ACTA ARITHMETICA
161.4 (2013)

Modular equations for some η-products

by

François Morain (Palaiseau)

1. Introduction. Let η denote Dedekind's function. When $N > 1$ is an integer, η-quotients of the form $f = \prod_{d|N} \eta(z/d)^{r_d}$ are functions on $\Gamma^0(N)$ when the integers r_d satisfy some properties known as Newman's Lemma [13]. In other words, there exists a bivariate polynomial $\Phi[f](X, J)$ such that $\Phi[f](f(z), j(z)) = 0$ for all z, where j is the classical modular invariant.

In some cases, there exist equations of the form $\Phi[f](X, G_3, G_2)$ where $\Phi[f](f(z), \gamma_3(z), \gamma_2(z)) = 0$ for the Weber functions γ_3, γ_2. Kiepert was the first to compute modular equations of this type for $f = \mathfrak{w}_p = \eta(z/p)/\eta(z)$ for $p \le 29$ (see [10]). Weber cites some examples in [15, §72]; Antoniadis [1] extended this to $p \le 61$.

In the present work, we study such equations for the double η-quotients $\mathfrak{w}^e_{p_1,p_2}$ introduced in [6]. We give all parameters (p_1, p_2, e) leading to equations in γ_2 and γ_3.

Section 2 recalls known facts on Weber and η functions. Section 3 deals with the case of $\mathfrak{w}_p$ where we introduce a faster variant of the classical algorithm to compute the modular equation via series expansions. Section 4 proves the necessary results for $\mathfrak{w}_{p_1,p_2}$, gives algorithms to compute the equations in the spirit of Section 3, and includes some numerical examples.

Notation. If u is some function, we will denote by $\Phi[u](X, J)$ the corresponding modular equation. If $u = j(nz)$, we will write Φ_n for simplicity.

2. Preliminaries

2.1. Properties of the functions γ_2 and γ_3. We will use the traditional notations

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

2010 *Mathematics Subject Classification*: Primary 11F03; Secondary 14G35, 11G18.
Key words and phrases: modular curves, class invariants, SEA algorithm.

DOI: 10.4064/aa161-4-1

for the two generators of $\mathrm{SL}_2(\mathbb{Z})$. We use the notation $f \circ M$ to denote the function $z \mapsto f(Mz)$. The modular invariant is $j(z) = j(q) = 1/q + 744 + \cdots$ with $q = \exp(2i\pi z)$ and it is invariant under $\mathrm{SL}_2(\mathbb{Z})$ (equivalently, under T and S).

The classical Weber functions are

$$\gamma_2(q) = j(q)^{1/3} = q^{-1/3}(1 + 248q + 4124q^2 + 34752q^3 + 213126q^4 + O(q^5)),$$
$$\gamma_3(q) = (j(q) - 1728)^{1/2} = q^{-1/2}(1 - 492\,q - 22590\,q^3 + O(q^5)).$$

It is known that $\gamma_2(q) \in q^{-1/3}(1 + \mathbb{Z}[[q]])$ and $\gamma_3(q) \in q^{-1/2}(1 + \mathbb{Z}[[q]])$.

If n is an integer, we denote $\zeta_n = \exp(2\pi i/n)$. One can prove that

$$\gamma_2 \circ T = \zeta_3^{-1}\gamma_2, \quad \gamma_2 \circ S = \gamma_2, \tag{2.1}$$
$$\gamma_3 \circ T = -\gamma_3, \quad \gamma_3 \circ S = -\gamma_3. \tag{2.2}$$

The following is classical (see, e.g., [3, Lemma 11.10]).

Proposition 2.1. *If f is a holomorphic modular function invariant under T and S, then f is a polynomial in j.*

This can be extended as follows (see [15, §54] and also [3, Theorem 11.9]).

Theorem 2.2. *Let f be a modular function.*

(a) *If f is invariant under T and S, then f is a rational function of j.*
(b) *If $f \circ T = -f$ and $f \circ S = -f$, then f is equal to γ_3 times a rational function of j.*
(c) *If $f \circ T = \zeta_3^{\mp 1} f$ and $f \circ S = f$, then f is equal to $\gamma_2^{\pm 1}$ times a rational function of j.*
(d) *If $f \circ T = -\zeta_3^{\mp 1} f$ and $f \circ S = -f$, then f is equal to $\gamma_3\gamma_2^{\pm 1}$ times a rational function of j. (Note that $-\zeta_3^{\mp 1} = \zeta_6^{\pm 1}$.)*

We will use the preceding results as follows. Given a function f satisfying one of the conditions in Theorem 2.2, there is some g (given as above) for which f/g is invariant under T and S, implying that f/g is a rational function of j. Furthermore, if f/g is holomorphic, then this rational function will turn out to be a polynomial; if the expansion of f/g has integer coefficients, then Hasse's principle will imply that this polynomial has integer coefficients. For ease of writing, this will lead to polynomials in J, G_2 (for γ_2), or G_3 (for γ_3).

