Computing the modular equation

Andrew V. Sutherland (MIT)

Barcelona-Boston-Tokyo Number Theory Seminar
in Memory of Fumiyuki Momose

The modular polynomial

Let $j(z)$ denote the classical modular function $j\colon \mathbb{H} \to \mathbb{C}$ with q-expansion

$$j(z) = 1/q + 744 + 196884q + \dots$$

For a positive integer N, the minimal polynomial of the function $j(Nz)$ over the field $\mathbb{C}(j)$ is the *modular polynomial* of level N.

Its coefficients actually lie in $\mathbb{C}[j]$, so we may regard it as a polynomial $\Phi_N(X, Y)$ in two variables.

Its coefficients are algebraic integers, and they are rational. So they lie in $\mathbb{Z}$.

The modular equation

Over $\mathbb{C}$, elliptic curves E_1 and E_2 are related by a cyclic isogeny of degree N if and only if

$$\Phi_N(j(E_1), j(E_2)) = 0.$$

Thus Φ_N parameterizes pairs of N-isogenous elliptic curves.
It (canonically) defines the modular curve $Y_0(N) = \Gamma_0(N)\backslash\mathbb{H}$.

The moduli interpretation of Φ_N remains valid over any field of characteristic prime to N.

Practical applications of modular polynomials

Examples:

- Point-counting (SEA).
- Computing the endomorphism ring of an elliptic curve.
- Constructing elliptic curves with the CM method.
- Computing discrete logarithms.
- Constructing Ramanujan graphs.

In most applications N is a prime ℓ, and we actually wish to compute Φ_ℓ over a finite field $\mathbb{F}_q$.

Explicit computations

History:

level	person (machine)	year
$N = 2$	Smith	1878
$N = 3$	Smith	1879
$N = 5$	Berwick	1916
$N = 7$	Herrmann	1974
$N = 11$	Kaltofen-Yui (VAX 11-780)	1984

Why is computing Φ_N so difficult?

Explicit computations

History:

level	person (machine)	year
$N = 2$	Smith	1878
$N = 3$	Smith	1879
$N = 5$	Berwick	1916
$N = 7$	Herrmann	1974
$N = 11$	Kaltofen-Yui (VAX 11-780)	1984

Why is computing Φ_N so difficult?

Φ_ℓ is big: $O(\ell^3 \log \ell)$ bits.

Example: $\Phi_{11}(X, Y)$

$$X^{12} + Y^{12} - X^{11}Y^{11} + 8184X^{11}Y^{10} - 28278756X^{11}Y^{9}$$
$$+ 53686822816X^{11}Y^{8} - 6105898865649 0X^{11}Y^{7}$$
$$+ 4257039313564 1712X^{11}Y^{6} - 1789952627288 3039048X^{11}Y^{5}$$
$$+ 4297837238774928467520X^{11}Y^{4}$$
$$- 5291348418446396138617 95X^{11}Y^{3}$$
$$+ 2720981165805664581552 2600X^{11}Y^{2}$$
$$- 3746420063567013935158 17612X^{11}Y$$
$$+ 2964709023552405752832 00000X^{11}$$
$$\ldots 8 \text{ pages omitted} \ldots$$
$$+ 3924233450945276549086 96\ldots 100 \text{ digits omitted} \ldots 000$$

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 $\Phi_\ell(X, Y)$

*Estimated

Algorithms to compute Φ_ℓ

q-expansions:

(Atkin ?, Elkies '92, '98, LMMS '94, Ito '95, Morain '95, Müller '95, BCRS '99)

Φ_ℓ:	$O(\ell^4 \log^{3+\epsilon} \ell)$	(via the CRT)
$\Phi_\ell \bmod q$:	$O(\ell^3 \log \ell \log^{1+\epsilon} q)$	($p > \ell + 1$)

Algorithms to compute Φ_ℓ

q-expansions:

(Atkin ?, Elkies '92, '98, LMMS '94, Ito '95, Morain '95, Müller '95, BCRS '99)

Φ_ℓ:	$O(\ell^4 \log^{3+\epsilon} \ell)$	(via the CRT)
$\Phi_\ell \bmod q$:	$O(\ell^3 \log \ell \log^{1+\epsilon} q)$	($p > \ell + 1$)

isogenies: (Charles-Lauter 2005)

Φ_ℓ:	$O(\ell^{5+\epsilon})$	(via the CRT)
$\Phi_\ell \bmod q$:	$O(\ell^{4+\epsilon} \log^{2+\epsilon} q)$	($q > 12\ell + 13$)

Algorithms to compute Φ_ℓ

q-expansions:

(Atkin ?, Elkies '92, '98, LMMS '94, Ito '95, Morain '95, Müller '95, BCRS '99)

Φ_ℓ:	$O(\ell^4 \log^{3+\epsilon} \ell)$	(via the CRT)
$\Phi_\ell \bmod q$:	$O(\ell^3 \log \ell \log^{1+\epsilon} q)$	($p > \ell + 1$)

isogenies: (Charles-Lauter 2005)

Φ_ℓ:	$O(\ell^{5+\epsilon})$	(via the CRT)
$\Phi_\ell \bmod q$:	$O(\ell^{4+\epsilon} \log^{2+\epsilon} q)$	($q > 12\ell + 13$)

evaluation-interpolation: (Enge 2009)

Φ_ℓ:	$O(\ell^3 \log^{4+\epsilon} \ell)$	(floating-point approx.)
$\Phi_\ell \bmod q$:	$O(\ell^3 \log^{4+\epsilon} \ell)$	(reduces Φ_ℓ)

A new algorithm to compute Φ_ℓ

Bröker-Lauter-S (2010), S (2012) and Ono-S (in progress).
We compute Φ_ℓ using isogenies and the CRT.

A new algorithm to compute Φ_ℓ

Bröker-Lauter-S (2010), S (2012) and Ono-S (in progress).
We compute Φ_ℓ using isogenies and the CRT.

For "suitable" primes p we compute Φ_ℓ mod p in expected time

$$O(\ell^2 \log^{3+\epsilon} p).$$

A new algorithm to compute Φ_ℓ

Bröker-Lauter-S (2010), S (2012) and Ono-S (in progress).
We compute Φ_ℓ using isogenies and the CRT.

For "suitable" primes p we compute Φ_ℓ mod p in expected time

$$O(\ell^2 \log^{3+\epsilon} p).$$

Under the GRH, we find many suitable p with $\log p = O(\log \ell)$.

Φ_ℓ:	$O(\ell^3 \log^{3+\epsilon} \ell)$	(via the CRT)
Φ_ℓ mod q:	$O(\ell^3 \log^{3+\epsilon} \ell)$	(via the explicit CRT)

Computing Φ_ℓ mod q uses $O(\ell^2 \log(\ell q))$ space.

A new algorithm to compute Φ_ℓ

Bröker-Lauter-S (2010), S (2012) and Ono-S (in progress).
We compute Φ_ℓ using isogenies and the CRT.

For "suitable" primes p we compute Φ_ℓ mod p in expected time

$$O(\ell^2 \log^{3+\epsilon} p).$$

Under the GRH, we find many suitable p with $\log p = O(\log \ell)$.

Φ_ℓ:	$O(\ell^3 \log^{3+\epsilon} \ell)$	(via the CRT)
Φ_ℓ mod q:	$O(\ell^3 \log^{3+\epsilon} \ell)$	(via the explicit CRT)

Computing Φ_ℓ mod q uses $O(\ell^2 \log(\ell q))$ space.

In practice the algorithm is *much* faster than other methods.
It is probabilistic, but the output is unconditionally correct.

Some performance highlights

Level records

1. **5003**: 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)

Single core CPU times (AMD 3.0 GHz), using prime $q \approx 2^{256}$.

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

Isogenies

For the rest of this talk ℓ is a prime not equal to $\operatorname{char} \mathbb{F}$.
Every ℓ-isogeny $\phi : E_1 \to E_2$ is thus separable, and its kernel is a (cyclic) subgroup of $E(\overline{\mathbb{F}})$ of order ℓ.

Conversely, every subgroup of $E(\overline{\mathbb{F}})$ of order ℓ is the kernel of an ℓ-isogeny, which we may compute explicitly using Vélu's formulas (but this may be costly).

Isogenies

For the rest of this talk ℓ is a prime not equal to $\operatorname{char} \mathbb{F}$.
Every ℓ-isogeny $\phi : E_1 \to E_2$ is thus separable, and its kernel is a (cyclic) subgroup of $E(\overline{\mathbb{F}})$ of order ℓ.

Conversely, every subgroup of $E(\overline{\mathbb{F}})$ of order ℓ is the kernel of an ℓ-isogeny, which we may compute explicitly using Vélu's formulas (but this may be costly).

We say that $\phi\colon E_1 \to E_2$ is *horizontal* if $\operatorname{End}(E_1) = \operatorname{End}(E_2)$.
Otherwise ϕ is a *vertical* isogeny

Horizontal isogenies are "easy" to compute.
Vertical isogenies are not.

Complex multiplication

Let E be an elliptic curve with $\mathrm{End}(E) \simeq \mathcal{O}$.

For any (proper) $\mathcal{O}$-ideal $\mathfrak{a}$, define the $\mathfrak{a}$-torsion subgroup

$$E[\mathfrak{a}] = \{P : \alpha P = 0 \text{ for all } \alpha \in \mathfrak{a}\}.$$

$E[\mathfrak{a}]$ is the kernel of an isogeny of degree $N(\mathfrak{a})$, and this yields a group action of the class group $\mathrm{cl}(\mathcal{O})$ on the set

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

Complex multiplication

Let E be an elliptic curve with $\mathrm{End}(E) \simeq \mathcal{O}$.

For any (proper) $\mathcal{O}$-ideal $\mathfrak{a}$, define the $\mathfrak{a}$-torsion subgroup

$$E[\mathfrak{a}] = \{P : \alpha P = 0 \text{ for all } \alpha \in \mathfrak{a}\}.$$

$E[\mathfrak{a}]$ is the kernel of an isogeny of degree $N(\mathfrak{a})$, and this yields a group action of the class group $\mathrm{cl}(\mathcal{O})$ on the set

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

Horizontal ℓ-isogenies are the action of an ideal with norm ℓ.
A horizontal isogeny of large degree may be equivalent to a product of isogenies of smaller degree, via relations in $\mathrm{cl}(\mathcal{O})$.

Under the ERH, "small" is $O(\log^2 |D|)$, where $D = \mathrm{disc}(\mathcal{O})$.

Isogeny graphs

The ℓ-isogeny graph G_ℓ has vertex set $\{j(E) : E/\mathbb{F}_q\}$ and edges (j_1, j_2) whenever $\Phi_\ell(j_1, j_2) = 0$.

