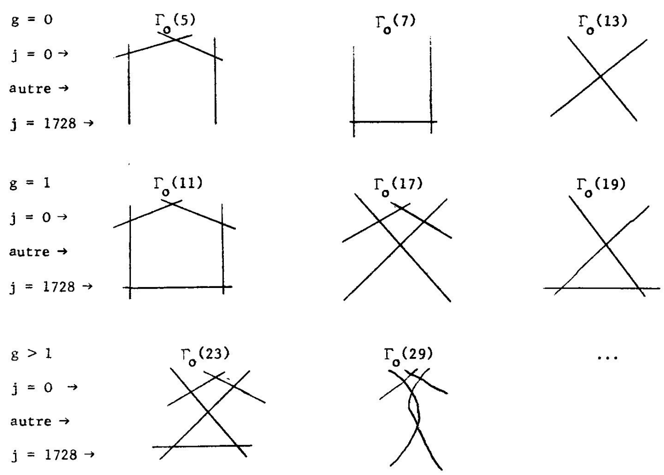
1 Canonical modular polynomials



[Deligne-Rapoport1973, Section VI.6]

Using Magma's calculator, we reproduce the first few canonical modular polynomials from its Modular Polynomial Databases.[1] We note the following, to return to.

(i) Difference from $j = 744$ equals $\#\mathrm{Aut}(E_{\mathrm{s.s.}}/\overline{\mathbb{F}}_p)$.

(ii) Constant term equals p^s where $s = 12/\gcd(p-1, 12) \stackrel{?}{=} \prod \left(\#\mathrm{Aut}(E_{\mathrm{s.s.}}/\overline{\mathbb{F}}_p)/2\right)$.

(iii) Linear coefficient reduces to supersingular j-invariants in the diagram above. (What is the pattern for their exponents?)

- $g = 0$

$$
\begin{aligned}
\Gamma_0(2) \qquad & x^3 + 48x^2 + (768 - j)x + 2^{12} \\
& \equiv x(x^2 - j) \mod 2 \\
\Gamma_0(3) \qquad & x^4 + 36x^3 + 270x^2 + (756 - j)x + 3^6 \\
& \equiv x(x^3 - j) \mod 3 \\
\Gamma_0(5) \qquad & x^6 + 30x^5 + 315x^4 + 1300x^3 + 1575x^2 + (750 - j)x + 5^3 \\
& \equiv x(x^5 - j) \mod 5 \\
\Gamma_0(7) \qquad & x^8 + 28x^7 + 322x^6 + 1904x^5 + 5915x^4 + 8624x^3 + 4018x^2 + (748 - j)x + 7^2 \\
& \equiv x\big(x^7 - (j - 1728)\big) \mod 7 \\
\Gamma_0(13) \qquad & x^{14} + 26x^{13} + 325x^{12} + 2548x^{11} + 13832x^{10} + 54340x^9 + 157118x^8 \\
& + 333580x^7 + 509366x^6 + 534820x^5 + 354536x^4 + 124852x^3 + 15145x^2 \\
& + (746 - j)x + 13^1 \\
& \equiv x\big(x^{13} - (j - 5)\big) \mod 13
\end{aligned}
$$

[1] available up to $\Gamma_0(127)$

- $g = 1$

$$
\begin{aligned}
\Gamma_0(11) \qquad & x^{12} - 5940x^{11} + 14701434x^{10} + (-139755j - 19264518900)x^9 \\
& + (723797800j + 13849401061815)x^8 + (67496j^2 - 1327909897380j \\
& - 4875351166521000)x^7 + (2291468355j^2 + 1036871615940600j \\
& + 400050977713074380)x^6 + (-5346j^3 + 4231762569540j^2 \\
& - 310557763459301490j + 122471154456433615800)x^5 + (161201040j^3 \\
& + 755793774757450j^2 + 17309546645642506200j \\
& + 6513391734069824031615)x^4 + (132j^4 - 49836805205j^3 \\
& + 6941543075967060j^2 - 64815179429761398660j \\
& + 104264884483130180036700)x^3 + (468754j^4 + 51801406800j^3 \\
& + 214437541826475j^2 + 77380735840203400j + 804140494949359194)x^2 \\
& + (-j^5 + 3732j^4 - 4586706j^3 + 2059075976j^2 - 253478654715j \\
& + 2067305393340)x + 11^6 \\
\equiv\ & x\big(x^{11} - j^2(j-1728)^3\big) \mod 11 \\
\Gamma_0(17) \qquad & x^{18} + 510x^{17} + 125001x^{16} + 19248080x^{15} + 2058738420x^{14} \\
& + (10846j + 160172066760)x^{13} + (6027384j + 9242645403716)x^{12} \\
& + \cdots \\
& + (-j^4 + 2982j^3 - 2547081j^2 + 567877726j - 8730057090)x + 17^3 \\
\equiv\ & x\big(x^{17} - j(j-8)^3\big) \mod 17 \\
\Gamma_0(19) \qquad & x^{20} - 152x^{19} + 11020x^{18} - 509732x^{17} + 16884502x^{16} - 423717176x^{15} \\
& + 8284685786x^{14} + (-950j - 127757600560)x^{13} \\
& + \cdots \\
& + (-j^3 + 2236j^2 - 1075910j + 37507528)x + 19^2 \\
\equiv\ & x\big(x^{19} - (j-7)(j-1728)^2\big) \mod 19
\end{aligned}
$$

