On the evaluation of modular polynomials

Andrew V. Sutherland
Massachusetts Institute of Technology

ECC 2012

http://arxiv.org/abs/1202.3985
http://arxiv.org/abs/1208.5370
A brief journey through space-time...
In a universe with $n$ dimensions, the amount of data that can be stored within a distance $r$ of the CPU is $O(r^n)$.

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

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

The RAM model permits algorithms with quasi-linear space and time complexity, but these complexities cannot be realized in practice. If we are given an algorithm whose theoretical space and time complexity are quasi-linear, reducing the space complexity will speed up the real-world running time of the algorithm, often dramatically.
In a universe with \( n \) dimensions, the amount of data that can be stored within a distance \( r \) of the CPU is \( O(r^n) \).

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

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

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

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

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

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

The induced homomorphism $\phi: E_1(\bar{k}) \to E_2(\bar{k})$ has a finite kernel. Conversely, every finite subgroup of $E_1(\bar{k})$ is the kernel of an isogeny.

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

We are primarily interested in isogenies of prime degree $\ell \neq \text{char } k$, which are necessarily separable isogenies with cyclic kernels.
The $\bar{k}$-isomorphism classes of elliptic curves $E/k$ are in bijection with the field $k$. For $E: y^2 = x^3 + Ax + B$, the $j$-invariant of $E$ is

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

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

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

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

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

The modular equation

Let \( j: \mathbb{H} \rightarrow \mathbb{C} \) be the classical modular function.

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

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

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

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

This moduli interpretation remains valid over any field whose characteristic is not equal to \( \ell \).

---

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

Isogenies play a key role in many applications:

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

Isogenies play a key role in many applications:

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

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

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

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

that lie in $F$ are precisely the $j$-invariants of the elliptic curves $\tilde{E}/F$ that are $\ell$-isogenous to $E$. 
Modular polynomials are very large...

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

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

Size of $\Phi_\ell(X, Y)$
... but instantiated modular polynomials are not.

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

Even if $q$ is quite large, say 4096 bits, for $\ell = 10007$ the size of $\phi_\ell(Y)$ is just 5MB, which is almost a million times smaller than $\Phi_\ell(X, Y)$. 
... but instantiated modular polynomials are not.

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

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

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

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

INRIA Project TANC, 2007
Results

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

**Theorem**

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

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

**Theorem**

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

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

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

The new results also yield improved space complexity bounds (and better performance) for many other algorithms that use isogenies.
A volcano
A volcano
For a prime $\ell$, an $\ell$-volcano is a connected undirected graph whose vertices are partitioned into levels $V_0, \ldots, V_d$ such that:

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

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

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

We allow self-loops and multi-edges, but this can happen only on the surface.
A 3-volcano of depth 2
The graph of ℓ-isogenies

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

Except for $j \in \{0, 1728\}$, the in-degree of each vertex of $G_\ell$ is equal to its out-degree.

Thus $G_\ell$ is a bi-directed graph on $k \setminus \{0, 1728\}$, which we may regard as an undirected graph.

It consists of ordinary and supersingular components.

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

---

An elliptic curve $E$ over a field of characteristic $p > 0$ is supersingular iff $E[p] = \{0\}$. 
Isogenies from an elliptic curve $E$ to itself are endomorphisms. They form a ring $\text{End}(E)$ under composition and point addition.

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

For an elliptic curve $E$ with complex multiplication:

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

In characteristic $p > 0$, every elliptic curve has CM, since the $p$-power Frobenius endomorphism $(x, y) \mapsto (x^p, y^p)$ does not lie in $\mathbb{Z}$. 
Horizontal and vertical isogenies

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

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

Thus one of the following holds:

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

In the latter two cases we say that $\varphi$ is a vertical isogeny.
The theory of complex multiplication

Let $E/k$ have CM by an imaginary quadratic order $\mathcal{O}$.

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

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

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

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

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

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

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

Theorem (Kohel)

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

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

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

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

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

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

The term volcano is due to Fouquet and Morain (ANTS V).
Modular polynomials via isogeny volcanoes [BLS]

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

1. Select a sufficiently large set of primes of the form $4p = t^2 - \ell^2v^2D$ with $\ell \nmid v$, $p \equiv 1 \mod \ell$, and $h(D) > \ell + 1$.

