Computing modular polynomials with the Chinese Remainder Theorem

Andrew V. Sutherland

Massachusetts Institute of Technology

ECC 2009

Reinier Bröker Kristin Lauter

Isogenies

An *isogeny* $\phi : E_1 \to E_2$ is a morphism of elliptic curves,
a rational map that preserves the identity.

Isogenies

An *isogeny* $\phi : E_1 \to E_2$ is a morphism of elliptic curves, a rational map that preserves the identity.

Over a finite field, E_1 and E_2 are isogenous if and only if

$$\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q).$$

Some applications of isogenies

Isogenies make hard problems easier:

- Counting the points on E
  Polynomial time (SEA).
- Constructing E with the CM method.
  $|D| \geq 10^{14}$ $h(D) \geq 5,000,000$ (CRT approach).
- Computing the endomorphism ring of E.
  Subexponential time (heuristically, Bisson-S 2009).

These algorithms all rely on modular polynomials $\Phi_\ell(X, Y)$.

Isogenies in elliptic curve cryptography

Isogenies allow the discrete logarithm problem to be transferred from one elliptic curve to another.

This raises a few questions:

1. How efficiently can we compute isogenies?
2. Are all isogenous curves created equal?

Isogenies in elliptic curve cryptography

Isogenies allow the discrete logarithm problem to be transferred from one elliptic curve to another.

This raises a few questions:

1. How efficiently can we compute isogenies?
2. Are all isogenous curves created equal?

The endomorphism ring $\mathrm{End}(E)$ is critical to both questions.

(Bröker-Charles-Lauter 2008, Jao-Miller-Venkatesan 2005, 2009).

Properties of isogenies

Degree

The kernel of $\phi : E_1 \to E_2$ is a finite subgroup of $E_1(\overline{F})$.
When ϕ is separable, we have $|\ker \phi| = \deg \phi$.

An ℓ-isogeny is a (separable) isogeny of degree ℓ.
For prime ℓ, the kernel is necessarily cyclic.

Orientation

We say that $\phi : E_1 \to E_2$ is *horizontal* if $\mathrm{End}(E_1) = \mathrm{End}(E_2)$.
Otherwise ϕ is *vertical*.

CM-action

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve.
Then $\mathrm{End}(E) \cong \mathcal{O} \subseteq \mathcal{O}_K$, for some imaginary quadratic field K.

CM-action

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve.
Then $\mathrm{End}(E) \cong \mathcal{O} \subseteq \mathcal{O}_K$, for some imaginary quadratic field K.

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 ideal with norm ℓ.

CM-action

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve.
Then $\mathrm{End}(E) \cong \mathcal{O} \subseteq \mathcal{O}_K$, for some imaginary quadratic field K.

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 ideal with norm ℓ.

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

CM-action

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve.
Then $\mathrm{End}(E) \cong \mathcal{O} \subseteq \mathcal{O}_K$, for some imaginary quadratic field K.

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 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" $= O(\log^2 |D|)$.

Isogenies from kernels

Any finite subgroup G of $E(\overline{F})$ determines a separable isogeny with G as its kernel

Given G, we can compute ϕ explicitly via Vélu's formula.

The complexity depends both on the size of $\ker\phi$,
and the field in which the points of $\ker\phi$ are defined.

When working in $\mathbb{F}_q$, we assume the coefficients of ϕ lie in $\mathbb{F}_q$.
But $\ker\phi$ may lie in an extension of degree up to $\ell^2 - 1$.

The classical modular polynomial Φ_ℓ

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

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

The classical modular polynomial Φ_ℓ

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

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

The ℓ-isogeny graph 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 $\Phi_\ell(X, j) \in \mathbb{F}_q[X]$.

The classical modular polynomial Φ_ℓ

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

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

The ℓ-isogeny graph 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 $\Phi_\ell(X, j) \in \mathbb{F}_q[X]$.

