Computing the Charlap-Coley-Robbins modular polynomials

F. Morain

Laboratoire d'Informatique de l'École polytechnique

Nancy, 2023/01/13

Contents

I. Introduction

Motivations for computing isogenies in ANT/crypto:

- original one (1989ff): Schoof-Elkies-Atkin (SEA);
- later (circa 2000): Kohel, Galbraith, Fouquet/FM (volcanoes);
- more recently (2006ff): Galbraith/Hess/Smart; Smart; Jao/Miller/Venkatesan; Teske; Couveignes, Rostovtsev/Stolbunov.
- post-quantum cryptography (2011ff): Defeo/Jao, etc.

Bibliography:

- Silverman; Lang's *Elliptic functions*.
- green book (Blake/Seroussi/Smart). Don't forget to read the original papers, when available...
- Gathen & Gerhard, etc.

Elliptic curves and isogenies

$$E : y^2 = x^3 + Ax + B \text{ over } \mathbf{K}, \mathrm{char}(\mathbf{K}) \notin \{2, 3\}.$$

Def. (torsion points) For $n \in \mathbb{N}$, $E[n] = \{P \in E(\overline{\mathbb{K}}), [n]P = O_E\}$.

Division polynomials:

$$[n](x,y) = \left(\frac{\varphi_n(x,y)}{\psi_n(x,y)^2}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3}\right)$$

$$\varphi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$$

$$4y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2$$

In $\mathbf{K}[x,y]/(y^2 - (x^3 + Ax + B))$, one has:

$$\psi_{2m+1}(x,y) = f_{2m+1}(x), \quad \psi_{2m} = 2yf_{2m}(x)$$

for some $f_m(x) \in \mathbf{K}[A,B,x]$.

Isogenies

Def. $\phi : E \rightarrow E^*$, $\phi(O_E) = O_{E^*}$; induces a morphism of groups.

First examples

1. Separable:

$$[k](x,y) = \left(\frac{\varphi_k}{\psi_k^2}, \frac{\omega_k}{\psi_k^3}\right)$$

2. Complex multiplication: $[i](x,y) = (-x, iy)$ on $E : y^2 = x^3 - x$.
3. Inseparable: $\varphi(x,y) = (x^p, y^p)$, $\mathbf{K} = \mathbb{F}_p$.

In the sequel:

- only separable isogenies;
- finite fields of large characteristic (see comments at the end).

Finding isogenies

Thm. If F is a finite subgroup of $E(\overline{\mathbf{K}})$, there exists ϕ and E^* s.t.

$$\phi : E \rightarrow E^* = E/F, \quad \ker(\phi) = F.$$

Facts:

- An equation of E^* can be computed using Vélu's formulas;
- the kernel polynomial (== denominator of ϕ) is $\mathscr{K}_F = X^d - \sigma_1 X^{d-1} + \cdots$ is a factor of $f_\ell(X)$ (in case ℓ odd and $d = (\ell-1)/2$).

Thm. All isogenous curves of degree ℓ to a given E are characterized by $\Phi_\ell(j(E^*), j(E)) = 0$, where Φ_ℓ is the traditional modular equation.

But: having $j(E^*)$ is not enough to find an equation for E^* (quadratic twists), nor the explicit isogeny.

Basic algorithm

Function *FindAllIsogenies(E, ℓ):*

Input : $E/\mathbb{F}_q = [A, B]$ an elliptic curve, ℓ an odd prime

Output: $\{(\sigma, A^*, B^*)\}$ parameters of curves E^* that are ℓ-isogenous to E if any

1. $\mathscr{L} \leftarrow$ roots of $\Phi_\ell(X, j(E)) = 0$ over $\mathbf{K}$
2. $\mathscr{R} \leftarrow \emptyset$
3. **for** $j^* \in \mathscr{L}$ **do**
   - $\mathscr{R} \leftarrow \mathscr{R} \cup \{(\sigma, A^*, B^*)\}$, the parameters of E^*
4. **return** $\mathscr{R}$.

