Genus 1 point counting in essentially quartic time and quadratic space

Andrew V. Sutherland

Massachusetts Institute of Technology

September 30, 2010

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

Genus 1 point counting in large characteristic

Let $q > 3$ be prime and let $E/\mathbb{F}_q$ be defined by

$$y^2 = x^3 + ax + b.$$

We wish to compute $\#E(\mathbb{F}_q) = q + 1 - t$. Let $n = \log q$.

Genus 1 point counting in large characteristic

Let $q > 3$ be prime and let $E/\mathbb{F}_q$ be defined by

$$y^2 = x^3 + ax + b.$$

We wish to compute $\#E(\mathbb{F}_q) = q + 1 - t$. Let $n = \log q$.

Algorithm	Time	Space
Totally Naive	$O(e^{2n+\epsilon})$	$O(n)$

Genus 1 point counting in large characteristic

Let $q > 3$ be prime and let $E/\mathbb{F}_q$ be defined by

$$y^2 = x^3 + ax + b.$$

We wish to compute $\#E(\mathbb{F}_q) = q + 1 - t$. Let $n = \log q$.

Algorithm	Time	Space
Totally Naive	$O(e^{2n+\epsilon})$	$O(n)$
Slightly Less Naive	$O(e^{n+\epsilon})$	$O(n)$

Genus 1 point counting in large characteristic

Let $q > 3$ be prime and let $E/\mathbb{F}_q$ be defined by

$$y^2 = x^3 + ax + b.$$

We wish to compute $\#E(\mathbb{F}_q) = q + 1 - t$. Let $n = \log q$.

Algorithm	Time	Space
Totally Naive	$O(e^{2n+\epsilon})$	$O(n)$
Slightly Less Naive	$O(e^{n+\epsilon})$	$O(n)$
BSGS	$O(e^{n/4+\epsilon})$	$O(e^{n/4+\epsilon})$

Genus 1 point counting in large characteristic

Let $q > 3$ be prime and let $E/\mathbb{F}_q$ be defined by

$$y^2 = x^3 + ax + b.$$

We wish to compute $\#E(\mathbb{F}_q) = q + 1 - t$. Let $n = \log q$.

Algorithm	Time	Space
Totally Naive	$O(e^{2n+\epsilon})$	$O(n)$
Slightly Less Naive	$O(e^{n+\epsilon})$	$O(n)$
BSGS	$O(e^{n/4+\epsilon})$	$O(e^{n/4+\epsilon})$
Pollard kangaroo	$O(e^{n/4+\epsilon})$	$O(n^2)$

Genus 1 point counting in large characteristic

Let $q > 3$ be prime and let $E/\mathbb{F}_q$ be defined by

$$y^2 = x^3 + ax + b.$$

We wish to compute $\#E(\mathbb{F}_q) = q + 1 - t$. Let $n = \log q$.

Algorithm	Time	Space
Totally Naive	$O(e^{2n+\epsilon})$	$O(n)$
Slightly Less Naive	$O(e^{n+\epsilon})$	$O(n)$
BSGS	$O(e^{n/4+\epsilon})$	$O(e^{n/4+\epsilon})$
Pollard kangaroo	$O(e^{n/4+\epsilon})$	$O(n^2)$
Schoof	$O(n^5 \operatorname{llog} n)$	$O(n^3)$

Genus 1 point counting in large characteristic

Let $q > 3$ be prime and let $E/\mathbb{F}_q$ be defined by

$$y^2 = x^3 + ax + b.$$

We wish to compute $\#E(\mathbb{F}_q) = q + 1 - t$. Let $n = \log q$.

Algorithm	Time	Space
Totally Naive	$O(e^{2n+\epsilon})$	$O(n)$
Slightly Less Naive	$O(e^{n+\epsilon})$	$O(n)$
BSGS	$O(e^{n/4+\epsilon})$	$O(e^{n/4+\epsilon})$
Pollard kangaroo	$O(e^{n/4+\epsilon})$	$O(n^2)$
Schoof	$O(n^5 \operatorname{llog} n)$	$O(n^3)$
SEA (Φ_ℓ precomputed)	$O(n^4 \operatorname{llog} n)$	$O(n^4)$
SEA (Φ_ℓ via [Enge 2009])	$O(n^4 \log^3 n \operatorname{llog} n)$	$O(n^3 \log n)$

Genus 1 point counting in large characteristic

Let $q > 3$ be prime and let $E/\mathbb{F}_q$ be defined by

$$y^2 = x^3 + ax + b.$$

We wish to compute $\#E(\mathbb{F}_q) = q + 1 - t$. Let $n = \log q$.

Algorithm	Time	Space
Totally Naive	$O(e^{2n+\epsilon})$	$O(n)$
Slightly Less Naive	$O(e^{n+\epsilon})$	$O(n)$
BSGS	$O(e^{n/4+\epsilon})$	$O(e^{n/4+\epsilon})$
Pollard kangaroo	$O(e^{n/4+\epsilon})$	$O(n^2)$
Schoof	$O(n^5 \operatorname{llog} n)$	$O(n^3)$
SEA (Φ_ℓ precomputed)	$O(n^4 \operatorname{llog} n)$	$O(n^4)$
SEA (Φ_ℓ via [Enge 2009])	$O(n^4 \log^3 n \operatorname{llog} n)$	$O(n^3 \log n)$
Today's talk	$O(n^4 \log^2 n \operatorname{llog} n)$	$O(n^2)$
Amortized	$O(n^4 \operatorname{llog} n)$	$O(n^2)$

A quote from the 2007 record holder (2500 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

The Classical Modular Polynomial $\Phi_\ell(X, Y)$

$\Phi_\ell \in \mathbb{Z}[X, Y]$ parameterizes pairs of ℓ-isogenous elliptic curves.
It is symmetric, with degree $\ell + 1$ in both X and Y.

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 $\Phi_\ell(X, Y)$

Plan of the talk

- A quick review of the SEA algorithm and its complexity.
- Instantiated modular polynomials using the CRT.
- Modular polynomials via isogeny volcanoes.
- Numerical results (5000+ digit record).

The elliptic curve group law

Point addition may defined by as follows:

$$(x_1, y_1) + (x_2, y_2) = (\lambda^2 - x_1 - x_2, (x_1 - x_3)\lambda - y_1),$$

where

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } x_1 \neq x_2 \\ (3x_1^2 + a)/(2y_1) & \text{if } x_1 = x_2 \end{cases}$$

The elliptic curve group law

Point addition may defined by as follows:

$$(x_1, y_1) + (x_2, y_2) = (\lambda^2 - x_1 - x_2, (x_1 - x_3)\lambda - y_1),$$

where

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } x_1 \neq x_2 \\ (3x_1^2 + a)/(2y_1) & \text{if } x_1 = x_2 \end{cases}$$

We can use this to compute multiples of a point $P = (x, y)$:

$$2P = \left(\frac{x^4 - 2ax^2 - 8bx + a^2}{(2y)^2}, \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{(2y)^3} \right)$$

$$3P = \left(\frac{x^9 - 12ax^7 - \cdots + 64b^3}{(3x^4 + 6ax^2 + 12bx - a^2)^2}, \frac{4x^{15} + 92ax^{13} + \cdots - 2048b^5}{(3x^4 + 6ax2 + 12bx - a^2)^3} \right)$$

$$4P = \cdots$$

Division polynomials

In general, the ℓth multiple of $P = (x, y)$ may be written as

$$\ell P = \left(\frac{\theta_\ell(x,y)}{\psi_\ell(x,y)^2}, \frac{\omega_\ell(x,y)}{\psi_\ell(x,y)^3} \right)$$

where $\theta_\ell, \omega_\ell, \psi_\ell$ are polynomials in x and y.

The ℓth *division polynomial* of E defined by

$$f_\ell = \begin{cases} \psi_\ell & \text{if } \ell \text{ is odd} \\ \psi_\ell/\psi_2 & \text{if } \ell \text{ is even} \end{cases}$$

is a univariate polynomial in x. It has degree $O(\ell^2)$ and its roots are the abscissa of the nontrivial points in $E[\ell]$.

Schoof's algorithm

1. For sufficiently many primes ℓ (up to $\approx n/2$):

   Determine which $t_\ell = 0, 1, \ldots, \ell - 1$ satisfies

   $$\pi^2 - [t_\ell]\pi + [q_\ell] \equiv 0 \bmod (f_\ell, E),$$

   where $t_\ell = t \bmod \ell$ and $q_\ell = q \bmod \ell$.
   π is the Frobenius endomorphism: $(x, y) \mapsto (x^q, y^q)$.

2. Use the CRT to determine t and $\#E(\mathbb{F}_q) = q + 1 - t$.

Schoof's algorithm

1. For sufficiently many primes ℓ (up to $\approx n/2$):

   Determine which $t_\ell = 0, 1, \ldots, \ell - 1$ satisfies

   $$\pi^2 - [t_\ell]\pi + [q_\ell] \equiv 0 \bmod (f_\ell, E),$$

   where $t_\ell = t \bmod \ell$ and $q_\ell = q \bmod \ell$.
   π is the Frobenius endomorphism: $(x, y) \mapsto (x^q, y^q)$.

2. Use the CRT to determine t and $\#E(\mathbb{F}_q) = q + 1 - t$.

The computation of (x^q, y^q) in $\mathbb{F}_q[x, y]/(f_\ell, E)$ dominates:

$$\text{Time} = \sum_\ell O(n\mathsf{M}(\ell^2 n)) = O(n^5 \operatorname{llog} n)$$

$$\text{Space} = \max_\ell O(\ell^2 n) = O(n^3)$$

SEA algorithm (Elkies version)

1. For sufficiently many primes ℓ (up to $\approx n$):

   Compute $\Phi_\ell(X, Y)$.
   Evaluate $\phi_\ell(Y) = \Phi_\ell(\mathrm{j}, Y)$, where $\mathrm{j} = \mathrm{j}(E)$.
   If ϕ_ℓ has a root $\tilde{\mathrm{j}}$ in $\mathbb{F}_q$:
      Compute a normalized isogeny to $\tilde{E}/\mathbb{F}_q$.
      Compute a factor g_ℓ of f_ℓ.
      Determine which $\lambda_\ell = 0, 1, \ldots, \ell - 1$ satisfies

$$\pi - [\lambda_\ell] \equiv 0 \bmod (g_\ell, E)$$

      and set $t_\ell = \lambda_\ell + q_\ell/\lambda_\ell \bmod \ell$.

2. Use the CRT to determine t and $\#E(\mathbb{F}_q) = q + 1 - t$.

SEA complexity

Task	Time	Space
Compute Φ_ℓ	$O(\ell^2 \log^3 \ell \mathsf{M}(\ell))$	$O(\ell^3 \log \ell)$
Compute ϕ_ℓ	$O(\ell^2 \mathsf{M}(\ell+n))$	$O(\ell^3 \log \ell)$
Find a root $\tilde{\jmath}$	$O(n\mathsf{M}(\ell n))$	$O(\ell n)$
Construct $\tilde{E}$	$O(\ell^2 \mathsf{M}(n))$	$O(\ell^2 n)$
Compute g_ℓ	$O(\ell^2 \mathsf{M}(n))$	$O(\ell n)$
Compute $\pi \bmod g_\ell, E$	$O(n\mathsf{M}(\ell n))$	$O(\ell n)$
Find λ_ℓ	$O(\ell \mathsf{M}(\ell n))$	$O(\ell n)$
Apply CRT	$O(\mathsf{M}(n) \log n)$	$O(n)$

Total time is $O(n^4 \log^3 n \operatorname{llog} n)$ using $O(n^3 \log n)$ space.