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

This is a pretty big polynomial...

$$H_D(x)$$

Visible Universe

...but this is a *really* big polynomial.

$$\Phi_l(X,Y)$$

$$H_D(x)$$

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, Morain '95, Müller '95, BCRS '99)

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

Algorithms to compute Φ_ℓ

***q*-expansions**:

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

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

isogenies: (Charles-Lauter 2005)

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

Algorithms to compute Φ_ℓ

***q*-expansions**:

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

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

isogenies: (Charles-Lauter 2005)

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

evaluation-interpolation: (Enge 2009)

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

A new algorithm to compute Φ_ℓ

We compute Φ_ℓ using isogenies and the CRT.

A new algorithm to compute Φ_ℓ

We compute Φ_ℓ using isogenies and the CRT.
For certain p we can compute $\Phi_\ell \bmod p$ in expected time

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

A new algorithm to compute Φ_ℓ

We compute Φ_ℓ using isogenies and the CRT.
For certain p we can compute Φ_ℓ mod p in expected time

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

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

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

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

A new algorithm to compute Φ_ℓ

We compute Φ_ℓ using isogenies and the CRT.
For certain p we can compute Φ_ℓ mod p in expected time

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

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

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

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

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

Performance highlights

Level records

1. $\ell = \mathbf{5003}$: Φ_ℓ
2. $\ell = \mathbf{10007}$: $\Phi_\ell \bmod m$
3. $\ell = \mathbf{50021}$: $\Phi_\ell^{\mathfrak{f}}$

Each in less than 24 hours elapsed time ($\approx$ 12 CPU-days), using $m \approx 2^{256}$.

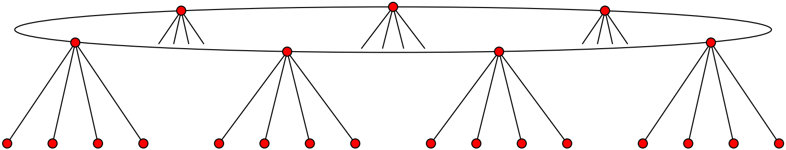
Speed records

1. $\ell = \mathbf{251}$: Φ_ℓ in 40s $\quad$ $\Phi_\ell \bmod m$ in 5.5s
2. $\ell = \mathbf{1009}$: Φ_ℓ in 3822s $\quad$ $\Phi_\ell \bmod m$ in 408s
3. $\ell = \mathbf{1009}$: $\Phi_\ell^{\mathfrak{f}}$ in 3.2s

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

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

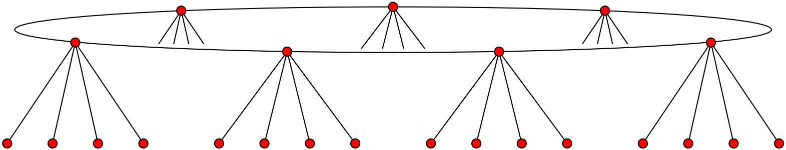
Mapping a volcano



Mapping a volcano

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

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



Mapping a volcano

Example

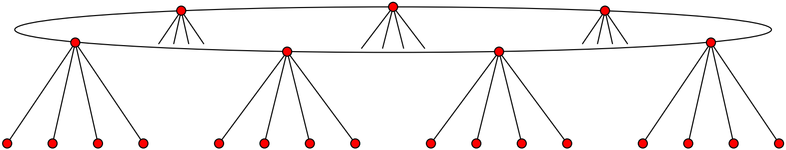
$\ell = 5, \quad p = 4451, \quad D = -151$

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

General requirements

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

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



Mapping a volcano

Example

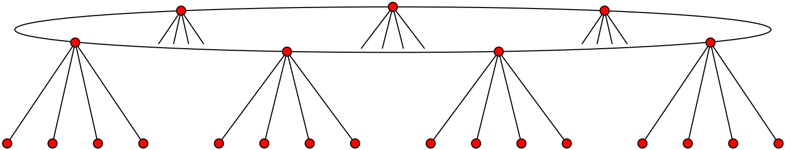
$\ell = 5, \quad p = 4451, \quad D = -151$