- $g > 1$

$$
\begin{aligned}
\Gamma_0(23) \qquad & x^{24} + 94392x^{23} + 4240527204x^{22} + (108774498j + 119018915927208)x^{21} \\
& + \cdots \\
& + (-j^{11} + 8196j^{10} - 28368090j^9 + 53962467848j^8 - 61514962720527j^7 \\
& + 43007336651707740j^6 - 18144237478297458590j^5 \\
& + 4374793948754527714200j^4 - 541459535600500383823479j^3 \\
& + 28035152457942175237515676j^2 - 389561380516779182551042062j \\
& + 312190445452533657242901912)x + 23^6 \\
\equiv\ & x\big(x^{23} - j^2(j+4)^6(j-1728)^3\big) \mod 23
\end{aligned}
$$

$$\begin{aligned}
\Gamma_0(29) \qquad & x^{30} - 1218x^{29} + 750375x^{28} - 312177460x^{27} + 97844061669x^{26} \\
& + (-236321j - 24383203360230)x^{25} + (946283688j + 4982726503407419)x^{24} \\
& + \cdots \\
& + (-j^7 + 5214j^6 - 10272861j^5 + 9480438286j^4 - 4108842162480j^3 \\
& + 728011816505784j^2 - 35575638370254161j + 107281337499515022)x + 29^3 \\
\equiv\ & x\big(x^{29} - j(j-2)^3(j+4)^3\big) \mod 29
\end{aligned}$$

We compare these to modular equations for $\big(\Gamma_0(p), \Gamma_1(N)\big)$ computed previously.

- $g = 0$[2]

$$\begin{aligned}
\big(\Gamma_0(2), \Gamma_1(3)\big) \qquad & d^3 - ad - 2 \\
\equiv\ & d(d^2 + a) \mod 2 \\
\big(\Gamma_0(3), \Gamma_1(4)\big) \qquad & \alpha^4 - 6\alpha^2 + (a^2 - 8)\alpha - 3 \\
\equiv\ & \alpha\big(\alpha^3 + (a^2 + 1)\big) \mod 3
\end{aligned}$$

- $g = 1$

$$\begin{aligned}
\big(\Gamma_0(5), \Gamma_1(4)\big) \qquad & \alpha^6 - 10\alpha^5 + 35\alpha^4 - 60\alpha^3 + 55\alpha^2 - (a^4 - 16a^2 + 26)\alpha + 5 \\
\equiv\ & \alpha\big(\alpha^5 - (a^4 - a^2 + 1)\big) \mod 5
\end{aligned} \tag{1.1}$$

$$\begin{aligned}
\big(\Gamma_0(5), \Gamma_1(3)\big) \qquad & \alpha^6 - 5a\alpha^4 + 40\alpha^3 - 5a^2\alpha^2 + (a^4 - 19a)\alpha - 5 \\
\equiv\ & \alpha\big(\alpha^5 + a(a+1)(a^2 - a + 1)\big) \mod 5
\end{aligned}$$

three supersingular points (or two? $A^4 - 19AB$)

Note: higher coefficients (degree > 1) are constants if $(p-1)(N-1)|12$ with a single supersingular point.

For later reference, we rewrite these equations as follows.

$$\begin{aligned}
\big(\Gamma_0(2), \Gamma_1(3)\big) \qquad & d^3 - ad - 2 && \Delta_1(3) = (a-3)(a^2 + 3a + 9) \\
\equiv\ & (d-2)(d+1)^2 \mod (a-3) && \text{unramified cusp} \\
\big(\Gamma_0(3), \Gamma_1(4)\big) \qquad & \alpha^4 - 6\alpha^2 + (a^2 - 8)\alpha - 3 && \Delta_1(4) = a^2(a+4)(a-4) \\
\equiv\ & (\alpha - 3)(\alpha + 1)^3 \mod a && \text{ramified cusp} \\
\equiv\ & (\alpha + 3)(\alpha - 1)^3 \mod (a+4)(a-4) && \text{unramified cusp } (A^2 - 16B) \\
\big(\Gamma_0(5), \Gamma_1(4)\big) \qquad & \alpha^6 - 10\alpha^5 + 35\alpha^4 - 60\alpha^3 + 55\alpha^2 - (a^4 - 16a^2 + 26)\alpha + 5 \\
\equiv\ & (\alpha - 5)(\alpha - 1)^5 \mod a(a+4)(a-4) \\
\big(\Gamma_0(5), \Gamma_1(3)\big) \qquad & \alpha^6 - 5a\alpha^4 + 40\alpha^3 - 5a^2\alpha^2 + (a^4 - 19a)\alpha - 5 \\
\equiv\ & (\alpha + 5)(\alpha - 1)^5 \mod (a-3)
\end{aligned}$$

[2] [Katz-Mazur1985, Theorem 10.13.12], [Diamond-Shurman2005, Section 3.8]: $\frac{p+1}{12}N^2\prod_{\ell|N}\left(1 - \frac{1}{\ell^2}\right) = 2g - 2 + 2c\big(\Gamma_1(N)\big)$

2 Examples

Here are two examples about how to derive a canonical modular polynomial $\mathrm{cmp}(x, j)$ (cf. [Choi2006, Example 2.4]).