Algorithms to compute Φ_ℓ

q-expansions:

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

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

isogenies: (Charles-Lauter 2005)

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

evaluation-interpolation: (Enge 2009)

Φ_ℓ:	$O(\ell^3\log^{4+\epsilon}\ell)$	(floating-point)

Computing Φ_ℓ with the CRT

Strategy: compute $\Phi_\ell \bmod p$ for sufficiently many primes p and use the CRT to compute Φ_ℓ (or $\Phi_\ell \bmod q$).

Computing Φ_ℓ with the CRT

Strategy: compute $\Phi_\ell \bmod p$ for sufficiently many primes p and use the CRT to compute Φ_ℓ (or $\Phi_\ell \bmod q$).

- For "special" primes p we can compute $\Phi_\ell \bmod p$ in time $O(\ell^2 \log^3 p \operatorname{llog} p)$ using isogeny volcanoes [BLS 2010].

Computing Φ_ℓ with the CRT

Strategy: compute $\Phi_\ell \bmod p$ for sufficiently many primes p and use the CRT to compute Φ_ℓ (or $\Phi_\ell \bmod q$).

- For "special" primes p we can compute $\Phi_\ell \bmod p$ in time $O(\ell^2 \log^3 p \operatorname{llog} p)$ using isogeny volcanoes [BLS 2010].
- Assuming the GRH, we can efficiently find sufficiently many such primes with $\log p = O(\log \ell)$.

Computing Φ_ℓ with the CRT

Strategy: compute $\Phi_\ell \bmod p$ for sufficiently many primes p and use the CRT to compute Φ_ℓ (or $\Phi_\ell \bmod q$).

- For "special" primes p we can compute $\Phi_\ell \bmod p$ in time $O(\ell^2 \log^3 p \operatorname{llog} p)$ using isogeny volcanoes [BLS 2010].
- Assuming the GRH, we can efficiently find sufficiently many such primes with $\log p = O(\log \ell)$.

Computes Φ_ℓ in $O(\ell^3 \log^3 \ell \operatorname{llog} \ell)$ time and $O(\ell^3 \log \ell)$ space.

We can directly compute $\Phi_\ell \bmod q$ using $O(\ell^2(n + \log \ell))$ space. But this is still bigger than we want (or need)...

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 $c \in \mathbb{Z}$.

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 is the closest integer to $\sum a_i c_i / M_i$, computed using $O(\log k)$ bits of precision.

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 is the closest integer to $\sum a_i c_i / M_i$, computed using $O(\log k)$ bits of precision.

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

Montgomery-Silverman 1990, Bernstein 1995, S 2009.

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

Strategy: lift $\mathrm{j} = \mathrm{j}(E)$ from $\mathbb{F}_q$ to $\mathbb{Z}$ and then compute

$$\phi_\ell(Y) = \Phi_\ell(\mathrm{j}, Y) \bmod p$$

for sufficiently many (special) primes p and use the explicit CRT to obtain $\phi_\ell \bmod q$.

This uses $O(\ell^2 \mathsf{M}(\log p))$ time for each p, in $O(\ell \log p)$ space.

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

Strategy: lift $\mathrm{j} = \mathrm{j}(E)$ from $\mathbb{F}_q$ to $\mathbb{Z}$ and then compute

$$\phi_\ell(Y) = \Phi_\ell(\mathrm{j}, Y) \bmod p$$

for sufficiently many (special) primes p and use the explicit CRT to obtain $\phi_\ell \bmod q$.

This uses $O(\ell^2 \mathsf{M}(\log p))$ time for each p, in $O(\ell \log p)$ space.

However, "sufficiently many" is $O(\ell n)$.
Total time is $O(\ell^3 n \mathsf{M}(\log \ell)$, using $O(\ell n + \ell \log \ell)$ space.

In situations where $n \ll \ell$ this may be useful, but not in SEA.

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

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

$$\phi_\ell(Y) = \Phi_\ell(\mathrm{j}, Y) \bmod p$$

for sufficiently many (special) primes p and use the explicit CRT to obtain $\phi_\ell \bmod q$.

This uses $O(\ell^2 \log^3 p \operatorname{llog} p)$ time for each p, in $O(\ell^2 \log \ell)$ space, and this can be reduced to $O(\ell^2)$.

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

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

$$\phi_\ell(Y) = \Phi_\ell(\mathrm{j}, Y) \bmod p$$

for sufficiently many (special) primes p and use the explicit CRT to obtain $\phi_\ell \bmod q$.

This uses $O(\ell^2 \log^3 p \operatorname{llog} p)$ time for each p, in $O(\ell^2 \log \ell)$ space, and this can be reduced to $O(\ell^2)$.

Now "sufficiently many" is $O(\ell + n)$.
Total time is $O(\ell^2 n \log^3 \ell \operatorname{llog} \ell)$, using $O(\ell n + \ell^2)$ space.

This is perfect for SEA, and can also be applied to the partial derivatives of Φ_ℓ, which we need to construct $\tilde{E}$.

Modified SEA complexity

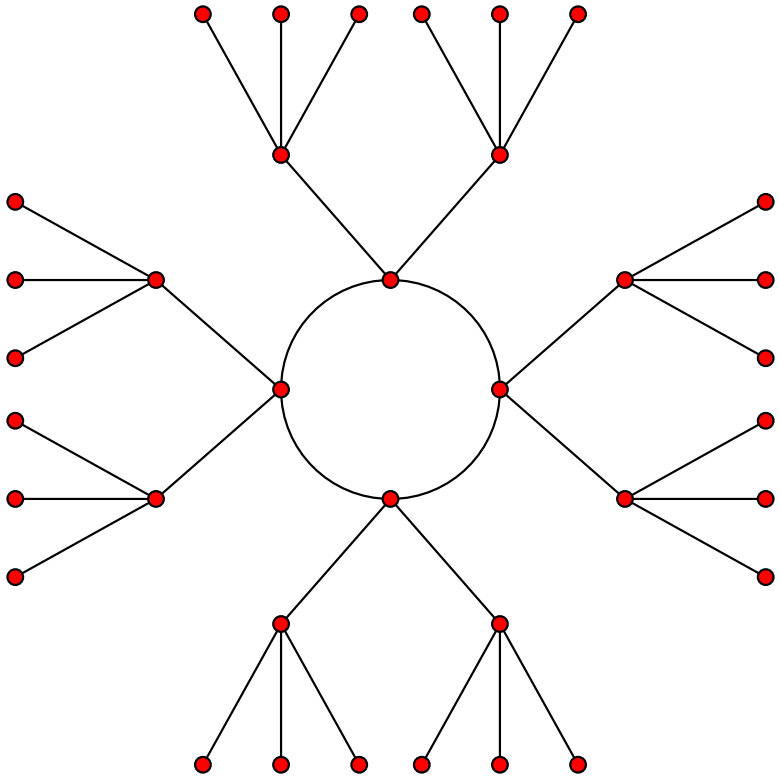
Task	Time	Space
Compute ϕ_ℓ	$O(\ell^2 \log^2 \ell \mathsf{M}(\ell))$	$O(\ell n + \ell^2)$
Find a root $\tilde{\jmath}$	$O(n\mathsf{M}(\ell n)$	$O(\ell n)$
Construct $\tilde{E}$	$O(\ell^2 \mathsf{M}(n))$	$O(\ell n)$
Compute g_ℓ	$O(\ell^2 \mathsf{M}(n))$	$O(\ell n)$
Compute $\pi \bmod h_\ell, E$	$O(n\mathsf{M}(\ell n)$	$O(\ell n)$
Find λ_ℓ	$O(\ell \mathsf{M}(\ell n))$	$O(\ell n)$
Apply CRT	$O(\mathsf{M}(n) \log n)$	$O(n)$

Total time is $O(n^4 \log^2 n \operatorname{llog} n)$ using $O(n^2)$ space.

We can simultaneously compute $\phi_\ell \bmod q$ for $O(\log^2 n)$ curves at essentially no additional cost.

Amortized complexity: $O(n^4 \operatorname{llog} n)$ time using $O(n^2)$ space.

A 3-volcano of depth 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.

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 ℓ+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 ℓ+1.

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

The ℓ-isogeny graph

The modular polynomial $\Phi_\ell \in \mathbb{Z}[X,Y]$ has the property

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

The ℓ-isogeny graph

The modular polynomial $\Phi_\ell \in \mathbb{Z}[X,Y]$ has the property

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

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

The neighbors of j are the roots of $\phi_\ell(X) = \Phi_\ell(X, j)$.

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 $j = 0, 1728$).
- Curves at level V_i of an ℓ-volcano 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.
- The depth is $d = \frac{1}{2} v_\ell \left(\frac{t^2 - 4p}{\mathrm{disc}(\mathcal{O})} \right)$.

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

The CM action

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with $\mathrm{End}(E) \cong \mathcal{O}$.

The class group $\mathrm{cl}(\mathcal{O})$ acts on the set

$$\{j(E/\mathbb{F}_q) : \mathrm{End}(E) \cong \mathcal{O}\}.$$

Horizontal ℓ-isogenies are the action of an $\mathcal{O}$-ideal with norm ℓ.

The CM action

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with $\mathrm{End}(E) \cong \mathcal{O}$.

The class group $\mathrm{cl}(\mathcal{O})$ acts on the set

$$\{j(E/\mathbb{F}_q) : \mathrm{End}(E) \cong \mathcal{O}\}.$$

Horizontal ℓ-isogenies are the action of an $\mathcal{O}$-ideal with norm ℓ.

The cardinality of V_0 is the order of the cyclic subgroup of $\mathrm{cl}(\mathcal{O})$ generated by an ideal with norm ℓ.

The CM action

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with $\mathrm{End}(E) \cong \mathcal{O}$.

The class group $\mathrm{cl}(\mathcal{O})$ acts on the set

$$\{j(E/\mathbb{F}_q) : \mathrm{End}(E) \cong \mathcal{O}\}.$$

Horizontal ℓ-isogenies are the action of an $\mathcal{O}$-ideal with norm ℓ.

The cardinality of V_0 is the order of the cyclic subgroup of $\mathrm{cl}(\mathcal{O})$ generated by an ideal with norm ℓ.

A horizontal isogeny of large degree may be equivalent to a sequence of isogenies of small degree, via relations in $\mathrm{cl}(\mathcal{O})$.

The CM action

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with $\mathrm{End}(E) \cong \mathcal{O}$.