Rem. $\#\mathscr{L} \in \{0, 2, 1, \ell+1\}$; more is known on the splitting of $\Phi_\ell(X, j(E))$ over $\mathbf{K}$.

Isogeny algorithms

Key ingredients:

- modular equations:
  - choose nice equations;
  - compute equations over $\mathbb{Z}[X]$ + instantiation over $\mathbf{K}$:
    • series over $\mathbb{Z}$ (or $\mathbb{Z}/p\mathbb{Z}$): (. . . , CCR, Atkin, . . .);
    • evaluation/interpolation: with floating points (Dupont/Enge); with curves modulo p (Charles + Lauter).
  - Compute $\Phi_\ell(X, j(E))$ directly using isogeny volcanoes (Sutherland *et al.*).

- compute ℓ-isogenies:
  - compute isgenous curve: magical (ugly) formulas by Atkin; alternatively: CCR.
  - compute isogeny: depends on q and p, BMSS, Lercier/Sirvent, etc.

II. Classical theory and computations

Eisenstein series: $\delta_r(n) = \sum_{d|n} d^r$

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

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

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

Fact: E_4 and E_6 are modular forms of weight 4 and 6 respectively, E_2 is almost modular.

$$\Delta(q) = \frac{E_4^3 - E_6^2}{1718} = q \prod_{n \geq 1} (1 - q^n)^{24} = \eta(q)^{24}$$

$$j(q) = \frac{E_4^3}{\Delta} = \frac{1}{q} + 744 + \sum_{n \geq 1} c_n \, q^n, c_n \in \mathbb{N}.$$

Identities involving Eisenstein's series

When $F(q) = \sum_{n \geq n_0} a_n q^n$, we introduce the operator

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

$$\Delta = \frac{E_4^3 - E_6^2}{1728}, \quad \frac{\Delta'}{\Delta} = E_2, \quad j = \frac{E_4^3}{\Delta}, \quad j - 1728 = \frac{E_6^2}{\Delta}, \tag{1}$$

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

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

(The last line is due to Ramanujan.)

A) Lattices

Def. $\mathscr{L} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and $\mathscr{L}' = \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2'$ are isomorphic iff there exists P in $SL_2(\mathbb{Z})$ s.t.

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = P \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Thm. $\mathscr{L}$ and $\mathscr{L}'$ are isomorphic iff $j(\mathscr{L}) = j(\mathscr{L}')$.

Def. $\mathscr{L}$ and $\mathscr{M}$ are isogenous iff $\exists \alpha \in \mathbb{C}, \alpha\mathscr{L} \subset \mathscr{M}$.

Most interesting case: $\mathscr{M}$ is a sublattice of $\mathscr{L}$ s.t. $\mathscr{L}/\mathscr{M}$ is cyclic of finite index. In other words:

$$\mathscr{M} = (a\omega_1 + b\omega_2)\mathbb{Z} + (c\omega_1 + d\omega_2)\mathbb{Z}$$

and $ad - bc = m$ with $\gcd(a,b,c,d) = 1$.

Fundamental theorem (modular polynomial):

Thm. $\exists \alpha \in \mathbb{C}$ s.t. $\alpha \mathscr{M} \subset \mathscr{L}$ iff $\exists m$ s.t. $\Phi_m(j(\mathscr{M}), j(\mathscr{L})) = 0$ s.t. with $\tau = \omega_2/\omega_1$ (imag. part > 0), $q = \exp(2i\pi\tau)$:

$$\Phi_m(X, \tau) = \prod_{A \in \mathscr{S}_m} (X - j(A\tau)) = \sum_{k=0}^{\mu_0(m)} C_k(\tau) X^k,$$

$$\mathscr{S}_m = \left\{ \left(\begin{array}{cc} a & b \\ 0 & d \end{array} \right), ad = m, \gcd(a, b, d) = 1, a > 0, d > b \geq 0 \right\}$$

of cardinality $\mu_0(m) = m \prod_{p|m} (1 + 1/p)$.