Example 2.1 $p = 5$ (cf. [Ahlgren2003, p788])

$$s := \frac{12}{\gcd(p-1, 12)} = 3 \qquad xx' = p^s = 5^3$$

$$u := \frac{p-1}{\gcd(p-1, 12)} = 1$$

$$\begin{aligned}
x' = \phi_p(z) &:= \left(\frac{\eta(z)}{\eta(pz)}\right)^{2s} \\
&= \left(\frac{q^{1/24}\prod_{n=1}^{\infty}(1-q^n)}{q^{5/24}\prod_{n=1}^{\infty}(1-q^{5n})}\right)^6 \\
&= q^{-1}\left(\frac{1-q-q^2+q^5+q^7-q^{12}-q^{15}+\cdots}{1-q^5-q^{10}+q^{25}+q^{35}-q^{60}-q^{75}+\cdots}\right)^6 \qquad c_i = \begin{cases}(-1)^k & \text{if } i = k(3k\pm 1)/2 \\ 0 & \text{otherwise}\end{cases} \\
&= \frac{1}{q} - 6 + 9q + 10q^2 - 30q^3 + 6q^4 - 25q^5 + 96q^6 + 60q^7 - 250q^8 + 45q^9 - 150q^{10} + \cdots \\
&= q^{-u} + \cdots
\end{aligned}$$

a univalent modular function on $\Gamma_0(5)$, with a simple pole at ∞

and a simple zero at 0 (the two cusps of $\Gamma_0(p)$): [Ono2004, Section 1.4, esp. Theorem 1.64], [Apostol1990, Sections 4.7-4.10, esp. Theorems 4.7 and 4.9]

There exists a unique degree-u polynomial $f(j)$ such that $f(j) - x'$ is a cusp form:

$$j = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + 333202640600q^5 + \cdots$$

$$f(j) = j - 750$$

Note that

- $j_0 := 750 \equiv 0$ is the unique supersingular j-invariant at 5.
- $$f(j) - x' \equiv 0 \mod 5 \tag{2.2}$$

Questions

- Is $f(j)$ a polynomial of supersingular j-invariants? Cf. [Kaneko-Zagier1998, Theorem 1] and [Milas-Mortenson-Ono2008, Theorems 1.1 and 1.5].

- Is x' a Hasse invariant? Cf. [Zhu2014, Remark 3.4].

Following [Choi2006, (2.4)],[3] we compute that

$$\begin{aligned} j_{up}^{(p)}(z) &= j_5^{(5)}(x',j) \\ &= x'^5 + 30x'^4 + 315x'^3 + 1300x'^2 + 1575x' \\ &= \frac{1}{q^5} - 6 + 5q(\cdots) \qquad\qquad \text{Why??} \end{aligned}$$

and get

$$\begin{aligned} \mathrm{cmp}(x',j') &= x' j_{up}^{(p)} - x'\big(f(j') - x\big) \\ \mathrm{cmp}(x,j) &= x^6 + 30x^5 + 315x^4 + 1300x^3 + 1575x^2 + (750-j)x + 5^3 \end{aligned}$$

More directly, adapting [Choi2006, (2.4)], we have

$$j_{u(p+1)}^{(p)}(x',j') \rightsquigarrow \mathrm{cmp}(x',j')$$

where $j'(z) = j(pz)$. Note that since

$$\begin{aligned} x' &= \frac{1}{q^u} + \cdots \\ j' &= \frac{1}{q^p} + \cdots \end{aligned}$$

and $p \nmid u$, this algorithm for computing $\mathrm{cmp}(x,j)$ <u>always</u> works.

Upshot (cf. [Zhu2015, (3.10)])

$$\begin{aligned} \psi^5 \colon\ E^0 &\to E^0(B\Sigma_5)/I \\ \mathbb{W}\big(\overline{\mathbb{F}}_5\big)[\![h = j - j_0]\!] &\to \mathbb{W}\big(\overline{\mathbb{F}}_5\big)[\![x,j]\!]/\big(\mathrm{cmp}(x,j)\big) \\ h \mapsto j' - 750 &= x + 1x'^5 + 30x'^4 + 315x'^3 + 1300x'^2 + 1575x' \\ &= x + (h - x^5 - 30x^4 - 315x^3 - 1300x^2 - 1575x)^5 + \cdots \\ &= h^5 + 30h^4 - 787185h^3 - 78654950h^2 + 113706048450h + 9128404218750 \\ &\quad + (-1575h^4 - 209750h^3 + 919941375h^2 + 146313952500h - 53794421543124)x \\ &\quad + (-1300h^4 - 78375h^3 + 765753000h^2 + 83642547500h - 47590693860000)x^2 \\ &\quad + (-315h^4 - 13200h^3 + 185819525h^2 + 17992315500h - 11702653105500)x^3 \\ &\quad + (-30h^4 - 1025h^3 + 17705550h^2 + 1622265375h - 1120917084750)x^4 \\ &\quad + (-1h^4 - 30h^3 + 590310h^2 + 52436200h - 37473142200)x^5 \end{aligned}$$

[3] It generalizes [Ahlgren2003, p788], which in turn generalizes [Bruinier-Kohnen-Ono2004, pp553-554]. In particular, by analogy to the latter, $j_5^{(5)}(z) = j_1^{(5)}(z)|T_0(5)$; in other notation, $h' = T_5 x'$. Compare the Eichler-Shimura congruence from (1.1):

$$T_5\alpha = \sum \alpha_i' = \sum \frac{5}{\alpha_i} = \sum \frac{\alpha_0 \cdots \alpha_5}{\alpha_i} = h = \alpha^5 - 10\alpha^4 + 35\alpha^3 - 60\alpha^2 + 55\alpha + \alpha' \equiv \alpha^5 + \alpha' \mod 5$$

(Hecke operator and involution commute [Atkin-Lehner1970, Lemma 11]).