The class group $\mathrm{cl}(\mathcal{O})$ acts on the set

$$\{j(E/\mathbb{F}_q) : \mathrm{End}(E) \cong \mathcal{O}\}.$$

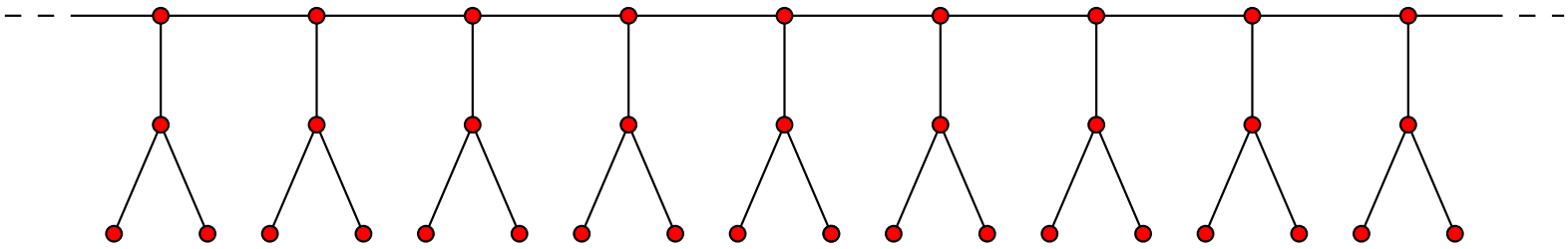
Horizontal ℓ-isogenies are the action of an $\mathcal{O}$-ideal with norm ℓ.

The cardinality of V_0 is the order of the cyclic subgroup of $\mathrm{cl}(\mathcal{O})$ generated by an ideal with norm ℓ.

A horizontal isogeny of large degree may be equivalent to a sequence of isogenies of small degree, via relations in $\mathrm{cl}(\mathcal{O})$.

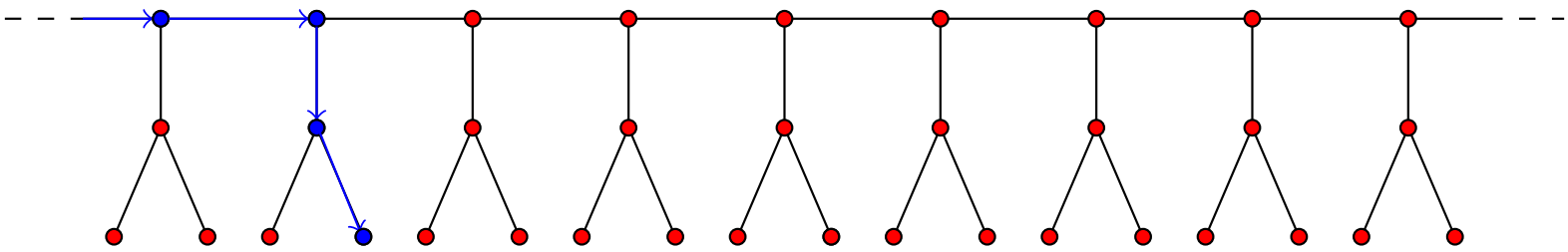
Under the ERH this is always true, and "small" $= O(\log^2 |D|)$.

Running the rim



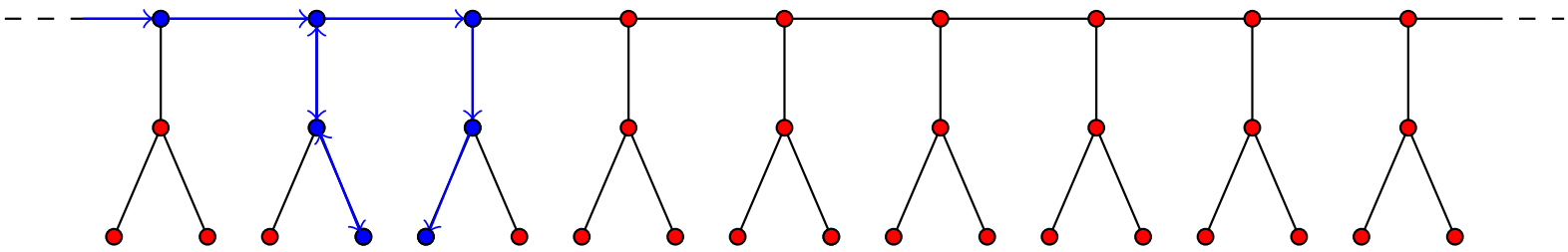
$$\Phi_2(X,Y) = X^3 + Y^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 + 40773375XY$$
$$+ 8748000000X - 162000Y^2 + 8748000000Y - 157464000000000$$

Running the rim



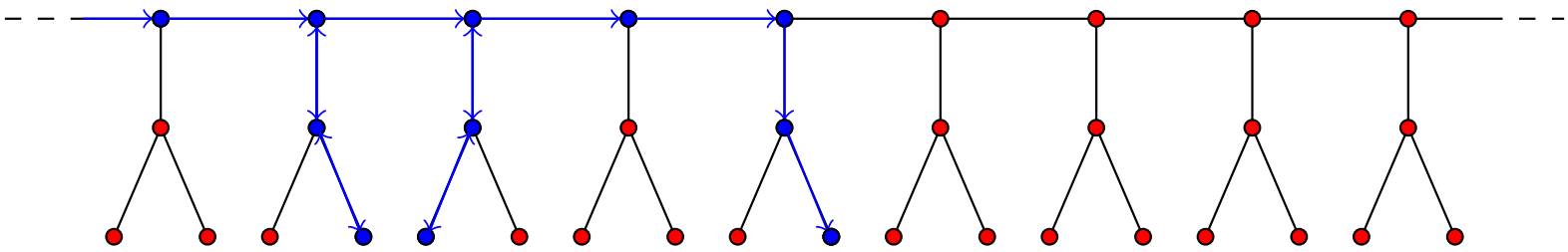
$$\Phi_2(X,Y) = X^3 + Y^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 + 40773375XY$$
$$+ 8748000000X - 162000Y^2 + 8748000000Y - 157464000000000$$

Running the rim



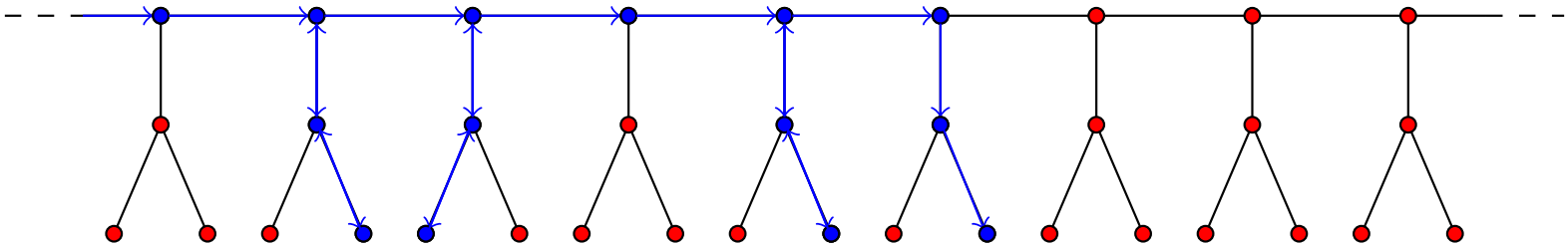
$$\Phi_2(X,Y) = X^3 + Y^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 + 40773375XY$$
$$+ 8748000000X - 162000Y^2 + 8748000000Y - 157464000000000$$

Running the rim



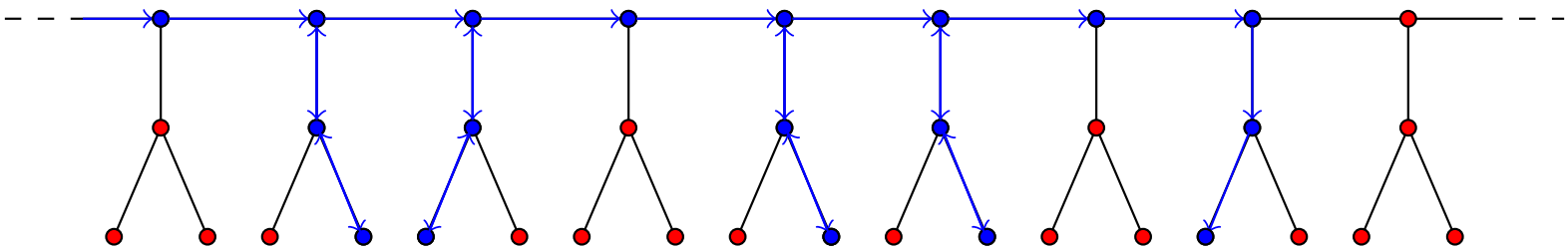
$$\Phi_2(X,Y) = X^3 + Y^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 + 40773375XY$$
$$+ 8748000000X - 162000Y^2 + 8748000000Y - 157464000000000$$

Running the rim



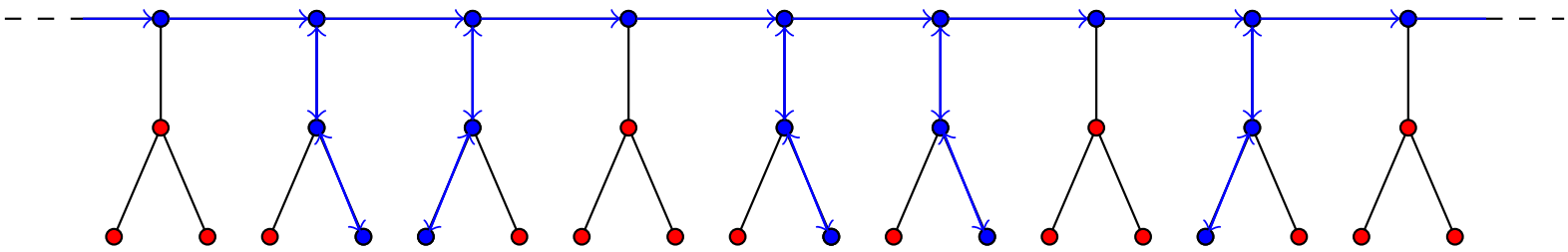
$$\Phi_2(X,Y) = X^3 + Y^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 + 40773375XY$$
$$+ 8748000000X - 162000Y^2 + 8748000000Y - 157464000000000$$