2. For each prime $p$, compute $\Phi_\ell(X, Y) \mod p$ as follows:
   a. Compute $\text{Ell}_\mathcal{O}(\mathbb{F}_p)$ using $H_D(X) \mod p$.
   b. Map the $\ell$-volcanoes intersecting $\text{Ell}_\mathcal{O}(\mathbb{F}_p)$ (without using $\Phi_\ell$).
   c. Interpolate $\Phi_\ell(X, Y) \mod p$.

3. Use the CRT to recover $\Phi_\ell$ over $\mathbb{Z}$ (or mod $q$ via the explicit CRT).

Under the GRH, the expected running time is $O(\ell^3 \log^3 + \epsilon \ell)$ using $O(\ell^3 \log \ell)$ space (or $O(\ell^2 \log q)$ space to compute $\Phi_\ell \mod q$).

We can similarly compute modular polynomials for other modular functions.
One can also use a CRT approach to compute $\Phi_N$ for composite $N$ [Ono-S in prog].
Explicit Chinese Remainder Theorem

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

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

where $M = \prod p_i$, $M_i = M/p_i$ and $a_i = 1/M_i \mod p_i$.

If $M > 2|c|$, we can recover $c \in \mathbb{Z}$.

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

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

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

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

Mapping a volcano
Mapping a volcano

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

General requirements
\(4p = t^2 - v^2\ell^2D, \quad p \equiv 1 \mod \ell\)
Mapping a volcano

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

General requirements
\[ 4p = t^2 - v^2 \ell D, \quad p \equiv 1 \mod \ell \]
\( \ell \nmid v, \quad \left( \frac{D}{\ell} \right) = 1, \quad h(D) \geq \ell + 2 \)
Mapping a volcano

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

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

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
\[ 4p = t^2 - v^2 \ell D, \quad p \equiv 1 \mod \ell \]
\[ \ell \nmid v, \quad \left( \frac{D}{\ell} \right) = 1, \quad h(D) \geq \ell + 2 \]

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

\[ 4p = t^2 - v^2 \ell^2 D, \quad p \equiv 1 \mod \ell \]
\( \ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2 \)
\( \ell_0 \neq \ell, \quad (\frac{D}{\ell_0}) = 1 \)

2. Enumerate surface using the action of \( \alpha_{\ell_0} \)
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
\[ 4p = t^2 - v^2 \ell D, \quad p \equiv 1 \mod \ell \]
\[ \ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2 \]
\[ \ell_0 \neq \ell, \quad (\frac{D}{\ell_0}) = 1, \quad \alpha_\ell = \alpha_{\ell_0}^k \]

2. Enumerate surface using the action of \( \alpha_{\ell_0} \)
\[
901 \xrightarrow{2} 1582 \xrightarrow{2} 2501 \xrightarrow{2} 351 \xrightarrow{2} 701 \xrightarrow{2} 2872 \xrightarrow{2} 2215 \xrightarrow{2}
\]
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
\( 4p = t^2 - v^2\ell^2D, \quad p \equiv 1 \mod \ell \)
\( \ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2 \)
\( \ell_0 \neq \ell, \quad (\frac{D}{\ell_0}) = 1, \quad \alpha_{\ell} = \alpha_{\ell_0}^k \)

2. Enumerate surface using the action of \( \alpha_{\ell_0} \)

\[
901 \xrightarrow{2} 1582 \xrightarrow{2} 2501 \xrightarrow{2} 351 \xrightarrow{2} 701 \xrightarrow{2} 2872 \xrightarrow{2} 2215 \xrightarrow{2} 
\]
Mapping a volcano

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

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

2. Enumerate surface using the action of \( \alpha_{\ell_0} \)

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

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

2. Enumerate surface using the action of \( \alpha_{\ell_0} \)

\[
901 \xrightarrow{2} 1582 \xrightarrow{2} 2501 \xrightarrow{2} 351 \xrightarrow{2} 701 \xrightarrow{2} 2872 \xrightarrow{2} 2215 \xrightarrow{2}
\]
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
\[ 4p = t^2 - v^2\ell^2D, \quad p \equiv 1 \mod \ell \]
\[ \ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2 \]
\[ \ell_0 \neq \ell, \quad (\frac{D}{\ell_0}) = 1, \quad \alpha_{\ell} = \alpha_{\ell_0}^k \]

