Using modular polynomials for eta products to compute isogenies

François Morain

USING MODULAR POLYNOMIALS FOR ETA PRODUCTS TO COMPUTE ISOGENIES

FRANÇOIS MORAIN

Abstract. Let $\mathcal{E}$ be an elliptic curve over a field $\mathbf{K}$ and ℓ a prime. There exists an elliptic curve $\mathcal{E}^*$ related to $\mathcal{E}$ by an isogeny of degree ℓ only if $\Phi_\ell(X, j(\mathcal{E})) = 0$, where $\Phi_\ell(X, Y)$ is the traditional modular polynomial. Moreover, this polynomial gives the coefficients of $\mathcal{E}^*$, together with parameters needed to build the isogeny explicitly. Since the traditional modular polynomial has large coefficients, many families with smaller coefficients can be used instead, as described by Elkies, Atkin and others. In this work, we concentrate on the computation of modular polynomials for eta products, as considered by Fricke. We review and complete the properties of these eta products to be able to perform the computations of these polynomials using classical algorithms. We give algebraic formulas à la Atkin to compute the coefficients of $\mathcal{E}^*$. Numerical examples and comparisons to other families are also given.

1. Introduction

Computing isogenies is the central ingredient of the Schoof-Elkies-Atkin (SEA) algorithm that computes the cardinality of elliptic curves over finite fields of large characteristic [16, 2, 7] and also [3]. We continue the work started in [12] looking for alternative families of modular polynomials that can be used for building isogenies, in the spirit of Atkin. The main emphasis is on modular polynomials built with modular forms instead of modular functions. The algorithmic approach is that of [12].

There are many families of modular polynomials that can be used, with different properties. Very generally, a modular polynomial is some bivariate polynomial $\Phi(X, J)$ where J corresponds to the j-invariant of the elliptic curve $\mathcal{E}$, and X stands for some modular function on $\Gamma_0(\ell)$, where ℓ is a prime. The prototype is $j(\mathcal{E}^*)$ (see below for more precise statements) that yields traditional modular polynomials. Alternative choices for X exist [12] for a list. They all lead to polynomials of (conjectured) height $O((\ell+1)\log \ell)$ but with small constants. In this work, we focus on the family of η-products $\eta(\tau)^r\eta(\ell\tau)^s$ for integers r and s satisfying arithmetic conditions. These functions and their associated modular polynomials $\Phi_{\ell,r,s}$ were already studied by Fricke (though in a different language). The case $r = s = 2$ for prime $\ell \equiv 11 \bmod 12$ was suggested by Atkin [2] to replace the Fricke/CCR polynomials introduced in [8, 4] (see also [12]). We prove properties of these that enable their efficient computation, including exact formulas for the conjugates and power sums series expansion.

Section 2) recalls classical results on modular forms, including properties of the η-function. In Section 3, we prove properties and needed formulas to compute $\Phi_{\ell,r,s}$. Section 4 explains how to compute the isogenous curve using partial derivatives of the polynomial $\Phi_{\ell,r,s}$, in the spirit of Atkin's work in the traditional case. We give numerical examples and height comparisons between modular polynomials in Section 5. An appendix contains numerical values for our polynomials, as well as a script for checking the results of Section 4.

Historical comment: the author produced two preprints [13] and [11] that he considers now as completely superseded by [12] and the present work as can be checked by the reader for him/herself.

Date: January 29, 2024.

2. Classical properties

Let τ be a complex number in the upper half plane. We write indifferently $f(\tau)$ or $f(q)$ some series, where $q = \exp(2i\pi\tau)$. Let $\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad - bc = 1 \right\}$. For many classical properties, we refer for instance to [5].

2.1. **Modular forms.** Let f be a modular form for Γ of integer weight $2k$ and character χ. By construction, this means that

$$f(M\tau) = \chi(d)(c\tau + d)^{2k} f(\tau)$$

for any matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in Γ.

If $M \in \mathrm{GL}_2(\mathbb{R})$, define

$$f|_{2k}M(\tau) = \det(M)^k (c\tau + d)^{-2k} f(M\tau).$$

2.1.1. *Eisenstein series and the Dedekind η-function.* The classical Eisenstein series we need are

$$E_2(q) = 1 - 24 \sum_{n=1}^{\infty} \delta_1(n) q^n,$$

$$E_4(q) = 1 + 240 \sum_{n=1}^{\infty} \delta_3(n) q^n,$$

$$E_6(q) = 1 - 504 \sum_{n=1}^{\infty} \delta_5(n) q^n,$$

where $\delta_r(n)$ denotes the sum of the r-th powers of the divisors of n. Other series E_{2k} can be defined for even $k > 3$. The series E_{2k} is a modular form of weight $2k$ for $k > 1$; the series E_2 is not a modular form, but the related function $F_\ell(\tau) = E_2(\tau) - \ell E_2(\ell\tau)$ is a modular form of weight 2 for $\Gamma_0(\ell)$.

Remember that the Dedekind function $\eta(q) = q^{1/24} e(q)$, where $e(q) = \prod_{n=1}^{\infty}(1 - q^n)$, satisfies

$$\eta(\tau + 1) = \zeta_{24}\eta(\tau), \quad \eta(-1/\tau) = \sqrt{-i\tau}\,\eta(\tau) \tag{1}$$

where ζ_n stands for a primitive n-th root of unity.

Also of interest are the discriminant $\Delta(q) = \eta(q)^{24}$, and the modular invariant

$$j(q) = \frac{E_4(q)^3}{\Delta(q)} = \frac{1}{q} + 744 + \cdots.$$

2.1.2. *Spaces.*

Theorem 2.1. *The space $\mathcal{M}_{2k}$ (resp. S_{2k}) of modular forms (resp. cuspidal forms) of weight $2k$ for Γ, is of dimension 1 (resp. 0) for $k = 2, 3, 4, 5, 7$. In these cases, $\mathcal{M}_{2k}$ is generated by E_{2k}. More generally,*

$$\dim(\mathcal{M}_{2k}) = \begin{cases} \lfloor k/6 \rfloor & \text{if } k \equiv 1 \bmod 6, \\ \lfloor k/6 \rfloor + 1 & \text{if } k \not\equiv 1 \bmod 6. \end{cases}$$

The unique cusp form of weight 12 is Δ.

The following comes from [17, §5.6.2].

Theorem 2.2. *A modular form f of weight $2k$ with integer coefficients can be expressed as a polynomial with integer coefficients in E_4, Δ if k is even and E_4, Δ, E_6 otherwise.*

2.1.3. *Modular equations for modular forms.* This is [5, Ex. 6.2.12 a)]. Here we are exclusively concerned with prime levels ℓ. The general case can be found in the literature.

Proposition 2.3. *The cosets of* $\Gamma_0(\ell)\backslash\Gamma$ *are* $R_c = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$ *for* $0 \le c < \ell$ *and* $R_\ell = \begin{pmatrix} 0 & -1 \\ 1 & \ell \end{pmatrix}$.

The following result is classical, using the definition of cosets.

Theorem 2.4. *Let* f *be a modular form of weight* w *for* $\Gamma_0(\ell)$. *The values* $f|_w(R_i)$ *are conjugate over* $\Gamma_0(\ell)$ *and define a polynomial*

$$\Phi[f](X) = \prod_R (X - f|_w(R_i)) = X^{\ell+1} + C_1(f)X^\ell + \cdots + C_{\ell+1}(f).$$

The coefficient $C_t(f)$ *is a modular form of weight* wt *for* Γ. *Another point of view is saying* $\Phi[f]$ *has (homogeneous) weight* $w(\ell+1)$ *so that all monomials* $X^{\ell+1-t}C_t$ *must have (homogeneous) weight* $w(\ell+1)$.

We have an analogous result for the power sums of $\Phi[f]$:

Corollary 2.5. *For* $t \ge 1$, *let*

$$S_t(f) = \sum_{i=1}^{\ell+1} (f|_w(R_i))^t$$

for $1 \le t \le \ell+1$. *The sum* $S_t(f)$ *is also a modular (cusp) form of weight* wt *for* Γ.

For cusp forms, we can be more precise, using Theorem 2.1.

Theorem 2.6. *If* f *is a cusp form of even weight* w, $C_t(f) = 0$ *(resp.* $S_t(f) = 0$*) for* $(w/2)t \in \{2, 3, 4, 5, 7\}$.

As a consequence of Theorem 2.2

Proposition 2.7. *The coefficient* $C_t(f)$ *(resp.* $S_t(f)$*) is expressible as a polynomial in* E_4, E_6 *and* Δ, *with integer coefficients if* f *does.*

2.2. **Transformation formula for η.** A key to our computation of the conjugates of η-products is the explicit transformation law for η. There are several known, and we use this one coming from [15].