Running the rim



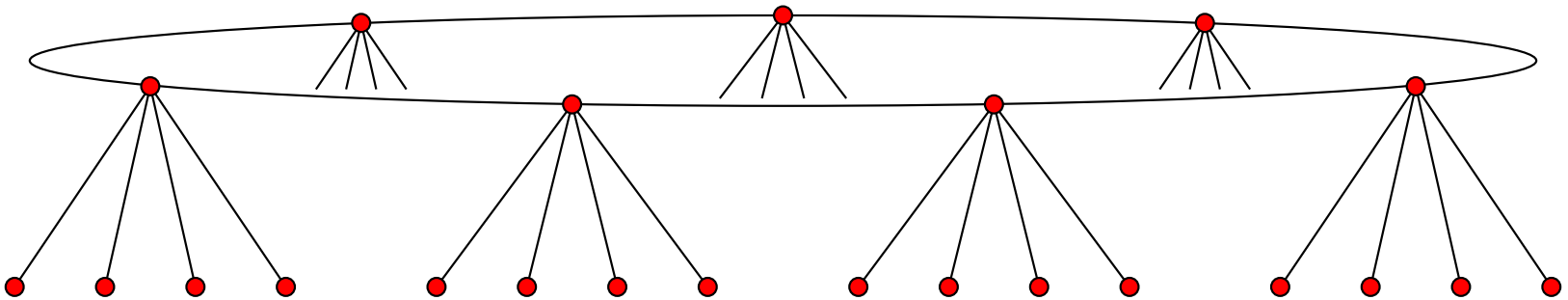
$$\Phi_2(X,Y) = X^3 + Y^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 + 40773375XY$$
$$+ 8748000000X - 162000Y^2 + 8748000000Y - 157464000000000$$

Running the rim



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

Mapping a volcano



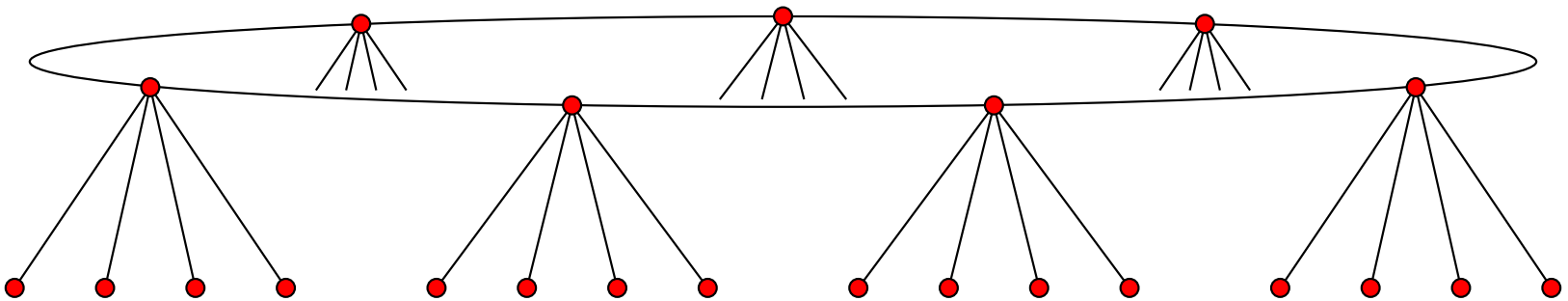
Mapping a volcano

Example

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

General requirements

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



Mapping a volcano

Example

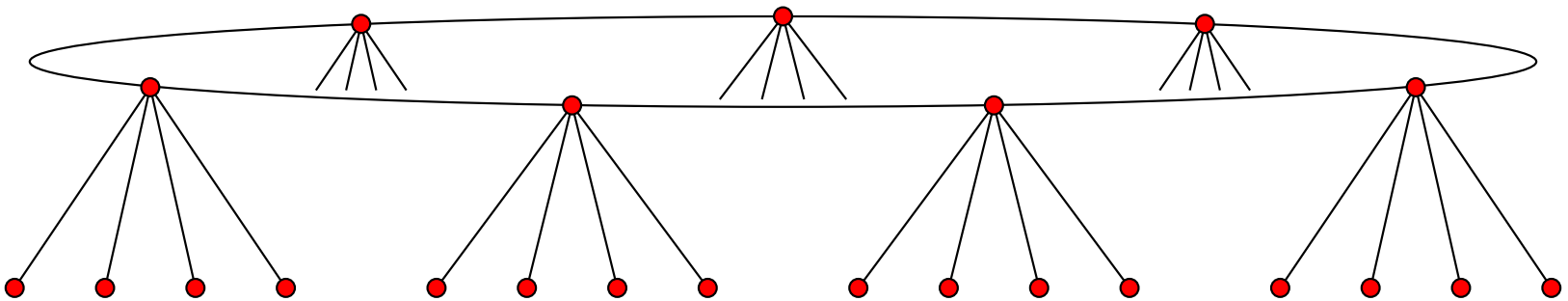
$\ell = 5, \quad p = 4451, \quad D = -151$

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

General requirements

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

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



Mapping a volcano

Example

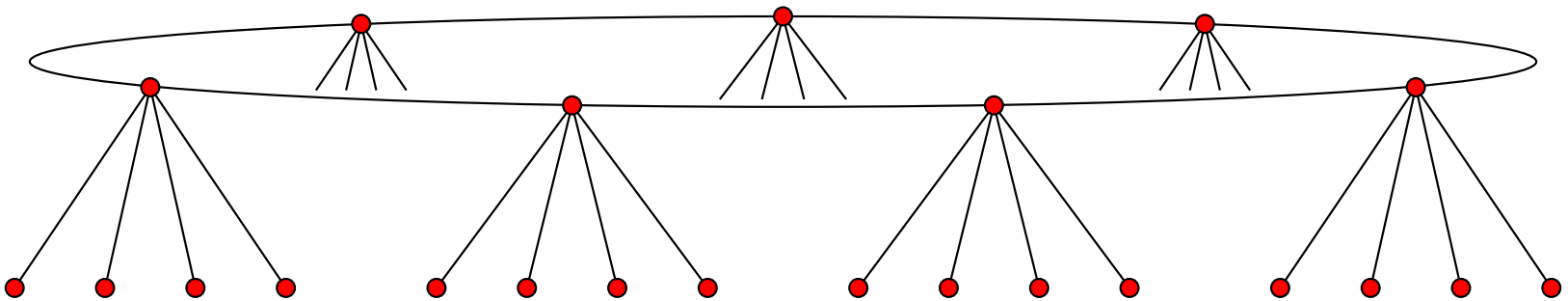
$\ell = 5, \quad p = 4451, \quad D = -151$

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

General requirements

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

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



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

Mapping a volcano

Example

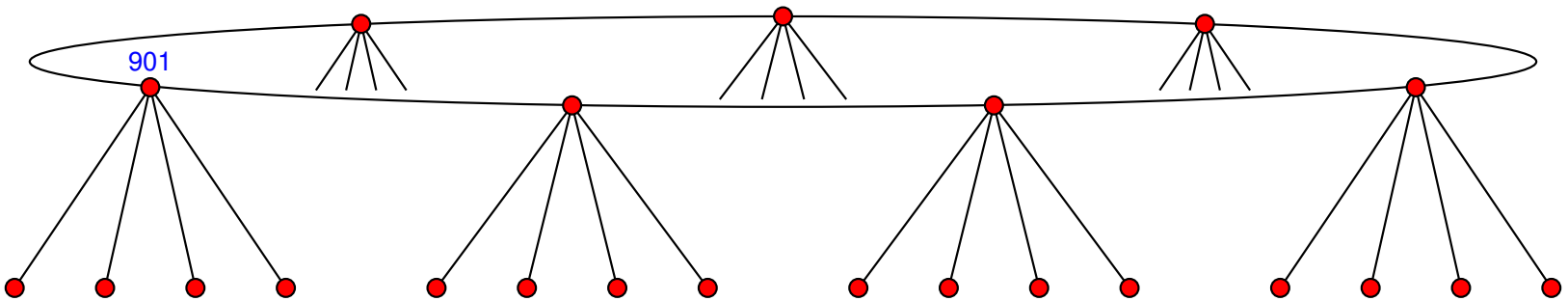
$\ell = 5, \quad p = 4451, \quad D = -151$

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

General requirements

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

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



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

Mapping a volcano

Example

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

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

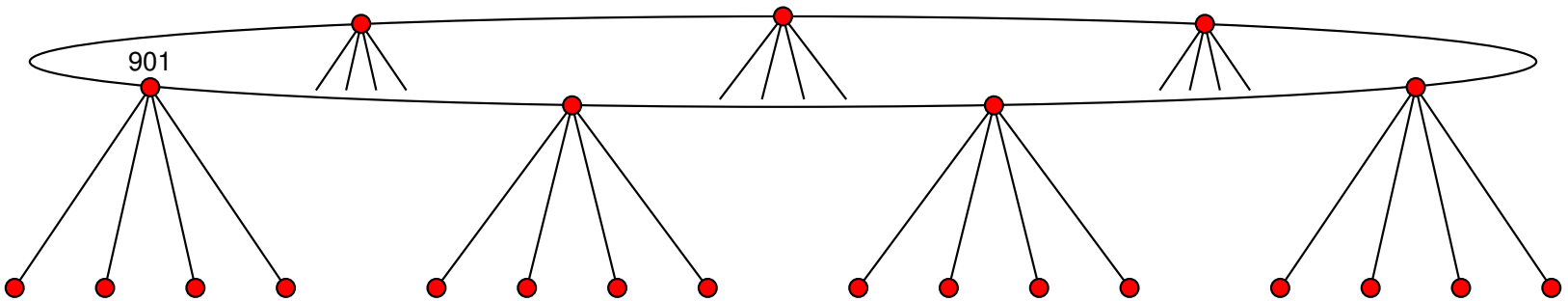
$\ell_0 = 2$

General requirements

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

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

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



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

Mapping a volcano

Example

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

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

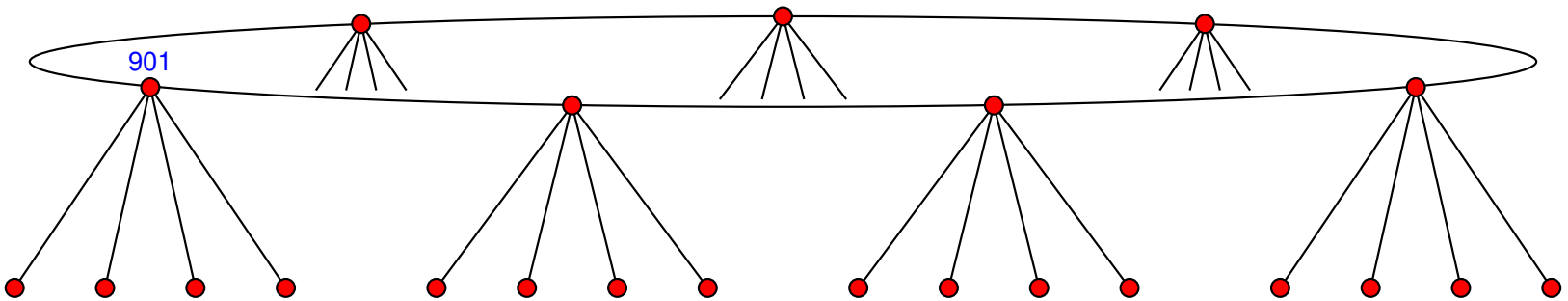
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

