$O(e^{n/4+\epsilon})$	$O(e^{n/4+\epsilon})$
Pollard kangaroo	$O(e^{n/4+\epsilon})$	$O(n^2)$
Schoof	$O(n^5 \operatorname{llog} n)$	$O(n^3)$
SEA*	$O(n^4 \log^3 n \operatorname{llog} n)$	$O(n^3 \log n)$
SEA (Φ_ℓ precomputed)	$O(n^4 \operatorname{llog} n)$	$O(n^4)$

*Complexity estimates for SEA-based algorithms are heuristic expected times.

Genus 1 point counting in large characteristic

Algorithms to compute $\#E(\mathbb{F}_q) = q + 1 - t$.

Algorithm	Time	Space
Totally naive	$O(e^{2n+\epsilon})$	$O(n)$
Slightly less naive	$O(e^{n+\epsilon})$	$O(n)$
Baby-step giant-step	$O(e^{n/4+\epsilon})$	$O(e^{n/4+\epsilon})$
Pollard kangaroo	$O(e^{n/4+\epsilon})$	$O(n^2)$
Schoof	$O(n^5 \operatorname{llog} n)$	$O(n^3)$
SEA*	$O(n^4 \log^3 n \operatorname{llog} n)$	$O(n^3 \log n)$
SEA (Φ_ℓ precomputed)	$O(n^4 \operatorname{llog} n)$	$O(n^4)$
SEA with Algorithm 1	$O(n^4 \log^2 n \operatorname{llog} n)$	$O(n^2 \log n)$
Amortized	$O(n^4 \operatorname{llog} n)$	$O(n^2 \log n)$

*Complexity estimates for SEA-based algorithms are heuristic expected times.