2. Enumerate surface using the action of \( \alpha_{\ell_0} \)

\[ \begin{align*}
901 & \xrightarrow{2} 1582 & \xrightarrow{2} 2501 & \xrightarrow{2} 351 & \xrightarrow{2} 701 & \xrightarrow{2} 2872 & \xrightarrow{2} 2215 & \xrightarrow{2} 2501 \\
\end{align*} \]
Mapping a volcano

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

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

2. Enumerate surface using the action of \( \alpha_{\ell_0} \)
\[ 901 \xrightarrow{2} 1582 \xrightarrow{2} 2501 \xrightarrow{2} 351 \xrightarrow{2} 701 \xrightarrow{2} 2872 \xrightarrow{2} 2215 \xrightarrow{2} \]
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

\[ 4p = t^2 - v^2 \ell^2 D, \quad p \equiv 1 \mod \ell \]

\( \ell \nmid v, \quad (D / \ell) = 1, \quad h(D) \geq \ell + 2 \)

\( \ell_0 \neq \ell, \quad (D / \ell_0) = 1, \quad \alpha_\ell = \alpha_\ell^k \)

2. Enumerate surface using the action of \( \alpha_{\ell_0} \)

901 \( \overset{2}{\rightarrow} \) 1582 \( \overset{2}{\rightarrow} \) 2501 \( \overset{2}{\rightarrow} \) 351 \( \overset{2}{\rightarrow} \) 701 \( \overset{2}{\rightarrow} \) 2872 \( \overset{2}{\rightarrow} \) 2215 \( \overset{2}{\rightarrow} \)
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
\[ 4p = t^2 - v^2 \ell^2 D, \quad p \equiv 1 \mod \ell \]
\[ \ell \nmid v, \quad \left( \frac{D}{\ell} \right) = 1, \quad h(D) \geq \ell + 2 \]
\[ \ell_0 \neq \ell, \quad \left( \frac{D}{\ell_0} \right) = 1, \quad \alpha_\ell = \alpha_{\ell_0}^k \]

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
\( 4p = t^2 - v^2 \ell^2 D, \quad p \equiv 1 \text{ mod } \ell \)
\( \ell \nmid v, \quad \left( \frac{D}{\ell} \right) = 1, \quad h(D) \geq \ell + 2 \)
\( \ell_0 \neq \ell, \quad \left( \frac{D}{\ell_0} \right) = 1, \quad \alpha_\ell = \alpha_{\ell_0}^k \)

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
\( 4p = t^2 - v^2\ell D, \quad p \equiv 1 \mod \ell \)
\( \ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2 \)
\( \ell_0 \neq \ell, \quad (\frac{D}{\ell_0}) = 1, \quad \alpha_\ell = \alpha_k^{\ell_0} \)

4. Enumerate floor using the action of \( \beta_{\ell_0} \)
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
\( 4p = t^2 - v^2 \ell^2 D, \quad p \equiv 1 \text{ mod } \ell \)
\( \ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2 \)
\( \ell_0 \neq \ell, \quad (\frac{D}{\ell_0}) = 1, \quad \alpha_{\ell} = \alpha_{\ell_0}^k, \quad \beta_{\ell_2} = \beta_{\ell_0}^{k'} \)

4. Enumerate floor using the action of \( \beta_{\ell_0} \)
\[
\begin{align*}
3188 & \rightarrow 945 \rightarrow 3144 \rightarrow 3508 \rightarrow 2843 \rightarrow 1502 \rightarrow 676 \rightarrow 2872 \\
2970 & \rightarrow 3497 \rightarrow 1180 \rightarrow 2464 \rightarrow 4221 \rightarrow 4228 \rightarrow 2434 \\
1478 & \rightarrow 3244 \rightarrow 2255 \rightarrow 2976 \rightarrow 3345 \rightarrow 1064 \rightarrow 1868 \\
3328 & \rightarrow 291 \rightarrow 3147 \rightarrow 2566 \rightarrow 4397 \rightarrow 2087 \rightarrow 3341 \\
\end{align*}
\]
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
\[ 4p = t^2 - v^2 \ell^2 D, \quad p \equiv 1 \text{ mod } \ell \]
\[ \ell \nmid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2 \]
\[ \ell_0 \neq \ell, \quad (\frac{D}{\ell_0}) = 1, \quad \alpha_\ell = \alpha_{\ell_0}^k, \quad \beta_{\ell_2} = \beta_{\ell_0}^{k'} \]