Second attempt: deduce $\psi^5(h)$ by comparing q-expansions

$$
\begin{aligned}
h' &= j' - 750 = \frac{1}{q^5} - 6 + 196884q^5 + \cdots \\
h &= j - 750 = \frac{1}{q} - 6 + 196884q + \cdots \\
x &= \frac{5^3}{x'} = 125q + 750q^2 + 3375q^3 + \cdots
\end{aligned}
$$

$$\Longrightarrow$$

$$h' = h^5 + 30h^4 - 1575h^4x - 787185h^3 + (-1300h^4x^2 + ?h^3x + ?h^2) + \cdots$$

unsuccessful

We do not yet know a nice formula for the higher coefficients in $\mathrm{cmp}(x, j)$ when $g = 0$, though based on the algorithm it is not hard to write down a few terms:

$$
\begin{array}{lll}
w_p = 2sp & = \frac{24p}{p-1} & = 2(s+12) \\
w_{p-1} = sp(2sp - 4s + 3) & = \frac{36p(9p-17)}{(p-1)^2} & = -(s+12)(2s-27) \\
w_{p-2} = \frac{2}{3}sp(2sp - 6s + 1)(sp - 3s + 4) & = \frac{64p(2p-5)(25p-73)}{(p-1)^3} & = \frac{4}{3}(s+12)(s-8)(4s-25) \\
w_{p-3} = \frac{1}{6}sp(2sp - 8s + 1)(2sp - 8s + 3)(sp - 4s + 7) & = \frac{18p(3p-11)(19p-55)(25p-97)}{(p-1)^4} & = -\frac{1}{2}(s+12)(2s-9)(3s-19)(6s-25) \\
w_{p-4} = \frac{1}{15}sp(sp - 5s + 3)(2sp - 10s + 3) & = \frac{576p(5p-21)(9p-41)(34p^2-275p+529)}{5(p-1)^5} & = \frac{4}{15}(s+12)(4s-15)(8s-27) \\
\qquad (2s^2p^2 - 20s^2p + 21sp + 50s^2 - 105s + 4) & & \qquad (8s^2 - 69s + 136)
\end{array}
$$

Example 2.3 $p = 11$

$s = 6 \qquad xx' = 11^6$

$u = 5$

$$
\begin{aligned}
x' = \phi_{11}(z) &= \left(\frac{\eta(z)}{\eta(11z)}\right)^{12} \\
&= \frac{1}{q^5} - \frac{12}{q^4} + \frac{54}{q^3} - \frac{88}{q^2} - \frac{99}{q} + 540 - 418q - 648q^2 + 594q^3 + 836q^4 + 1056q^5 - 4092q^6 - 353q^7 + \cdots
\end{aligned}
$$

a modular function on $\Gamma_0(11)$ with Nebentypus: [Apostol1990, pp86-87]

There exists a unique $f(j)$ such that $f(j) - x'$ is a cusp form $(0 \mod 11)$:

$$
\begin{aligned}
f(j) &= j^5 - 3732j^4 + 4586706j^3 - 2059075976j^2 + 253478654715j - 2067305393340 \\
&\equiv j^2(j-1)^3 \mod 11
\end{aligned}
$$

Adapting [Choi2006, (2.4)], we compute $\mathrm{cmp}(x',j') \rightsquigarrow \mathrm{cmp}(x,j)$ and get

$$\begin{aligned}\mathrm{cmp}(x,j) = x^{12} &- 5940x^{11} + 14701434x^{10} + (-139755j - 19264518900)x^9 \\ &+ \cdots \\ &+ (-j^5 + 3732j^4 - 4586706j^3 + 2059075976j^2 - 253478654715j \\ &+ 2067305393340)x + 11^6 \\ \equiv\ & x\big(x^{11} - f(j)\big) \mod 11\end{aligned}$$

Upshot

$$\begin{aligned}\psi^{11}\colon\ E^0 &\to E^0(B\Sigma_{11})/I \\ \mathbb{W}\big(\overline{\mathbb{F}}_{11}\big)[\![h = j]\!] &\to \mathbb{W}\big(\overline{\mathbb{F}}_{11}\big)[\![x,j]\!]/\big(\mathrm{cmp}(x,j)\big)\end{aligned}$$

It seems that $\mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![x,j]\!]/\big(\mathrm{cmp}(x,j)\big)$ is not always the correct target of the total power operation for an E-theory, which arises from completion at a single supersingular point; x' needs to split off a factor with q-expansion $\dfrac{1}{q} + \cdots$, to be paired with j as in (2.2).

In view of the above, for all primes p, we have

$$\begin{aligned}\psi^p\colon\ L_{K(2)}\mathrm{TMF}(?)^0 &\to L_{K(2)}\mathrm{TMF}(?)^0(B\Sigma_p)/I \\ \mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![h = f(j)]\!] &\to \mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![x,j]\!]/\big(\mathrm{cmp}(x,j)\big) \\ h &\mapsto f(j') = x + j^{(p)}_{up}(x',j')\end{aligned}$$

Locally at each supersingular point, the above total power operation splits off a factor

$$\begin{aligned}\psi^p\colon\ E^0 &\to E^0(B\Sigma_p)/I \\ \mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![h = j - j_0]\!] &\to \mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![x_0,j]\!]/\big(\mathrm{cmp}_0(x_0,j)\big) \\ h &\mapsto j' - j_0\end{aligned}$$

In particular,

$$\begin{aligned}x_0' &\equiv j - j_0 \mod p \\ \Longrightarrow\ \mathrm{cmp}_0(x_0',j') &\equiv x_0'\big((x_0')^p - (j' - j_0)\big) \equiv (j - j_0)(j^p - j') \mod p\end{aligned}$$

which symmetrizes to the Kronecker congruence

$$\big(j - (j')^p\big)(j^p - j') \equiv 0 \mod p$$

We check $h = j - j_0$ against the explicit models of $\big(\Gamma_0(p), \Gamma_1(N)\big)$ and see how the q-expansions match up.