When $m = \ell$ is prime:

$$\mathscr{S}_\ell = \left\{ \left(\begin{array}{cc} 1 & b \\ 0 & \ell \end{array} \right), 0 \leq b < \ell \right\} \cup \left\{ \left(\begin{array}{cc} \ell & 0 \\ 0 & 1 \end{array} \right) \right\}$$

of cardinality $\ell + 1$.

Modular polynomials

Thm.

- $\Phi_m(X,Y) \in \mathbb{Z}[X,Y]$;
- $\Phi_m(Y,X) = \Phi_m(X,Y)$;
- if m is squarefree, then the coefficient of highest degree of $\Phi_m(X,X)$ is ± 1.

Prop. ("Cyclotomic" properties)
(a) If $(m_1, m_2) = 1$, then

$$\Phi_{m_1 m_2}(X,J) = \text{Resultant}_Z(\Phi_{m_1}(X,Z), \Phi_{m_2}(Z,J)).$$

(b) If $m = \ell^e$ with $e > 1$, then

$$\Phi_{\ell^e}(X,J) = \text{Resultant}_Z(\Phi_\ell(X,Z), \Phi_{\ell^{e-1}}(Z,J))/\Phi_{\ell^{e-2}}(Z,J)^\ell.$$

Thm. (Kronecker) If ℓ is prime, then

$$\Phi_\ell(X,Y) \equiv (X^\ell - Y)(Y^\ell - X) \bmod \ell.$$

Height

Thm. (P. Cohen)
$H(\Phi_m) = 6\mu_0(m)(\log m - 2\sum_{p|m}(\log p)/p + O(1))$.

ℓ	101	211	503	1009	2003
$H(\Phi_\ell)$	3985	9256	24736	53820	115125
PCohen	2768	6743	18736	41832	91320

Thm. (Bröker & Sutherland)

$$H(\Phi_\ell) \leq 6\ell\log\ell + 16\ell + 14\sqrt{\ell}\log\ell.$$

$\Rightarrow$ Φ_ℓ has $O(\ell^2)$ coefficients of size $\ell\log\ell$, or a $\tilde{O}(\ell^3)$-bit object.

Ex.

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

B) Computing modular polynomials over $\mathbb{Z}[X]$

Remember that

$$j(q) = \frac{1}{q} + 744 + \sum_{n \geq 1} c_n q^n, \quad c_n \in \mathbb{Z}^+$$

Then $\Phi_\ell(X,Y)$ is such that $\Phi_\ell(j(q), j(q^\ell))$ vanishes identically.

Naive method: indeterminate coefficients (over $\mathbb{Q}$ or small p's); at least $\tilde{O}((\ell^2)^\omega)$ operations over $\mathbb{Q}$.

Ex.

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

a) Series computations

Enneper (1890) use q-expansion of j and $j(q^\ell)$ with $O(\ell^2)$ terms; Atkin used this modulo CRT primes (embarassingly parallel). $\tilde{O}(\ell^3 \mathsf{M}(p))$

1. a) Compute power sums for $1 \leq r \leq \ell$:

$$S_r(q) = j(\ell\tau)^r + \sum_{k=0}^{\ell-1} j\left(\frac{\tau+k}{\ell}\right)^r = S_{r,0}(q) + S_{r,1}(w)$$

with $w = q^{1/\ell}$; $S_{r,1}$ *a priori* in $\mathbb{Q}(\zeta_\ell)$, but in fact over $\mathbb{Q}$, hence $S_{r,1}(w) = S_{r,1}(q)$;

b) recognize $S_r(q) = S_r(J)$.

2. Go back to $\Phi(X,J)$ using Newton formulas.

b) Evaluation/interpolation (Enge; Dupont)

$$\Phi_\ell(X,J) = X^{\ell+1} + \sum_{u=0}^{\ell} C_u(J)X^u, \quad C_u(J) \in \mathbb{Z}[J], \deg(C_u(J)) \leq \ell+1.$$

All computations are done using precision $H = O(\ell \log \ell)$.