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

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

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



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

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

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

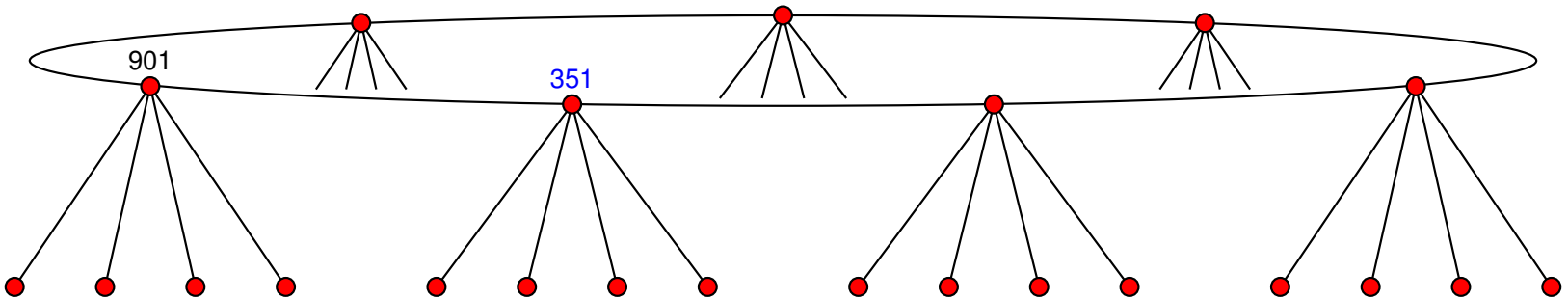
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

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

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

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



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

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

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

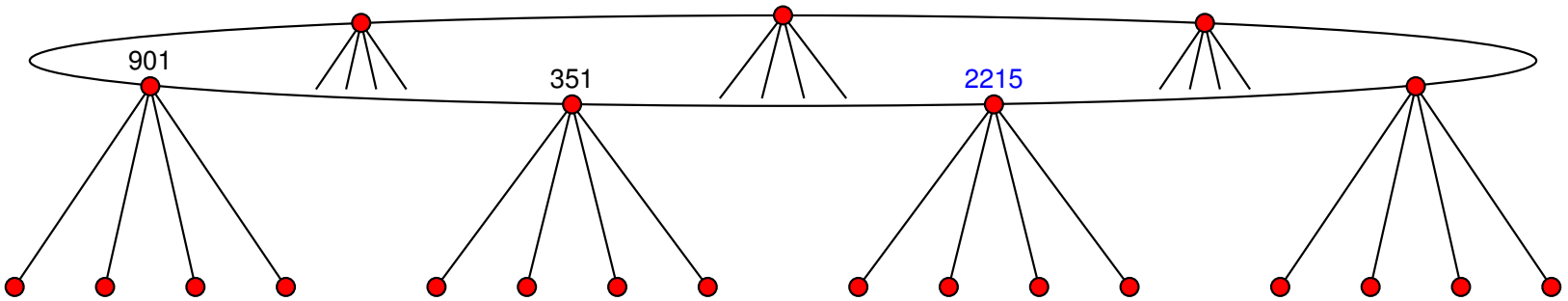
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

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

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

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



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

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

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

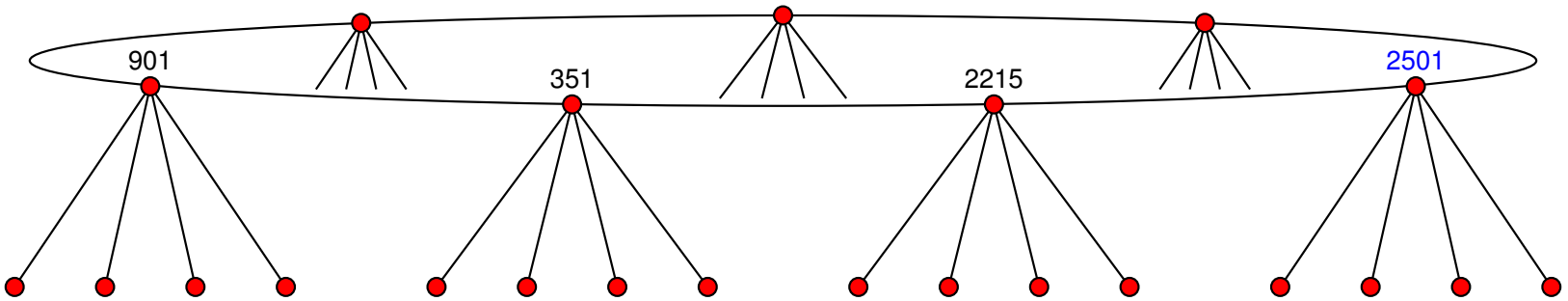
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

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

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

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



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

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

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

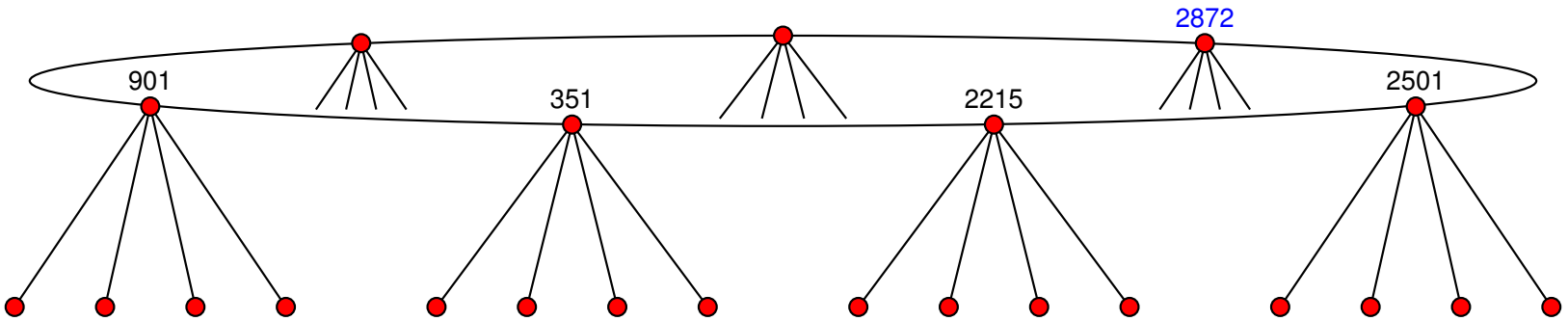
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

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

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

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



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

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

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

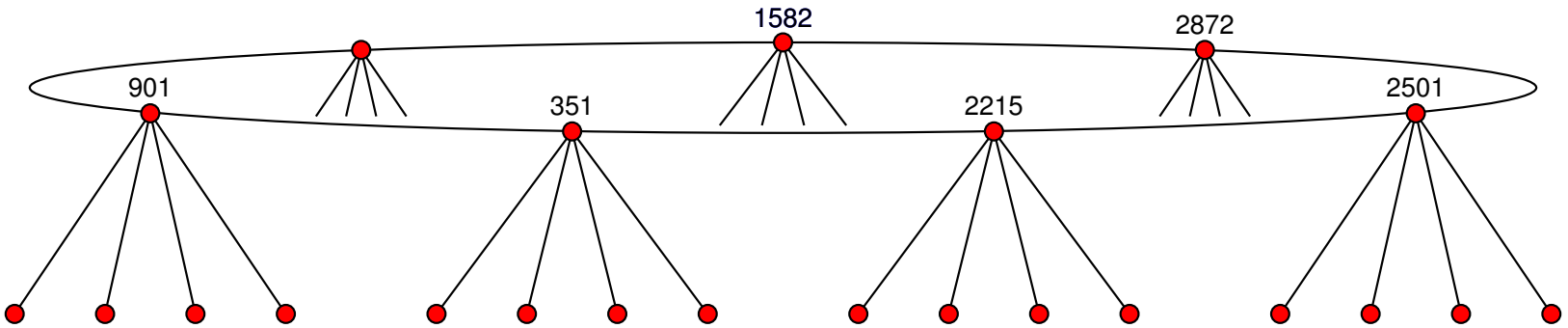
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

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

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

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



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

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

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

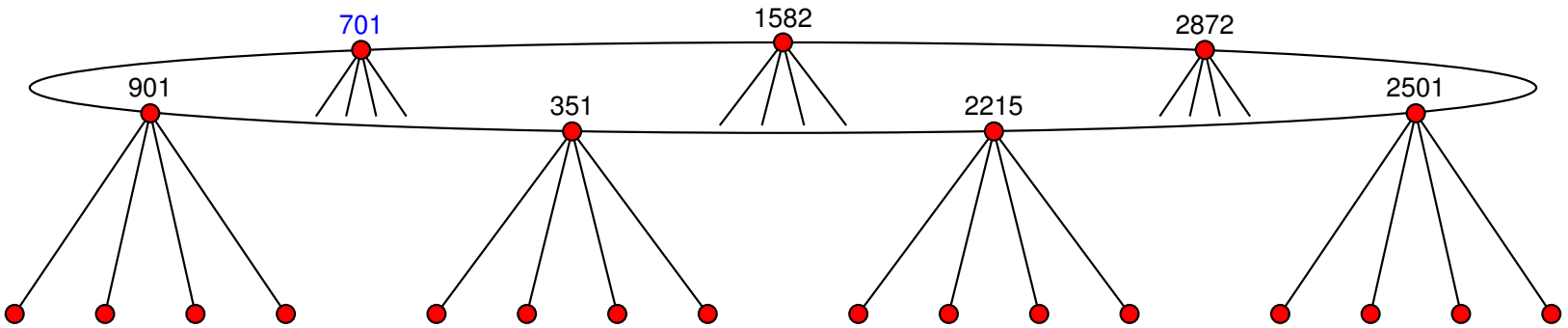
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

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

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

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



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

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

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

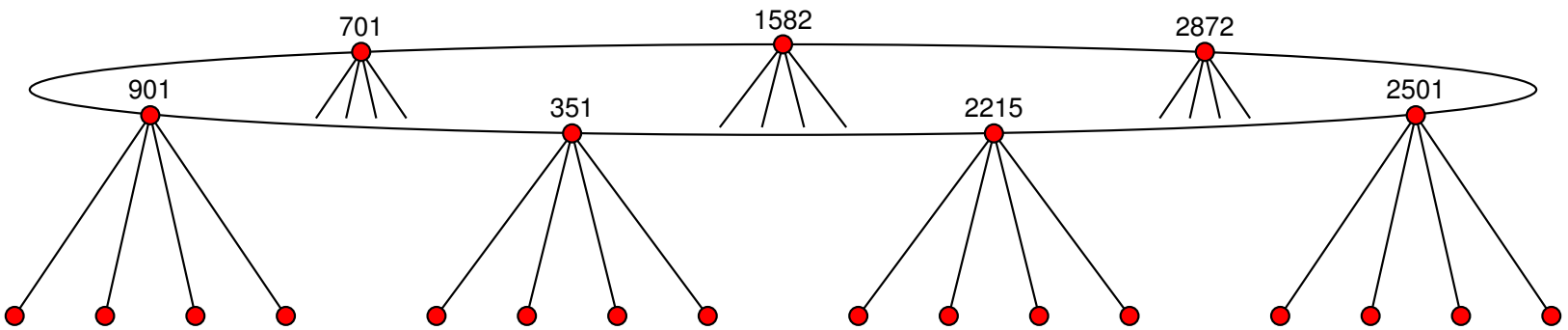
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