From the algorithmic point of view, we have to recognize a polynomial with integer coefficients applied to $j(q)$, given the first terms of a series $\mathcal{T}(q)$. Note that we need the order of this series to be > 0. We proceed step by step.

Function RecognizePolyInJ($\mathcal{T}$)
Input: a series $\mathcal{T} = c_v q^v + \cdots + O(q^1)$ with integer coefficients, $v \le 0$ and $c_v \neq 0$.

OUTPUT: a polynomial $P(X)$ of degree $-v$ such that $\mathcal{T} = P(j(q))$.

1. $\mathcal{R} := \mathcal{T}$; $i :=$ valuation$(\mathcal{R})$; $P := 0$;
2. while $i \le 0$ do
   {at this point $\mathcal{R} = r_i q^i + \cdots + O(q^1)$ with $r_i \neq 0$}
   2.1. $P := P + r_i X^{-i}$;
   2.2. $\mathcal{R} := \mathcal{R} - r_i j(q)^{-i}$;
   2.3. $i :=$ valuation$(\mathcal{R})$;
3. return P.

Note that we can precompute the powers of $j(q)$ whenever needed, so that each call to the function requires $O(v^2)$ operations. In large cases, computations can be done using results calculated modulo small primes and reconstructed via the CRT (as done by Atkin, see [11]).

2.2. Formulas for the η-function. The following is taken from [7] and will be our main tool in the computations of Section 4. Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ denote the full modular group.

THEOREM 2.3. *Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ be normalised 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*

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

For $K \in \mathbb{N}$ write

$$u_K a + v_K K c = \delta_K = \gcd(a, Kc) = \gcd(a, K).$$

Then

$$\eta\left(\frac{z}{K}\right) \circ M = \varepsilon \left(\begin{pmatrix} \frac{a}{\delta_K} & -v_K \\ \frac{Kc}{\delta_K} & u \end{pmatrix} \right) \sqrt{\delta_K (cz+d)}\, \eta\left(\frac{\delta_K z + (u_K b + v_K K d)}{\frac{K}{\delta_K}} \right),$$

where the square root is chosen with positive real part.

We can decompose the formula into several parts: $\varepsilon(M) = \mathrm{Jac}(M)\zeta_{24}^{\mathcal{E}(M)}$ where we distinguish the Jacobi symbol part and the exponent of ζ_{24}; then, we have the square root part $\mathcal{Q}(M)$ and the η-part $\mathcal{N}(M)$. When dealing with an η-quotient, the above formulas are applied by multiplicativity on the different pieces $\eta(z/d)$ (see below).

3. Generalized Weber functions

3.1. Definition and properties. Let $N > 3$ be an odd integer. For all factorizations $N = ad$, let $e = \gcd(a, d)$ and consider the functions

$$P_{c,d,a} = i^{(a-1)/2} \left(\frac{c}{e}\right) \sqrt{d}\, \frac{\eta((c+dz)/a)}{\eta(z)}$$

for $0 \le c < a$ with $\gcd(c,e) = 1$. These functions were introduced in [15, §72]. It is easy to see that $P_{0,1,N} = i^{(N-1)/2}\eta(z/N)/\eta(z) = i^{(N-1)/2}\mathfrak{w}_N(z)$ where the function $\mathfrak{w}_N$ was studied in [5].