Theorem 2.8. *Let* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ *be normalized such that* $c \ge 0$, *and* $d > 0$ *if* $c = 0$. *Write* $c = c_1 2^{\lambda(c)}$ *with* c_1 *odd; by convention,* $c_1 = \lambda(c) = 1$ *if* $c = 0$. *Define*

$$\varepsilon(M) = \left(\frac{a}{c_1}\right) \zeta_{24}^{ab + c(d(1-a^2)-a) + 3c_1(a-1) + \frac{3}{2}\lambda(c)(a^2-1)}.$$

Then $\eta(M\tau) = \varepsilon(M)\sqrt{c\tau + d}\,\eta(\tau)$.

Some cases appear frequently.

Lemma 2.9. *i) when* $a = 1$, $\varepsilon(M) = \zeta_{24}^{b-c}$;
ii) when $a = 2$, *we must have* c *odd, so that* $\varepsilon(M) = \left(\frac{2}{c}\right)\zeta_{24}^{2b-c(3d-1)}$;
iii) when $a = 3$, $\varepsilon(M) = \left(\frac{3}{c_1}\right)\zeta_{24}^{3b-c(8d+3)+6c_1+12\lambda(c)}$;
iv) When a *is a prime* > 3, *then* $a^2 - 1 = 24K$ *which gives*

$$\varepsilon(M) = \left(\frac{a}{c_1}\right) \zeta_{24}^{a(b-c)+3c_1(a-1)+12K\lambda(c)}.$$

Let us consider some arithmetical properties related to the preceding quantities.

Lemma 2.10. *With the notations of Lemma 2.9, let ℓ be an odd prime and $1 \le c < \ell$; let $\overline{c}$ be such that $\ell u + c\overline{c} = 1$ for some u by Bézout's identity. Then*
a) $\sum_{c=1}^{\ell-1} \overline{c} = 0$*;*
b) $\sum_{c=1}^{\ell-1} c_1$ *is even.*

Proof: a) use the involution $(c, \overline{c})$.
b) we sum an even number of odd numbers and this yields an even number. □

3. Modular polynomials for η-products

3.1. **General results.** This is [5, Proposition 5.9.2].

Proposition 3.1. *Let $f(\tau) = \prod_{m|N} \eta^{r_m}(m\tau)$ with $w = \sum_{m|N} r_m/2 \in \mathbb{Z}$. Then f is a modular function of weight w for some $\Gamma_0(M)$ character χ if and only if $\sum_{m|N} m r_m \equiv 0 \bmod 24$ and $\sum_{m|N}(N/m) r_m \equiv 0 \bmod 24$. We can choose M as the lcm of N and the denominator of $\sum_{m|N} r_m/(24m)$ and*

$$\chi(d) = \left(\frac{(-1)^w P}{d}\right), \quad P = \prod_{m|N} m^{r_m}.$$

3.2. **The prime case.** We concentrate here on functions $f(\tau) = \mathrm{Fr}_{\ell,r,s} = \eta(\tau)^r \eta(\ell\tau)^s$ for r and s satisfying the conditions of Proposition 3.1: f is a modular form of weight $w = (r+s)/2 \in \mathbb{Z}$ for $\Gamma_0(\ell)$, with $r + \ell s \equiv r\ell + s \equiv 0 \bmod 24$. Note these two conditions are equivalent when $r = s$ or $\ell > 3$; in the latter case we use $\ell^2 \equiv 1 \bmod 24$. We are interested in even weight modular forms. This has direct arithmetical implications.

Lemma 3.2. *a) When $\ell = 2$, r and s are even.*
b) When ℓ is odd, r and s have the same parity. The case s odd can only happen when $\ell \equiv 1 \bmod 4$.

Proof: a) when $\ell = 2$, this implies r even and forces s to be even too since we want $(r+s)/2$ in $\mathbb{Z}$.
b) When ℓ is odd, $r + s \equiv 0 \bmod 2$. If $\ell \equiv 3 \bmod 4$ and $s \equiv 1 \bmod 2$, we have $(r+s)/2$ odd. □

3.2.1. *Preparatory work.* For the coset R_ℓ, we compute

$$\eta(R_\ell\tau) = \eta(-1/(\tau+\ell)) = \sqrt{-i(\tau+\ell)}\,\eta(\tau+\ell) = \sqrt{-i}\,\zeta_{24}^{\ell}\,\sqrt{\tau+\ell}\,\eta(\tau).$$

For the evaluation of $\eta(\ell(R_\ell\tau))$, we need

$$\begin{pmatrix} 0 & -\ell \\ 1 & \ell \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} = U_\ell\, V_\ell,$$

so that

$$\eta(\ell(R_\ell\tau)) = \ell^{-1/2}\sqrt{-i(\tau+\ell)}\,\eta(\tau/\ell+1) = \sqrt{-i}\,\zeta_{24}\ell^{-1/2}\sqrt{\tau+\ell}\,\eta(\tau/\ell).$$

Let us turn our attention to R_c for $c > 0$. Define

$$U_c = \begin{pmatrix} 1 & -1 \\ c & 1-c \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

to get

$$\eta(R_c\tau) = \eta(U_c(V\tau)) = \varepsilon(U_c)\sqrt{c(\tau+1)+1-c}\,\zeta_{24}\eta(\tau).$$

Since by Lemma 2.9, $\varepsilon(U_c) = \zeta_{24}^{-1-c}$, this simplifies to

$$\zeta_{24}^{-c}\sqrt{c\tau+1}\,\eta(\tau).$$

For the other part, we first have $\eta(\ell(R_0\tau)) = \eta(\ell\tau)$. When $c > 0$, write

$$\begin{pmatrix} \ell & 0 \\ c & 1 \end{pmatrix} = U'_c\, V'_c \quad \text{with } U'_c = \begin{pmatrix} \ell & -\overline{c} \\ c & u \end{pmatrix} \in \Gamma, \quad V'_c = \begin{pmatrix} 1 & \overline{c} \\ 0 & \ell \end{pmatrix}$$

where $u\ell + \overline{c}c = 1$. This gives us

$$\begin{aligned} \eta(\ell(R_c\tau)) &= \eta(U'_c(V'_c\tau)) \\ &= \varepsilon(U'_c)\sqrt{c(V'_c\tau)+u}\,\eta\left(\frac{\tau+\overline{c}}{\ell}\right) \\ &= \varepsilon(U'_c)\ell^{-1/2}\sqrt{c\tau+c\overline{c}+\ell u}\,\eta\left(\frac{\tau+\overline{c}}{\ell}\right) \\ &= \varepsilon(U'_c)\ell^{-1/2}\sqrt{c\tau+1}\,\eta\left(\frac{\tau+\overline{c}}{\ell}\right). \end{aligned}$$

Along the same lines

Proposition 3.3. *Let* $W_\ell = \begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}$ *be the (matrix of the) Fricke involution. Then*

$$\mathrm{Fr}_{\ell,r,s}|_w W_\ell\tau = (-1)^{w/2}\ell^{(r-s)/4}\eta(\tau)^s\eta(\ell\tau)^r.$$

3.2.2. *The conjugates of* $\mathrm{Fr}_{\ell,r,s}$.

Proposition 3.4. *Let* $f = \mathrm{Fr}_{\ell,r,s}$. *The conjugates* $g_c(\tau) = f|_w(R_c\tau)$ *for* $0 \le c \le \ell$ *are* $g_0(\tau) = f(\tau)$ *and*

$$g_c(\tau) = \xi(R_c)\,\ell^{-s/2}\,\eta(\tau)^r\eta\left(\frac{\tau+\overline{c}}{\ell}\right)^s \text{ for } 0 < c < \ell, \quad g_\ell(\tau) = \xi(R_\ell)\,\ell^{-s/2}\,\eta(\tau)^r\eta(\tau/\ell)^s,$$

where

$$\xi(R_c) = \zeta_{24}^{-rc}\varepsilon(U'_c)^s \text{ for } 0 < c < \ell \text{ and } \xi(R_\ell) = (-i)^w = \zeta_{24}^{-3(r+s)}. \tag{2}$$

Proof: first

$$\begin{aligned} f|_w(R_\ell\tau) &= (\tau+\ell)^{-w}f(R_\ell\tau) \\ &= (\tau+\ell)^{-w}(\tau+\ell)^{(r+s)/2}\left(\sqrt{-i}\,\zeta_{24}^{\ell}\eta(\tau)\right)^r\left(\sqrt{-i}\,\zeta_{24}\,\ell^{-1/2}\,\eta(\tau/\ell)\right)^s \\ &= (-i)^w\zeta_{24}^{r\ell+s}\,\ell^{-s/2}\,\eta(\tau)^r\eta(\tau/\ell)^s. \end{aligned}$$

Using $r\ell + s \equiv 0 \bmod 24$ yields the result.