Function ComputePhi*(ℓ, f, (f_r), $\deg_X$):*

Input : ℓ an odd prime; f a function, f_r conjugates

Output: $\Phi_\ell[f](X,J)$ with degree $\deg_X$ in X

for $\deg_X + 1$ *values of* z_i **do**

  compute $f_r(z_i)$ to precision H and build $\prod_{r=1}^{\ell+1}(X - f_r(z_i)) = X^{\ell+1} + \sum_{u=0}^{\ell} C_u(j(z_i))X^u$; $O(\mathsf{M}(\ell)\log \ell)$ ops

for $u \leftarrow 0$ **to** ℓ **do**

  interpolate C_u from $(j(z_i), C_u(j(z_i)))$ for $1 \leq i \leq \deg_X + 1$

return $\Phi_\ell[f](X,J)$

All 1.2 + 2 has cost $O(\ell \mathsf{M}(\ell)(\log \ell)\mathsf{M}(H)) = \tilde{O}(\ell^3)$.

C) Isogeny volcanoes

Bröker, Lauter, Sutherland (2010): Under the Generalized Riemann Hypothesis (GRH), expected running time of $O(\ell^3(\log \ell)^3 \log\log \ell)$, and compute $\Phi_\ell \bmod p$ using $O(\ell^2(\log \ell)^2 + \ell^2 \log p)$ space.

- Need class polynomials $H_D(X)$ (sometimes $H_{\ell^2 D}(X)$).
- Interpolate the values of all quantities modulo p.
- Extensible to partial differentials.

- Works also in Sutherland's algo for direct evaluation over $\mathbf{K}$ using explicit CRT.

III. Elkies's approach to the isogeny problem

Using power series for the Tate curve

$$Y^2 = X^3 - \frac{E_4(q)}{48}X + \frac{E_6(q)}{864}$$

is ℓ-isogenous to

$$Y^2 = X^3 - \frac{E_4(q^\ell)}{48}X + \frac{E_6(q^\ell)}{864}$$

$\sigma_r =$ power sums of the roots of the kernel polynomial:

$$\sigma_1(q) = \frac{\ell}{2}(\ell E_2(q^\ell) - E_2(q)).$$

Use series identities to get formulas for $E_4(q^\ell)$ and $E_6(q^\ell)$, $\sigma_1(q)$ from known values.
Also:

$$A - A^* = 5(6\sigma_2 + 2A\sigma_0), \qquad B - B^* = 7(10\sigma_3 + 6A\sigma_1 + 4B\sigma_0),$$

$+$ induction relation for σ_k with $k > 3$.

Consequence: A^* and B^* belong to $\mathbb{Q}[\sigma_1, A, B]$.

The case of $\Phi_\ell(X, Y)$

Thm. (Schoof95)
With $\tilde{j} = j(q^\ell)$:

1) $\Phi_\ell(j, \tilde{j}) = 0$.

2) $j' \partial_X + \ell \tilde{j}' \partial_Y = 0$.

3)
$$\frac{j''}{j'} - \ell \frac{\tilde{j}''}{\tilde{j}'} = -\frac{j'^2 \partial_{XX} + \cdots}{j' \partial_X}.$$

All this yields $E_4(q^\ell)$, $E_6(q^\ell)$, σ_1.

Cost: $O(\ell^2)$ operations in $\mathbf{K}$.

Finding smaller equations and their formulas

- Traditional approach: $\Phi_\ell(X,Y)$. Formulas given by Schoof.
- Elkies 1992: *ad hoc* modular equations + formulas for each ℓ; cumbersome.
- Atkin: canonical with η-products, laundry method (conjecturally smallest); magical formulas using differentials of order 1 and 2.
- Müller (Enge): Hecke operators + somewhat *ad hoc* tables. Same Atkin formulas.
- Smallest models for $X_0(\ell)$ in two variables, not related to j; formulas?

Alternative: Charlap-Coley-Robbins (1991).