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

General requirements

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

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

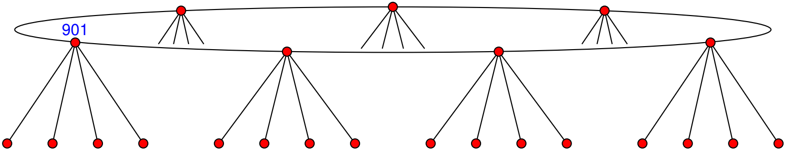


1. Find a root of $H_D(X)$

Mapping a volcano

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

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



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

Mapping a volcano

Example

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

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

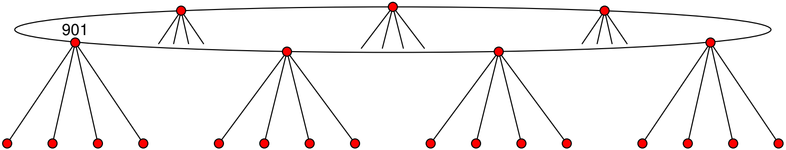
$\ell_0 = 2$

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

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

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

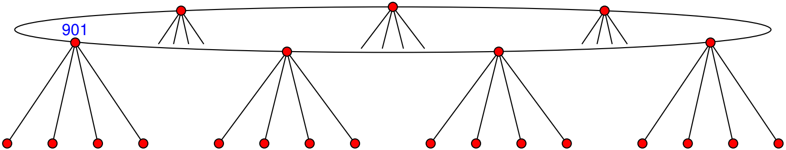
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

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

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

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



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

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

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

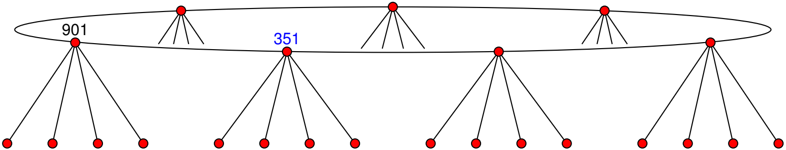
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

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

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

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



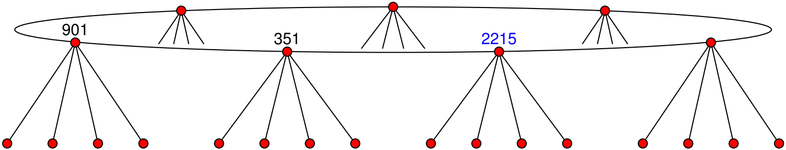
2. Enumerate surface using the action of α_{ℓ_0}

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

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

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

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

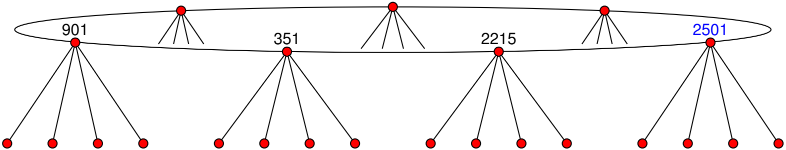
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

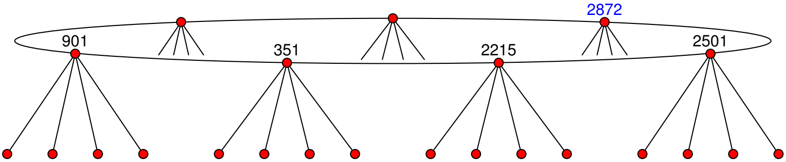
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

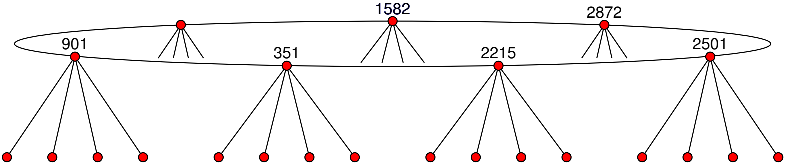
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