Suppose $c > 0$. Then

$$\begin{aligned} f|_w(R_c\tau) &= (c\tau+1)^{-w}f(R_\ell\tau) \\ &= \left(\zeta_{24}^{-c}\eta(\tau)\right)^r\left(\varepsilon(U'_c)\,\ell^{-1/2}\,\eta\left(\frac{\tau+\overline{c}}{\ell}\right)\right)^s \\ &= \zeta_{24}^{-rc}\varepsilon(U'_c)^s\,\ell^{-s/2}\,\eta(\tau)^r\eta\left(\frac{\tau+\overline{c}}{\ell}\right)^s. \quad \square \end{aligned}$$

To simplify the rest of the exposition, we scale all conjugates by $\ell^{s/2}$. In other words, we let $f_0(\tau) = \xi(R_0)f(\tau)$ with $\xi(R_0) = \ell^{s/2}$, and

$$f_c(\tau) = \xi(R_c)\,\eta(\tau)^r\eta\left(\frac{\tau+\overline{c}}{\ell}\right)^s \text{ for } 0 < c < \ell, \quad f_\ell(\tau) = \xi(R_\ell)\,\eta(\tau)^r\eta(\tau/\ell)^s.$$

Let us give the results for the three cases $\ell \in \{2, 3\}$ and $\ell > 3$.

Proposition 3.5. *a) When $\ell = 2$, which implies r and s even, the conjugates are*

$$f_0(\tau) = 2^{s/2} f(\tau), \quad f_1(\tau) = \zeta_{24}^{-r} \eta(\tau)^r \eta((\tau-1)/2)^s, \quad f_2(\tau) = \zeta_8^{-(r+s)} \eta(\tau)^r \eta(\tau/2)^s.$$

b) When $\ell = 3$, the conjugates are $f_0(\tau) = 3^{s/2} f(\tau)$,

$$f_1(\tau) = \zeta_{24}^{-r+s} \eta(\tau)^r \eta((\tau-2)/3)^s, \quad f_2(\tau) = \zeta_{24}^{-2r-s} \eta(\tau)^r \eta((\tau-1)/3)^s, \quad f_3(\tau) = \zeta_8^{-(r+s)} \eta(\tau)^r \eta(\tau/3)^s.$$

c) When $\ell > 3$, let $K = (\ell^2-1)/24$. The conjugates are $f_0(\tau) = \ell^{s/2} f(\tau)$,

$$f_c(\tau) = \zeta_{24}^{s\phi(c)} \eta(\tau)^r \eta((\tau+\overline{c})/\ell)^s \text{ for } 1 \le c \le \ell\text{-}1, \quad f_\ell(\tau) = \zeta_8^{-(r+s)} \eta(\tau)^r \eta(\tau/\ell)^s,$$

where $\phi(c) = -\ell\overline{c} + 3c_1(\ell-1) + 12K\lambda(c)$.

Proof: a) using $(\overline{c}, u) = (-1, 1)$, the root of unity for f_1 is

$$\zeta_{24}^{-r} \left(\left(\frac{2}{1} \right) 1 \right)^s = \zeta_{24}^{-r}.$$

b) For $c = 1$, we find $(\overline{c}, u) = (-2, 1)$, and

$$f_1(\tau) = \zeta_{24}^{-r+s} \eta(\tau)^r \eta((\tau-2)/3)^s.$$

For $c = 2$, we get $(\overline{c}, u) = (-1, 1)$, and

$$f_2(\tau) = \zeta_{24}^{-2r-s} \eta(\tau)^r \eta((\tau-1)/3)^s.$$

c) When $\ell > 3$, we use $\ell^2 - 1 = 24K$ to write

$$\xi(R_c) = \zeta_{24}^{-rc} \left(\left(\frac{\ell}{c_1} \right) \zeta_{24}^{-\ell(c+\overline{c})+3c_1(\ell-1)+12K\lambda(c)} \right)^s$$

that is

$$\xi(R_c) = \left(\frac{\ell}{c_1} \right)^s \zeta_{24}^{-rc-s\ell(c+\overline{c})+s(3c_1(\ell-1)+12K\lambda(c))} = \left(\frac{\ell}{c_1} \right)^s \zeta_{24}^{s(-\ell\overline{c}+3c_1(\ell-1)+12K\lambda(c))} = \left(\frac{\ell}{c_1} \right)^s \zeta_{24}^{s\phi(\ell,c)}.$$

□

Now, we look at the field of coefficients of the conjugates. We make the convention that $\overline{c} = 0$ when $c = \ell$.

Proposition 3.6. *a) $f(q) \in \mathbb{Z}[[q]]$.*

b) Put $z^\ell = q$. For $0 < c \le \ell$, the expansion of $f_c(\tau)$ belongs to $\mathbb{Z}[\zeta_{24\ell}^s][[z]]$.

Proof: a) let us start with

$$f(\tau) = \eta(\tau)^r \eta(\ell\tau)^s = (q^{1/24} e(q))^r (q^{\ell/24} e(q^\ell))^s = q^{(r\ell+s)/24} \tilde{f}(q)$$

where $\tilde{f}$ is a series with coefficients in $\mathbb{Z}$.

b) Using $z = q^{1/\ell}$, write

$$f_c(\tau) = \xi(R_c)(q^{1/24} e(q))^r (\zeta_{24\ell}^{\overline{c}} z^{1/24} e(\zeta_\ell^{\overline{c}} z))^s = \xi(R_c) \zeta_{24\ell}^{s\overline{c}} z^{(r\ell+s)/24} e(z^\ell)^r e(\zeta_\ell^{\overline{c}} z)^s. \quad \square$$

Remark that when $s \mid 24$, the coefficient rings found above are somewhat smaller since we have $\zeta_{24}^s = \zeta_{24/s}$ and $\zeta_{24\ell}^s = \zeta_{(24/s)\ell}$.

Compute for v a positive integer

$$e(q)^v = \sum_{n=0}^{\infty} e(v, n) q^n$$

for coefficients $e(v, n)$ in $\mathbb{Z}$.

Theorem 3.7. *Let $\ell > 3$ and t be a positive integer. Define $\mathcal{P}_t = \sum_{c=0}^{\ell} f_c(\tau)^t$. When s or t is even, $\mathcal{P}_t$ is a cusp form with coefficients in $\mathbb{Z}$. When s and t are odd, $\mathcal{P}_t$ has a z-expansion with coefficients in $\mathbb{Z}[\sqrt{\ell}]$.*

Proof: Write

$$\begin{aligned}\mathcal{P}_t(\tau) &= \sum_{c=0}^{\ell} f_c(\tau)^t = \ell^{ts/2}\eta(q)^{rt}\eta(q^\ell)^{st} + \sum_{c=1}^{\ell} \xi(R_c)^t \eta(q)^{rt}\eta\left(\frac{\tau+\overline{c}}{\ell}\right)^{st}, \\ &= \eta(q)^{rt}\left(\ell^{ts/2}\eta(q^\ell)^{st} + \sum_{c=1}^{\ell} \xi(R_c)^t \eta\left(\frac{\tau+\overline{c}}{\ell}\right)^{st}\right), \\ &= \eta(q)^{rt}\left(\ell^{ts/2}\eta(q^\ell)^{st} + \mathcal{S}_t(\tau)\right).\end{aligned}$$

With $z = q^{1/\ell}$, the sum $\mathcal{S}_t(\tau)$ has z-expansion $z^{st/24}S_t(z)$ with

$$\begin{aligned}S_t(z) &= \xi(R_\ell)^t e(z)^{st} + \sum_{c=1}^{\ell-1} \xi(R_c)^t\, \zeta_{24\ell}^{st\overline{c}}\, e(\zeta_\ell^{\overline{c}} z)^{st} \\ &= \sum_{n=0}^{\infty} e(st,n)\, z^n \left(\xi(R_\ell)^t + \sum_{c=1}^{\ell-1} \xi(R_c)^t\, \zeta_{24\ell}^{st\overline{c}}\, \zeta_\ell^{n\overline{c}}\right).\end{aligned}$$