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

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

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



3. Descend to the floor using Vélu's formula

Mapping a volcano

Example

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

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

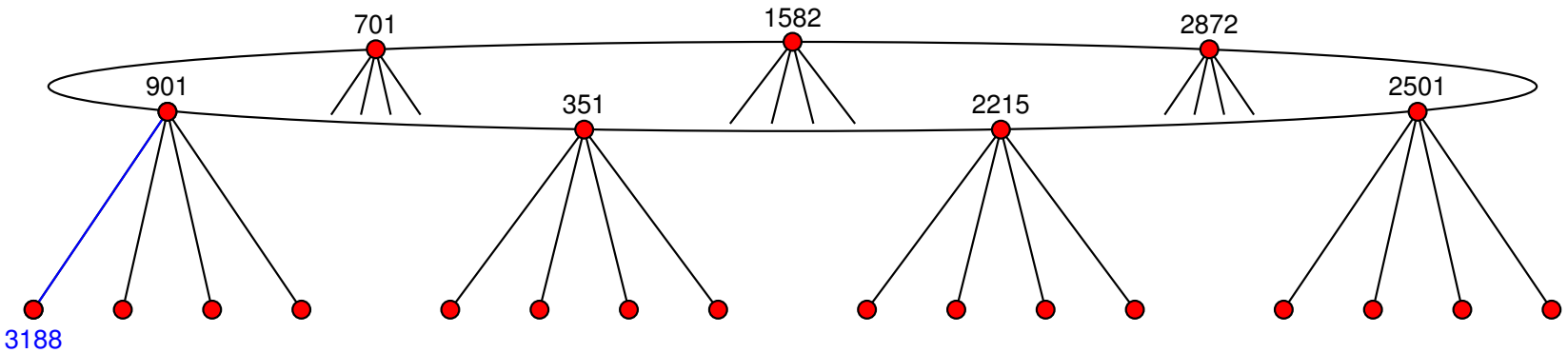
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

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

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

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



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

Mapping a volcano

Example

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

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

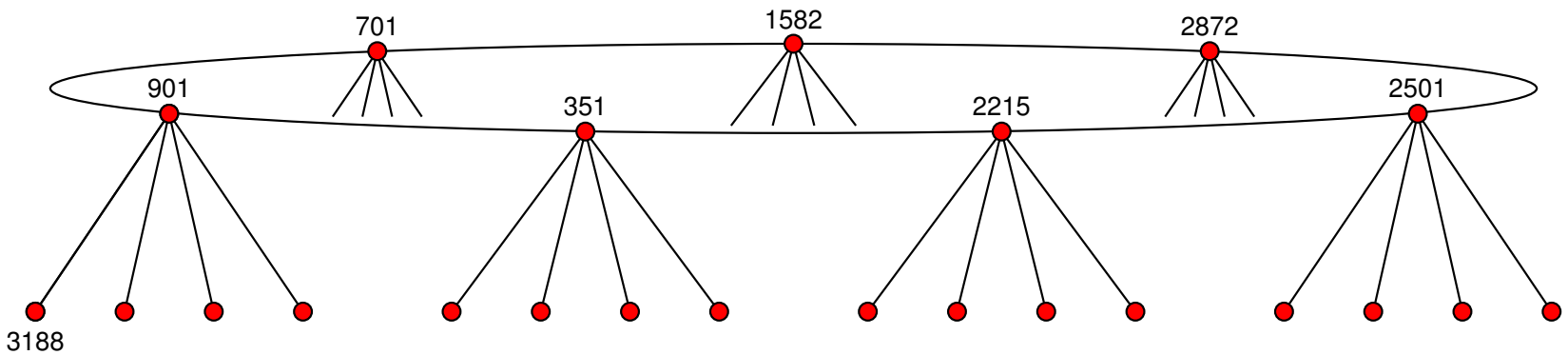
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

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

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

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



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

Mapping a volcano

Example

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

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

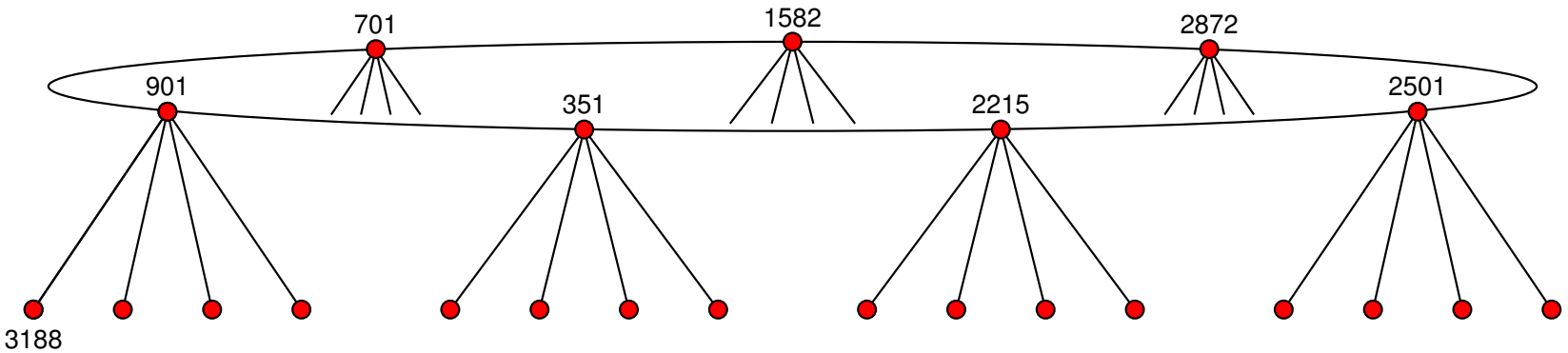
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

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

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

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



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

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

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

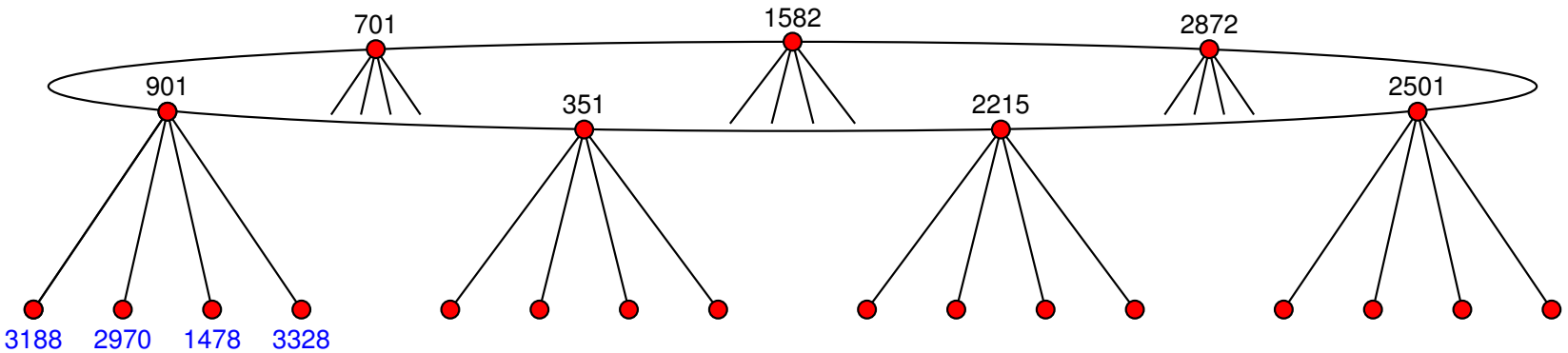
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

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

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

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



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

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

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

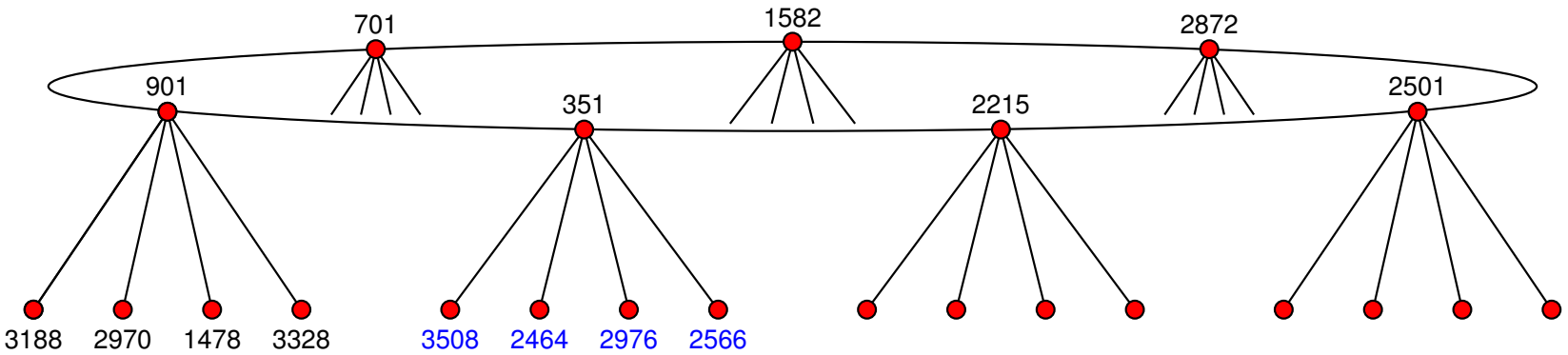
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

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

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

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



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

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

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

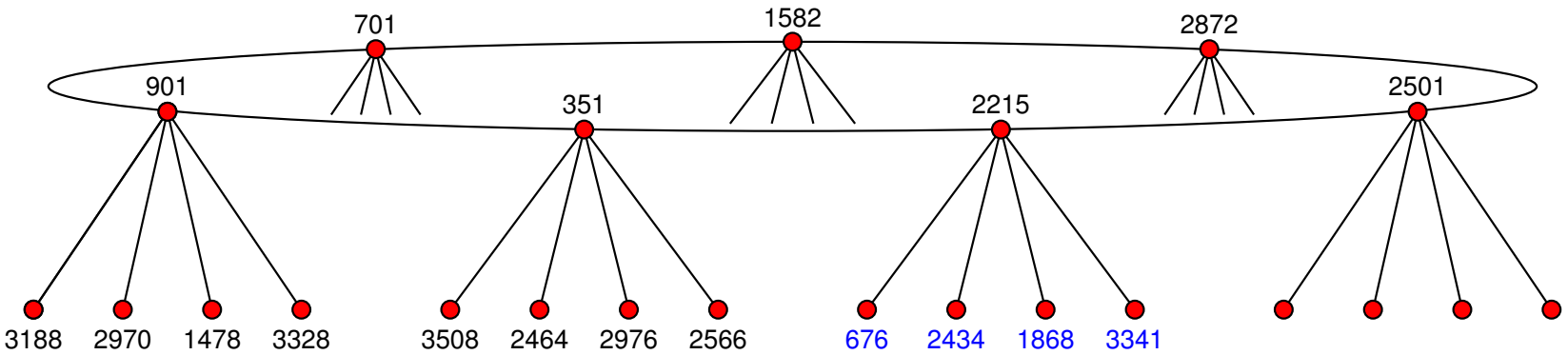
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