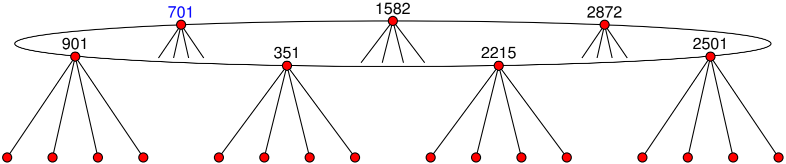
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

General requirements

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

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

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



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

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

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

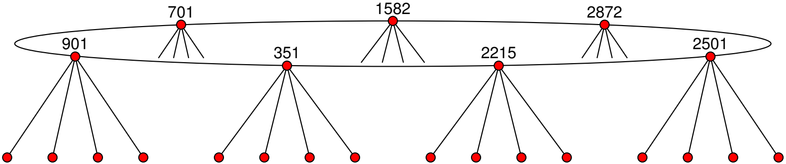
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

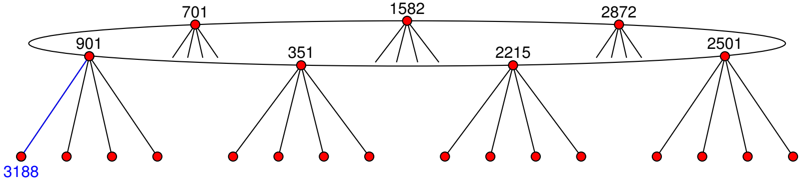
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

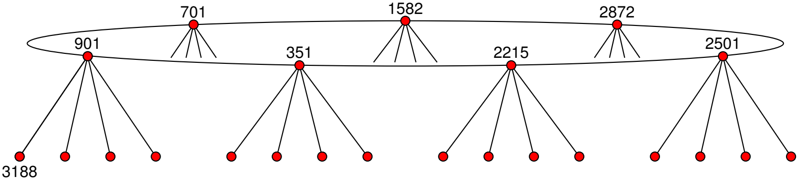
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3$

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

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

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

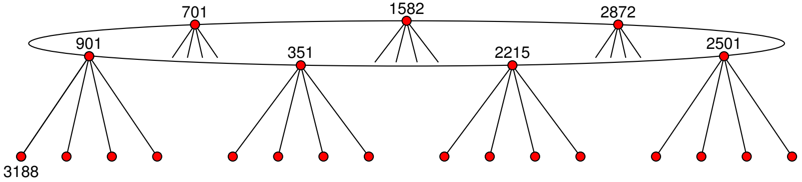
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

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

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

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

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

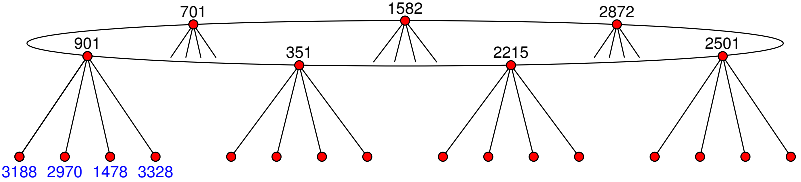
Mapping a volcano

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

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

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

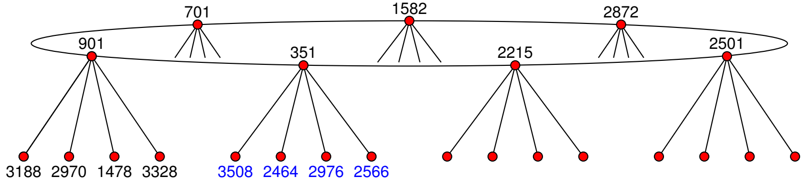
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

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

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

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



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

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

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

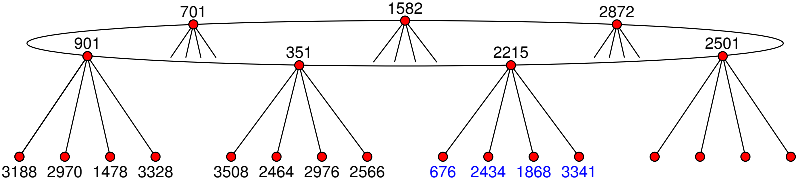
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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