IV. Charlap-Coley-Robbins

A) Theory

$$
\begin{array}{c}
\mathbb{Q}(A,B)[X]/(f_\ell(X,A,B)) \\
\Big| \; (\ell-1)/2 \\
\mathbb{Q}(A,B)[X]/(U_\ell(X,A,B)) \\
\Big| \; \ell+1 \\
\mathbb{Q}(A,B)
\end{array}
$$

Using traces

Classical: use the trace T_1 of an element in $\mathbb{Q}(A,B)[X]/(f_\ell(X,A,B))$.
Let $P=(x_1,y_1)\neq O_E$. Other points are $P_j=[j]P=(x_j,y_j)$ can be expressed using division polynomials.
For $0\leq k\leq \ell+1$

$$T_k=\sum_{j=1}^{d} x_j^k=\sum_{j=1}^{d}\left(x_1-\frac{\psi_{j-1}(x_1)\psi_{j+1}(x_1)}{\psi_j(x_1)^2}\right)^k$$

so that $T_1=x_1+\cdots+x_d$ and $T_0=d=(\ell-1)/2$. The minimal polynomial $U_\ell(X)=X^{\ell+1}+u_1X^\ell+\cdots+u_0$ of T_1 defines the lower extension.

Use Newton's identities to reconstruct the factor $\prod_{i=1}^{d}(X-x_i)=X^d-T_1X^{d-1}+\cdots$ over the intermediate extension.

Using traces

Classical: use the trace T_1 of an element in $\mathbb{Q}(A,B)[X]/(f_\ell(X,A,B))$.
Let $P=(x_1,y_1)\neq O_E$. Other points are $P_j=[j]P=(x_j,y_j)$ can be expressed using division polynomials.
For $0\leq k\leq \ell+1$

$$T_k=\sum_{j=1}^{d} x_j^k=\sum_{j=1}^{d}\left(x_1-\frac{\psi_{j-1}(x_1)\psi_{j+1}(x_1)}{\psi_j(x_1)^2}\right)^k$$

so that $T_1=x_1+\cdots+x_d$ and $T_0=d=(\ell-1)/2$. The minimal polynomial $U_\ell(X)=X^{\ell+1}+u_1X^\ell+\cdots+u_0$ of T_1 defines the lower extension. $T_1=\sigma$!

Use Newton's identities to reconstruct the factor $\prod_{i=1}^{d}(X-x_i)=X^d-T_1X^{d-1}+\cdots$ over the intermediate extension. $\leftarrow$ kernel polynomial!

CCR polynomials

Thm. There exists three polynomials $U_\ell(X,Y,Z)$, $V_\ell(X,Y,Z)$, $W_\ell(X,Y,Z)$ in $\mathbb{Z}[X,Y,Z,1/\ell]$ of degree $\ell+1$ in X such that $U_\ell(\sigma,A,B)=0$, $V_\ell(A^*,A,B)=0$, $W_\ell(B^*,A,B)=0$.

Thm. When $\ell>3$, U_ℓ, V_ℓ, W_ℓ live in $\mathbb{Z}[X,Y,Z]$.

Prop. Assigning respective weights 1, 2, 3 to X, Y, Z, the monomials in U_ℓ, V_ℓ and W_ℓ have generalized degree $\ell+1$.

Computations of U_ℓ: use power sums of roots; numerical computation possible via E_2 (which can be expressed using a hypergeometric function and theta functions – see A. Bostan).

Ex. $U_5(X,Y,Z)=X^6+20YX^4+160ZX^3-80Y^2X^2-128YZX-80Z^2$.

Prop. Maximal size of integer during computation of U_ℓ (resp. V_ℓ, W_ℓ) is $\approx 2\ell$ (resp. 4ℓ, 6ℓ).