Weber proves that in all cases, $P_{c,d,a}^{24}$ are roots of a modular equation. In some cases, the results are better, for instance:

THEOREM 3.1. *If* $\gcd(N,6) = 1$ *and* $12 \mid c$, *then the* $P_{c,d,a}^2\gamma_2^{N-1}\gamma_3^{(N-1)/2}$ *are roots of a modular equation.*

3.2. Computations in the prime order case. For a prime $N = p > 3$, this setting simplifies to

$$x_{0,p,1} = p\left(\frac{\eta(pz)}{\eta(z)}\right)^2, \quad x_{12h,1,p} = (-1)^{(p-1)/2}\left(\frac{\eta\left(\frac{12h+z}{p}\right)}{\eta(z)}\right)^2, 0 \le h < p.$$

THEOREM 3.2. *The numbers* $x_{c,d,a}\gamma_2(z)^{p-1}\gamma_3(z)^{(p-1)/2}$ *are roots of a modular equation whose coefficients are rational functions of* $j(z)$. *In particular, the constant term is* $(-1)^{(p-1)/2}p$.

Antoniadis [1] extended the results of Kiepert to $p \le 61$ and gave more properties of the polynomials. He computed the equation by solving a linear system in the unknown coefficients of the equation, using the q-expansion of $j(q)$ and the fact that $x_{0,p,1}$ must be a root of the equation.

A standard approach (already known to Enneper [8, §52]) is to compute the power sums of the roots of the equation, recognize them as polynomials in our variables, and then terminate using the classical Newton relations. Inspecting our roots, we see that the q-expansion of $x_{0,p,1}$ has positive order, and all $x_{12h,1,p}$ have negative order. So the power sums can be computed using the $x_{12h,1,p}$ only; we can find formulas for the q-expansion of $\sum_{h=0}^{p-1} x_{12h,1,p}^k$ if needed.

A better approach is to look at the reciprocal polynomial, whose roots are the $1/x_{0,p,1}$ and $1/x_{12h,1,p}$, and only the first one contributes to the power sums. Write $(p-1)/12 = e'/\delta$ as an irreducible fraction with $6 \mid \delta$. Noting that

$$p/x_{0,p,1} = q^{(1-p)/12}(1 + \cdots) = q^{-e'/\delta}(1 + \cdots),$$

we can use the discussion following Theorem 2.2 to conclude that all coefficients are polynomials in J, G_2 or G_3.

The algorithm is:

1. Compute $S_k = p/x_{0,p,1}^k$ and recognize it as a polynomial in the usual variables.
2. Use Newton's formulas.
3. Remove the powers of p.

Note that the largest power is $(p/x_{0,p,1})^{p+1} = q^{-(p^2-1)/12}(1+\cdots)$ where the exponent is an integer as soon as $p > 3$. Therefore, we need up to $(p^2-1)/12$ terms in the j-series.

For example, let us give some computational details in the case $p = 11$. We compute

$$S_1 = 11/x_{0,11,1} = q^{-5/6} - 2q^{1/6} - q^{7/6} + 2q^{13/6} + O(q^{19/6}).$$

Dividing by the expansion of $\gamma_2\gamma_3$, we find $1+242q+O(q^2)$, which must be a polynomial in $j(q)$, hence the constant 1. The other coefficients are given in Table 1. We have replaced γ_2 (resp. γ_3) by G_2 (resp. G_3). The corresponding polynomial is (after reductions between variables)

$$F^{12} - G_3G_2F^{11} - 242G_2^2F^{10} - 19965G_3F^9 - 585640G_2F^8 + 159440490F^6 - 285311670611.$$

Taking its reciprocal and removing the spurious powers of 11 yields

$$\Phi[-\mathfrak{w}_{11}^2](F, G_2, G_3) = F^{12} - 990F^6 + 440G_2F^4 + 165G_3F^3 + 22G_2^2F^2 + G_3G_2F - 11,$$

already computed by Weber.

Note that one drawback of this approach is the large degree and size of the coefficients before reduction via Newton formulas. However, if computations are performed using CRT primes, this is not a problem, since we compute the final polynomial modulo the primes.

The smallest cases are

$$\begin{aligned}
\Phi[\mathfrak{w}_5^2](X, G_2) &= X^6 + 10X^3 - G_2X + 5,\\
\Phi[-\mathfrak{w}_7^2](X, G_3) &= X^8 + 14X^6 + 63X^4 + 70X^2 + G_3X - 7,\\
\Phi[\mathfrak{w}_{13}^2](X, J) &= X^{14} + 26X^{13} + 325X^{12} + 2548X^{11} + 13832X^{10}\\
&\quad + 54340X^9 + 157118X^8 + 333580X^7 + 509366X^6\\
&\quad + 534820X^5 + 354536X^4 + 124852X^3 + 15145X^2\\
&\quad + (746 - J)X + 13.
\end{aligned}$$