The most inner sum is

$$S'_t(n) = \sum_{c=1}^{\ell-1} \left(\frac{\ell}{c_1}\right)^{st} \zeta_{24}^{st(-\ell\overline{c}+3c_1(\ell-1)+12K\lambda(c))}\, \zeta_{24\ell}^{st\overline{c}}\, \zeta_\ell^{n\overline{c}}.$$

which we rewrite (using the fact that $\ell^2 - 1 = 24K$):

$$S'_t(n) = \sum_{c=1}^{\ell-1} \left(\frac{\ell}{c_1}\right)^{st} \zeta_{24}^{st(3c_1(\ell-1)+12K\lambda(c))}\, \zeta_\ell^{-Kst\overline{c}}\, \zeta_\ell^{n\overline{c}} = \sum_{c=1}^{\ell-1} \left(\frac{\ell}{c_1}\right)^{st} \zeta_8^{st(c_1(\ell-1)+4K\lambda(c))}\, \zeta_\ell^{(n-Kst)\overline{c}} \tag{3}$$

The case s even: the sum $S'_t(n)$ simplifies to

$$\sum_{c=1}^{\ell-1} \zeta_8^{stc_1(\ell-1)}\, \zeta_\ell^{(n-Kst)\overline{c}}.$$

The eight-th root of unity is in fact equal to

$$\nu = \zeta_2^{c_1 t(s/2)(\ell-1)/2} = (-1)^{ts(\ell-1)/4} \tag{4}$$

and no longer depends on c_1, since it is odd. Let us prove that $\xi(R_\ell)^t = \nu$. Write $\ell = 2\ell' + 1$, so that $r + s(2\ell'+1) \equiv 0 \bmod 24$. Since s is even, we get

$$\frac{r+s}{2} + s\ell' \equiv 0 \bmod 12$$

which implies that $4 \mid (r+s)$ and

$$\frac{r+s}{4} + (s/2)\ell' \equiv 0 \bmod 6$$

showing that $\frac{r+s}{4}$ and $(s/2)\ell'$ have the same parity, yielding the result.

Therefore

$$S'_t(n) = \nu \sum_{c=1}^{\ell-1} \left(\zeta_\ell^{n-Kst}\right)^{\overline{c}}$$

and we recover a familiar situation: if $n \equiv Kst \bmod \ell$, the sum is $\nu(\ell-1)$ and $\nu(0-1)$ otherwise, so that

$$S_t(z) = \sum_{n\geq 0, n\equiv Kst \bmod \ell}^{\infty} e(st,n)\, z^n \left(\xi(R_\ell)^t - \nu + \nu\ell\right) + \sum_{n\geq 0, n\not\equiv Kst \bmod \ell}^{\infty} e(st,n)\, z^n \left(\xi(R_\ell)^t - \nu\right).$$

Write the euclidean division $Kst = \mu\ell + n_0$, $0 \leq n_0 < \ell$. We rewrite S_t as:

$$S_t(z) = (-1)^{t(r+s)/4}\, \ell\, z^{n_0} \sum_{n\geq 0}^{\infty} e(st, n_0+\ell n)\, q^n$$

and

$$\mathcal{P}_t = \eta(q)^{rt} \left(\ell^{st/2} \eta(q^\ell)^{st} + (-1)^{t(r+s)/4}\, \ell\, z^{n_0+st/24} \sum_{n\geq 0}^{\infty} e(st, n_0+\ell n)\, q^n \right).$$

The next rewriting yields

$$\mathcal{P}_t = e(q)^{rt} \left(\ell^{st/2} q^{t(r+\ell s)/24} \sum_{n\geq 0}^{\infty} e(st,n)\, q^{\ell n} + (-1)^{t(r+s)/4}\, \ell\, q^{rt/24} z^{n_0+st/24} \sum_{n\geq 0}^{\infty} e(st, n_0+\ell n)\, q^n \right).$$

We remark that

$$q^{rt/24} z^{n_0+st/24} = z^{t(\ell r+s)/24+n_0}$$

where the exponent can be rewritten as

$$t\frac{\ell r+s}{24} + Kst - \mu\ell = \frac{t}{24}\,\ell(r+\ell s) - \mu\ell$$

so that

$$\mathcal{P}_t = e(q)^{rt} \left(\ell^{st/2} q^{t(r+\ell s)/24} \sum_{n\geq 0}^{\infty} e(st,n)\, q^{\ell n} + (-1)^{t(r+s)/4}\, \ell\, q^{t(r+\ell s)/24-\mu} \sum_{n\geq 0}^{\infty} e(st, n_0+\ell n)\, q^n \right),$$

which can be rewritten first as

$$\mathcal{P}_t = q^{t(r+\ell s)/24-\mu} e(q)^{rt} \left(\ell^{st/2} q^{\mu} \sum_{n\geq 0}^{\infty} e(st,n)\, q^{\ell n} + (-1)^{t(r+s)/4}\, \ell \sum_{n\geq 0}^{\infty} e(st, n_0+\ell n)\, q^n \right), \tag{5}$$

which proves the result is an effective usable way. Another possible writing is

$$\mathcal{P}_t = \ell^{st/2} \Delta^{rt} \left(q^{t\ell s/24} \sum_{n\geq 0}^{\infty} e(st,n)\, q^{\ell n} \right) + (-1)^{t(r+s)/4}\, \ell\, \Delta^{rt} \left(q^{t\ell s/24-\mu} \sum_{n\geq 0}^{\infty} e(st, n_0+\ell n)\, q^n \right).$$

Note that $t\ell s/24 - \mu = (st + 24n_0)/(24\ell)$.

The case s odd: when t is even, we perform the same computation as for s even, leading to the evaluation of θ in this case. We use $t = 2t'$ and $r + s \equiv 0 \bmod 2$ to get

$$\theta = (-1)^{-t'(r+s)/2} - (-1)^{t's(\ell-1)/2}.$$

We have also

$$\frac{r+s}{2} + s\ell' \equiv 0 \bmod 12$$

which shows the two numbers of the sum have the same parity and $\theta = 0$.

When t is odd, the situation is more complex. Remember that $\ell = 1 + 4\mu$ by Lemma 3.2, from which $K = \mu(2\mu+1)/3$ with $\mu \bmod 3 \in \{0,1\}$. The sum (3) becomes

$$S'_t(n) = \sum_{c=1}^{\ell-1} \left(\frac{\ell}{c_1}\right)^{st} \zeta_2^{st\mu(c_1+\lambda(c))}\, \zeta_\ell^{(n-Kst)\overline{c}} = \zeta_2^{\mu} \sum_{c=1}^{\ell-1} \left(\frac{c_1}{\ell}\right) \zeta_2^{K\lambda(c)}\, \zeta_\ell^{(n-Kst)\overline{c}}$$

since s, t and c_1 are odd and $\ell \equiv 1 \bmod 4$. This sum is in fact

$$S'_t(n) = \zeta_2^{\mu} \sum_{c=1}^{\ell-1} \left(\frac{c}{\ell}\right) \zeta_\ell^{(n-Kst)\overline{c}}$$

using the following result.

Lemma 3.8. *Suppose $\ell \equiv 1 \bmod 4$. For all $1 \le c \le \ell - 1$, one has*

$$\left(\frac{c_1}{\ell}\right) \zeta_2^{K\lambda(c)} = \left(\frac{c}{\ell}\right).$$

Proof: When μ is even, this implies K is and $\ell \equiv 1 \bmod 8$, so that

$$\left(\frac{c}{\ell}\right) = \left(\frac{2}{\ell}\right)^{\lambda(c)} = \left(\frac{c_1}{\ell}\right) \zeta_2^{K\lambda(c)}$$

which gives the proof. When μ is odd, we have K odd and $\ell \equiv 5 \bmod 8$, so that

$$\left(\frac{c}{\ell}\right) = (-1)^{\lambda(c)} \left(\frac{c_1}{\ell}\right) = (-1)^{K\lambda(c)} \left(\frac{c_1}{\ell}\right)$$

and the proof follows. □

Proposition 3.9. *The value of $S'_t(n)$ is 0 when $n \equiv Kst \bmod \ell$ and $(-1)^{\mu}\left(\frac{n-Kst}{\ell}\right)\sqrt{\ell}$ otherwise.*

Proof:
a) When $n \equiv Kst \bmod \ell$, we get

$$S'_t(n) = \zeta_2^{\mu} \sum_{c=1}^{\ell-1} \left(\frac{c}{\ell}\right)$$

that we rewrite

$$\sum_{u=0}^{\ell-2} \left(\frac{g}{\ell}\right)^u = 0$$

where g is a generator of $(\mathbb{Z}/\ell\mathbb{Z})^*$.

b) Suppose now that $n \not\equiv Kst \bmod \ell$ and put $n' = (n - Kst) \bmod \ell$. We need to evaluate

$$S'_t(n) = \zeta_2^{\mu} \sum_{c=1}^{\ell-1} \left(\frac{c}{\ell}\right) \zeta_\ell^{n'\overline{c}}.$$