Function *UseCCR(E, ℓ):*

Input : $E/\mathbb{F}_q = [A, B]$ an elliptic curve, ℓ an odd prime

Output: (σ, A^*, B^*) parameters of a curve E^* that is ℓ-isogenous to E

1. $\mathscr{L}_U \leftarrow$ roots of $U_\ell(X, A, B)$ over $\mathbb{F}_q$
2. **if** $\mathscr{L}_U \neq \emptyset$ **then**
   - 2.0. Let σ be an element of $\mathscr{L}_U$
   - 2.1. $\mathscr{L}_V \leftarrow$ roots of $V_\ell(X, A, B)$ over $\mathbb{F}_q$
   - 2.2. $\mathscr{L}_W \leftarrow$ roots of $W_\ell(X, A, B)$ over $\mathbb{F}_q$
   - **for** $v \in \mathscr{L}_V$ **do**
     - **for** $w \in \mathscr{L}_W$ **do**
       - **if** (σ, v, w) *is an ℓ-isogeny* **then**
         - **return** (σ, v, w).

Cost: 3 polynomial exponentiations + ≤ 4 isogeny tests.

Purely algebraic approaches

Triangular sets: Schost *et al.*; change of order algorithm.

Noro/Yasuda/Yokoyama (2020):
In particular (representation à la Hecke):

$$A^* = \frac{N_{\ell,A}(X,A,B)}{U_\ell'(X)}, \quad B^* = \frac{N_{\ell,B}(X,A,B)}{U_\ell'(X)}$$

(Only here: $U_\ell'(X) = \frac{\partial U_\ell}{\partial X}$.)
$N_{\ell,A}$ (resp. $N_{\ell,B}$) are polynomials with integer coefficients and of generalized weight $2\ell+4$ (resp. $2\ell+6$). Computations by any evaluation/interpolation method.

Ex. (with a sign flip)

$$N_{5,A} = 630AX^5 - 9360BX^4 - 8240A^2X^3 + 24480BAX^2$$

$$+(1120A^3 - 28800B^2)X - 3200BA^2.$$

B) Atkin's more powerful variant

We also discuss here the alternative modular equation suggested by (CCR). They use an equation of degree (q+1) in E2*,whose coefficients are forms of appropriate weights expressible in terms of E4 and E6 (or,by applying Wq, in terms of E4q and E6q). In the equivalent of cases 1 and 3 above,they find a value of E2* in GF(p).
The procedure with which they then continue is however intolerably long,and a better continuation is as follows.

Differentiate their equation twice at the cusp infinity(i.e.with E2*,E4,E6);the first time we get E4q,and the second E6q.

Homogeneous properties of U

Notation:

$$\partial_\sigma = \frac{\partial U}{\partial \sigma}, \partial_4 = \frac{\partial U}{\partial E_4}, \partial_6 = \frac{\partial U}{\partial E_6}, \text{etc.}.$$

U is homogeneous with weights, so that (generalized Euler theorem)

$$(\ell+1)U = \sigma\partial_\sigma + 2E_4\partial_4 + 3E_6\partial_6. \tag{4}$$

Note that partial derivatives are also homogeneous:

$$\begin{aligned} \ell\partial_\sigma &= \sigma\partial_{\sigma\sigma} + 2E_4\partial_{\sigma 4} + 3E_6\partial_{\sigma 6}, & (5)\\ (\ell-1)\partial_4 &= \sigma\partial_{\sigma 4} + 2E_4\partial_{44} + 3E_6\partial_{46}, & (6)\\ (\ell-2)\partial_6 &= \sigma\partial_{\sigma 6} + 2E_4\partial_{46} + 3E_6\partial_{66}. & (7)\end{aligned}$$

Getting the isogenous curve (1/4)

Differentiate $U(\sigma, E_4, E_6) = 0$ to get

$$\sigma' \partial_\sigma + E_4' \partial_4 + E_6' \partial_6 = 0, \tag{8}$$

$\sigma = \frac{\ell}{2}\left(\ell \tilde{E}_2 - E_2\right)$ leading to

$$\sigma' = \frac{\ell}{2}\left(\ell^2 \tilde{E}_2' - E_2'\right) = \frac{\ell}{24}\left(\ell^2(\tilde{E}_2^2 - \tilde{E}_4) - (E_2^2 - E_4)\right).$$

Replace $\ell \tilde{E}_2$ by $2\sigma/\ell + E_2$ to get

$$\sigma' = \frac{\ell}{24}\left(\frac{4\sigma^2}{\ell^2} + \frac{4\sigma}{\ell} E_2 - (\ell^2 \tilde{E}_4 - E_4)\right),$$

that we plug in (8) together with the expressions for ${E_4}'$ and ${E_6}'$ from equation (3) to get a polynomial of degree 1 in E_2 whose coefficient of E_2 is

$$\sigma \partial_\sigma + 2E_4 \partial_4 + 3E_6 \partial_6,$$

which we recognize in (4).