Elliptic curve point-counting record

The number of points on the elliptic curve E defined by

$$y^2 = x^3 + 2718281828x + 3141592653,$$

modulo the 5011 digit prime $q = 16219299585 \cdot 2^{16612} - 1$ is

832376989144494660061901849139137826006983637060450015930966792818374113674093822766991283099784662700961700402058294019077483170516664837812554817443350162223605440005388394920224519114859867338191660095508592165253852678528425242409787965445004279587342458591036506936232600658549556769058427604042111029080666232135885662070661039670759580341918109430064160840690748363019037103169978894180556726367014400296781983798513562269371401276427209286702254047174078470090179859044119920875037921597111234401965330999966802919477217848269921000166896074288408594435094209873544111246489768281188102940915774276149848136182361339830763026929994181385485521401057780125259890724056418895533398724332427935709677002908601694738205973033005180695050658325875330867074804800846369800427134645786532440716786520228221019906549532681092997885462429828848191629734823903084330670554604329550248173093287043318053279349574487888250634839378070873512388679880513270375903317908018724535858724374676948741127267380730950376658888626598248661629797105514800663321182698336395879329897043562635494364468648603965666427837093575009979091922302413453716095887661432089373163729653025768255602712754566610542223232815622048111888283590483215892528728153087049654418794163034575764891117186500373809179386465716056073958857886659984917838400020437572986666397067817373834345665795929791423993337711367782253801663601524105377974544793563993306843722670306771161287047597472887406025615382942435530946142941286376701601044870872578234027597836843487328902748704620332776144279810260429883073285589599324633304714799454649284242674253031456570427212647114749626733565213374345500028792023241372392282583915035127429507360477358589223431309277807734657260856177926792519303039018061981527730802570037763611305288011473023638233485202658040753778732701374828945119730466794287776855342753062039220963874377784056109451569365074409960841197308143039014826264985208136415400640444310783428595398820909262235042372724084881154327002269478397116252120617133360022725560655793168849910978673768497963315764527084692590231159741512227876106228667690675220660368352958211682369185130591727246266188297335557699886564695842936108180916269218186627033806670410268119981312684367950007662547286040906474918681544527436706758684340705546340218913583981657248854325413365511159096364567006934774498652603685110454112058470354530606364865125892179309145232011129504637984158694189917505410413787131053621887908831837273005465881200616271744801682487747455898185251772280214510451501147795355549876845352299986818351761176510147685763441401085581041504532073709350521509138632615043242120075498047323584645534885609879194689611448558254656126144564114585216077473899495865951260743060858121346172363099567656218607271568564820461501120120151130071222866692995902742821076909338903008105256035587100453995367274039693249124208063895271529559939433116410268948242637362685355343705851022198361778056561670358618600362869633742502575881826442008352428041311901722720144145496595474571658798526002326473049911956443052879398278852076549881257512212397410752449734278198437764650895576661713374034975968504613998353274345412501516980948460568909969569149381714599518690006692709694985259939147512067607822447906251226268487530127334952892006417959671845610112264392529305960900316499742776349439331789385107265962594378264662933791621325648258956921290293302567147491547700031400327806411025863588895745234111758218534120042661084581341547473844325846515861998968494758420093653389525358841111602719608689990147420125919714782372925248139486000292277961255490293815989577215748050074789669970241086912740183577851714893063771521660961916647508039799566216795719789535522117245526322307106532444336693310674420401403916024565818587474014367724032840804548958008255550795224583691902547110401601200028499012649426967495115480636409733058979879385173976155641587413347889866287021950635203417893709652546248256133417835452925731715740688561063321641057055461825084563212070367457331486354681841758049252732599116595430817436406080011315918900828645131242470137313661372714961047058097433021586751093908895745441684195336715770412686321350796787391486224738612016911715739107481092463845433183146882764205897555692474146749724490484592370638492569933497005028781048032734897097622833295643389100786217086915770725300529087910723550751401318787576647364571766936818440620554990814181207394577639163458834949267687793194747139050054400221521434458599314044867381063285572380923329713520153405615749711252696047443494747652497316648062057666953271152425843341789770616064557079435236406353029020560141015314103419765029534921177065625577774688408769857858804251711896591035794406728856602939161842221528770720582112364327715631856765897848302241231421628544594675301323023661942160414993178396196877455996341128827795369279474773827993735868297936899429512496912028871093270632848624677436722012981685194580777814009291336645358259624246494437340122223955248

Elliptic curve point counting record

Task	Total CPU Time
Compute ϕ_ℓ^{f}	32 days
Find a root $\tilde{j}$	995 days
Compute g_ℓ	3 days
Compute $\pi \bmod g_\ell, E$	326 days
Find λ_ℓ	22 days

$\phi_\ell^{\mathrm{f}}(Y) = \Phi_\ell^{\mathrm{f}}(j(E), Y)$ was computed for ℓ from 5 to 11681.
Exactly 700 of 1400 were found to be Elkies primes.
Atkin primes were not used.

The largest ϕ_ℓ^{f} was under 20MB in size and took about two hours to compute using 1 core.

Modular polynomial evaluation record

For $\ell = 100019$ and $q = 2^{86243} - 1$ we computed $\phi_\ell^{\mathrm{f}}(Y) = \Phi_\ell^{\mathrm{f}}(j(E), Y)$.

This is much larger than one would need to set a 25,000 digit point-counting record.

The size of ϕ_ℓ^{f} is about **1 GB**.

For comparison:

- The size of $\Phi_\ell^{\mathrm{f}} \bmod q$ is about **2 TB**.
- The size of $\Phi_\ell \bmod q$ is about **50 TB**.
- The size of Φ_ℓ is more than **10 PB**.

Improved space complexity of computing horizontal isogenies

The algorithm of [Bisson-S 2011] for computing the endomorphism ring of an elliptic curve $E/\mathbb{F}_q$ runs in $L[1/2, \sqrt{3}/2]$ expected time and uses $L[1/2, 1/\sqrt{3}]$ space (under GRH).

The space complexity can now be improved to $L[1/2, 1/\sqrt{12}]$.

A similar improvement applies to algorithms for computing horizontal isogenies of large degree [Jao-Soukharev 2010].