- $\Gamma_1(3)\colon\ y^2 + Axy + By = x^3,\ \ |A| = 1,\ \ |B| = 3,\ \ \Delta = B^3(A^3 - 27B),\ \ j = A^3(A^3 - 24B)^3/\Delta$
  At $p = 2$,

$$\begin{cases} H = A \implies \frac{H}{B^{1/3}} = h = j - j_0 = \frac{1}{q} + \cdots \\ j = \frac{\left(\frac{1}{q}B^{1/3}\right)^{12}}{q} + \cdots = \frac{1}{q^{13}}B^4 + \cdots = \frac{1}{q} + \cdots \end{cases} \implies B = q^3 + \cdots$$

At $p=5$, $(p-1)/2=2$,[4]

$$\left\{\begin{array}{l} H = A^4 + 16AB \implies \frac{H}{B^{4/3}} = h = \big((j-j_0)(j-j_1)\big)^2 = \frac{1}{q^4} + \cdots \\ j = \frac{\left(\frac{1}{q^4}B^{4/3}\right)^3}{q} + \cdots = \frac{1}{q^{13}}B^4 + \cdots = \frac{1}{q} + \cdots \end{array}\right. \implies B = q^3 + \cdots$$

- $\Gamma_1(4)$: $y^2+Axy+ABy = x^3+Bx^2$, $|A|=1$, $|B|=2$, $\Delta = A^2B^4(A^2-16B)$, $j=(A^4-16A^2B+16B^2)^3/\Delta$

  At $p=3$, $(p-1)/2=1$,

$$\left\{\begin{array}{l} H = A^2 + 4B \implies \frac{H}{B} = h = j - j_0 = \frac{1}{q} + \cdots \\ j = \frac{\left(\frac{1}{q}B\right)^6}{q} + \cdots = \frac{1}{q^7}B^6 + \cdots = \frac{1}{q} + \cdots \end{array}\right. \implies B = q + \cdots$$

  At $p=5$, $(p-1)/2=2$,

$$\left\{\begin{array}{l} H = A^4 + 24A^2B + 16B^2 \implies \frac{H}{B^2} = h = (j-j_0)^2 = \frac{1}{q^2} + \cdots \\ j = \frac{\left(\frac{1}{q^2}B^2\right)^3}{q} + \cdots = \frac{1}{q^7}B^6 + \cdots = \frac{1}{q} + \cdots \end{array}\right. \implies B = q + \cdots$$

3 Modular equations for Lubin-Tate formal groups

Theorem 3.1 *Let $\mathbb{G}_0$ be a formal group of height 2 over $\overline{\mathbb{F}}_p$, and let $\mathbb{G}$ be its universal deformation. Write A_m for the ring $\mathcal{O}_{\mathrm{Sub}_m(\mathbb{G})}$ studied in [Strickland1997], which classifies degree-p^m subgroups of the formal group $\mathbb{G}$. Then $A_0 \cong \mathbb{W}(\overline{\mathbb{F}}_p)[\![h]\!]$ and $A_1 \cong \mathbb{W}(\overline{\mathbb{F}}_p)[\![h,\alpha]\!]/\big(w(h,\alpha)\big)$, where*

$$w(h,\alpha) = (\alpha - p)\big(\alpha + (-1)^p\big)^p - \big(h - p^2 + (-1)^p\big)\alpha$$

Proof Choose a $\mathcal{P}_N$-model for $\mathbb{G}$ as in [Zhu2015, Section 2], and consider a formal neighborhood that contains a single supersingular point in characteristic p with j-invariant j_0 (clearly such a neighborhood is preserved under a deformation of p-power Frobenius, as the Frobenius is an automorphism over $\overline{\mathbb{F}}_p$). Define $h := j - j_0$. By the Serre-Tate theorem and [Zhu2015, Remark 3.2], there exists a unique polynomial

$$w(h,\alpha) = \alpha^{p+1} + \sum_{i=0}^{p} w_i \alpha^i \tag{3.2}$$

with $w_i \in \mathbb{W}(\overline{\mathbb{F}}_p)[\![h]\!]$ such that $A_1 \cong A_0[\alpha]/\big(w(h,\alpha)\big)$. Moreover, by [Ando1995, Theorem 4], we can choose α such that $w_0 = (-1)^{p+1}p$.

Note that the ring A_1, with parameters h and α, is precisely the ring A parametrized by T and $\mathbf{N}\big(X(P)\big)$, respectively, in [Katz-Mazur1985, Section 7.7]. We now imitate the derivation from Section 2 of a canonical modular polynomial, with parameters j' and x', and derive a polynomial relation between their counterparts h' and α', which are the images of h and α under the Atkin-Lehner involution.

[4] [Silverman2009, V.4.1a]

By [Katz-Mazur1985, 12.4.1], [Zhu2015, Remark 3.2] and in view of the dehomogenization procedure in [Zhu2015, Example 2.6, Proposition 2.8, and Example 3.4], since $h = j - j_0$, the modular function α' on $\Gamma_0(p)$ has a q-expansion

$$\alpha' = \mu q^{-1} + O(1)$$

for some $\mu \in \mathbb{W}(\overline{\mathbb{F}}_p)^\times \cap \mathbb{Z}$. Thus there exist $w_i' \in p\mathbb{Z}$, $2 \leq i \leq p$ such that

$$(\alpha')^p + w_p'(\alpha')^{p-1} + \cdots + w_2'\alpha' = \mu^p q^{-p} + O(1)$$

On the other hand, since $j'(z) = j(pz)$, we have

$$h' = j' - j_0 = q^{-p} + O(1)$$

Comparing the two displays above, we then have

$$(\alpha')^p + w_p'(\alpha')^{p-1} + \cdots + w_2'\alpha' = \mu^p h' + c + O(q)$$

for some $c \in \mathbb{Z}$. Passing to the mod-p reduction of this identity, we see that $c \in p\mathbb{Z}$. Therefore we can redefine h (and w_i, $2 \leq i \leq p$ in (3.2) accordingly) such that

$$(\alpha')^p + w_p'(\alpha')^{p-1} + \cdots + w_2'\alpha' = h' + O(q)$$

without changing the expressions for A_0 and A_1 (note that α' is independent of the choice of h). From this we obtain

$$(\alpha')^{p+1} + w_p'(\alpha')^p + \cdots + w_2'(\alpha')^2 = h'\alpha' + O(1)$$