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

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

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



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

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

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

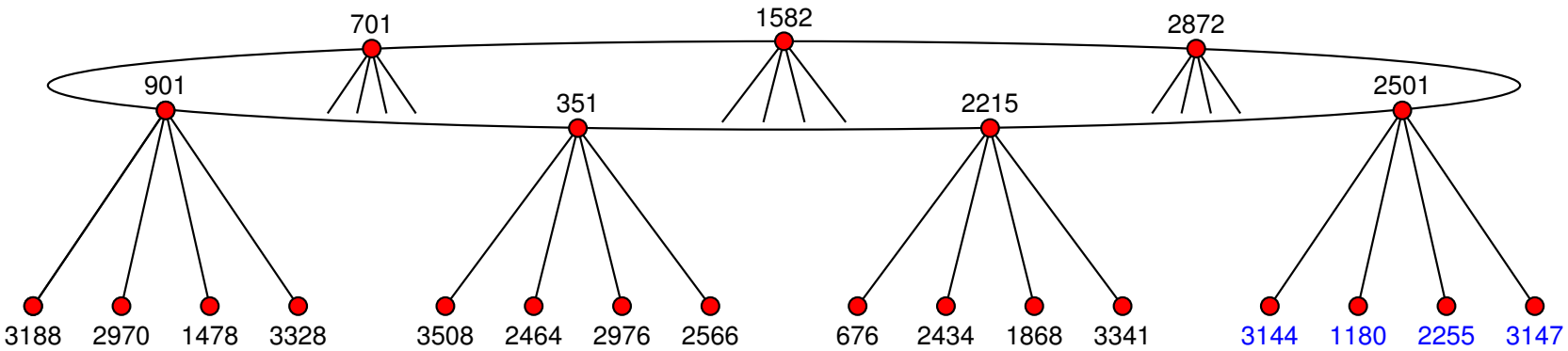
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

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

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

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



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

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

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

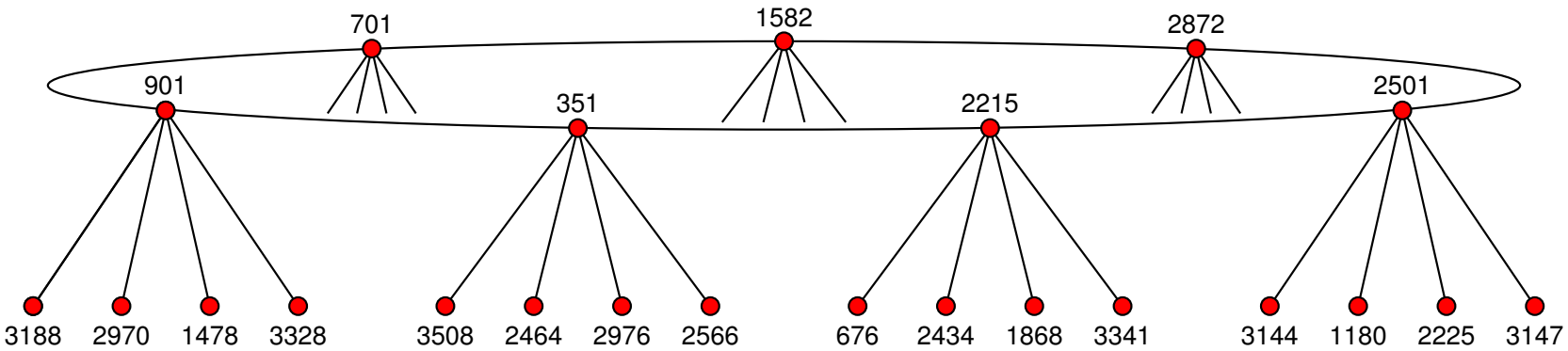
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

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

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

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



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

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

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

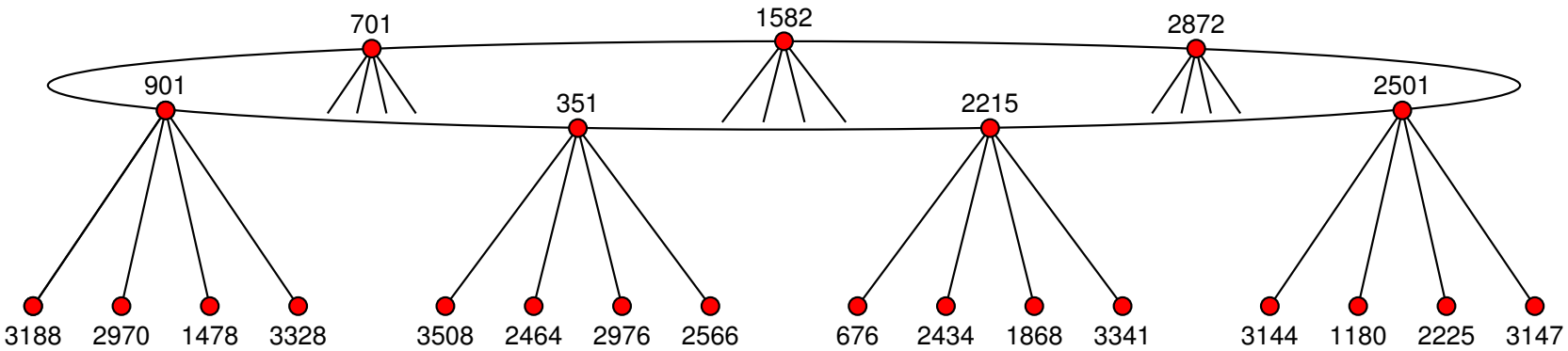
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

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

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

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



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

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

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

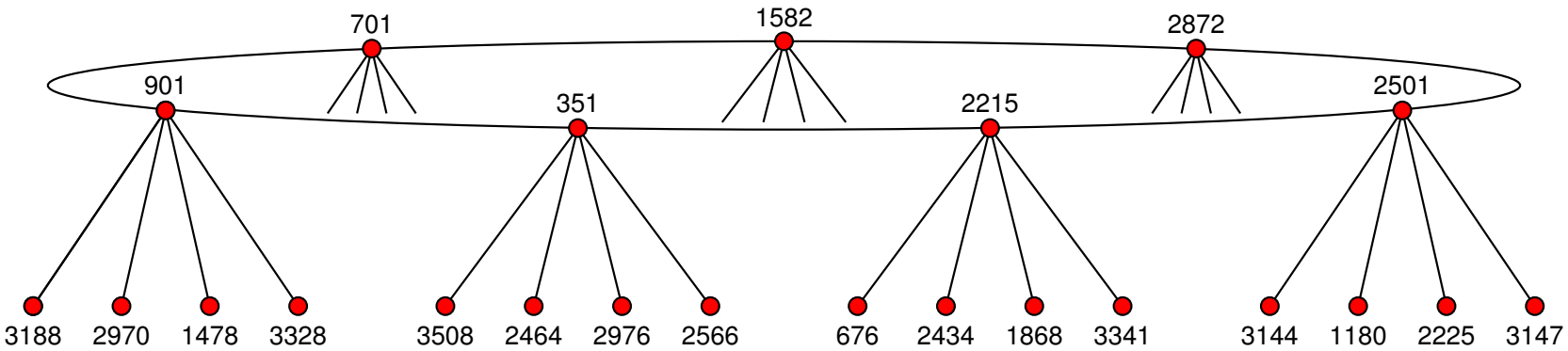
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

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

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

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



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

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

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

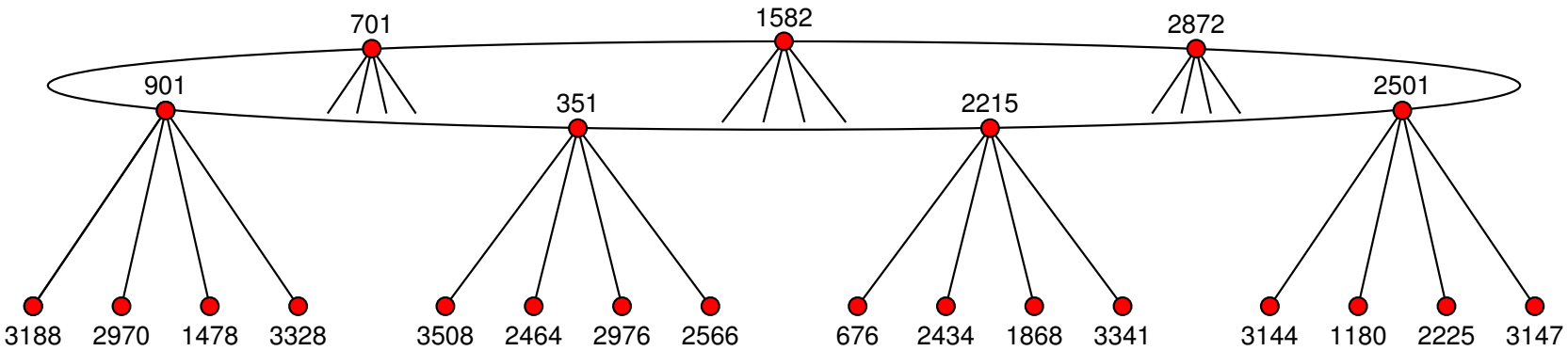
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

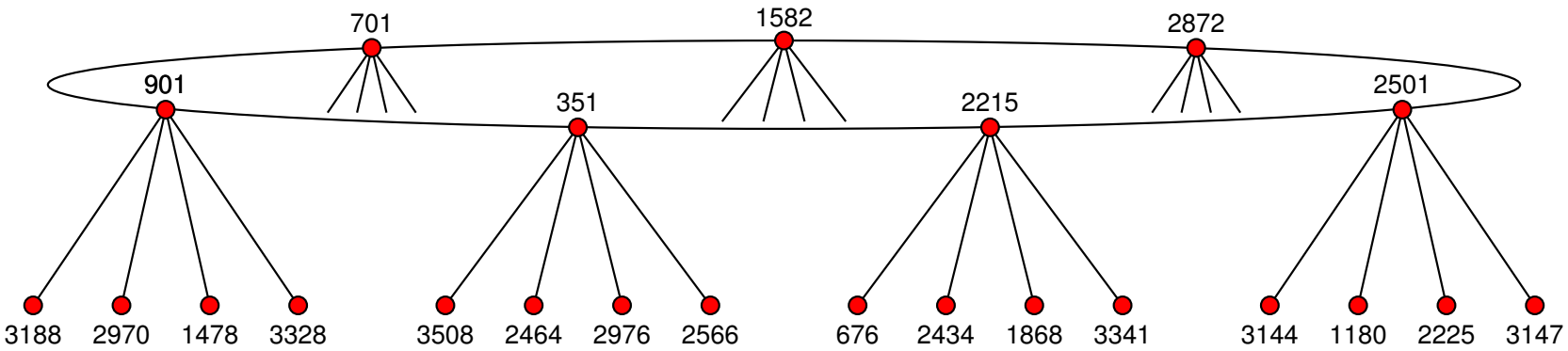
$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$