Remark. We concentrated here on the prime index case. The same work can be done for composite indices. Note also that we could use resultants for that task, in view of the following. Suppose p is prime and M is an integer prime to p; write $N = pM$. Write

$$\mathfrak{w}_{pM}^s(z) = (\mathfrak{w}_p(z)\mathfrak{w}_M(z/p))^s.$$

On the other hand

$$\Phi[\mathfrak{w}_p^{s_1}](\mathfrak{w}_p^{s_1}(z), j(z)) = 0, \quad \Phi[\mathfrak{w}_M^{s_2}](\mathfrak{w}_M^{s_2}(z/p), j(z/p)) = 0,$$
$$\Phi_p(j(z), j(z/p)) = 0.$$

Table 1. Computations for $p = 11$

k	$(11/x_{0,11,1})^k$
2	$q^{-5/3} - 4q^{-2/3} + 2q^{1/3} + \cdots = G_2^2(J - 1244)$
3	$q^{-5/2} - 6q^{-3/2} + 9q^{-1/2} + 10q^{1/2} + \cdots = G_3(J^2 - 1002J + 59895)$
4	$q^{-10/3} - 8q^{-7/3} + 20q^{-4/3} - 70q^{2/3} + \cdots$
	$= G_2(J^3 - 2488J^2 + 1510268J - 135655520)$
5	$q^{-25/6} - 10q^{-19/6} + 35q^{-13/6} - 30q^{-7/6} - 105q^{-1/6} + 238q^{5/6} + \cdots$
	$= G_3G_2^2(J^3 - 2246J^2 + 1287749J - 145411750)$
6	$q^{-5} - 12q^{-4} + 54q^{-3} - 88q^{-2} - 99q^{-1} + 540 - 418q + \cdots$
	$= J^5 - 3732J^4 + 4586706J^3 - 2059075976J^2$
	$+253478654715J - 2067305393340$
7	$q^{-35/6} - 14q^{-29/6} + 77q^{-23/6} - 182q^{-17/6} + 924q^{-5/6} - 1547q^{1/6} + \cdots$
	$= G_3G_2(J^5 - 3490J^4 + 4063139J^3 - 1796527998J^2$
	$+247854700555J - 4740750382830)$
8	$q^{-20/3} - 16q^{-17/3} + 104q^{-14/3} - 320q^{-11/3} + 260q^{-8/3} + 1248q^{-5/3}$
	$-3712q^{-2/3} + 1664q^{1/3} + \cdots$
	$= G_2^2(J^6 - 4976J^5 + 9210680J^4 - 7786404608J^3$
	$+2955697453292J^2 - 418137392559040J + 12629117378938720)$
9	$q^{-15/2} - 18q^{-13/2} + 135q^{-11/2} - 510q^{-9/2} + 765q^{-7/2} + 1242q^{-5/2}$
	$-7038q^{-3/2} + 8280q^{-1/2} + 9180q^{1/2} + \cdots = G_3(J^7 - 4734J^6 + 8386065J^5$
	$-6877048710J^4 + 2611195915626J^3$
	$-398512009001700J^2 + 16457557949779815J - 41283301866181650)$
10	$q^{-25/3} - 20q^{-22/3} + 170q^{-19/3} - 760q^{-16/3} + 1615q^{-13/3} + 476q^{-10/3}$
	$-11210q^{-7/3} + 22440q^{-4/3} + 1615q^{-1/3} - 64600q^{2/3} + \cdots$
	$= G_2(J^8 - 6220J^7 + 15382190J^6 - 19242776200J^5 + 12809764457825J^4$
	$-4368737795118764J^3 + 669619352632925750J^2 - 339210078721896250000J$
	$+233702090524237500000)$
11	$q^{-55/6} - 22q^{-49/6} + 209q^{-43/6} - 1078q^{-37/6} + 2926q^{-31/6} - 1672q^{-25/6}$
	$-15169q^{-19/6} + 47234q^{-13/6} - 31350q^{-7/6} - 107426q^{-1/6}$
	$+218680q^{5/6} + \cdots$
	$= G_3G_2^2(J^8 - 5978J^7 + 14256527J^6 - 17312108670J^5$
	$+11327366012605J^4 - 3889904574252522J^3 + 631138185556080950J^2$
	$-38141443583282670180J + 473098671409604281800)$
12	$q^{-10} - 24q^{-9} + 252q^{-8} - 1472q^{-7} + 4830q^{-6} - 6048q^{-5} - 16744q^{-4}$
	$+84480q^{-3} - 113643q^{-2} - 115920q^{-1} + 534612 - 370920q + \cdots$
	$= J^{10} - 7464J^9 + 23101236J^8 - 38353325536J^7 + 36913772324730J^6$
	$-20784851556729552J^5 + 6580486714450069928J^4$
	$-1063011399511905159360J^3 + 72005127765018136775955J^2$
	$-1322204967509387392211000J + 14245837105866886701919 32$