4. Enumerate floor using the action of \( \beta_{\ell_0} \)

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

\[ 4p = t^2 - v^2\ell^2D, \quad p \equiv 1 \mod \ell \]

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

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

4. Enumerate floor using the action of \( \beta_{\ell_0} \)

\[
\begin{align*}
3188 & \quad \overset{2}{\rightarrow} \quad 945 & \quad \overset{2}{\rightarrow} \quad 3144 & \quad \overset{2}{\rightarrow} \quad 3508 & \quad \overset{2}{\rightarrow} \quad 2843 & \quad \overset{2}{\rightarrow} \quad 1502 & \quad \overset{2}{\rightarrow} \quad 676 & \quad \overset{2}{\rightarrow} \\
2970 & \quad \overset{2}{\rightarrow} \quad 3497 & \quad \overset{2}{\rightarrow} \quad 1180 & \quad \overset{2}{\rightarrow} \quad 2464 & \quad \overset{2}{\rightarrow} \quad 4221 & \quad \overset{2}{\rightarrow} \quad 4228 & \quad \overset{2}{\rightarrow} \quad 2434 & \quad \overset{2}{\rightarrow} \\
1478 & \quad \overset{2}{\rightarrow} \quad 3244 & \quad \overset{2}{\rightarrow} \quad 2255 & \quad \overset{2}{\rightarrow} \quad 2976 & \quad \overset{2}{\rightarrow} \quad 3345 & \quad \overset{2}{\rightarrow} \quad 1064 & \quad \overset{2}{\rightarrow} \quad 1868 & \quad \overset{2}{\rightarrow} \\
3328 & \quad \overset{2}{\rightarrow} \quad 291 & \quad \overset{2}{\rightarrow} \quad 3147 & \quad \overset{2}{\rightarrow} \quad 2566 & \quad \overset{2}{\rightarrow} \quad 4397 & \quad \overset{2}{\rightarrow} \quad 2087 & \quad \overset{2}{\rightarrow} \quad 3341 & \quad \overset{2}{\rightarrow}
\end{align*}
\]
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
\( 4p = t^2 - v^2 \ell^2 D, \quad p \equiv 1 \mod \ell \)
\( \ell \mid v, \quad (\frac{D}{\ell}) = 1, \quad h(D) \geq \ell + 2 \)
\( \ell_0 \neq \ell, \quad (\frac{D}{\ell_0}) = 1, \quad \alpha_\ell = \alpha_{\ell_0}^k, \quad \beta_\ell^2 = \beta_{\ell_0}^{k'} \)

4. Enumerate floor using the action of \( \beta_{\ell_0} \)

\[
\begin{align*}
3188 & \xrightarrow{2} 945 & 2 \xrightarrow{2} 3144 & 2 \xrightarrow{2} 3508 & 2 \xrightarrow{2} 2843 & 2 \xrightarrow{2} 1502 & 2 \xrightarrow{2} 676 & 2 \xrightarrow{2} \\
2970 & \xrightarrow{2} 3497 & 2 \xrightarrow{2} 1180 & 2 \xrightarrow{2} 2464 & 2 \xrightarrow{2} 4221 & 2 \xrightarrow{2} 4228 & 2 \xrightarrow{2} 2434 & 2 \xrightarrow{2} \\
1478 & \xrightarrow{2} 3244 & 2 \xrightarrow{2} 2255 & 2 \xrightarrow{2} 2976 & 2 \xrightarrow{2} 3345 & 2 \xrightarrow{2} 1064 & 2 \xrightarrow{2} 1868 & 2 \xrightarrow{2} \\
3328 & \xrightarrow{2} 291 & 2 \xrightarrow{2} 3147 & 2 \xrightarrow{2} 2566 & 2 \xrightarrow{2} 4397 & 2 \xrightarrow{2} 2087 & 2 \xrightarrow{2} 3341 & 2 \xrightarrow{2}
\end{align*}
\]
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
\[ 4p = t^2 - v^2 \ell^2 D, \quad p \equiv 1 \mod \ell \]
\[ \ell \nmid v, \quad \left( \frac{D}{\ell} \right)_l = 1, \quad h(D) \geq \ell + 2 \]
\[ \ell_0 \neq \ell, \quad \left( \frac{D}{\ell_0} \right)_l = 1, \quad \alpha_\ell = \alpha_\ell^{k_0}, \quad \beta_\ell^2 = \beta_{\ell_0}^{k'_0} \]