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

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

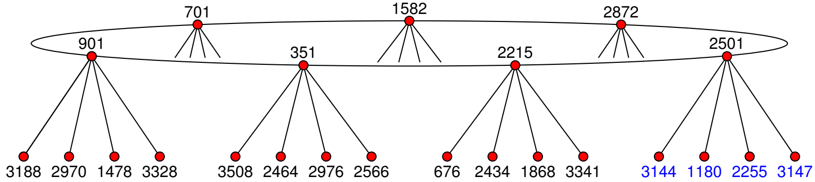
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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

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

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

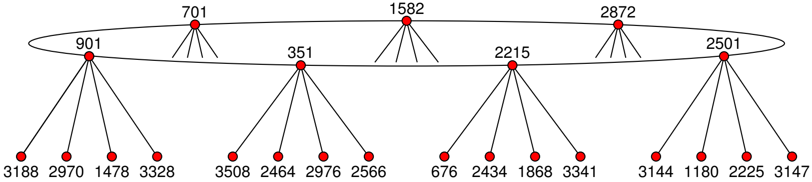
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

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

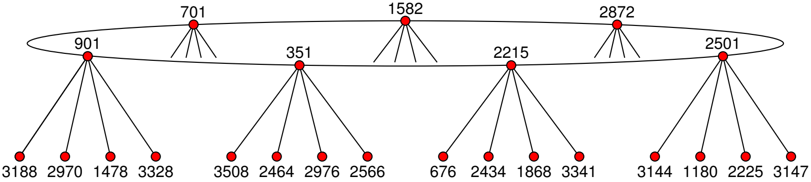
Mapping a volcano

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

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$
$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$
$\ell_0 \neq \ell, \, (\frac{D}{\ell_0}) = 1, \, \alpha_\ell = \alpha_{\ell_0}^k, \, \beta_{\ell^2} = \beta_{\ell_0}^{k'}$



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

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

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

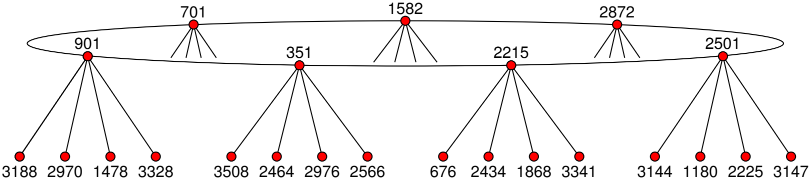
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

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}

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

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

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

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

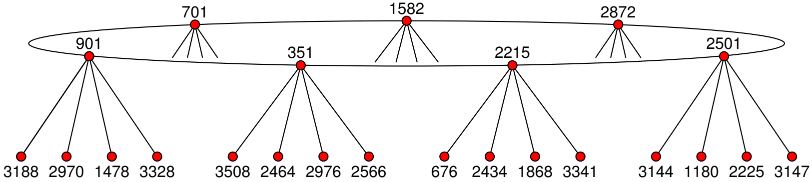
Mapping a volcano

Example

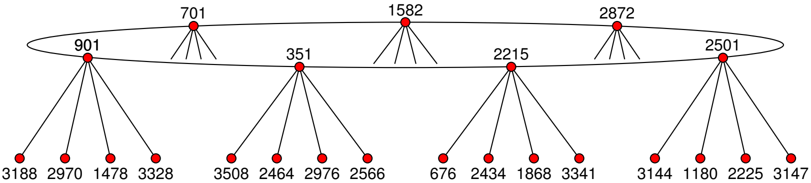
$\ell \;= 5, \quad p = 4451, \quad D = -151$
$t \;= 52, \quad v = 2, \quad h(D) = 7$
$\ell_0 = 2, \quad \alpha_5 = \alpha_2^3, \quad \beta_{25} = \beta_2^7$