Since $c\overline{c} = 1 \bmod \ell$, they are both quadratic or non-quadratic residues. Therefore

$$\begin{aligned} \sum_{c=1}^{\ell-1} \left(\frac{c}{\ell}\right) \zeta_\ell^{n'\overline{c}} &= \sum_{c \text{ quadratic residue}} \zeta_\ell^{n'\overline{c}} - \sum_{c \text{ non quadratic residue}} \zeta_\ell^{n'\overline{c}} \\ &= \sum_{c \text{ quadratic residue}} \zeta_\ell^{n'c} - \sum_{c \text{ non quadratic residue}} \zeta_\ell^{n'c}. \end{aligned}$$

Since n' is non-zero, $c \mapsto n'c$ is a permutation of the quadratic (resp. non-quadratic residues) if and only if n' is a square modulo ℓ. Otherwise the two populations are exchanged. Finally, remember (see e.g. [6]) that using the two periods

$$S_0 = \sum_{c \text{ quadratic residue}} \zeta_\ell^c, \quad S_1 = \sum_{c \text{ non quadratic residue}} \zeta_\ell^c,$$

one has $S_0 + S_1 = -1$, $S_0 - S_1 = \sqrt{\ell}$. This finishes the proof and the sign can be deduced from μ and n'. $\square$

3.2.3. *Properties of $\Phi_{\ell,r,s}$.*

Proposition 3.10. *Assigning weights w, 12, 4 and 6 respectively to X, Δ, E_4, and E_6, all coefficients of $\Phi_{\ell,r,s}(X, E_4, E_6, \Delta)$ are of weight $w(\ell+1)$.*

Proposition 3.11. *The polynomial $\Phi_{\ell,r,s}(X, E_4, E_6, \Delta)$ has coefficients in $\mathbb{Z}$.*

Proof: all roots of $\Phi_{\ell,r,s}$ have expansions in $\mathbb{Q}(\zeta_{24\ell})$; so do their elementary symmetric functions. Any element of the Galois group of the extension, say $\zeta_{24\ell} \mapsto \zeta_{24\ell}^a$ for $\gcd(a, 24\ell) = 1$, permutes the roots. Therefore all symmetric functions are polynomials with integer coefficients. The result follows from Proposition 2.7. $\square$

Using a reasoning close to that of [12, §2.5.1], we get

Proposition 3.12. *The height of $\Phi_{\ell,r,s}$ is approximately $(s/6)\ell \log \ell$.*

The following result is coherent with Proposition 3.10.

Proposition 3.13. *For prime $\ell \geq 2$, the product of the roots of $\Phi[\mathrm{Fr}_{\ell,r,s}]$ is*

$$\pm \ell^{s/2} \Delta^{(r+s)(\ell+1)/24}.$$

Proof: the product of the roots of $\Phi[\mathrm{Fr}_{\ell,r,s}]$ is

$$P_0 = (\ell^{s/2} f(\tau)) \cdot \eta(\tau)^{r\ell} \cdot \left(\prod_{c=1}^{\ell} \xi(R_c) \right) \cdot \prod_{c=1}^{\ell} \eta((\tau + \overline{c})/\ell)^s = \left(\ell^{s/2} \prod_{c=1}^{\ell} \xi(R_c) \right) \cdot \eta(\ell\tau)^s \eta(\tau)^{r(\ell+1)} P_1^s$$

where

$$P_1 = \prod_{c=1}^{\ell} \eta((\tau + \overline{c})/\ell) \text{ and } \prod_{c=1}^{\ell} \xi(R_c) = \zeta_8^{-(r+s)} \left(\prod_{c=1}^{\ell-1} \left(\frac{\ell}{c_1} \right) \right)^s \zeta_{24}^{s \sum_{c=1}^{\ell-1} \phi(c)}.$$

We write the sum as

$$S = \sum_{c=1}^{\ell-1} \phi(c) = \sum_{c=1}^{\ell-1} -\ell\overline{c} + 3c_1(\ell-1) + 12K\lambda(c) = -\ell \sum_{c=1}^{\ell-1} \overline{c} + 3(\ell-1) \sum_{c=1}^{\ell-1} c_1 + 12K \sum_{c=1}^{\ell-1} \lambda(c).$$

By Lemma 2.10, the first term is 0, the second is 0 mod 12 so that the whole term is 0 mod 12. The product is therefore ζ_{24}^{-6w+sS} with $S \equiv 0 \bmod 12$, so is ± 1 since w is even.

We need to compute

$$P_1 = \prod_{c=1}^{\ell} \eta((\tau + \overline{c})/\ell) = \prod_{k=-(\ell-1)/2}^{(\ell-1)/2} \eta((\tau + k)/\ell).$$

As usual, we write $q^{1/\ell} = z$, and we let $\ell' = (\ell-1)/2$:

$$P_1 = \prod_{k=-\ell'}^{\ell'} \left(z^{1/24} \zeta_{24\ell}^k \prod_{n \geq 1} (1 - z^n \zeta_\ell^{kn}) \right) = q^{1/24} \prod_{k=-\ell'}^{\ell'} \prod_{n \geq 1} (1 - z^n \zeta_\ell^{kn}).$$

Split the product into P_2 for $\ell \mid n$ and P_3 for $\ell \nmid n$. We find

$$P_2 = \prod_{\ell|n} \prod_{k=-\ell'}^{\ell'} (1 - z^n \zeta_\ell^{kn}) = \prod_{n\geq 1} (1-q^n)^\ell = q^{-\ell/24}\eta(\tau)^\ell.$$

Let us look at the polynomial $P(Z) = \prod_{k=-\ell'}^{\ell'}(1 - Z\zeta_\ell^{kn})$. When n is prime to ℓ, $k \mapsto (kn) \bmod \ell$ is a permutation of the ζ_ℓ^i, hence $P(Z) = 1 - Z^\ell$ and we deduce

$$P_3 = \prod_{\ell\nmid n}(1-q^n) = \frac{\prod_{n\geq 1}(1-q^n)}{\prod_{\ell|n}(1-q^{n\ell})} = \frac{q^{-1/24}\eta(\tau)}{q^{-\ell/24}\eta(\ell\tau)}$$

so that P_1 simplifies to

$$P_1 = \frac{\eta(\tau)^{\ell+1}}{\eta(\ell\tau)}.$$

Gathering all terms:

$$P_0 = \ell^{s/2}\eta(\tau)^{r(\ell+1)}\eta(\ell\tau)^s P_1^s = \ell^{s/2}\zeta_{24}^{-6w+sS}\eta(\tau)^{(r+s)(\ell+1)}.$$

We remark that $(r+s)(\ell+1) = (r+s\ell) + (\ell r + s) \equiv 0 \bmod 24$, which yields the result. □

3.2.4. *Best parameters.* By Proposition 3.12, the height of $\Phi_{\ell,r,s}$ is approximately $(s/6)(\ell+1)\log\ell$, using minimal s's is interesting. A short program yields solutions. In all cases, we can find solutions with $s = 2$.

ℓ	r	s	w	P
2	8	8	8	1
3	6	6	6	1
1 mod 12	12	12	12	1
	22	2	12	1
5 mod 12	4	4	4	1
	14	2	8	1
	9	3	6	5
7 mod 12	6	6	6	1
	10	2	6	1
11 mod 12	2	2	2	1

These cases were found by Fricke [8, (14) p. 340]. We gave the pair $(9,3)$ for $\ell \equiv 5 \bmod 12$ as example of what we could try with odd values.

Fricke gave the form of the modular polynomials in the case $s = 2$ [8, (4)–(7) p. 343]. His results are not limited to the prime case, but this is what we need here. The constant term coincides with our own formula proven above.