Writing $Z = \mathfrak{w}_{pM}^s(z)$, $X = \mathfrak{w}_p(z)$, $Y = \mathfrak{w}_M(z/p)$, the different quantities are related via the algebraic equations

$$Z = X^s Y^s, \quad \Phi[\mathfrak{w}_p^{s_1}](X^{s_1}, J) = 0, \quad \Phi[\mathfrak{w}_M^{s_2}](Y^{s_2}, J') = 0, \quad \Phi_p(J, J') = 0,$$

and the variables can be eliminated via resultants to get a modular equation in Z and J, which has to be factored to get the correct polynomial.

4. Double η-quotients

4.1. Definition and statement of the result. For primes p_1 and p_2, let

$$\mathfrak{w}_{p_1,p_2}^s = \left(\frac{\eta(z/p_1)\eta(z/p_2)}{\eta(z/(p_1p_2))\eta(z)}\right)^s = \left(\frac{\mathfrak{w}_{p_1}(z)}{\mathfrak{w}_{p_1}(z/p_2)}\right)^s$$

where $s = 24/\gcd(24, (p_1-1)(p_2-1))$ is the smallest integer such that sr is an integer, where $r = (p_1-1)(p_2-1)/24$. Note that $s \mid 24$; and $s \mid 6$ when p_1 and p_2 are odd primes. It is shown in [7] that the function $\mathfrak{w}_{p_1,p_2}^s$ is a function on $\Gamma^0(p_1p_2)$; conjugates of $\mathfrak{w}_{p_1,p_2}^s$ are also computed, leading to properties of the modular equation $\Phi[\mathfrak{w}_{p_1,p_2}^s](X, J)$. This polynomial has X-degree $(p_1+1)(p_2+1)$ for $p_1 \neq p_2$ (resp. $p_1^2 + p_1$ if $p_1 = p_2$).

We can now state the result that we will prove in this section. More precise results are given along the proof.

THEOREM 4.1. *Let p_1, p_2 be two primes,*

$$N = p_1p_2, \qquad s = 24/\gcd(24, (p_1-1)(p_2-1)),$$

$e \neq s$ a divisor of s and $\delta = s/e$. If $N \equiv 1 \bmod \delta$ and the parameters are chosen in Table 2*, then there exists a modular equation $\Phi[(-1)^{\delta+1}\mathfrak{w}_{p_1,p_2}^e](X)$*

Table 2. Values of p_1 and p_2 leading to a modular equation $\Phi[(-1)^{\delta+1}\mathfrak{w}_{p_1,p_2}^e](X)$

p_1	p_2	s	e	δ
2	2	24	8	3
2	5 mod 12	6	2	3
2	11 mod 12	12	4	3
3	3	6	3	2
3	7 mod 12	2	1	2
3	11 mod 12	6	3	2
5 mod 12	5 mod 12	3	1	3
5 mod 12	11 mod 12	3	1	3
7 mod 12	7 mod 12	2	1	2
7 mod 12	11 mod 12	2	1	2
11 mod 12	11 mod 12	6	1	6

whose coefficients are polynomials in γ_3, γ_2, and which has the same X-degree as $\Phi[\mathfrak{w}^s_{p_1,p_2}](X, J)$.

The following lemma is used in the proof of the theorem.