General requirements

$4p = t^2 - v^2\ell^2 D, \quad p \equiv 1 \bmod \ell$
$\ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2$
$\ell_0 \neq \ell, \; (\frac{D}{\ell_0}) = 1, \; \alpha_\ell = \alpha_{\ell_0}^k, \; \beta_{\ell^2} = \beta_{\ell_0}^{k'}$

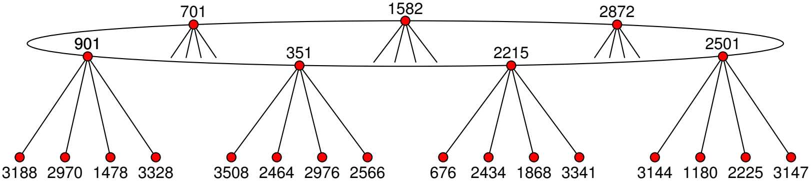


Interpolation



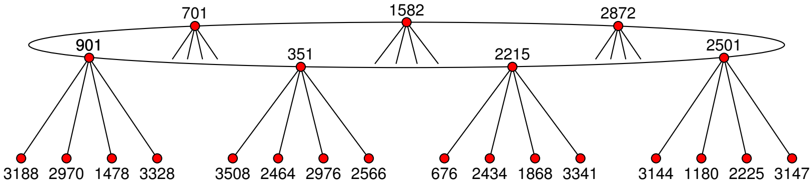
$$\Phi_5(X, 901) = (X - 701)(X - 351)(X - 3188)(X - 2970)(X - 1478)(X - 3328)$$
$$\Phi_5(X, 351) = (X - 901)(X - 2215)(X - 3508)(X - 2464)(X - 2976)(X - 2566)$$
$$\Phi_5(X, 2215) = (X - 351)(X - 2501)(X - 3341)(X - 1868)(X - 2434)(X - 676)$$
$$\Phi_5(X, 2501) = (X - 2215)(X - 2872)(X - 3147)(X - 2255)(X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

Interpolation



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

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

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 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 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 $O(\ell^2 \log \ell)$.

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

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

we apply the CRT to obtain

$$\begin{aligned}
\Phi_5(X, Y) &= X^6 + Y^6 - X^5Y^5 + 3720(X^5Y^4 + X^4Y^5) - 4550940(X^5Y^3 + X^3Y^5) \\
&+ 2028551200(X^5Y^2 + X^2Y^5) - 246683410950(X^5Y + XY^5) + 1963211489280(X^5 + Y^5) \\
&+ 1665999364600X^4Y^4 + 107878928185336800(X^4Y^3 + X^3Y^4) \\
&+ 383083609779811215375(X^4Y^2 + X^2Y^4) + 128541798906828816384000(X^4Y + XY^4) \\
&+ 1284733132841424456253440(X^4 + Y^4) - 4550940(X^3Y^5 + X^5Y^3) \\
&- 441206965512914835246100X^3Y^3 + 26898488858380731577417728000(X^3Y^2 + X^2Y^3) \\
&- 192457934618928299655108231168000(X^3Y + XY^3) \\
&+ 280244777828439527804321565297868800(X^3 + Y^3) \\
&+ 5110941777552418083110765199360000X^2Y^2 \\
&+ 36554736583949629295706472332656640000(X^2Y + XY^2) \\
&+ 6692500042627997708487149415015068467200(X^2 + Y^2) \\
&- 264073457076620596259715790247978782949376XY \\
&+ 53274330803424425450420160273356509151232000(X + Y) \\
&+ 141359947154721358697753474691071362751004672000.
\end{aligned}$$