The neighbors of $j_1 \in \mathbb{F}_q$ are the roots of $\Phi_\ell(j_1, Y)$ that lie in $\mathbb{F}_q$.

Isogeny graphs

The ℓ-isogeny graph G_ℓ has vertex set $\{j(E) : E/\mathbb{F}_q\}$ and edges (j_1, j_2) whenever $\Phi_\ell(j_1, j_2) = 0$.

The neighbors of $j_1 \in \mathbb{F}_q$ are the roots of $\Phi_\ell(j_1, Y)$ that lie in $\mathbb{F}_q$.

Isogenous curves are either both ordinary or both supersingular, thus we may speak of the ordinary and supersingular components of G_ℓ.

We will focus on the ordinary components of G_ℓ.

We have an infinite family of graphs, one for each prime ℓ, all with the same vertex set.

ℓ-volcanoes

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 regular connected graph of degree at most 2.

ℓ-volcanoes

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 regular connected graph of degree at most 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 $\ell+1$.

ℓ-volcanoes

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 regular connected graph of degree at most 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 $\ell+1$.

The integers ℓ, d, and $|V_0|$ uniquely determine the shape.

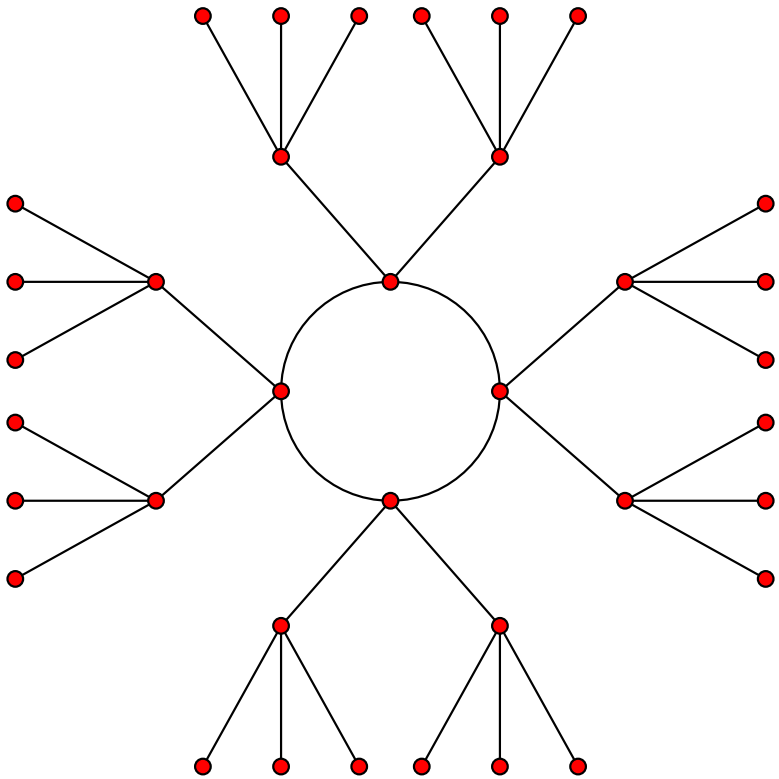
The ℓ-isogeny graph G_ℓ

Some facts about G_ℓ (Kohel, Fouquet-Morain):

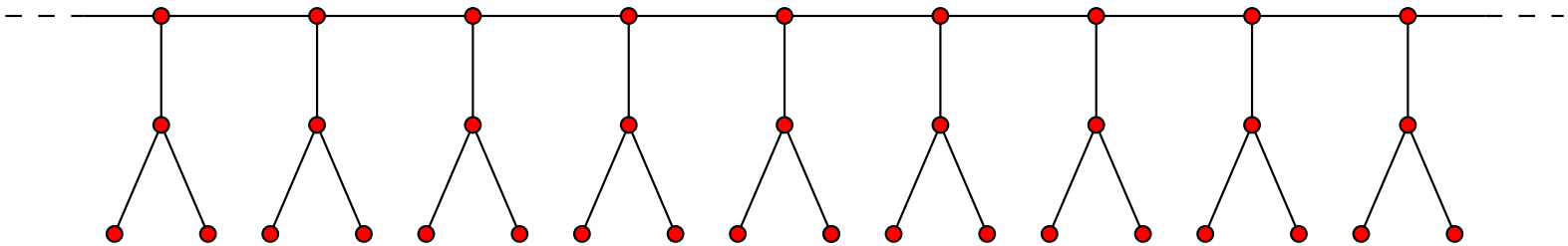
- The ordinary components of G_ℓ are ℓ-volcanoes (provided they don't contain $j = 0, 1728$).
- The curves in level V_i of a given ℓ-volcano all have the same endomorphism ring, isomorphic to an imaginary quadratic order $\mathcal{O}_i$.
- The order $\mathcal{O}_0$ is maximal at ℓ, and $\mathcal{O}_i \subset \mathcal{O}_0$ has index ℓ^i.

Curves in the same ℓ-volcano are necessarily isogenous, but isogenous curves need not lie in the same ℓ-volcano.