Getting the isogenous curve (2/4)

$$(\ell+1)UE_2+\frac{\ell}{4}\left(4\sigma^2/\ell^2-(\ell^2\tilde{E}_4-E_4)\right)\partial_\sigma-2E_6\partial_6-3E_4^2\partial_4=0 \quad (9)$$

from which we deduce $\tilde{E}_4$ since $U(\sigma,E_4,E_6)=0$.

Finding $\tilde{E}_6$: we differentiate (8)

$$\begin{aligned} & \sigma''\partial_\sigma+\sigma'(\sigma'\partial_{\sigma\sigma}+E_4'\partial_{\sigma 4}+E_6'\partial_{\sigma 6}) \\ + \quad & E_4''\partial_4+E_4'(\sigma'\partial_{4\sigma}+E_4'\partial_{44}+E_6'\partial_{46}) \\ + \quad & E_6''\partial_6+E_6'(\sigma'\partial_{6\sigma}+E_4'\partial_{64}+E_6'\partial_{66})=0 \end{aligned}$$

We compute in sequence

$$12E_2''=2E_2E_2'-E_4'=E_2\,(E_2^2-E_4)/6-(E_2E_4-E_6)/3,$$

$$12\tilde{E}_2''=2\tilde{E}_2\tilde{E}_2'-\tilde{E}_4'=\tilde{E}_2\,(\tilde{E}_2^2-\tilde{E}_4)/6-\,(\tilde{E}_2\tilde{E}_4-\tilde{E}_6)/3,$$

$$\to \sigma''=\frac{\ell}{2}\,(\ell^3\tilde{E}_2''-E_2'')$$

Getting the isogenous curve (3/4)

Differentiate Ramanujan's relations:

$$E_4'' = \frac{1}{3}(E_2'E_4 + E_2E_4' - E_6'), \quad E_6'' = \frac{1}{2}(E_2'E_6 + E_2E_6' - 2E_4E_4'),$$

Finally yields an expression as polynomial in E_2:

$$C_2E_2^2 + C_1E_2 + C_0 = 0.$$

The unknown $\tilde{E}_6$ is to be found in C_0 only.

Prop. (By luck ?) The coefficients C_1 and C_2 vanish for a triplet such that $U_\ell(\sigma, E_4, E_6) = 0$.

Sketch of the proof: Replace $\partial_{\sigma\sigma}$, ∂_{44} and ∂_{66} by their values from (5). Factoring the resulting expressions yields the same factor $\sigma\partial_\sigma + 2E_4\partial_4 + 3E_6\partial_6$, which cancels C_1 and C_2.$\square$

Getting the isogenous curve (4/4)

We are left with

$$\tilde{E}_6 = -\frac{N}{\ell^6\,\partial_\sigma^3}$$

where N is a polynomial in degree 3 in ℓ

$$N = -E_6\partial_\sigma^3\ell^3 + c_2\ell^2 + 12\partial_\sigma^2\sigma(3E_4^2\partial_6 + 2E_6\partial_4)\ell - \partial_\sigma^3\sigma^3.$$

The coefficient c_2 has an ugly expression (that may be simplified??).

C) The case $\ell \equiv 11 \bmod 12$

```
The number and size of the terms in their modular
equation are also larger than those in mine,
especially when q=11(mod 12). In that case, the
cuspform eta**2(tau)*eta**2(q*tau) could be used
instead of E2* to form the modular equation. This
both saves on size and number of coefficients,and
has convenient derivatives; the reader can by now
easily work out the precise algorithm.
```

Properties

In this case, Atkin suggests to replace σ with $f(q) = \eta(q)^2\eta(q^\ell)^2$ another modular form of weight 2.