4. Enumerate floor using the action of \( \beta_{\ell_0} \)

\[ 3188 \xrightarrow{2} 945 \xrightarrow{2} 3144 \xrightarrow{2} 3508 \xrightarrow{2} 2843 \xrightarrow{2} 1502 \xrightarrow{2} 676 \xrightarrow{2} \]
\[ 2970 \xrightarrow{2} 3497 \xrightarrow{2} 1180 \xrightarrow{2} 2464 \xrightarrow{2} 4221 \xrightarrow{2} 4228 \xrightarrow{2} 2434 \xrightarrow{2} \]
\[ 1478 \xrightarrow{2} 3244 \xrightarrow{2} 2255 \xrightarrow{2} 2976 \xrightarrow{2} 3345 \xrightarrow{2} 1064 \xrightarrow{2} 1868 \xrightarrow{2} \]
\[ 3328 \xrightarrow{2} 291 \xrightarrow{2} 3147 \xrightarrow{2} 2566 \xrightarrow{2} 4397 \xrightarrow{2} 2087 \xrightarrow{2} 3341 \xrightarrow{2} \]
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
\[ 4p = t^2 - v^2\ell^2D, \quad p \equiv 1 \mod \ell \]
\[ \ell \nmid v, \quad \left( \frac{D}{\ell} \right) = 1, \quad h(D) \geq \ell + 2 \]
\[ \ell_0 \neq \ell, \quad \left( \frac{D}{\ell_0} \right) = 1, \quad \alpha_{\ell} = \alpha_{\ell_0}^k, \quad \beta_{\ell^2} = \beta_{\ell_0}^{k'} \]

4. Enumerate floor using the action of \( \beta_{\ell_0} \)

\[
\begin{align*}
3188 & \to 945 & \to 3144 & \to 3508 & \to 2843 & \to 1502 & \to 676 & \to 3147 \\
2970 & \to 3497 & \to 1180 & \to 2464 & \to 4221 & \to 4228 & \to 2434 & \\
1478 & \to 3244 & \to 2255 & \to 2976 & \to 3345 & \to 1064 & \to 1868 & \\
3328 & \to 291 & \to 3147 & \to 2566 & \to 4397 & \to 2087 & \to 3341 \\
\end{align*}
\]
Mapping a volcano

Example

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

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

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

General requirements

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

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

$\ell_0 \neq \ell$, $(\frac{D}{\ell_0}) = 1$, $\alpha_{\ell} = \alpha_{\ell_0}^k$, $\beta_{\ell_2} = \beta_{\ell_0}^{k'}$

4. Enumerate floor using the action of $\beta_{\ell_0}$

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

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

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

$3328 \xrightarrow{2}{291} \xrightarrow{2}{3147} \xrightarrow{2}{2566} \xrightarrow{2}{4397} \xrightarrow{2}{2087} \xrightarrow{2}{3341}$
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
\( 4p = t^2 - v^2\ell^2D, \quad p \equiv 1 \mod \ell \)
\( \ell \nmid v, \quad (D_{\ell}) = 1, \quad h(D) \geq \ell + 2 \)
\( \ell_0 \neq \ell, \quad (D_{\ell_0}) = 1, \quad \alpha_{\ell} = \alpha_{\ell_0}^k, \quad \beta_{\ell^2} = \beta_{\ell_0}^{k'} \)