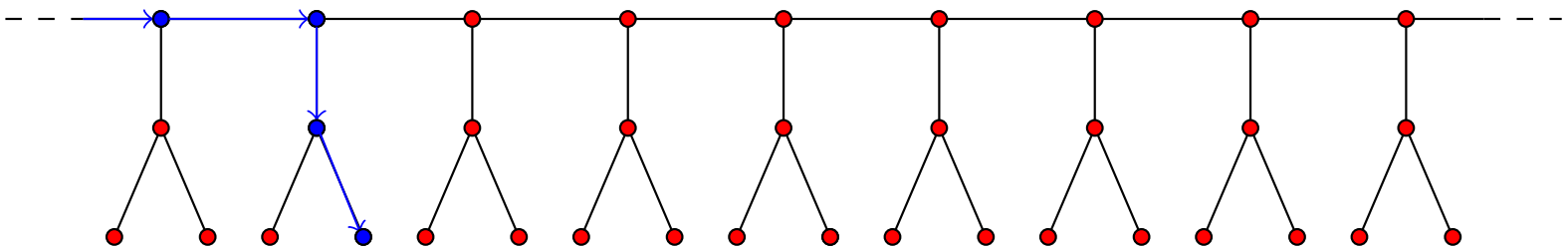
A 3-volcano of depth 2



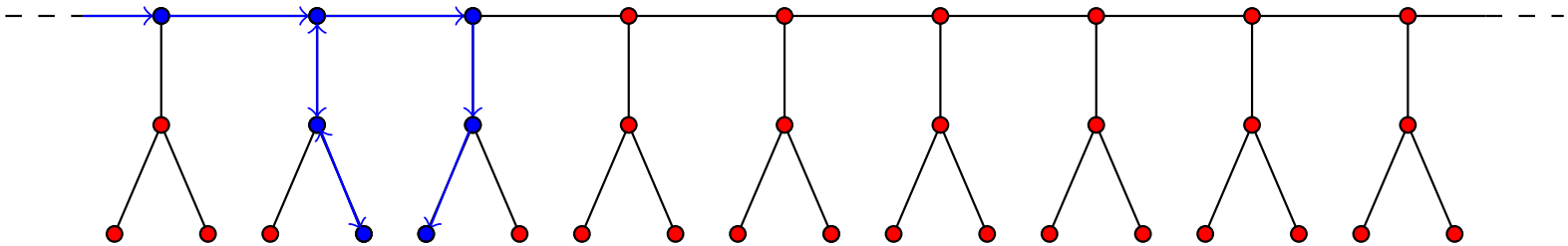
Running the rim



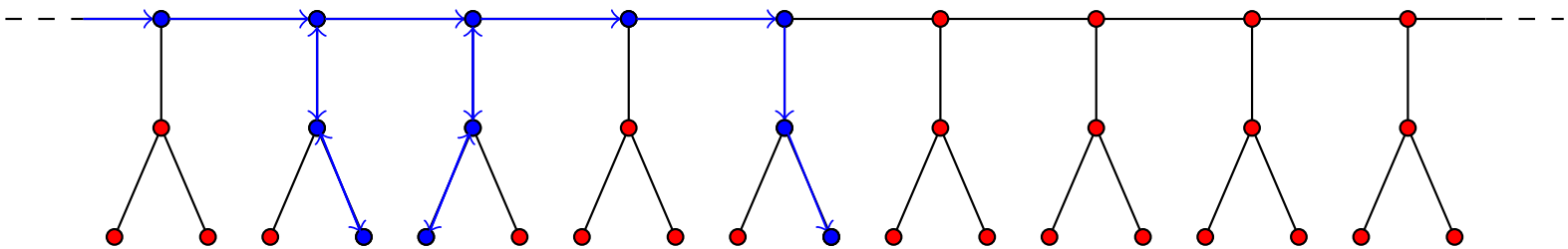
Running the rim



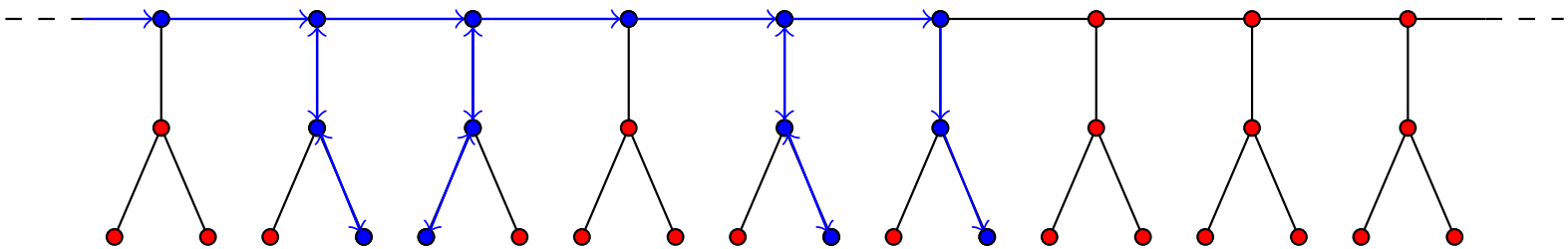
Running the rim



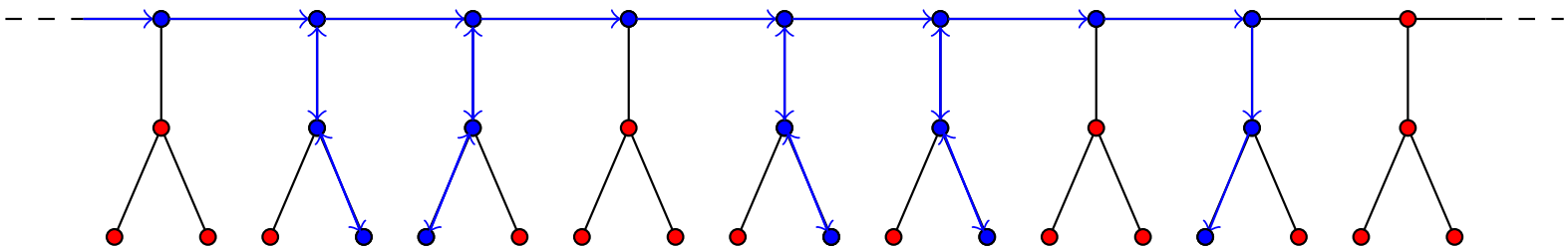
Running the rim



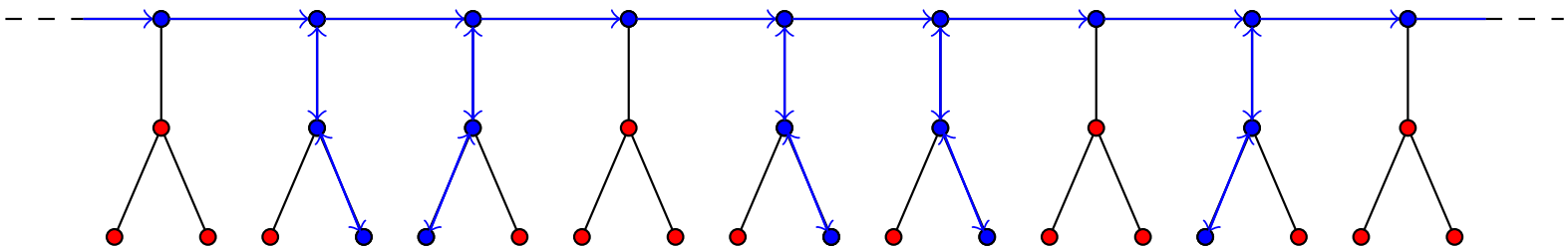
Running the rim



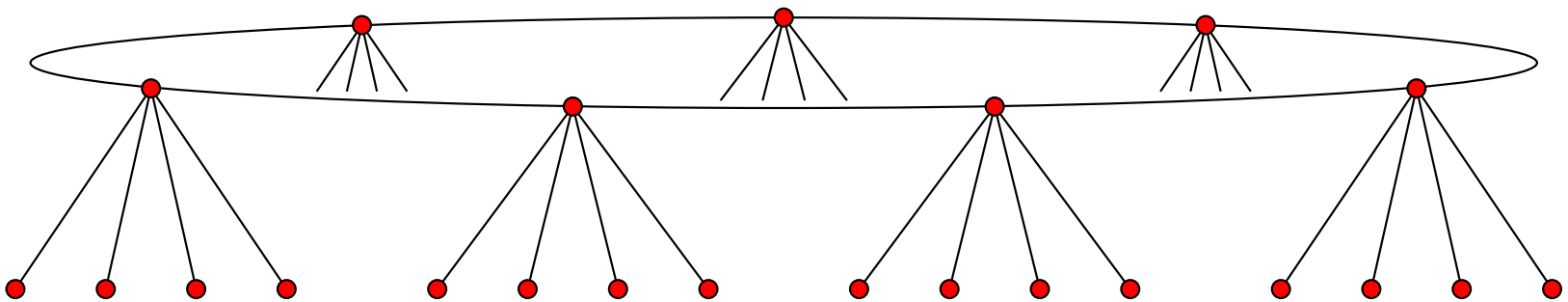
Running the rim



Running the rim



Mapping a volcano



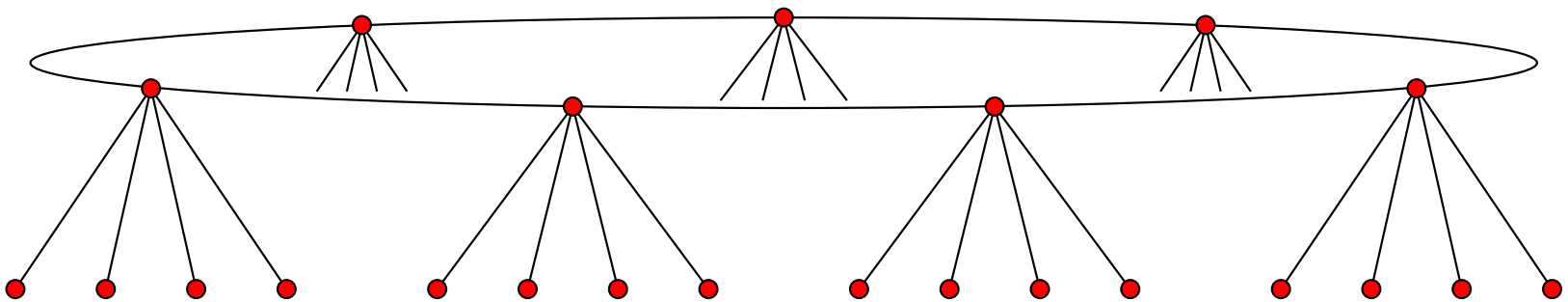
Mapping a volcano

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

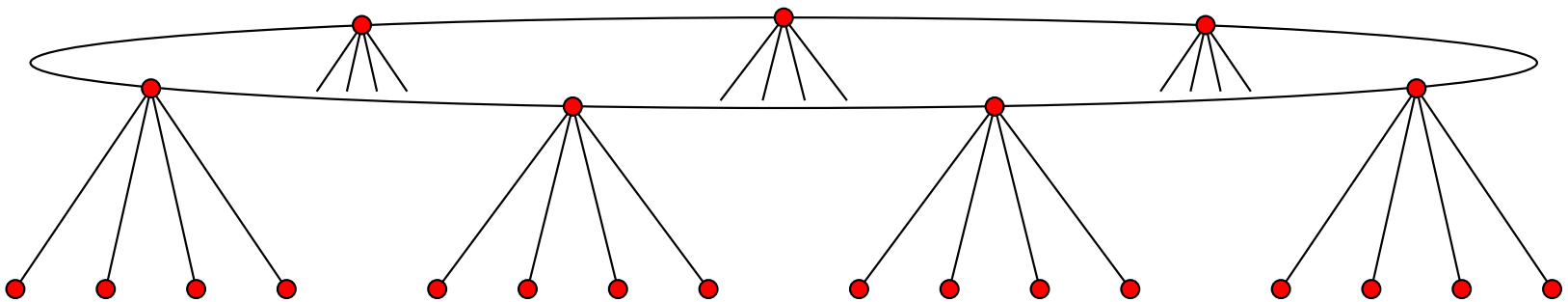
$\ell = 5, \quad p = 4451, \quad D = -151$

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

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

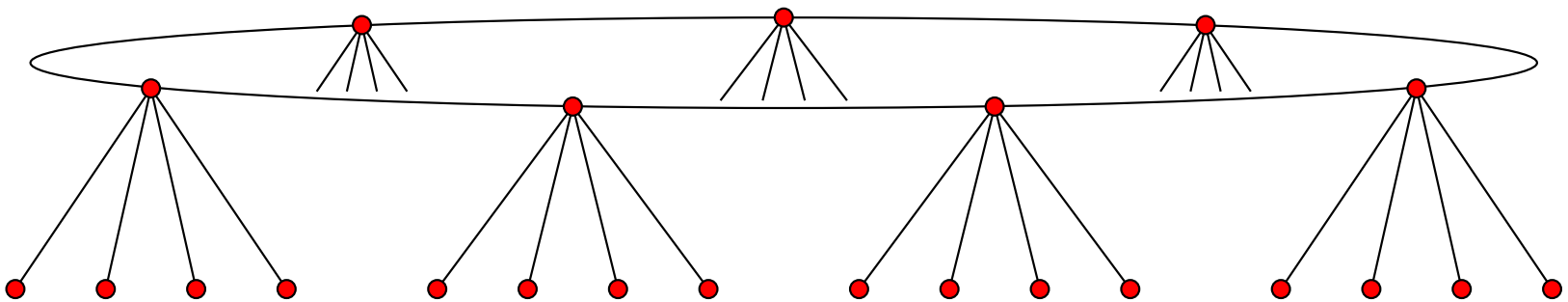
$\ell = 5, \quad p = 4451, \quad D = -151$

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

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

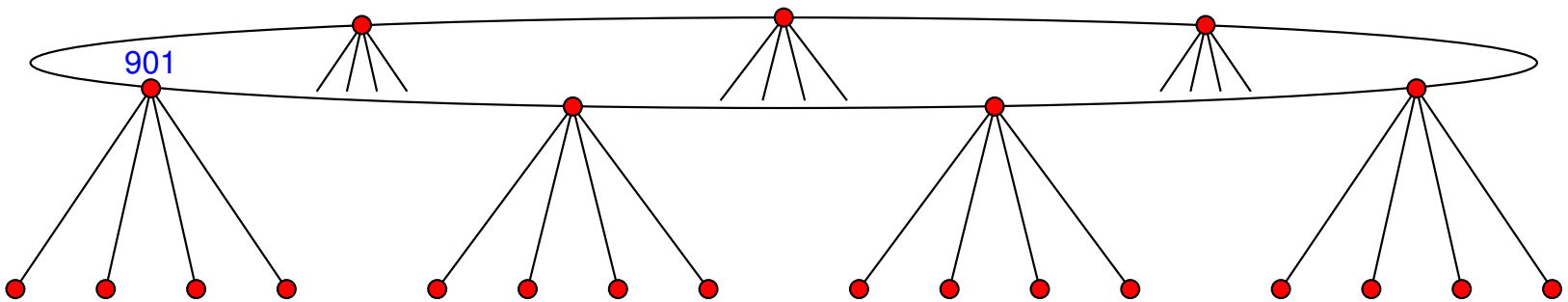
$\ell = 5, \quad p = 4451, \quad D = -151$