Theorem 3.14. *Let $N > 3$ be an odd integer, not a square and $\psi = N\prod_{p|N}(1+1/p)$. Then if $N \equiv 1,5,7,11 \bmod 12$, the forms of $\Phi_{N,r,2}$ are the following*

$$\Phi_{N,22,2} = X^\psi + \alpha_1\Delta X^{\psi-1} + (\alpha_2 E_4^3 + \beta_2 E_6^2)\Delta X^{\psi-2} + (\alpha_3 E_4^3 + \beta_3 E_6^2)\Delta^2 X^{\psi-3} + \cdots + \alpha_\psi \Delta^\psi,$$

$$\Phi_{N,14,2} = X^\psi + \alpha_2 E_4 \Delta X^{\psi-2} + (\alpha_3 E_4^3 + \beta_3 E_6^2)\Delta X^{\psi-3} + \alpha_4 E_4^2 \Delta^2 X^{\psi-4} + \cdots + \alpha_\psi \Delta^{2\psi/3},$$

$$\Phi_{N,10,2} = X^\psi + \alpha_2\Delta X^{\psi-2} + \alpha_3 E_6 \Delta X^{\psi-3} + (\alpha_4 E_4^3 + \beta_4 E_6^2)\Delta X^{\psi-4} + \alpha_5 E_6 \Delta^2 X^{\psi-5} + \cdots + \alpha_\psi \Delta^{\psi/2},$$

$$\Phi_{N,2,2} = X^\psi + \alpha_6\Delta X^{\psi-6} + \alpha_8 E_4 \Delta X^{\psi-8} + \alpha_9 E_6 \Delta X^{\psi-9} + \alpha_{10} E_4^2 \Delta X^{\psi-10} + \alpha_{11} E_4 E_6 \Delta X^{\psi-11} + \cdots + \alpha_\psi \Delta^{\psi/6},$$

for integers α_i and β_i, each different each time.

Proof: From Theorem 2.6, we identify *a priori* null coefficients. If $(w/2)t < 24$, the coefficient is Δ multiplied by a form of weight $(w/2)t - 12$, and depending on the result, we must multiply by some powers of E_4, E_6. This explains another part of the formulas. The same reasoning is valid for $24 < (w/2)t < 48$, where the coefficient must be a multiple of Δ^2. In the case $wt = 24u$, some care must be taken, which explains the expressions $(\alpha E_4^3 + \beta E_6^2)\Delta^u$. □

3.3. **Computing the modular polynomial $\Phi_{\ell,r,s}$.** Almost all methods described in [12] can be used, but for the isogeny approach (see below). From Corollary 2.5, we know the form of the coefficients in terms of E_4, E_6 and Δ. This can be used during series computations exploiting equation (5) or floating point evaluations.

Considering only $s = 2$ and r even, we get

$$\mathrm{Fr}_{\ell,r,s}^{12} = \Delta^{r/2}\tilde{\Delta},$$

which gives us $\tilde{\Delta}$. The quantities on the rhs are available from the isogeny computations. But the resulting equation for $\mathrm{Fr}_{\ell,r,2}$ has at least two solutions over $\mathbb{F}_p$, which means that we cannot compute the modular polynomial of this function easily. Note that the same problem occurs for Atkin's canonical modular polynomials, where we have an easy access to $F = \eta(\ell\tau)/\eta(\tau)$ such that $F^{24} = \tilde{\Delta}/\Delta$.

4. Computing the isogenous curve *à la* Atkin

Writing κ_r for the power sums of the roots of the kernel polynomial of the isogeny, we have

$$\kappa = \kappa_1 = \frac{\ell}{2}(\ell E_2(q^\ell) - E_2(q)) = -\frac{\ell}{2}F_\ell(q). \tag{6}$$

It is known that computing this kernel polynomial can be performed using (κ, A^*, B^*). The idea is to generalize the approach in [1, 2] (see also [9]), to get explicit formulas for these quantities using q-series. As a matter of fact, we need relations between $\tilde{E}_{2k} = E_{2k}(q^\ell)$, from which all other quantities follows: $A^* = -3\ell^4\tilde{E}_4$, etc.

4.0.1. *Formulas.* When $f(q) = \sum_{n\geq n_0} a_n q^n$, we introduce the operator

$$f'(q) = \frac{1}{2i\pi}\frac{df}{d\tau} = q\frac{df}{dq} = \sum_{n\geq n_0} n a_n q^n. \tag{7}$$

Several identities are classical:

$$\Delta = \frac{E_4^3 - E_6^2}{1728}, \quad j = \frac{E_4^3}{\Delta}, \quad j - 1728 = \frac{E_6^2}{\Delta}, \tag{8}$$

$$\frac{j'}{j} = -\frac{E_6}{E_4}, \quad \frac{j'}{j-1728} = -\frac{E_4^2}{E_6}, \quad j' = -\frac{E_4^2 E_6}{\Delta}, \quad \frac{\Delta'}{\Delta} = E_2, \tag{9}$$

to which we add the Ramanujan differential system:

$$3{E_4}' = E_4E_2 - E_6, \quad 2{E_6}' = E_6E_2 - E_4^2, \quad 12{E_2}' = E_2^2 - E_4. \tag{10}$$

4.1. **Properties of $\Phi_{\ell,r,s}$.** The polynomial $\Phi = \Phi_{\ell,r,s}(X, E_4, E_6)$ – replacing Δ for the price of denominators – is homogeneous with weight $w(\ell+1)$. We write

$$\partial_X = \frac{\partial\Phi}{\partial X}, \partial_4 = \frac{\partial\Phi}{\partial E_4}, \partial_6 = \frac{\partial\Phi}{\partial E_6}.$$

and propagate the notation to double derivatives. First, we have

$$w(\ell+1)\Phi = wX\partial_X + 4E_4\partial_4 + 6E_6\partial_6, \tag{11}$$

together with

$$w\ell\partial_X = wX\partial_{XX} + 4E_4\partial_{X4} + 6E_6\partial_{X6}, \tag{12}$$

$$(w(\ell+1)-4)\partial_4 = wX\partial_{X4} + 4E_4\partial_{44} + 6E_6\partial_{46}, \tag{13}$$

$$(w(\ell+1)-6)\partial_6 = wX\partial_{X6} + 4E_4\partial_{46} + 6E_6\partial_{66}. \tag{14}$$

4.2. **Computing κ.**

Proposition 4.1. *The value of κ is*

$$\kappa = \frac{\ell\,\left(6\,E_4^2\,\partial_6 + 4\,E_6\,\partial_4\right)}{sX\partial_X}.$$

Proof: Differentiate $X = \eta^r(\tau)\eta^s(\ell\tau)$ to get

$$24\frac{X'}{X} = r\,\frac{\Delta'}{\Delta} + s\ell\,\frac{\tilde{\Delta}'}{\tilde{\Delta}} = rE_2 + s\ell\tilde{E}_2$$

from which we get X'. Starting from $X'\partial_X + E_4'\partial_4 + E_6'\partial_6 = 0$, and injecting the value of X' and relations coming from (10), we find

$$\frac{X}{24}\left(rE_2 + s\ell\tilde{E}_2\right)\partial_X + \frac{1}{3}(E_4E_2 - E_6)\partial_4 + \frac{1}{2}\left(E_6E_2 - E_4^2\right)\partial_6 = 0,$$

which we rewrite

$$\left(\frac{r}{2}X\partial_X + 4E_4\partial_4 + 6E_6\partial_6\right)E_2 + \frac{s}{2}\ell X\partial_X\tilde{E}_2 = 4E_6\partial_4 + 6E_4^2\partial_6.$$

Using $4E_4\partial_4 + 6E_6 = -wX\partial_X$ and (6) gives us

$$X\partial_X\left(\left(\frac{r+s}{2} - w\right)E_2 + \kappa\frac{s}{\ell}\right) = 4E_6\partial_4 + 6E_4^2\partial_6,$$

which gives the result. □

4.3. **Computing $\tilde{E}_4$ and $\tilde{E}_6$.**

4.3.1. *Using differentials.*

Proposition 4.2. *The value of $\tilde{E}_4$ is given by*

$$\tilde{E}_4 = -\frac{M}{ws^2\ell^2X^2E_4E_6^2\partial_X^3}$$

where M is a polynomial given at the end of the proof.