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

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

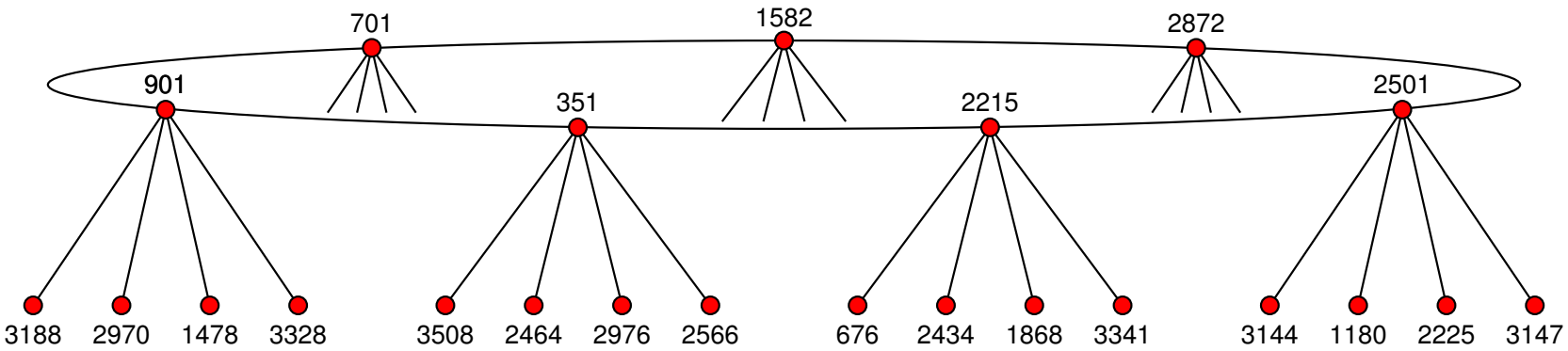


Interpolation



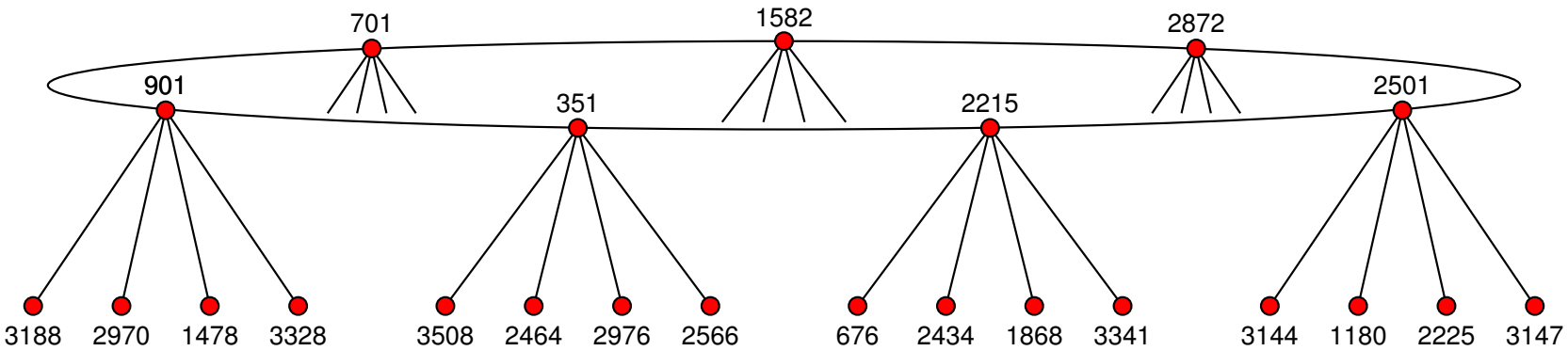
$$\Phi_5(X,\ 901) = (X - 701)(X - 351)(X - 3188)(X - 2970)(X - 1478)(X - 3328)$$
$$\Phi_5(X,\ 351) = (X - 901)(X - 2215)(X - 3508)(X - 2464)(X - 2976)(X - 2566)$$
$$\Phi_5(X,2215) = (X - 351)(X - 2501)(X - 3341)(X - 1868)(X - 2434)(X - 676)$$
$$\Phi_5(X,2501) = (X - 2215)(X - 2872)(X - 3147)(X - 2255)(X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

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 $\Phi_\ell(X, Y) \bmod p$

Choose a suitable $D = O(\ell^2)$ and $\log p = O(\log \ell)$.

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 $\Phi_\ell(X, Y) \bmod p$.	$O(\ell^2 \log^{3+\epsilon} \ell)$

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

Alternative modular polynomials

In practice, the modular polynomials Φ_ℓ are not used in SEA. There are alternatives (due to Atkin, Müller, and others) that are smaller by a large constant factor (100x to 1000x is typical).

The isogeny-volcano approach of [BLS 2010] can compute many types of (symmetric) modular polynomials derived from modular functions other than $\mathrm{j}(z)$, but these do not include the modular polynomials commonly used with SEA.

They do include modular polynomials $\Phi_\ell^{\mathfrak{f}}$ derived from the Weber function $\mathfrak{f}(z)$. These are smaller than Φ_ℓ by a factor of 1728, but they have never (?) been used with SEA before.

The Weber modular polynomials $\Phi_\ell^{\mathfrak{f}}$

The Weber $\mathfrak{f}$-function is related to the $\mathfrak{j}$-function via

$$\mathfrak{j} = \frac{(\mathfrak{f}^{24} - 16)^3}{\mathfrak{f}^{24}}$$

Provided that $\mathrm{End}(E)$ has discriminant $D \equiv 1 \bmod 8$ with $3 \nmid D$, the polynomial $\phi_\ell^{\mathfrak{f}}(Y) = \Phi_\ell^{\mathfrak{f}}(\mathfrak{f}(E), Y)$ effectively parameterizes ℓ-isogenies from E.

This condition is easily checked (without knowing D), and if it fails, powers of $\mathfrak{f}$, or other modular functions may be used.

Numerical results: modular polynomial records

- $\ell = 10079$: 120 cpu-days (2.4 GHz AMD) to compute a Müller polynomial of size 16GB [Enge 2007].
- $\ell = 10079$: 1 cpu-hour (3.0 GHz AMD) to compute Φ_ℓ^{f} of size 3GB [BLS 2010].
- $\ell = 60013$: 13 cpu-days (3.0 GHz AMD) to compute Φ_ℓ^{f} of size 748GB [BLS 2010].
- $\ell = 100019$: 100 cpu-days (3.0 GHz AMD) to compute $\phi_\ell^{\mathrm{f}} \bmod (2^{86243} - 1)$ of size 1GB [S 2010].

For $\ell = 100019$, the size of Φ_ℓ^{f} is over 1TB and Φ_ℓ is over 1PB.

Numerical results: 5011-digit point counting record

The number of points on the elliptic curve E defined by

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

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

832376989144494660061901849139137826006983637060450015930966792818374113674093822766991283099784662700961700402058294019077483170516664837812554817443350162223605440005388394920224519114859867338191660095508592165253852678528425242409787965445004279587342458591036506936232600658549556769058427604042111029080666232135885662070661039670759580341918109430064160840690748363019037103169978894180556726367014400296781983798513562269371401276427209286702254047174078470090179859044119920875037921597111234401965330999966802919477217848269921000166896074288408594435094209873544111246489768281188102940915774276149848136182361339830763026929994181385485521401057780125259890724056418895533987243324279357096770029086016947382059730330051806950506583258753330867074804800846369390042713464578653244071678652022822101990654953268109299788546242982884819162973482390308433067055460432955024817309328704331805327934957448788825063483937878070873512388679880513270375903317908018724535858724374676948741127267380730950376658888626598248661629797105514800663321182698336395879329897043562635494364468486039656666427837093575009979091922302413453716095887661432089373163729653025768255602712754566610542223232815622048111888283590483215892528728153087049654418794163034575764891117186500373809179386465716056073958857886659984917838400020437572986666397067817373843456657959297914239933377113677822538016636015241053779745447935639933068437226703067711612870475974728874060256153829424355309461429412863767016010448708725782340275978368434887328902748704620332776144279810260429883073285585959932463330471479945464928424267425303145657042721264711474962673356521337434550002879202324137239228258391503512742950736034773585892234313092778077346572608561779267925193030390180619815277308025700377636113052880114730236382334852026580407537787327013748289451197304667942877768553427530620392209638743777840561094515693650744099608411973081430390148262649852081364154006404443107834285953988209092622350423727240848811543270022694783971162521206171333600227255606557931688499109786737684979633157645270846925902311597415122278761062286676906752206603683529582116823691851305917272462661882973355576998865646958429361081809162692181866270338066704102681199813126843679500076625472860409064749186815445274367067586843407055463402189135839816572488543254133655111590963645670069347744986526036851104541120584703545306063648651258921793091452320111295046379841586941899175054104137871310536218879088318372730054658812006162717448016824877474558981852517722802145104515011477953555498768453522999868183517611765101476857634414010855810415043207370935052150913863261504324212007549804732358464553488560987919468961144855825465612614456411458521607747389949586595126074306085812134617236309956765621860727156856482046150112012015113007122286669299590274282107690933890300810525603558710045399536727403969324912420806389527152955993943311641026894824263736268535534370585102219836177805656167035861860036286963374250257588182644200835242804131190172272014414549659547457165879852600232647304991195644305287939827885207654988125751221239741075244973427819843776465089557666171337403497596850461399835327434541250151698094846056890996956914938171459951869000669270969498525993914751206760782244790625122626848753012733495289200641795967184561011226439252930596090031649974277634943933178938510726596259437826466293379162132564825895692129029330256714749154770003140032780641102586358889574523411175821853412004266108458134154747384432584651586199896849475842009365338952535884111160271960868999014742012591971478237292524813948600029227796125549029381598957721574805007478966997024108691274018357785171489306377152166096191664750803979956621679571978953552211724552632230710653244433669331067442040140391602456581858747401436772403284080454895800825555079522458369190254711040601200028499012649426967495115480636409733058979879385173976155641587413347889866287021950635203417893709652546248256133417835452925731715740688561063321641057055461825084563212070367457331486354681841758049252732599116595430817436406080011315918900828645131242470137313661372714961047058097433021586751093908895745441684195336715770412686321350796787391486224738612016911715739107481092463845433183146882764205897555692474146749724490484592370638492569933497005028781048032734897097622833295643389100786217086915770725300529087910723550751401318787576647364571766938618440620554990814181207394577639163458834949267687793194747139050054400221521434458599314044867381063285572380923329713520153405615749711252696047443494747652497316648062057666953271152425843341789770616064557079435236406353029020560141015314103419765029534921177065625577774688408769857858804251711896591035794406728856602939161842221528770720582112364327715631856765897848302241231421628544594675301323023661942160414993178396196877455996341128827795369279474773827993735868297936899429512496912028871093270632848246774367220129816851945807778140092913366453585259624246494437340122223955248

Numerical results: 5011-digit point counting record

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

$\phi_\ell^{\mathrm{f}}(Y) = \Phi_\ell^{\mathrm{f}}(X, \jmath(E))$ 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.