4. Enumerate floor using the action of \( \beta_{\ell_0} \)

\[
\begin{align*}
3188 & \rightarrow_2 945 & \rightarrow_2 3144 & \rightarrow_2 3508 & \rightarrow_2 2843 & \rightarrow_2 1502 & \rightarrow_2 676 & \rightarrow_2 \\
2970 & \rightarrow_2 3497 & \rightarrow_2 1180 & \rightarrow_2 2464 & \rightarrow_2 4221 & \rightarrow_2 4228 & \rightarrow_2 2434 & \rightarrow_2 \\
1478 & \rightarrow_2 3244 & \rightarrow_2 2255 & \rightarrow_2 2976 & \rightarrow_2 3345 & \rightarrow_2 1064 & \rightarrow_2 1868 & \rightarrow_2 \\
3328 & \rightarrow_2 291 & \rightarrow_2 3147 & \rightarrow_2 2566 & \rightarrow_2 4397 & \rightarrow_2 2087 & \rightarrow_2 3341 & \rightarrow_2 \\
\end{align*}
\]
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
\[ 4p = t^2 - v^2 \ell^2 D, \quad p \equiv 1 \mod \ell \]
\[ \ell \nmid v, \quad \left(\frac{D}{\ell}\right) = 1, \quad h(D) \geq \ell + 2 \]
\[ \ell_0 \neq \ell, \quad \left(\frac{D}{\ell_0}\right) = 1, \quad \alpha_\ell = \alpha_{\ell_0}^k, \quad \beta_{\ell_2} = \beta_{\ell_0}^{k'} \]
Interpolating $\Phi_\ell \mod p$

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

$$\Phi_5(X, 901) = X^6 + 1337X^5 + 543X^4 + 497X^3 + 4391X^2 + 3144X + 3262$$

$$\Phi_5(X, 351) = X^6 + 3174X^5 + 1789X^4 + 3373X^3 + 3972X^2 + 2932X + 4019$$

$$\Phi_5(X, 2215) = X^6 + 2182X^5 + 512X^4 + 435X^3 + 2844X^2 + 2084X + 2709$$

$$\Phi_5(X, 2501) = X^6 + 2991X^5 + 3075X^4 + 3918X^3 + 2241X^2 + 3755X + 1157$$

$$\Phi_5(X, 2872) = X^6 + 389X^5 + 3292X^4 + 3909X^3 + 161X^2 + 1003X + 2091$$

$$\Phi_5(X, 1582) = X^6 + 1803X^5 + 794X^4 + 3584X^3 + 225X^2 + 1530X + 1975$$

$$\Phi_5(X, 701) = X^6 + 515X^5 + 1419X^4 + 941X^3 + 4145X^2 + 2722X + 2754$$
Interpolating $\Phi_\ell \mod p$

\[
\Phi_5(X, Y) = X^6 + (4450Y^5 + 3720Y^4 + 2433Y^3 + 3499Y^2 + 70Y + 3927)X^5 \\
(3720Y^5 + 3683Y^4 + 2348Y^3 + 2808Y^2 + 3745Y + 233)X^4 \\
(2433Y^5 + 2348Y^4 + 2028Y^3 + 2025Y^2 + 4006Y + 2211)X^3 \\
(3499Y^5 + 2808Y^4 + 2025Y^3 + 4378Y^2 + 3886Y + 2050)X^2 \\
(70Y^5 + 3745Y^4 + 4006Y^3 + 3886Y^2 + 905Y + 2091)X \\
(Y^6 + 3927Y^5 + 233Y^4 + 2211Y^3 + 2050Y^2 + 2091Y + 2108)
\]
The Weber function

The Weber $f$-function is defined by

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

and satisfies

$$j(\tau) = \left( f(\tau)^{24} - 16 \right)^3 / f(\tau)^{24}.$$

The coefficients of $\Phi_f^\ell$ are roughly 72 times smaller. This means we need 72 times fewer primes.

The polynomial $\Phi_f^\ell$ is roughly 24 times sparser. This means we need 24 times fewer interpolation points.

Overall, we get nearly a \textbf{1728-fold speedup} using $\Phi_f^\ell$. 
Modular polynomials for $\ell = 11$

**Classical:**

$$X^{12} + Y^{12} - X^{11}Y^{11} + 8184X^{11}Y^{10} - 28278756X^{11}Y^9 + 53686822816X^{11}Y^8$$

$$- 61058988656490X^{11}Y^7 + 42570393135641712X^{11}Y^6 - 17899526272883039048X^{11}Y^5$$

$$+ 4297837238774928467520X^{11}Y^4 - 529134841844639613861795X^{11}Y^3 + 2720981165805664581552600X^{11}Y^2$$

$$- 374642006356701393515817612X^{11}Y + 2964709023552405240575283200000X^{11}$$

$$+ 8 \text{ pages omitted} \ldots$$

$$+ 392423345094527654908696462408720049099524723370674627089936420642670174061941686739245465600 \ldots 000$$