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

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

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

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

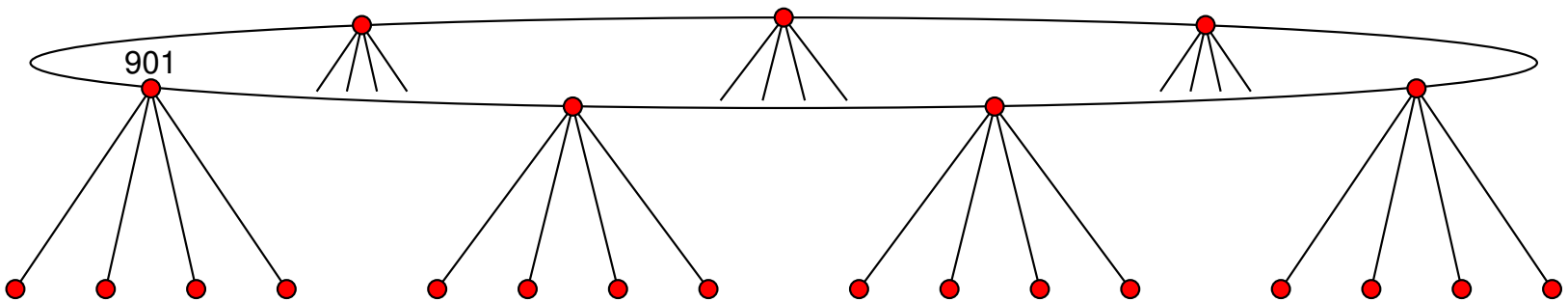
$\ell_0 = 2$

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

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

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

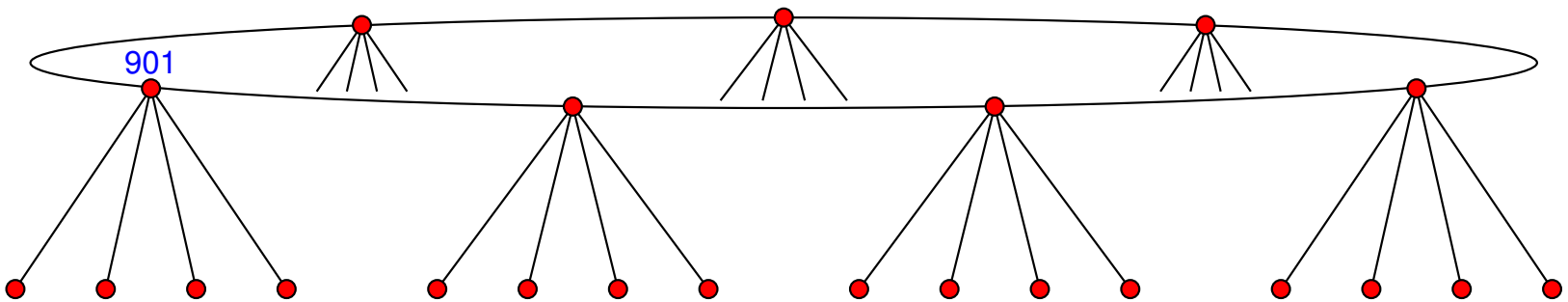
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

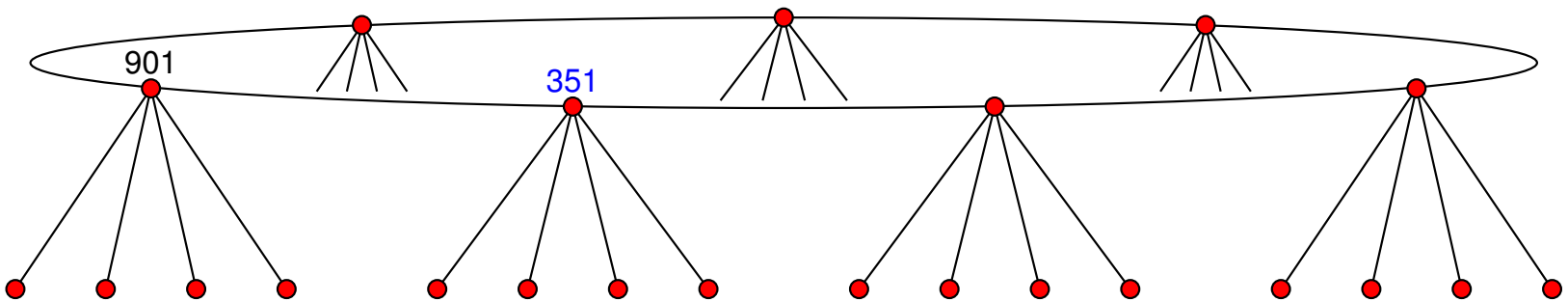
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

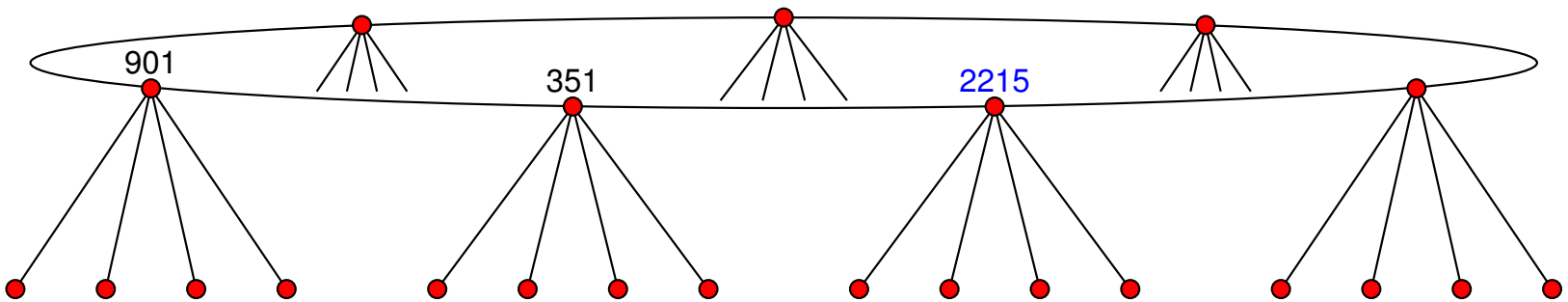
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

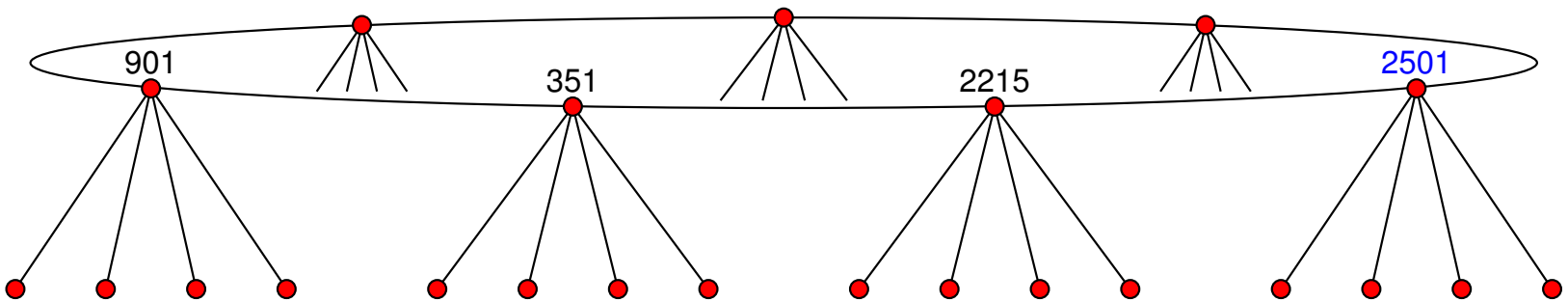
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

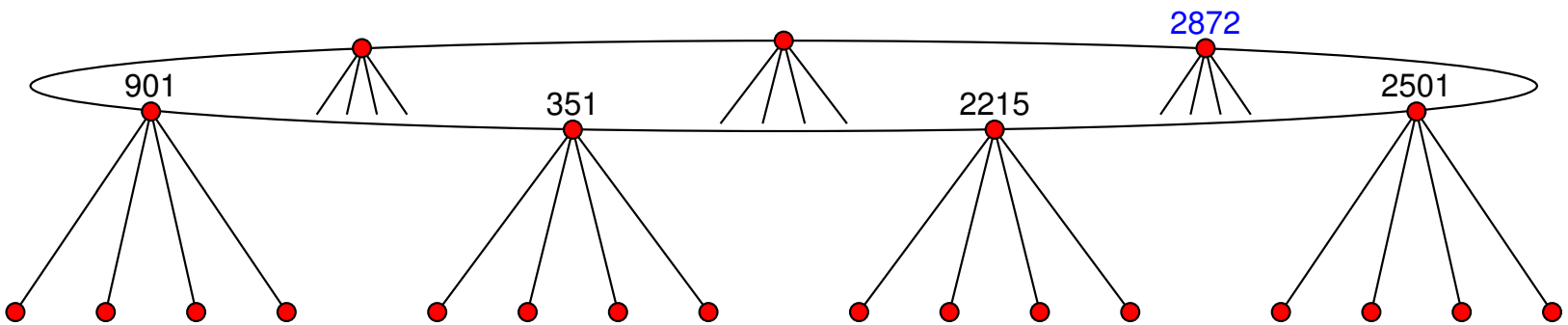
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

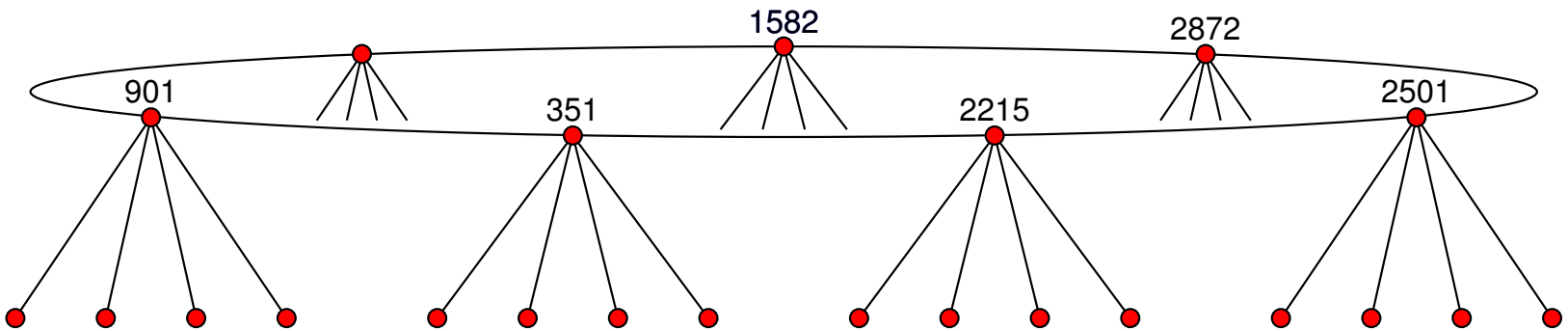
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