Ex.

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

which is sparser $U_{11}(X)$.

CCRA is homogeneous:

$$(\ell+1)CCRA_\ell = f\partial_f + 2E_4\partial_4 + 3E_6\partial_6. \qquad (10)$$

We have $f^{12} = \Delta(z)\Delta(\ell z)$ and therefore we deduce the discriminant $\tilde{\Delta} = f^{12}/\Delta$, yielding a relation for $\tilde{E}_4$ and $\tilde{E}_6$.

Computing σ

Write

$$\frac{f'}{f} = 2\frac{\eta'}{\eta} + 2\ell\frac{\tilde{\eta}'}{\tilde{\eta}} = \frac{1}{12}(\ell\tilde{E}_2 + E_2),$$

from which we deduce f'.

Starting from $f'\partial_f + E_4'\partial_4 + E_6'\partial_6 = 0$, and replacing by the known values, we find

$$(f\partial_f + 4E_4\partial_4 + 6E_6\partial_6)E_2 + f\ell\tilde{E}_2\partial_f - 6E_4^2\partial_6 - 4E_6\partial_4 = 0,$$

which is

$$f\ell\partial_f(\ell\tilde{E}_2 - E_2) - 6E_4^2\partial_6 - 4E_6\partial_4 = 0,$$

which gives us

$$\boxed{\sigma = \frac{\ell\left(3\,\partial_6 E_4^2 + 2\,\partial_4 E_6\right)}{f\partial_f}.}$$

Computing $\tilde{E}_4$

We differentiate f' to obtain:

$$f'' = \frac{1}{12}\left(f'(\ell\tilde{E}_2 + E_2) + f(\ell^2\tilde{E}_2' + E_2')\right)$$

$$= \frac{f}{12^2}\left((\ell\tilde{E}_2 + E_2)^2 + \ell^2(\tilde{E}_2^2 - \tilde{E}_4) + (E_2^2 - E_4)\right).$$

We inject this together with $\tilde{E}_2 = (E_2 + 2\sigma/\ell)/\ell$ into

$$\begin{aligned} & f''\partial_f + f'(f'\partial_{ff} + E_4'\partial_{f4} + E_6'\partial_{f6}) \\ + \quad & E_4''\partial_4 + E_4'(f'\partial_{4f} + E_4'\partial_{44} + E_6'\partial_{46}) \\ + \quad & E_6''\partial_6 + E_6'(f'\partial_{6f} + E_4'\partial_{64} + E_6'\partial_{66}) = 0 \end{aligned}$$

This yields a polynomial of degree 2 in E_2 whose coefficients of degree 2 and 1 turn out to vanish. We are left with

$$\tilde{E}_4 = -\frac{M}{\ell^2 f^2 E_4 E_6 \partial_f^3}$$

with a bulky expression for M.

Computing $\tilde{E}_6$

Prop. (applying Atkin-Lehner involution)

$$U_\ell(-\ell\sigma, A^*, B^*) = 0, \quad V_\ell(\ell^4 A, A^*, B^*) = 0, \quad W_\ell(\ell^6 B, A^*, B^*) = 0,$$

with $A^* = \ell^4 \tilde{E}_4$, $B^* = \ell^6 \tilde{E}_6$.

Also:

$$\tilde{\Delta} = \frac{\tilde{E}_4^3 - \tilde{E}_6^2}{1728}$$

So that $\tilde{E}_6$ is a root of the gcd of the two polynomials.
In practice, there is one root. Otherwise, use a heavy further differential!!!

V. Conclusions

When is this useful?

- you don't like using Atkin's laundry hammer;
- (technical, rare) when some $\partial_X = 0$, the triplet (U, V, W) is useful;
- for small ℓ, either use sparse formulas $(U_\ell, N_{\ell,A}, D_{\ell,A})$ or only U_ℓ and the ugly formulas.

Working ugly formulas can be done using multipliers for Borweins' like modular polynomials as explained by R. Dupont. But this is another story. . . !