In view of the expression for A_1 (under the Atkin-Lehner involution) and the q-expansions for α' and h', we see that the last term $O(1)$ above must be constant. Applying the Atkin-Lehner involution to this polynomial relation between α' and h', we then conclude that the coefficients w_i, $2 \leq i \leq p$ in (3.2) are all constants. It remains to determine their values, which follows from the next proposition. □

Proposition 3.3 *Let M_n and $M_{n,p}$ be the modular schemes in [Katz1973, Section 1.13], the latter being finite and flat over the former of degree $p+1$. In a punctured formal neighborhood of the cusps $\overline{M}_n - M_n$, the scheme $M_{n,p}$, viewed as a relative curve over M_n, has an equation*

$$(\alpha - p)\big(\alpha + (-1)^p\big)^p = 0$$

Proof Choose the particular local coordinate in [Ando1995, Theorem 4] on the universal elliptic curve over $M_{n,p}$, and define the parameter α as in [Zhu2015, Section 3.1, esp. Construction 3.1 (ii) and Remark 3.2]. In view of [Zhu2015, Remark 3.15], the stated equation then follows from the discussion in the first new paragraph on page Ka-23 of [Katz1973] (note that when $p = 2$, the isogeny π in [Katz1973, Section 1.11] differs by a sign from the restriction of the isogeny $\Psi_N^{(p)}$, $N = n$, in [Zhu2015, Section 3] around the ramified cusp 0 of $\Gamma_0(p)$). □

By [Strickland1998, Theorem 1.1] and [Rezk2009, Theorem B], we have the following.

Corollary 3.4 *Let E be a Morava E-theory of height 2 at the prime p. There is a total power operation*

$$\begin{aligned} \psi^p\colon\ E^0 &\to E^0(B\Sigma_p)/I \\ \mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![h]\!] &\to \mathbb{W}\big(\overline{\mathbb{F}}_p\big)[\![h,\alpha]\!]/\big(w(h,\alpha)\big) \end{aligned}$$

where

$$w(h,\alpha)=(\alpha-p)\big(\alpha+(-1)^p\big)^p-\big(h-p^2+(-1)^p\big)\alpha$$

4 Computations

From Corollary 3.4 we can compute $\psi^p(h)$ via involution as usual ~~algorithmically, if not explicitly~~, which leads to a uniform presentation of the Dyer-Lashof algebra for Morava E-theory at height 2 (cf. [Zhu2015, Remark 6.6]).

Here are two attempts for computing $\psi^p(h)$ explicitly. Assume $p>2$.

(i) Can a computer manipulate polynomials of indefinite degree? Cf. [Kerner2008, Appendix C].

$$\begin{aligned}
(\alpha-p)(\alpha-1)^p &= (\alpha-p)\sum_{i=0}^{p}\binom{p}{i}\alpha^i(-1)^{p-i}\\
&= \sum_{i=0}^{p}\binom{p}{i}\alpha^{i+1}(-1)^{p-i}-p\sum_{i=0}^{p}\binom{p}{i}\alpha^i(-1)^{p-i}\\
&= \sum_{j=1}^{p+1}\binom{p}{j-1}\alpha^j(-1)^{p-j+1}-p\sum_{j=0}^{p}\binom{p}{j}\alpha^j(-1)^{p-j}\\
&= \sum_{j=2}^{p+1}\left[\binom{p}{j-1}(-1)^{p-j+1}-p\binom{p}{j}(-1)^{p-j}\right]\alpha^j+\cdots \qquad \binom{p}{p+1}=0\\
&= \sum_{j=2}^{p+1}(-1)^{p-j+1}\left[\binom{p}{j-1}+p\binom{p}{j}\right]\alpha^j+\cdots\\
\implies\quad w(h,\alpha) &= (-p)(-1)^p-h\alpha+\sum_{j=2}^{p+1}(-1)^{p-j+1}\left[\binom{p}{j-1}+p\binom{p}{j}\right]\alpha^j\\
&= p-h\alpha+\sum_{j=2}^{p+1}(-1)^{j}\left[\binom{p}{j-1}+p\binom{p}{j}\right]\alpha^j\\
&= p-h\alpha+\sum_{j=2}^{p+1}\left[\binom{p}{j-1}+p\binom{p}{j}\right](-\alpha)^j
\end{aligned}$$

$$\implies \qquad 0 = p - h\alpha + \sum_{j=2}^{p+1}\left[\binom{p}{j-1} + p\binom{p}{j}\right]\alpha^j \qquad\qquad \alpha \mapsto -\alpha,\ h \mapsto -h$$
$$= \alpha^{p+1} + 2p\alpha^p + \cdots - h\alpha + p$$
$$\implies \alpha' = \frac{p}{\alpha} = h - \sum_{j=2}^{p+1}\left[\binom{p}{j-1} + p\binom{p}{j}\right]\alpha^{j-1}$$
$$= h - \sum_{i=1}^{p}\left[\binom{p}{i} + p\binom{p}{i+1}\right]\alpha^{i}$$
$$\implies \qquad h' = \alpha + \sum_{k=1}^{p}\left[\binom{p}{k} + p\binom{p}{k+1}\right]\left(h - \sum_{i=1}^{p}\left[\binom{p}{i} + p\binom{p}{i+1}\right]\alpha^{i}\right)^k$$