Proof: We differentiate X' to obtain:

$$24X'' = X'(s\ell\tilde{E}_2 + rE_2) + X(s\ell\tilde{E}_2' + rE_2') = \frac{X}{24}\left((s\ell\tilde{E}_2 + rE_2)^2 + 2\left(s\ell^2(\tilde{E}_2^2 - \tilde{E}_4) + r(E_2^2 - E_4)\right)\right) \tag{15}$$

where $\tilde{E}_4$ appears. We inject this together with the diagonal derivatives of (12-14), the value $\tilde{E}_2 = (E_2 + 2\kappa/\ell)/\ell$ and the second derivatives computed from (10) into the differential of $X'\partial_X + E_4'\partial_4 + E_6'\partial_6 = 0$:

$$\begin{array}{rl} & X''\partial_X + X'(X'\partial_{XX} + E_4'\partial_{X4} + E_6'\partial_{X6}) \\ + & E_4''\partial_4 + E_4'(X'\partial_{4X} + E_4'\partial_{44} + E_6'\partial_{46}) \\ + & E_6''\partial_6 + E_6'(X'\partial_{6X} + E_4'\partial_{64} + E_6'\partial_{66}) = 0 \end{array} \tag{16}$$

to get a polynomial of degree 2 in E_2 whose coefficients of degree 2 and 1 (this one starts with $(s + r - 2w)$) turn out to vanish. We are left with

$$\tilde{E}_4 = -\frac{M}{ws^2\ell^2X^2E_4E_6^2\partial_f^3}$$

where[1]

$$M = -E_4^2X^2w(12E_4^3sw + 4E_4^3w^2 - E_6^2rs - 14E_6^2sw)\partial_X^3$$
$$+8wX(E_4^3 - E_6^2)(E_4^3X\partial_{X4}sw - E_4^3\partial_4\ell sw + 6E_4^3E_6\partial_{46}s - E_4^3\partial_4sw - E_6^2X\partial_{X4}sw + E_6^2\partial_4\ell sw$$
$$-6E_4^3\partial_4s - 4E_4^3\partial_4w - 6E_6^3\partial_{46}s + E_6^2\partial_4sw - 4E_6^2\partial_4s)\partial_X^2$$
$$+32E_4\partial_4w(E_4^3 - E_6^2)^2(2X\partial_{X4}s - \partial_4\ell s - \partial_4s - 2\partial_4)\partial_X + 64E_4\partial_4^2s(E_4^3 - E_6^2)^2(2E_4\partial_{X4} + 3E_6\partial_{X6})$$

Differentiating (15) gives us X''' and makes $\tilde{E}_4'$ appear, and this involves the quantity $\tilde{E}_6$ we are looking for:

$$24^2X''' = X'\left((s\ell\tilde{E}_2 + rE_2)^2 + 2\left(s\ell^2(\tilde{E}_2^2 - \tilde{E}_4) + r(E_2^2 - E_4)\right)\right)$$
$$+X\left(\cdots - 2s\ell^3\tilde{E}_4' + \cdots\right)$$

and use the expression of $\tilde{E}_4'$ from (10). Going further with a lot differentials would look like a formidable task.

4.3.2. *Using representation as fractions.* An alternative to find A^* and B^* is to compute the polynomials $\mathcal{A}_{\ell,r,s}$ and $\mathcal{B}_{\ell,r,s}$ such that

$$A^* = \frac{\mathcal{A}_{\ell,r,s}}{\frac{\partial\Phi_{\ell,r,s}}{\partial X}}, \quad B^* = \frac{\mathcal{B}_{\ell,r,s}}{\frac{\partial\Phi_{\ell,r,s}}{\partial X}}$$

as suggested in [14] (see [12] for efficient algorithms).

For instance for

$$\Phi_{11,2,2}(X, E_4, E_6, \Delta) = X^{12} - 990\Delta X^6 + 440\Delta E_4X^4 + 165\Delta E_6X^3 + 22\Delta E_4^2X^2 + \Delta E_4E_6X - 11\Delta^2,$$

we compute

$$\mathcal{A}_{11,2,2} = -43956E_4X^{11} + 3801600\Delta X^7 + 44520300\Delta E_4X^5 + 1520640\Delta E_6X^4 - 19235040\Delta E_4^2X^3$$
$$-7319565\Delta E_4E_6X^2 + (-974292\Delta E_4^3 - 627264000\Delta^2)X - 43923\Delta E_4^2E_6,$$
$$\mathcal{B}_{11,2,2} = -3543144E_6X^{11} - 59875200\Delta X^8 - 35925120\Delta E_4X^6 + 3514519800\Delta E_6X^5$$
$$-1560972160\Delta E_4E_6X^3 + (-584782110\Delta E_4^3 + 1051996999680\Delta^2)X^2 - 77937640\Delta E_4^2E_6X$$
$$-3543122\Delta E_4^4 + 3479224320\Delta^2E_4.$$

[1] We did not attempt to simplify this formula as much as could be.

4.3.3. *Last words.* Remember that for $s = 2$ and r even, we have $f^{12} = \Delta^{r/2}\tilde{\Delta}$, giving us $\tilde{\Delta}$.

When $r = s$, $f = \mathrm{Fr}_{\ell,r,r}$ is transformed by the Fricke involution (see Proposition 3.3), so that the quantity $\tilde{E}_6$ satisfies (remembering the scaling done on f):

$$\Phi_{\ell,r,r}((-\ell)^{r/2}f, \ell^4\tilde{E}_4, \ell^6\tilde{E}_6, \tilde{\Delta}) = 0. \tag{17}$$

When $r/2$ is odd, $\tilde{E}_6$ appears with power 1 in the polynomial, so that we can get its value easily.

As a conclusion, the natural approach has lengthy algorithm to compute $\tilde{E}_4$ but no other storage, and can sometimes be used in in the above approach. Otherwise, we must store another polynomial of degree ℓ with large height. Final evaluations require $O(\ell^2)$ computations.

4.4. **Numerical example.** Consider $E : Y^2 = X^3 + X + 3$ over $\mathbb{F}_{1009}$. The polynomial $\Phi_{11,2,2}$ has two roots: 676 and 944. We take $f = 676$. We first compute $\kappa = 681$. Then we compute $\tilde{E}_4 = 430$ by either method. The use of $\mathcal{B}_{11,2,2}$ leads to $\tilde{E}_6 = 732$. This we could achieve using (17), too. Note that we can check the answers directly if the polynomials V_{11} and W_{11} of [12] are available.

5. Implementation and numerical results

A lot of trials were done using Maple programs, some of which were then rewritten in Magma (version 2.26-10), for speed. See the author's web page. Computing the polynomials for $\ell \leq 100$ takes a few minutes on a classical laptop. Checking them is done using SEA, as mentioned in [14].

Building on [12], we give some examples of the *relative height* $\tilde{H}$ for some polynomials $\Phi(X, J)$ (for the first three columns) and $P(X, E_4, E_6, \Delta)$ for the other ones. Here $\tilde{H}(P) = H(P)/((\ell + 1)\log\ell)$. Note that these quantities seem to stabilize when ℓ increases and are in accordance with Proposition 3.12.

ℓ	$\tilde{H}(\Phi_\ell^t)$	$\tilde{H}(\Phi_\ell^c)$	$\tilde{H}(\Phi_\ell^*)$	$\tilde{H}(U_\ell)$	$\tilde{H}(\Phi_{\ell,r,r})$	$\tilde{H}(\Phi_{\ell,14,2})$	$\tilde{H}(\Phi_{\ell,10,2})$	$\tilde{H}(\Phi_{\ell,22,2})$
2	15.72	4.00	−−	−−	1.333	−−	−−	−−
3	11.14	1.51	−−	0.32	0.75	−−	−−	−−
5	11.243	0.762	−−	0.526	0.466	0.238	−−	−−
7	9.787	0.582	−−	0.640	0.746	−−	0.273	−−
11	10.130	1.842	1.120	0.670	0.240	−−	−−	−−
13	9.565	0.367	0.941	0.688	1.875	−−	−−	0.367
17	9.581	0.958	0.714	0.690	0.632	0.316	−−	−−
19	9.365	0.648	0.630	0.695	0.970	−−	0.332	−−
23	9.438	1.995	0.419	0.698	0.333	−−	−−	−−
101	−−	1.111	0.159	0.778	0.739	0.369	−−	−−
103	−−	0.740	0.249	0.779	1.111	−−	0.374	−−
107	−−	2.218	0.228	0.781	0.369	−−	−−	−−
109	−−	0.379	0.213	0.782	2.219	−−	−−	0.379

Data are computed using the polynomials available in Magma: Φ_ℓ^c is called *canonical polynomial* and Φ_ℓ^* is called *Atkin polynomial*.

Still, Atkin's minimal functions remain the best choice for large ℓ's.

6. Conclusions

In this article, we have studied Fricke's modular polynomials for eta products, adding an explicit formula for the conjugates and power sums that we can use to compute them. We insisted on the case where the index is prime, and the same work can be done for some composite numbers as described in [8]. This will be the subject of another supplementary work. It was the occasion to

gather properties of modular polynomials for modular forms, whereas the case of modular functions is more frequently considered.

As a result, we have new families of modular polynomials that can be used for isogeny computations.

References

[1] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime. Draft, 1988.

[2] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime (II). Draft. Available on `http://listserv.nodak.edu/archives/nmbrthry.html`, 1992.

[3] I. Blake, G. Seroussi, and N. Smart. *Elliptic curves in cryptography*, volume 265 of *London Math. Soc. Lecture Note Ser.* Cambridge University Press, 1999.

[4] L. S. Charlap, R. Coley, and D. P. Robbins. Enumeration of rational points on elliptic curves over finite fields. Draft; a copy is available at `http://www.lix.polytechnique.fr/Labo/Francois.Morain/Introuvables/Drafts/ccr.pdf`, 1991.