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

$$
\begin{aligned}
\Phi_5(X, Y) &= X^6 + Y^6 - X^5Y^5 + 3720(X^5Y^4 + X^4Y^5) - 4550940(X^5Y^3 + X^3Y^5) \\
&\quad + 2028551200(X^5Y^2 + X^2Y^5) - 246683410950(X^5Y + XY^5) + 1963211489280(X^5 + Y^5) \\
&\quad + 1665999364600X^4Y^4 + 107878928185336800(X^4Y^3 + X^3Y^4) \\
&\quad + 383083609779811215375(X^4Y^2 + X^2Y^4) + 128541798906828816384000(X^4Y + XY^4) \\
&\quad + 1284733132841424456253440(X^4 + Y^4) - 4550940(X^3Y^5 + X^5Y^3) \\
&\quad - 441206965512914835246100X^3Y^3 + 26898488858380731577417728000(X^3Y^2 + X^2Y^3) \\
&\quad - 192457934618928299655108231168000(X^3Y + XY^3) \\
&\quad + 280244777828439527804321565297868800(X^3 + Y^3) \\
&\quad + 5110941777552418083110765199360000X^2Y^2 \\
&\quad + 36554736583949629295706472332656640000(X^2Y + XY^2) \\
&\quad + 6692500042627997708487149415015068467200(X^2 + Y^2) \\
&\quad - 264073457076620596259715790247978782949376XY \\
&\quad + 53274330803424425450420160273356509151232000(X + Y) \\
&\quad + 141359947154721358697753474691071362751004672000.
\end{aligned}
$$

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

The algorithm

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

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 $\Phi_\ell \bmod m$.

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

For "small" m, use explicit CRT $\bmod m$.
For "large" m, standard CRT for large m.
For m in between, use a hybrid approach.

Chinese remaindering

Let $S = \{p_1, \ldots, p_n\}$, $M = \prod p_i$, $M_i = M/p_i$, and $a_i \equiv M_i^{-1} \bmod p_i$.
For each coefficient c of Φ_ℓ, let $c_i \equiv c \bmod p_i$ and assume $4|c| < M$.

Standard CRT: $c \equiv \sum c_i a_i M_i \bmod M$.

Explicit CRT mod m [Bernstein]:

$$c \equiv \left(\sum c_i a_i M_i - rM\right) \bmod m$$

where r is the closest integer to $\sum c_i a_i / M_i$.

Online algorithm: process each c_i as it is computed, then discard it!

Assuming $\log p_i = O(\log l)$:

- Space complexity: $O(\ell^2 \log(\ell m))$.
- Time complexity: $O(\ell^3 \log^{3+\epsilon} \ell + \ell^3 \mathsf{M}(\log m))$

With hybrid approach, time is $O(\ell^3 \log^{3+\epsilon} \ell)$ independent of m.

See `arXiv.org/abs/0902.4670` for more details.

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 $O(\ell^2 \log(\ell m))$.

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: $h(\Phi_\ell) \le 6\ell\log\ell + 17\ell$ (Bröker-S 2009).

Conjectural bound: $h(\Phi_\ell) \le 6\ell\log\ell + 12\ell$ (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 $\mathfrak{f}$-function.

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:

$$X^{12} + Y^{12} - X^{11}Y^{11} + -1X^{11}Y^{11} + 8184X^{11}Y^{10} - 28278756X^{11}Y^{9} + 53686822816X^{11}Y^{8}$$
$$- 61058988656490X^{11}Y^{7} + 42570393135641712X^{11}Y^{6} - 17899526272883039048X^{11}Y^{5}$$
$$+ 4297837238774928467520X^{11}Y^{4} - 529134841844639613861795X^{11}Y^{3} + 27209811658056645815522600X^{11}Y^{2}$$
$$- 374642006356701393515817612X^{11}Y + 296470902355240575283200000X^{11}$$

. . . 8 pages omitted . . .

$+ 3924233450945276549086 \ldots$ 100 digits omitted $\ldots 000$

Atkin:

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

Weber:

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

Performance comparison

function	ℓ	floating-point	CRT	ratio
classical j	251	688	40	17.2
	503	8320	410	20.3
	1009	107200	3822	28.0
Weber $\mathfrak{f}$	1009	16.2	3.2	5.1
	5003	4504	492	9.2
	10007	66758	4931	13.5

floating-point vs. CRT

(3.0 GHz AMD Phenom CPU seconds, $m \approx 2^{256}$)