Adapting the proof of [Zhu2015, Proposition 6.4] does the trick here!

$$= \alpha + \sum_{k=1}^{p}\left[\binom{p}{k} + p\binom{p}{k+1}\right]\sum_{m_k=0}^{k}\binom{k}{m_k}h^{k-m_k}\left(-\sum_{i=1}^{p}\left[\binom{p}{i} + p\binom{p}{i+1}\right]\alpha^{i}\right)^{m_k}$$
$$= -\alpha^{p^2} - 2p^2\alpha^{p^2-1} + \cdots + \sum_{k=1}^{p}\left[\binom{p}{k} + p\binom{p}{k+1}\right]h^k$$
$$\equiv ?\ \bmod w(h,\alpha)$$

(ii) Change of variables

$$w(h,\alpha) = (\alpha - p)(\alpha-1)^p + (1 + p^2 - h)\alpha$$
$$\begin{cases} \beta = \alpha - 1 & \text{a unit} \\ y = p^2 - h \end{cases} \qquad \Big\Downarrow$$
$$(1 + \beta - p)\beta^p + (1+y)(1+\beta) = 0$$
$$\big(1 - (1+\beta')\big)\beta^p + 1 + y = 0$$
$$1 + y = \beta^p\beta' \qquad\qquad \text{multiplicativity of units}$$
$$y' = (\beta')^p\beta - 1$$
$$= \left(\frac{y+1}{\beta^p}\right)^p \beta - 1$$
$$= \frac{(y+1)^p}{\beta^{p^2-1}} - 1$$

Reducing β^{p^2-1} and then inverting it is complicated. Also,

$$\begin{aligned}
&\begin{cases} \beta^{p+1}+(1-p)\beta^p+(1+y)\beta+(1+y)=\beta^p(\beta+1-p)+(1+y)(\beta+1) \\ \beta^p=(1+y)(\beta+1)\cdot(1+y)^{-1}(\beta^{p-1}-\beta^{p-2}+\beta^{p-3}-\cdots+1)-1 \end{cases} \\
\implies\ & 1=-\beta^p(\beta+1-p)\cdot(1+y)^{-1}(\beta^{p-1}-\beta^{p-2}+\beta^{p-3}-\cdots+1)-\beta^p \\
\implies\ & \beta'=\frac{1+y}{\beta^p} \\
&\quad=-(\beta+1-p)(\beta^{p-1}-\beta^{p-2}+\beta^{p-3}-\cdots+1)-(1+y) \\
&\quad=-\beta^p+p\beta^{p-1}-p\beta^{p-2}+p\beta^{p-3}-\cdots+p-1-(1+y)
\end{aligned}$$

Reducing the p'th power of this last expression seems hard.

5 More about the eta-quotient

For the genus-zero primes p (each with a single supersingular j-invariant), it is straightforward to show that

$$\text{constant term of } -\phi_p(z)=2s=\#\mathrm{Aut}(E_{\mathrm{s.s.}}/\overline{\mathbb{F}}_p)$$

as noted in Section 1 ($768-j$, etc.).

In view of the construction of ϕ_p from Δ, it is not surprising that ϕ_p has vanishing "p-local Serre derivative" [Ahlgren2003, Section 4] (cf. [Zhu2015, (4.10)]):

$$\begin{aligned}
&\text{"}G_p:=\frac{\theta\phi_p}{\phi_p}+\frac{pE_2|V(p)-E_2}{p-1}=0\text{"} \\
\iff\ & \vartheta_p\phi_p:=D\phi_p+\left(\frac{k/12-h}{p-1}\cdot p\mathcal{E}_2|V(p)+\frac{h-pk/12}{p-1}\cdot\mathcal{E}_2\right)\phi_p=0
\end{aligned}$$

where weight $k=0$, $h=-u=-1$ [Ahlgren2003, Lemma 2.2]. This generalizes to all primes in [Choi2006, Theorem 3.4]. In fact, there is a version of p-local Serre derivative for each (l,p)-type sequence $\{g_m^{(p)}\}$.[5]

It is illegitimate to deduce from this and [Zhu2015, Theorem 4.13] that

$$\begin{aligned}
\ell_{2,p}(x')&=\frac{1}{p}\log\frac{(x')^p\cdot x'}{x_0\cdots x_p} \\
&=\frac{1}{p}\log\frac{(x')^{p+1}}{p^s}
\end{aligned}$$

[5] Sequences of modular functions:

[Bruinier-Kohnen-Ono2004]	$\mathrm{SL}_2(\mathbb{Z})$	$\{j_m(z)\}$	$(-1,1)$-type	$j_1(z)=j(z)-744$	$H_\tau(z)$
[Ahlgren2003]	$\Gamma_0(p),\ g=0$	$\{j_m^{(p)}(z)\}$	$(-1,p)$-type	$j_1^{(p)}(z)=\phi_p(z)\equiv f(j) \mod p$	$H_\tau^{(p)}(z)$
[Choi2006, (2.4)]	$\Gamma_0(p),\ g>0$	$\{j_m^{(p)}(z)\}$	$(-u,p)$-type	$j_1^{(p)}(z)=j(z)$ $j_u^{(p)}(z)=\phi_p(z)\equiv f(j) \mod p$	
[Choi2006, Definition 3.1]	$\Gamma_0(N)$	$\{g_m^{(N)}(z)\}$	(l,p)-type		$[g_m^{(N)}]_\tau(z),\ [g_m^{(N)}]_t(z),\ [g_m^{(N)}]_\infty(z)$

must then be zero, because ϕ_p is not on $\Gamma_1(N)$ and is not a unit either.