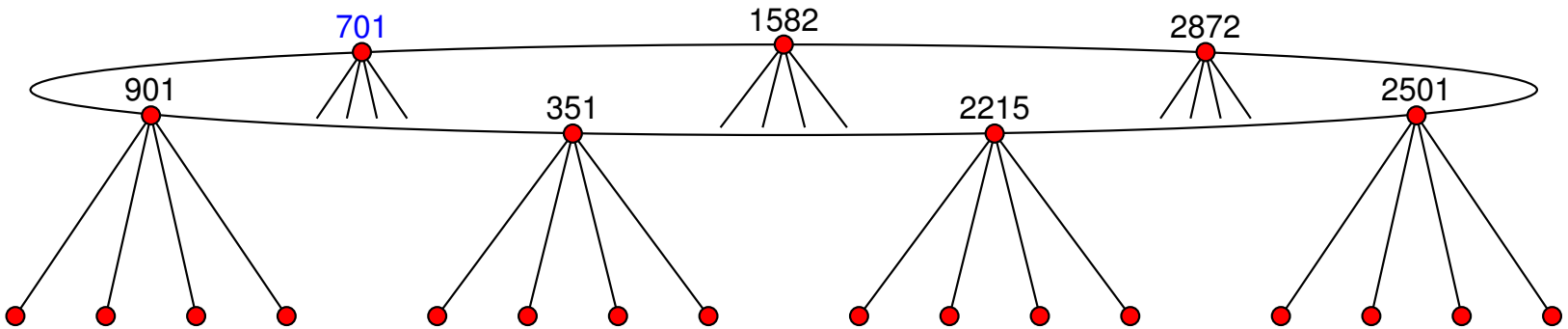
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

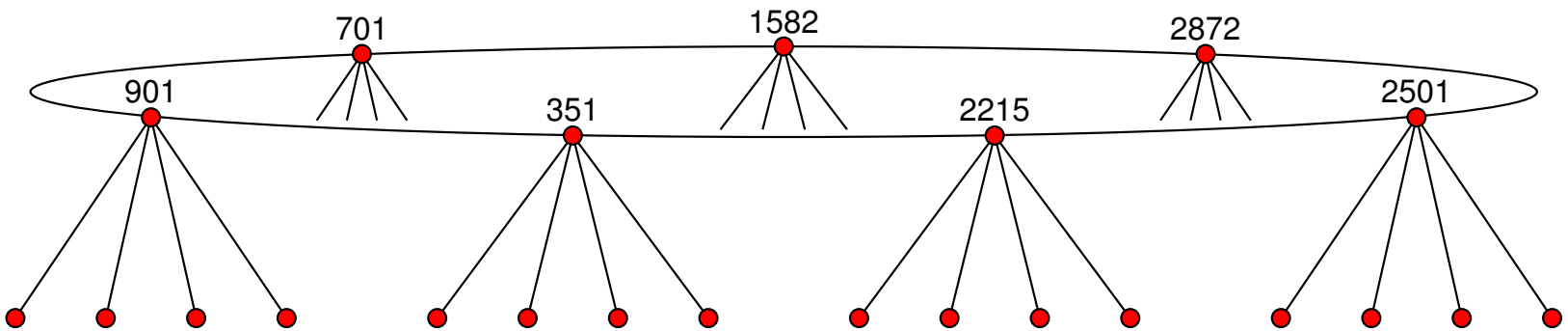
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

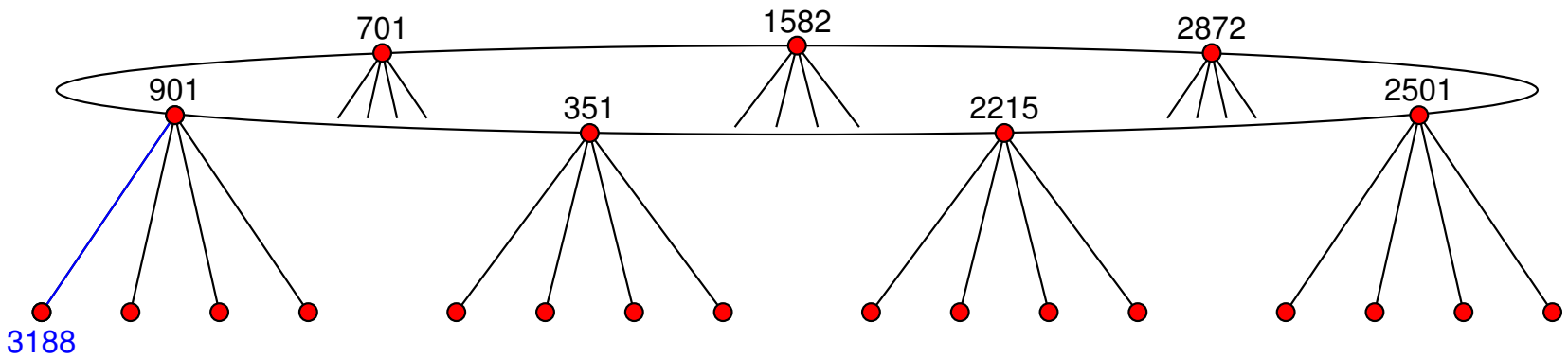
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

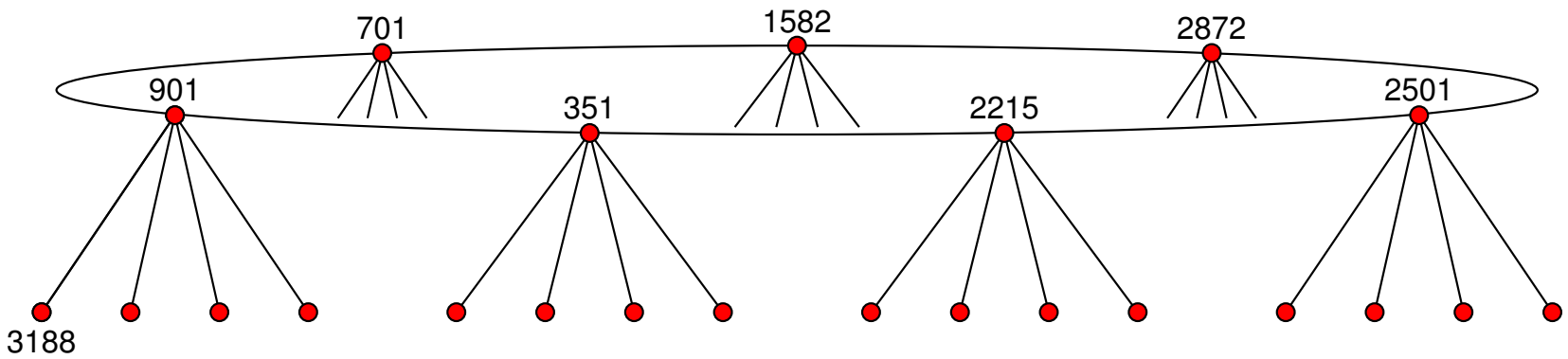
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

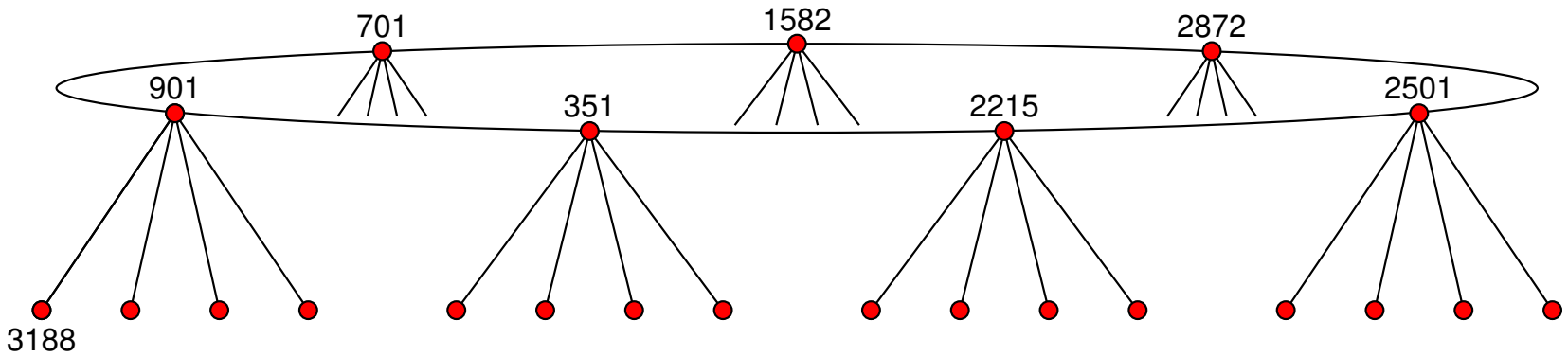
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

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

Mapping a volcano

Example

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

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

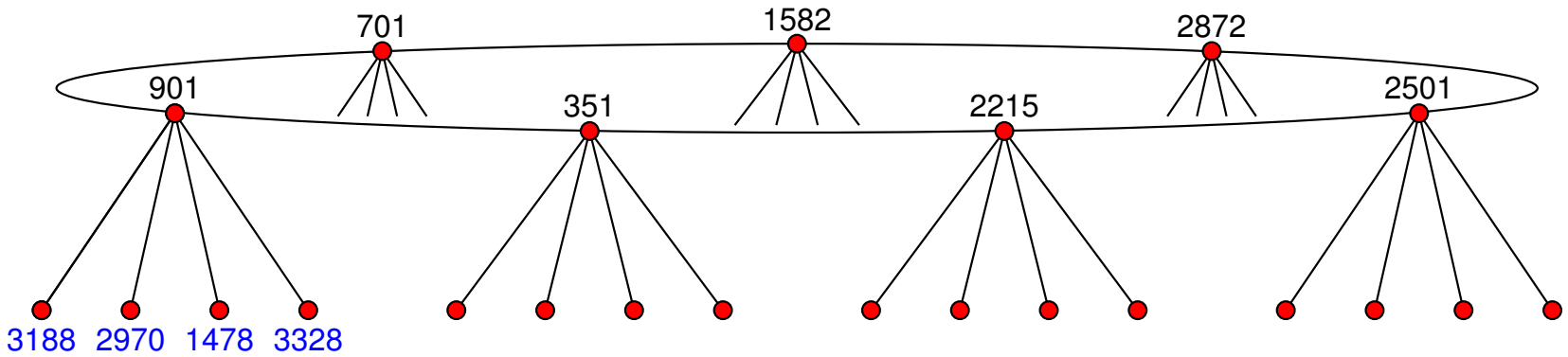
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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