[5] H. Cohen and F. Strömberg. *Modular forms – a classical approach*, volume 179 of *Graduate Studies in Mathematics*. American Mathematical Society, 2017.

[6] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer–Verlag, 2nd edition, 1980.

[7] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In D. A. Buell and J. T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 21–76. American Mathematical Society, International Press, 1998.

[8] R. Fricke. *Die elliptischen Funktionen und ihre Anwendungen – Zweiter Teil : Die Algebraischen Ausführungen*. Teubner, Leipzig, 1922.

[9] F. Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *J. Théor. Nombres Bordeaux*, 7:255–282, 1995.

[10] F. Morain. Modular equations for some η-products. *Acta Arith.*, 161(4):301–326, 2013.

[11] F. Morain. Using the Charlap-Coley-Robbins polynomials for computing isogenies between elliptic curves. In preparation, February 2023.

[12] F. Morain. Using Fricke modular polynomials to compute isogenies. `http://www.lix.polytechnique.fr/Labo/Francois.Morain`, January 2024. Preprint.

[13] F. Morain. Computing the Charlap-Coley-Robbins modular polynomials, 2023.

[14] M. Noro, M. Yasuda, and K. Yokoyama. Symbolic computation of isogenies of elliptic curves by Vélu's formula. *Comment. Math. Univ. St. Pauli*, 68:93–130, 2020.

[15] R. Schertz. Weber's class invariants revisited. *J. Théor. Nombres Bordeaux*, 14:325–343, 2002.

[16] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7:219–254, 1995.

[17] J.-P. Serre. *A course in arithmetic*, volume No. 7 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French.

[18] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2020. `https://www.sagemath.org`.

Appendix A. Some values of Fricke polynomials

We compute

$$\mathrm{Fr}_{2,8,8}(X) = X^3 - \Delta E_4 X + 16\Delta^2,$$
$$\mathrm{Fr}_{3,6,6}(X) = X^4 + 18\Delta X^2 - E_6\Delta X - 27\Delta^2.$$

The following examples show that the height depends on s:

$$\mathrm{Fr}_{5,14,2}(X) = X^6 + 10\Delta^2 X^3 - \Delta^3 E_4 X + 5\Delta^4,$$
$$\mathrm{Fr}_{5,4,4}(X) = X^6 - 90\Delta X^3 + 20\Delta E_4 X^2 - \Delta E_4^2 X + 25\Delta^2,$$
$$\mathrm{Fr}_{5,18,6}(X) = X^6 + 30\Delta X^5 + 315\Delta^2 X^4 + 1300\Delta^3 X^3 + 1575\Delta^4 X^2 + \Delta^4(-E_4^3 + 750\Delta)X + 125\Delta^6,$$

$$\mathrm{Fr}_{7,10,2}(X) = X^8 + 14\Delta X^6 + 63\Delta^2 X^4 + 70\Delta^3 X^2 + \Delta^3 E_6 X - 7\Delta^4,$$

$$\mathrm{Fr}_{7,6,6}(X) = X^8 + 308\Delta X^6 + 42\Delta E_6 X^5 + 76734\Delta^2 X^4 - 8988\Delta^2 E_6 X^3$$
$$+7\Delta^2(27E_4^3 + 15868\Delta)X^2 + \Delta^2(-E_4^3 + 258\Delta)E_6 X - 343\Delta^4.$$

For $\ell = 11$, we find

$$\mathrm{Fr}_{11,2,2}(X) = X^{12} - 990\,\Delta\,X^6 + 440\,E_4\,\Delta\,X^4 - 165\,E_6\,\Delta\,X^3 + 22\,E_4^2\,\Delta X^2 - E_6\,E_4\,\Delta\,X - 11\,\Delta^2,$$

which is sparser than $U_{11}(X) = X^{12} - 1650E_4X^{10} - 55000E_6X^9 - 928125E_4^2X^8 + \cdots$. Lastly

$$\mathrm{Fr}_{13,22,2}(X) = X^{14} + 26\Delta X^{13} + 325\Delta^2 X^{12} + 2548\Delta^3 X^{11} + 13832\Delta^4 X^{10} + 54340\Delta^5 X^9$$
$$+157118\Delta^6 X^8 + 333580\Delta^7 X^7 + 509366\Delta^8 X^6 + 534820\Delta^9 X^5 + 354536\Delta^{10} X^4$$
$$+124852\Delta^{11} X^3 + 15145\Delta^{12} X^2 - \Delta^{12}(E_4^3 - 746\Delta)X + 13\Delta^{14}.$$

We remark that sometimes the equations present interesting simpler forms using powers of the invariant and J, as is also known for traditional modular equations (see [7], [10] among others). For instance, when replacing A and B by expressions in J and G_3 such that $J = G_3^2 + 1728$, we find factors of $\mathrm{Fr}_{5,4,4}(X^2)$:

$$X^6 G_3^6 \pm 10G_3^3(G_3^2 + 1728)X^3 \mp G_3(G_3^2 + 1728)^2 X + 5G_3^4 + 17280G_3^2 + 14929920.$$

The same phenomenon occurs for $\ell = 7$, X replaced by X^3 and $J = G_2^3$, etc.

Appendix B. A script to check the computations

This `SageMath` [18] script can also be downloaded from the author's web page.

```
# returns (2) * dX^-1 * X^-1 * s^-1 * ell * (3*E4^2*d6 + 2*E6*d4)
def double_eta_check_sigma():
#     R.<ell,r,s,E2,E4,E6,sigma,d4,d6,X,dX>=PolynomialRing(Rationals(),11)
    # w = (r+s)/2 is the weight
    E4p=(E2*E4 - E6)/3
    E6p=(E2*E6-E4^2)/2
    E2p=(E2^2-E4)/12
    E2t=(E2+2*sigma/ell)/ell
    Xp=(X/24)*(r*E2+s*ell*E2t)
    tmp=Xp*dX+E4p*d4+E6p*d6
    tmp=tmp.numerator()
    # check that coeff of E2 is zero
    c1=tmp.coefficient({E2:1})
    # is a multiple of (w*X*dX + 4*E4*d4 + 6*E6*d6), hence 0
    print("c1=", c1.factor())
    # find sigma as a root of constant coefficient
    sig=tmp.coefficient({E2:0})
    sig=-sig.coefficient({sigma:0})/sig.coefficient({sigma:1})
    # sig contains the value of sigma
    return sig.factor()

# returns
# (-1) * dX^-3 * X^-2 * s^-2 * ell^-2 * E6^-1 * E4^-1 * (r+s)^(-1) *
#         * (-6*ell*r^2*s*E4^5*d6*X*dX^2+...)
def double_eta_check_E4t():
    w = (r+s)/2
```

```
    sig=double_eta_check_sigma()
    E4p=(E2*E4 - E6)/3
    E6p=(E2*E6-E4^2)/2
    E2p=(E2^2-E4)/12
    E2t=(E2+2*sig/ell)/ell
    Xp=(X/24)*(r*E2+s*ell*E2t)
    Xpp=(X/24^2)*((s*ell*E2t+r*E2)^2+2*(s*ell^2*(E2t^2-E4t)+r*(E2^2-E4)))
    E4pp=1/3*(E2p*E4+E2*E4p-E6p)
    E6pp=1/2*(E2p*E6+E2*E6p-2*E4*E4p)
    # inject diagonal derivatives
    dXX = (          w*ell*dX-4*E4*dX4 -6*E6*dX6)/X/w
    d44 = ((w*(ell+1)-4)*d4-w*X*dX4-6*E6*d46)/(4*E4)
    d66 = ((w*(ell+1)-6)*d6-w*X*dX6-4*E4*d46)/(6*E6)
    tmp=        Xpp*dX+ Xp*(Xp*dXX+E4p*dX4+E6p*dX6)
    tmp=tmp + E4pp*d4+E4p*(Xp*dX4+E4p*d44+E6p*d46)
    tmp=tmp + E6pp*d6+E6p*(Xp*dX6+E4p*d46+E6p*d66)
    tmp=tmp.numerator()
    print("degree(tmp, E2)=", tmp.degree(E2))
    c2=tmp.coefficient({E2:2})
    print("E4t.c2=", c2.factor())
    c1=tmp.coefficient({E2:1})
    print("E4t.c1=", c1)
    c0=tmp.coefficient({E2:0})
    e4t=-c0.coefficient({E4t:0})/c0.coefficient({E4t:1})
    return e4t.factor()
```

LIX - Laboratoire d'informatique de l'École polytechnique *and* GRACE - Inria Saclay–Île-de-France
Email address: morain@lix.polytechnique.fr