However, the above does seem to make sense $K(1)$-locally. Recall from [Lubin1979, Definition above Theorem E] that the universal ring parametrizing canonical (degree-p) subgroups is

$$\mathfrak{A}_2 \cong \mathbb{Z}_p\left[\!\left[t, \frac{p}{t}, \frac{p^p}{t^{p+1}}\right]\!\right] \sim \mathbb{Z}_p\left[\!\left[\alpha, \alpha', \frac{(\alpha')^{p+1}}{p}\right]\!\right] \sim \mathbb{Z}_p\left[\!\left[x, x', \frac{(x')^{p+1}}{p^s}\right]\!\right]$$

We know that $K(1)$-localization inverts $h \sim \alpha' \sim x'$, so that

$$\ell_{2,p}(x') = 0 \implies \frac{(x')^{p+1}}{p^s} \in \mu_p \implies A_1 \cong \mathfrak{A}_2$$

meaning, tautologically, that $K(1)$-locally the unique degree-p subgroup is the canonical subgroup.

Question: What does $\vartheta_p \circ x' = 0$ indicate, if anything, for the diagram below? [Katz1973, Appendices 1 and 2]

$$\begin{tikzcd}
0 \arrow[r] & \omega \arrow[r] \arrow[d, "\cdot \alpha' \sim x'"'] & H^1_{\mathrm{DR}}(C/S) \arrow[r] \arrow[d] & \omega^{-1} \arrow[r] \arrow[d, "\cdot h'"] & 0 \\
0 \arrow[r] & \omega^{(p)} \arrow[r] \arrow[d, "\vartheta_p"'] & H^1_{\mathrm{DR}}(C^{(p)}/S) \arrow[r] \arrow[d, "\nabla(D)"] & \omega^{(-p)} \arrow[r] & 0 \\
 & {} & H^1_{\mathrm{DR}}(C^{(p)}/S) \otimes \omega^{(2p)} & &
\end{tikzcd}$$

♠ Look into more of [Katz1973] for a structural explanation of the appearance of Serre derivatives in homotopy-theoretic context.

References

[Ahlgren2003] Scott Ahlgren, The theta-operator and the divisors of modular forms on genus zero subgroups, Math. Res. Lett. **10** (2003), no. 6, 787–798. MR2024734(2004m:11059)

[Ando1995] Matthew Ando, Isogenies of formal group laws and power operations in the cohomology theories E_n, Duke Math. J. **79** (1995), no. 2, 423–485. MR1344767(97a:55006)

[Apostol1990] Tom M. Apostol, Modular functions and Dirichlet series in number theory, second ed., Graduate Texts in Mathematics, vol. 41, Springer-Verlag, New York, 1990. MR1027834(90j:11001)

[Atkin-Lehner1970] A. O. L. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160. MR0268123(42 #3022)

[Bruinier-Kohnen-Ono2004] Jan H. Bruinier, Winfried Kohnen, and Ken Ono, The arithmetic of the values of modular functions and the divisors of modular forms, Compos. Math. **140** (2004), no. 3, 552–566. MR2041768(2005h:11083)

[Choi2006] D. Choi, On values of a modular form on $\Gamma_0(N)$, Acta Arith. **121** (2006), no. 4, 299–311. MR2224397(2006m:11051)

[Deligne-Rapoport1973] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349. MR0337993(49 #2762)

[Diamond-Shurman2005] Fred Diamond and Jerry Shurman, A first course in modular forms, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR2112196(2006f:11045)

[Kaneko-Zagier1998] M. Kaneko and D. Zagier, Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 97–126. MR1486833(99b:11064)

[Katz1973] Nicholas M. Katz, p-adic properties of modular schemes and modular forms, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350. MR0447119(56 #5434)

[Katz-Mazur1985] Nicholas M. Katz and Barry Mazur, Arithmetic moduli of elliptic curves, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR772569(86i:11024)

[Kerner2008] D. Kerner, Enumeration of uni-singular algebraic hypersurfaces, Proc. Lond. Math. Soc. (3) **96** (2008), no. 3, 623–668. MR2407815(2009e:14088)

[Lubin1979] Jonathan Lubin, Canonical subgroups of formal groups, Trans. Amer. Math. Soc. **251** (1979), 103–127. MR531971(80j:14039)

[Milas-Mortenson-Ono2008] Antun Milas, Eric Mortenson, and Ken Ono, Number theoretic properties of Wronskians of Andrews-Gordon series, Int. J. Number Theory **4** (2008), no. 2, 323–337. MR2404804(2009g:11054)

[Ono2004] Ken Ono, The web of modularity: arithmetic of the coefficients of modular forms and q-series, CBMS Regional Conference Series in Mathematics, vol. 102, Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004. MR2020489(2005c:11053)

[Rezk2009] Charles Rezk, The congruence criterion for power operations in Morava E-theory, Homology, Homotopy Appl. **11** (2009), no. 2, 327–379. MR2591924(2011e:55021)

[Silverman2009] Joseph H. Silverman, The arithmetic of elliptic curves, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094(2010i:11005)

[Strickland1997] Neil P. Strickland, Finite subgroups of formal groups, J. Pure Appl. Algebra **121** (1997), no. 2, 161–208. MR1473889(98k:14065)

[Strickland1998] N. P. Strickland, Morava E-theory of symmetric groups, Topology **37** (1998), no. 4, 757–779. MR1607736(99e:55008)

[Zhu2014] Yifei Zhu, The power operation structure on Morava E-theory of height 2 at the prime 3, Algebr. Geom. Topol. **14** (2014), no. 2, 953–977. MR3160608

[Zhu2015] Yifei Zhu, The Hecke algebra action on Morava E-theory of height 2, available at http://www.math.northwestern.edu/~zyf/draft.pdf.