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

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

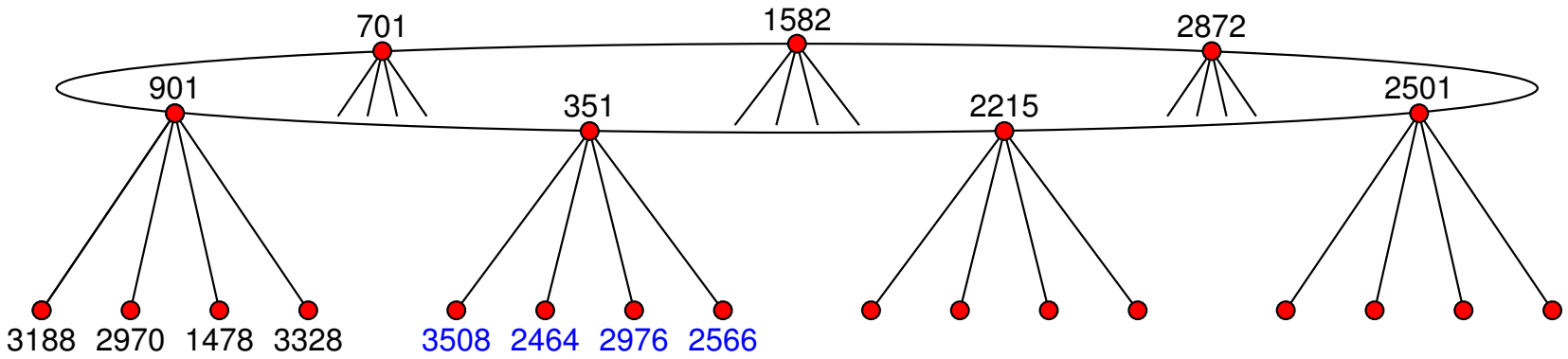
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

$3188 \xrightarrow{2} 945 \xrightarrow{2} 3144 \xrightarrow{2} 3508 \xrightarrow{2} 2843 \xrightarrow{2} 1502 \xrightarrow{2} 676 \xrightarrow{2}$

$2970 \xrightarrow{2} 3497 \xrightarrow{2} 1180 \xrightarrow{2} 2464 \xrightarrow{2} 4221 \xrightarrow{2} 4228 \xrightarrow{2} 2434 \xrightarrow{2}$

$1478 \xrightarrow{2} 3244 \xrightarrow{2} 2255 \xrightarrow{2} 2976 \xrightarrow{2} 3345 \xrightarrow{2} 1064 \xrightarrow{2} 1868 \xrightarrow{2}$

$3328 \xrightarrow{2} 291 \xrightarrow{2} 3147 \xrightarrow{2} 2566 \xrightarrow{2} 4397 \xrightarrow{2} 2087 \xrightarrow{2} 3341 \xrightarrow{2}$

Mapping a volcano

Example

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

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

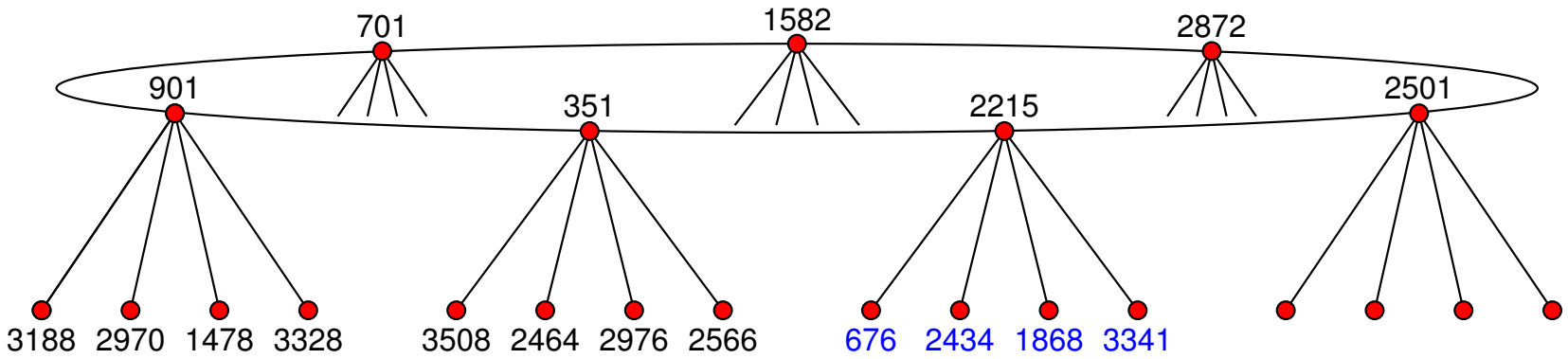
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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

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

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

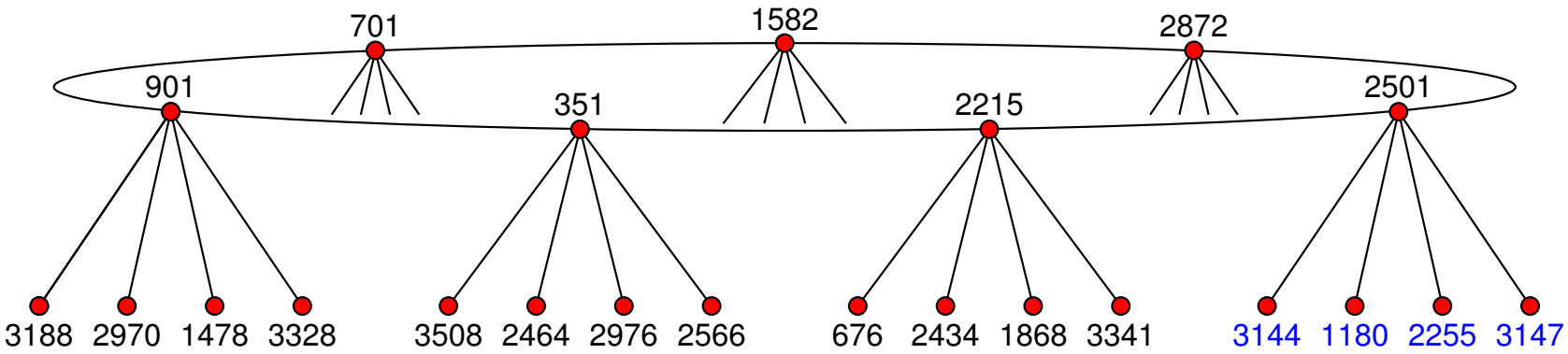
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

$3188 \xrightarrow{2} 945 \xrightarrow{2} 3144 \xrightarrow{2} 3508 \xrightarrow{2} 2843 \xrightarrow{2} 1502 \xrightarrow{2} 676 \xrightarrow{2}$

$2970 \xrightarrow{2} 3497 \xrightarrow{2} 1180 \xrightarrow{2} 2464 \xrightarrow{2} 4221 \xrightarrow{2} 4228 \xrightarrow{2} 2434 \xrightarrow{2}$

$1478 \xrightarrow{2} 3244 \xrightarrow{2} 2255 \xrightarrow{2} 2976 \xrightarrow{2} 3345 \xrightarrow{2} 1064 \xrightarrow{2} 1868 \xrightarrow{2}$

$3328 \xrightarrow{2} 291 \xrightarrow{2} 3147 \xrightarrow{2} 2566 \xrightarrow{2} 4397 \xrightarrow{2} 2087 \xrightarrow{2} 3341 \xrightarrow{2}$

Mapping a volcano

Example

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

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

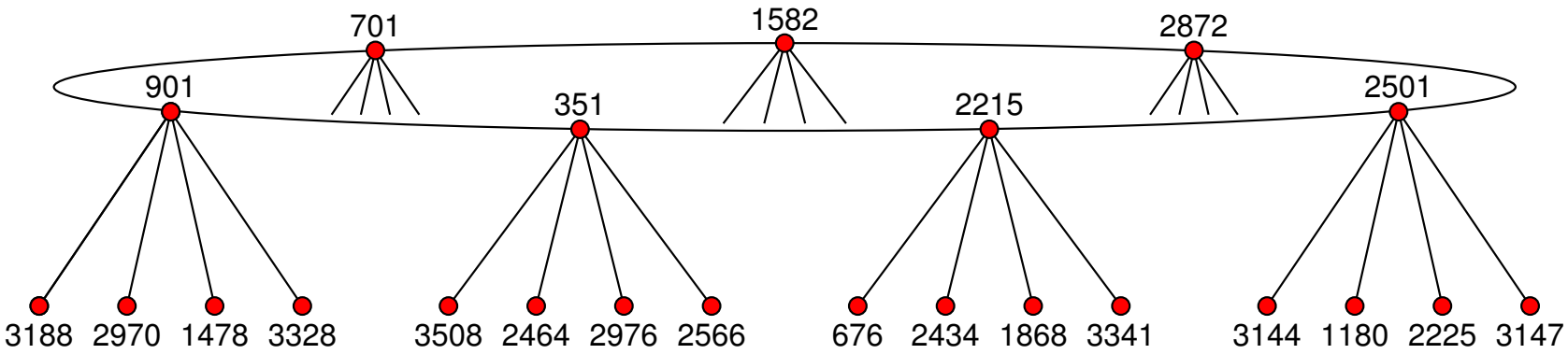
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

$3188 \xrightarrow{2} 945 \xrightarrow{2} 3144 \xrightarrow{2} 3508 \xrightarrow{2} 2843 \xrightarrow{2} 1502 \xrightarrow{2} 676 \xrightarrow{2}$

$2970 \xrightarrow{2} 3497 \xrightarrow{2} 1180 \xrightarrow{2} 2464 \xrightarrow{2} 4221 \xrightarrow{2} 4228 \xrightarrow{2} 2434 \xrightarrow{2}$

$1478 \xrightarrow{2} 3244 \xrightarrow{2} 2255 \xrightarrow{2} 2976 \xrightarrow{2} 3345 \xrightarrow{2} 1064 \xrightarrow{2} 1868 \xrightarrow{2}$

$3328 \xrightarrow{2} 291 \xrightarrow{2} 3147 \xrightarrow{2} 2566 \xrightarrow{2} 4397 \xrightarrow{2} 2087 \xrightarrow{2} 3341 \xrightarrow{2}$

Mapping a volcano

Example

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

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

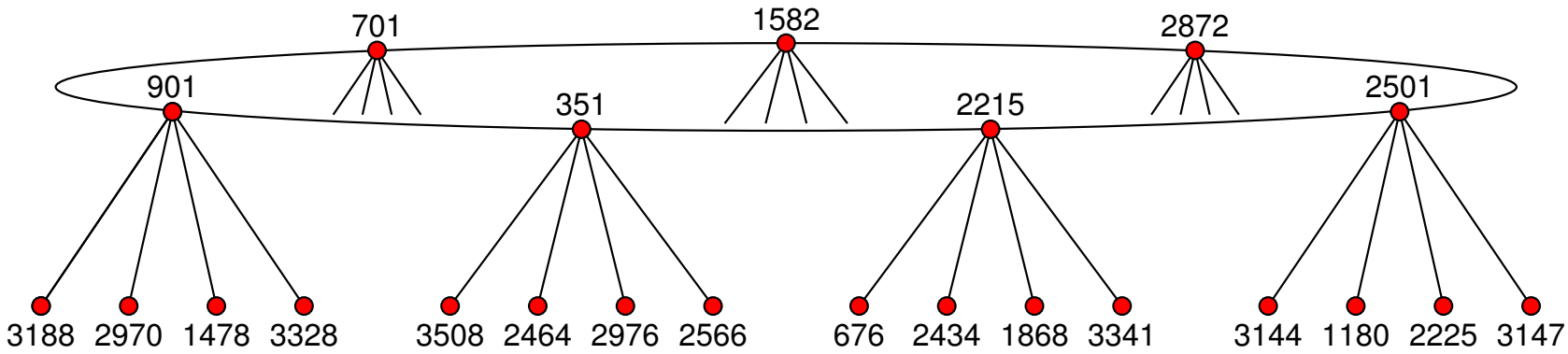
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