**Atkin:**

$$X^{12} - X^{11}Y + 744X^{11} + 196680X^{10} + 187X^9Y + 21354080X^9 + 506X^8Y + 830467440X^8$$

$$- 11440X^7Y + 16875327744X^7 - 57442X^6Y + 208564958976X^6 + 184184X^5Y + 1678582287360X^5$$

$$+ 1675784X^4Y + 9031525113600X^4 + 1867712X^3Y + 32349979904000X^3 - 8252640X^2Y + 74246810880000X^2$$

$$- 19849600XY + 9899773440000X + Y^2 - 8720000Y + 5841107200000$$

**Weber:**

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

Level records

1. 10009: \( \Phi_\ell \)
2. 20011: \( \Phi_\ell \mod q \)
3. 60013: \( \Phi_f \)

Speed records

1. 251: \( \Phi_\ell \) in 28s \( \Phi_\ell \mod q \) in 4.8s (vs 688s)
2. 1009: \( \Phi_\ell \) in 2830s \( \Phi_\ell \mod q \) in 265s (vs 107200s)
3. 1009: \( \Phi_f \) in 2.8s

Effective throughput when computing \( \Phi_{1009} \mod q \) is 100Mb/s.

---

Single core CPU times (AMD 3.0 GHz), using prime \( q \approx 2^{256} \).
Polynomials \( \Phi_f \) for \( \ell \leq 5000 \) available at http://math.mit.edu/~drew.
Computing $\phi_\ell(Y)$ with the CRT (naïve approach)

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

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

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

Uses $O(\ell^2 \log^3 + \epsilon p)$ expected time for each $p$, and $O(\ell^2 \log p)$ space.
Computing $\phi_\ell(Y)$ with the CRT (naïve approach)

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

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

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

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

However, “sufficiently many” is now $O(\ell n)$, where $n = \log q$.

Total expected time is $O(\ell^3 n \log^{3+\epsilon} \ell)$, using $O(\ell n + \ell^2 \log \ell)$ space.

This approach is not very useful:

- If $n$ is large (e.g. $n \approx \ell$), it takes way too long (quartic in $\ell$).
- If $n$ is small (e.g. $n \approx \log \ell$), it doesn’t save any space.
Computing $\phi_\ell(Y)$ with the CRT (Algorithm 1)

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

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

for sufficiently many primes $p$, where $\Phi_\ell = \sum c_{ik} X^i Y^k$. Obtain $\phi_\ell \mod q$ via the explicit CRT.
Computing $\phi_\ell(Y)$ with the CRT (Algorithm 1)

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

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

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

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

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

This algorithm can also evaluate the partial derivatives of $\Phi_\ell$ needed
to construct normalized equations for $\tilde{E}$ (important for SEA).
Computing $\phi_\ell(Y)$ with the CRT (Algorithm 2)

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

1. For each of $\ell + 2$ $j$-invariants $y_i$, compute $z_i = \prod_k (j(E) - j_k)$, where the $j_k$ range over $\ell + 1$ neighbors of $y_i$ in $G_\ell(\mathbb{F}_p)$.

2. Interpolate $\phi_\ell(Y) \in \mathbb{F}_p$ as the unique polynomial of degree $\ell + 1$ for which $\phi_\ell(y_i) = z_i$.

Obtain $\phi_\ell \mod q$ via the explicit CRT.
Computing $\phi_\ell(Y)$ with the CRT (Algorithm 2)

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

1. For each of $\ell + 2$ $j$-invariants $y_i$, compute $z_i = \prod_k (j(E) - j_k)$, where the $j_k$ range over $\ell + 1$ neighbors of $y_i$ in $G_\ell(\mathbb{F}_p)$.

2. Interpolate $\phi_\ell(Y) \in \mathbb{F}_p$ as the unique polynomial of degree $\ell + 1$ for which $\phi_\ell(y_i) = z_i$.