$3188 \xrightarrow{2} 945 \xrightarrow{2} 3144 \xrightarrow{2} 3508 \xrightarrow{2} 2843 \xrightarrow{2} 1502 \xrightarrow{2} 676 \xrightarrow{2}$

$2970 \xrightarrow{2} 3497 \xrightarrow{2} 1180 \xrightarrow{2} 2464 \xrightarrow{2} 4221 \xrightarrow{2} 4228 \xrightarrow{2} 2434 \xrightarrow{2}$

$1478 \xrightarrow{2} 3244 \xrightarrow{2} 2255 \xrightarrow{2} 2976 \xrightarrow{2} 3345 \xrightarrow{2} 1064 \xrightarrow{2} 1868 \xrightarrow{2}$

$3328 \xrightarrow{2} 291 \xrightarrow{2} 3147 \xrightarrow{2} 2566 \xrightarrow{2} 4397 \xrightarrow{2} 2087 \xrightarrow{2} 3341 \xrightarrow{2}$

Mapping a volcano

Example

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

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

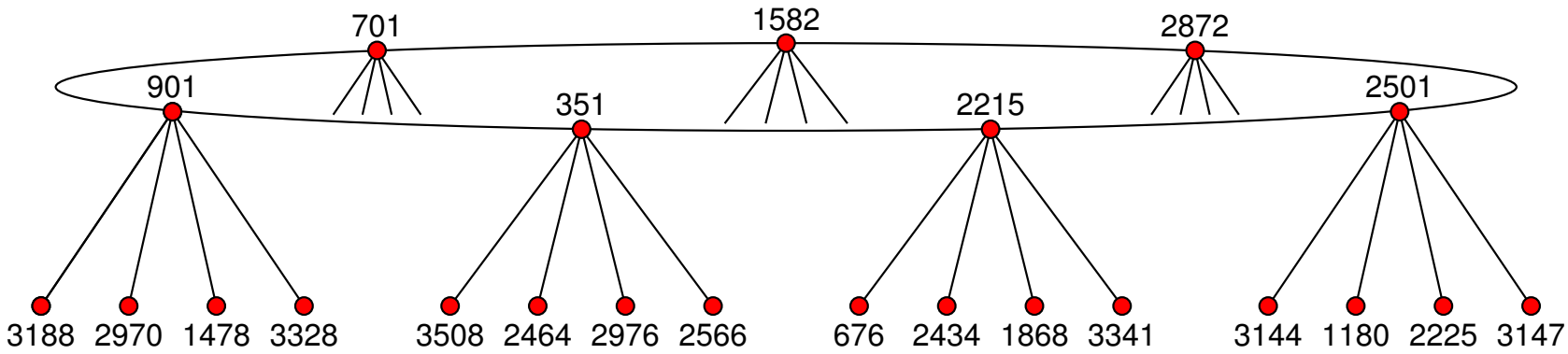
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

$3188 \xrightarrow{2} 945 \xrightarrow{2} 3144 \xrightarrow{2} 3508 \xrightarrow{2} 2843 \xrightarrow{2} 1502 \xrightarrow{2} 676 \xrightarrow{2}$

$2970 \xrightarrow{2} 3497 \xrightarrow{2} 1180 \xrightarrow{2} 2464 \xrightarrow{2} 4221 \xrightarrow{2} 4228 \xrightarrow{2} 2434 \xrightarrow{2}$

$1478 \xrightarrow{2} 3244 \xrightarrow{2} 2255 \xrightarrow{2} 2976 \xrightarrow{2} 3345 \xrightarrow{2} 1064 \xrightarrow{2} 1868 \xrightarrow{2}$

$3328 \xrightarrow{2} 291 \xrightarrow{2} 3147 \xrightarrow{2} 2566 \xrightarrow{2} 4397 \xrightarrow{2} 2087 \xrightarrow{2} 3341 \xrightarrow{2}$

Mapping a volcano

Example

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

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

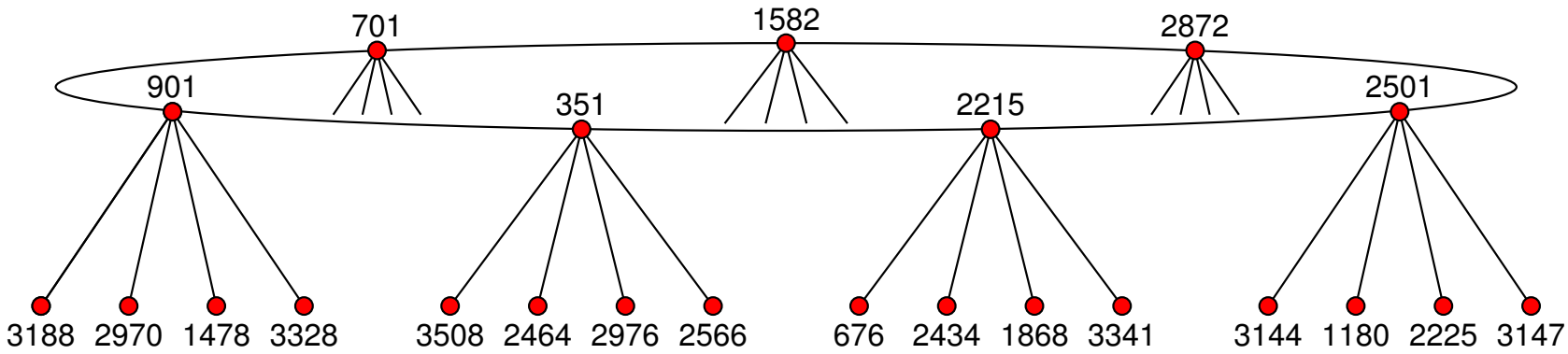
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

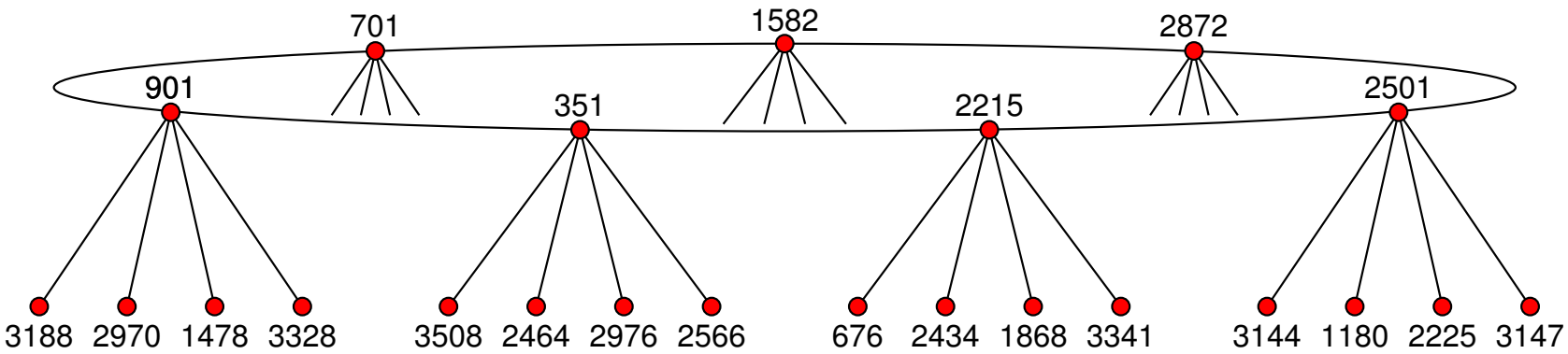
$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

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

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

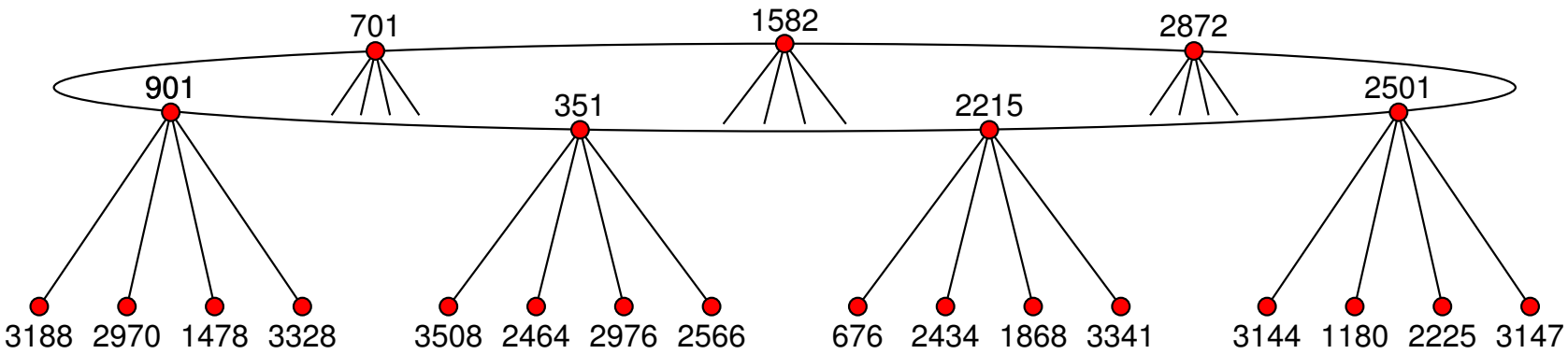


Interpolation



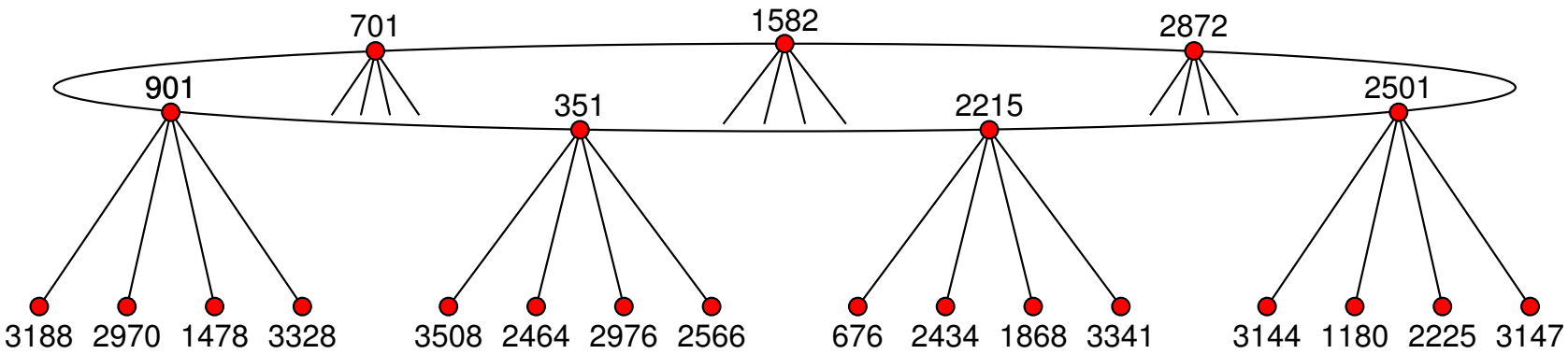
$$\Phi_5(X,\ 901) = (X - 701)(X - 351)(X - 3188)(X - 2970)(X - 1478)(X - 3328)$$
$$\Phi_5(X,\ 351) = (X - 901)(X - 2215)(X - 3508)(X - 2464)(X - 2976)(X - 2566)$$
$$\Phi_5(X, 2215) = (X - 351)(X - 2501)(X - 3341)(X - 1868)(X - 2434)(X - 676)$$
$$\Phi_5(X, 2501) = (X - 2215)(X - 2872)(X - 3147)(X - 2255)(X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

Interpolation



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

Interpolation



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

Computing $\Phi_\ell(X, Y)$ mod p

Assume D and p are suitably chosen with $D = O(\ell^2)$ and $\log p = O(\log \ell)$, and that $H_D(X)$ has been precomputed.

1.	Find a root of $H_D(X)$ over $\mathbb{F}_p$.	$O(\ell \log^{3+\epsilon} \ell)$
2.	Enumerate the surface(s) using $\mathrm{cl}(D)$-action.	$O(\ell \log^{2+\epsilon} \ell)$
3.	Descend to the floor using Vélu.	$O(\ell \log^{1+\epsilon} \ell)$
4.	Enumerate the floor using $\mathrm{cl}(\ell^2 D)$-action.	$O(\ell^2 \log^{2+\epsilon} \ell)$
5.	Build each $\Phi_\ell(X, j_i)$ from its roots.	$O(\ell^2 \log^{3+\epsilon} \ell)$
6.	Interpolate $\Phi_\ell(X, Y)$ mod p.	$O(\ell^2 \log^{3+\epsilon} \ell)$

Time complexity is $O(\ell^2 \log^{3+\epsilon} \ell)$.
Space complexity is $O(\ell^2 \log \ell)$.

After computing $\Phi_5(X, Y)$ mod p for the primes:

$$4451, 6911, 9551, 28111, 54851, 110051, 123491, 160591, 211711, 280451, 434111, 530851, 686051, 736511,$$

we apply the CRT to obtain

$$\begin{aligned}
\Phi_5(X, Y) &= X^6 + Y^6 - X^5Y^5 + 3720(X^5Y^4 + X^4Y^5) - 4550940(X^5Y^3 + X^3Y^5) \\
&\quad + 2028551200(X^5Y^2 + X^2Y^5) - 246683410950(X^5Y + XY^5) + 1963211489280(X^5 + Y^5) \\
&\quad + 1665999364600X^4Y^4 + 107878928185336800(X^4Y^3 + X^3Y^4) \\
&\quad + 38308360979811215375(X^4Y^2 + X^2Y^4) + 12854179890682881638400 0(X^4Y + XY^4) \\
&\quad + 1284733132841424456253440(X^4 + Y^4) - 4550940(X^3Y^5 + X^5Y^3) \\
&\quad - 4412069655129148352461 00X^3Y^3 + 26898488858380731577417728000(X^3Y^2 + X^2Y^3) \\
&\quad - 19245793461892829965510823116 8000(X^3Y + XY^3) \\
&\quad + 28024477782843952780432156529 7868800(X^3 + Y^3) \\
&\quad + 5110941777552418083110765199360000X^2Y^2 \\
&\quad + 3655473658394962929570647233265664 0000(X^2Y + XY^2) \\
&\quad + 6692500042627997708487149415015068467200(X^2 + Y^2) \\
&\quad - 2640734570766205962597157902479787829493 76XY \\
&\quad + 5327433080342442545042016027335650915123 2000(X + Y) \\
&\quad + 1413599471547213586977534746910713627510046 72000.
\end{aligned}$$

After computing $\Phi_5(X, Y)$ mod p for the primes:

$$4451, 6911, 9551, 28111, 54851, 110051, 123491, 160591, 211711, 280451, 434111, 530851, 686051, 736511,$$

we apply the CRT to obtain

$$\begin{aligned}
\Phi_5(X, Y) &= X^6 + Y^6 - X^5Y^5 + 3720(X^5Y^4 + X^4Y^5) - 4550940(X^5Y^3 + X^3Y^5) \\
&\quad + 2028551200(X^5Y^2 + X^2Y^5) - 246683410950(X^5Y + XY^5) + 1963211489280(X^5 + Y^5) \\
&\quad + 1665999364600X^4Y^4 + 107878928185336800(X^4Y^3 + X^3Y^4) \\
&\quad + 38308360979811215375(X^4Y^2 + X^2Y^4) + 12854179890682881638400 0(X^4Y + XY^4) \\
&\quad + 1284733132841424456253440(X^4 + Y^4) - 4550940(X^3Y^5 + X^5Y^3) \\
&\quad - 4412069655129148352461 00X^3Y^3 + 26898488858380731577417728000(X^3Y^2 + X^2Y^3) \\
&\quad - 19245793461892829965510823116 8000(X^3Y + XY^3) \\
&\quad + 28024477782843952780432156529 7868800(X^3 + Y^3) \\
&\quad + 5110941777552418083110765199360000X^2Y^2 \\
&\quad + 3655473658394962929570647233265664 0000(X^2Y + XY^2) \\
&\quad + 6692500042627997708487149415015068467200(X^2 + Y^2) \\
&\quad - 2640734570766205962597157902479787829493 76XY \\
&\quad + 5327433080342442545042016027335650915123 2000(X + Y) \\
&\quad + 1413599471547213586977534746910713627510046 72000.
\end{aligned}$$

(but note that $\Phi_5^{\mathrm{f}}(X, Y) = X^6 + Y^6 - X^5Y^5 + 4XY$).

The algorithm

Given a prime $\ell > 2$ and an integer $q > 0$:

1. Pick a discriminant D suitable for ℓ.
2. Select a set of primes S suitable for ℓ and D.
3. Precompute H_D, $\mathrm{cl}(D)$, $\mathrm{cl}(\ell^2 D)$, and CRT data.
4. For each $p \in S$, compute $\Phi_\ell \bmod p$ and update CRT data.
5. Perform CRT postcomputation and output $\Phi_\ell \bmod q$.

To compute Φ_ℓ over $\mathbb{Z}$, just use $q = \prod p$.

For "small" q, use explicit CRT mod q.
For "large" q, standard CRT for large q.
For q in between, use a hybrid approach.

Explicit Chinese remainder theorem

Suppose $c \equiv c_i \bmod p_i$ for n 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 is the closest integer to $\sum c_i a_i / p_i$.

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

Montgomery-Silverman, Bernstein, S.

Complexity

Theorem (GRH)

For every prime $\ell > 2$ there is a suitable discriminant D with $|D| = O(\ell^2)$ for which there are $\Omega(\ell^3 \log^3 \ell)$ primes $p = O(\ell^6 (\log \ell)^4)$ that are suitable for ℓ and D.

Heuristically, $p = O(\ell^4)$. In practice, $\lg p < 64$.

Theorem (GRH)

The expected running time is $O(\ell^3 \log^3 \ell \log\log \ell)$.
The space required is $O(\ell^2 \log(\ell q))$.

Complexity

Theorem (GRH)

For every prime $\ell > 2$ there is a suitable discriminant D with $|D| = O(\ell^2)$ for which there are $\Omega(\ell^3 \log^3 \ell)$ primes $p = O(\ell^6 (\log \ell)^4)$ that are suitable for ℓ and D.

Heuristically, $p = O(\ell^4)$. In practice, $\lg p < 64$.

Theorem (GRH)

The expected running time is $O(\ell^3 \log^3 \ell \log\log \ell)$.
The space required is $O(\ell^2 \log(\ell q))$.

The algorithm is trivial to parallelize.

An explicit height bound for Φ_ℓ

Let ℓ be a prime.
Let $h(\Phi_\ell)$ be the (natural) logarithmic height of Φ_ℓ.

Asymptotic bound: $h(\Phi_\ell) = 6\ell \log \ell + O(\ell)$ (Paula Cohen 1984).

An explicit height bound for Φ_ℓ

Let ℓ be a prime.
Let $h(\Phi_\ell)$ be the (natural) logarithmic height of Φ_ℓ.

Asymptotic bound: $h(\Phi_\ell) = 6\ell \log \ell + O(\ell)$ (Paula Cohen 1984).

Explicit bound: $h(\Phi_\ell) \leq 6\ell \log \ell + 18\ell$ (Bröker-S 2009).

Conjectural bound: $h(\Phi_\ell) \leq 6\ell \log \ell + 12\ell$ (for $\ell > 30$).

The explicit bound holds for all ℓ.
The conjectural bound is known to hold for $30 < \ell < 3600$.

Other modular functions

We can compute polynomials relating $f(z)$ and $f(\ell z)$ for other modular functions, including the Weber function

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

which 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 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:

$$X^{12} + Y^{12} - X^{11}Y^{11} + 8184X^{11}Y^{10} - 28278756X^{11}Y^9 + 53686822816X^{11}Y^8$$
$$- 61058988656490X^{11}Y^7 + 42570393135641712X^{11}Y^6 - 178995262728830390 48X^{11}Y^5$$
$$+ 4297837238774928467520X^{11}Y^4 - 5291348418446396138617 95X^{11}Y^3 + 272098116580566458155226 00X^{11}Y^2$$
$$- 3746420063567013935158176 12X^{11}Y + 2964709023552405752832000 00X^{11}$$

. . . 8 pages omitted . . .

$+ 392423345094527654908696$ . . . 100 digits omitted . . . 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:

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

Weber modular polynomials

For $\ell = 1009$, the size of $\Phi_\ell^{\mathfrak{f}}$ is 2.3MB, versus 3.9GB for Φ_ℓ, and computing $\Phi_\ell^{\mathfrak{f}}$ takes 2.8s, versus 2830s for Φ_ℓ.

The current record is $\ell = 60013$.
Working mod q, level $\ell > 100019$ has been achieved.

The polynomials $\Phi_\ell^{\mathfrak{f}}$ for all $\ell < 5000$ are available for download:

`http://math.mit.edu/~drew`