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

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

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

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

29 / 34
Genus 1 point counting in large characteristic

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

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Time</th>
<th>Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Totally naive</td>
<td>$O(e^{2n+\epsilon})$</td>
<td>$O(n)$</td>
</tr>
<tr>
<td>Slightly less naive</td>
<td>$O(e^{n+\epsilon})$</td>
<td>$O(n)$</td>
</tr>
<tr>
<td>Baby-step giant-step</td>
<td>$O(e^{n/4+\epsilon})$</td>
<td>$O(e^{n/4+\epsilon})$</td>
</tr>
<tr>
<td>Pollard kangaroo</td>
<td>$O(e^{n/4+\epsilon})$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Schoof</td>
<td>$O(n^5 \log n)$</td>
<td>$O(n^3)$</td>
</tr>
<tr>
<td>SEA</td>
<td>$O(n^4 \log^3 n \log n)$</td>
<td>$O(n^3 \log n)$</td>
</tr>
<tr>
<td>SEA (Φℓ precomputed)</td>
<td>$O(n^4 \log n)$</td>
<td>$O(n^4)$</td>
</tr>
</tbody>
</table>

*Complexity estimates for SEA-based algorithms are heuristic expected times.
Genus 1 point counting in large characteristic

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

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Time</th>
<th>Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Totally naive</td>
<td>$O(e^{2n+\epsilon})$</td>
<td>$O(n)$</td>
</tr>
<tr>
<td>Slightly less naive</td>
<td>$O(e^{n+\epsilon})$</td>
<td>$O(n)$</td>
</tr>
<tr>
<td>Baby-step giant-step</td>
<td>$O(e^{n/4+\epsilon})$</td>
<td>$O(e^{n/4+\epsilon})$</td>
</tr>
<tr>
<td>Pollard kangaroo</td>
<td>$O(e^{n/4+\epsilon})$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Schoof</td>
<td>$O(n^5 \log n)$</td>
<td>$O(n^3)$</td>
</tr>
<tr>
<td>SEA*</td>
<td>$O(n^4 \log^3 n \log n)$</td>
<td>$O(n^3 \log n)$</td>
</tr>
<tr>
<td>SEA ($\Phi_\ell$ precomputed)</td>
<td>$O(n^4 \log n)$</td>
<td>$O(n^4)$</td>
</tr>
<tr>
<td>SEA with Algorithm 1</td>
<td>$O(n^4 \log^2 n \log n)$</td>
<td>$O(n^2 \log n)$</td>
</tr>
<tr>
<td>Amortized</td>
<td>$O(n^4 \log n)$</td>
<td>$O(n^2 \log n)$</td>
</tr>
</tbody>
</table>

*Complexity estimates for SEA-based algorithms are heuristic expected times.
The number of points on the elliptic curve $E$ defined by
\[ y^2 = x^3 + 2718281828x + 314159263, \]
modulo the 5011 digit prime $q = 16219299585 \cdot 2^{16612} - 1$ is

<table>
<thead>
<tr>
<th>Elliptic curve point-counting record</th>
</tr>
</thead>
<tbody>
<tr>
<td>$y^2 = x^3 + 2718281828x + 314159263$</td>
</tr>
</tbody>
</table>

31/34
### Elliptic curve point counting record

<table>
<thead>
<tr>
<th>Task</th>
<th>Total CPU Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute $\phi_{\ell}^f$</td>
<td>32 days</td>
</tr>
<tr>
<td>Find a root $\tilde{j}$</td>
<td>995 days</td>
</tr>
<tr>
<td>Compute $g_\ell$</td>
<td>3 days</td>
</tr>
<tr>
<td>Compute $\pi \mod g_\ell, E$</td>
<td>326 days</td>
</tr>
<tr>
<td>Find $\lambda_\ell$</td>
<td>22 days</td>
</tr>
</tbody>
</table>

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

The largest $\phi_{\ell}^f$ was under 20MB in size and took about two hours to compute using 1 core.
Modular polynomial evaluation record

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

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

The size of $\phi_{\ell}$ is about 1 GB.

For comparison:

- The size of $\Phi_{\ell}$ mod $q$ is about 2 TB.
- The size of $\Phi_{\ell}$ mod $q$ is about 50 TB.
- The size of $\Phi_{\ell}$ is more than 10 PB.
Improved space complexity of computing horizontal isogenies

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

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

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