LEMMA 4.2. *Let $\delta \in \{2, 3, 6\}$ be as above and suppose $N = p_1 p_2 \equiv 1 \bmod \delta$. Then $p_i \equiv -1 \bmod \delta$.*

Proof. For $\delta = 2$, $N \equiv 1 \bmod 2$ gives the conclusion. When $3 \mid \delta$, we cannot have $p_i = 3$ since $N \equiv 1 \bmod \delta$. For δ equal to 3 (resp. 6), surely we cannot have $p_i \equiv 1 \bmod 3$ (resp. 6). This leaves $p_i \equiv -1 \bmod 3$ (resp. 6). ∎

The proof of the theorem will use several intermediate results that we will present in a form as compact as possible. When $p_1 \neq p_2$, we will make the convention that p_1 is odd (so that we may have $p_2 = 2$). Moreover, we let u and v be two integers such that $up_1 + vp_2 = 1$. To simplify the proof, we will be mostly looking at properties using p_2, this case being complicated when $p_2 = 2$. Reciprocally, using p_1 and p_2 supposes that $p_1 \neq p_2$. The results and proofs are of course symmetric under exchanging p_1 and p_2. In case of equality, we will write $p_1 = p_2 = p$.

4.2. The conjugates of $\mathfrak{w}_{p_1,p_2}$. In [7] are given the conjugates of $\mathfrak{w}^s_{p_1,p_2}$ (with some minor typos). Here, we need the precise expansions of $\mathfrak{w}_{p_1,p_2}$. In view of Theorem 2.3, the value of $\mathfrak{w}_{p_1,p_2} \circ M$ can be written as

$$\mathfrak{w}_{p_1,p_2} \circ M = \mathrm{Jac}(M)\zeta_{24}^{\mathcal{E}(M)}\mathcal{Q}(M)\mathcal{N}(M)$$

where the first part cumulates Jacobi symbols, the second the exponents of ζ_{24}, the third is the product of the square roots and the last one the η-quotient. To ease notations, we also put $\phi = \zeta_{24}^{24r} = \zeta_{24}^{(p_1-1)(p_2-1)}$. We use the notations and philosophy of computations from [7].

PROPOSITION 4.3. *Let p_1 and p_2 be two primes. In all cases, we have the $N+1$ conjugate functions of Table 3. The remaining $p_1 + p_2$ conjugates are found in Table 4, where in the case of $C_{2,\nu}$, we set $\nu \equiv -(\mu p_1)^{-1} \bmod p_2$, $v_2 = (1 + p_1\mu\nu)/p_2$ for $\mu \neq 0$ (equivalently $\nu \neq 0$; $\mu = 0$ corresponds to $\nu = 0$). When $\nu > 0$, we get*

$$\theta_2(\nu) = \begin{cases} \mu((p_2+1)v_2 + 1) + \nu & \text{if } p_2 \neq 2, \\ (3p_1 + 2)(\nu + 1)/2 & \text{if } p_2 = 2. \end{cases}$$

Moreover

$$\theta_2(0) = \begin{cases} uv(p_2+1) + u - 1 & \text{if } p_2 \neq 2, \\ (3u + 2)(u - 1)/2 & \text{if } p_2 = 2. \end{cases}$$

Table 3. Conjugate functions for any N

M	$\mathfrak{w}_{p_1,p_2} \circ M$	ord	l
$T^\nu = \begin{pmatrix} 1 & \nu \\ 0 & 1 \end{pmatrix}$	$A_\nu(z) = \frac{\eta\left(\frac{z+\nu}{p_1}\right)\eta\left(\frac{z+\nu}{p_2}\right)}{\eta(z+\nu)\eta\left(\frac{z+\nu}{p_1p_2}\right)}$	$-\frac{r}{p_1p_2}$	$\zeta_N^{-\nu r}$
	$= \mathfrak{w}_{p_1,p_2}(z+\nu)$, $0 \le \nu < N$		
$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$B(z) = \frac{\eta(p_1z)\eta(p_2z)}{\eta(z)\eta(p_1p_2z)} = \mathfrak{w}_{p_1,p_2}(Nz)$	$-r$	1

Table 4. Conjugates for $p_1 \neq p_2$

M	$\mathfrak{w}_{p_1,p_2} \circ M$
$M_{1,\mu} = \begin{pmatrix} \mu p_2 & -1 \\ 1 & 0 \end{pmatrix}$	$C_{1,\nu}(z) = \phi^{\theta_1(\nu)}\varepsilon_1 \frac{\eta\left(\frac{z+\nu}{p_1}\right)\eta(p_2(z+\nu))}{\eta(z+\nu)\eta\left(\frac{p_2(z+\nu)}{p_1}\right)}$, $0 \le \nu < p_1$
$M_{1,0} = \begin{pmatrix} vp_2 & -up_1 \\ 1 & 1 \end{pmatrix}$	
$M_{2,\mu} = \begin{pmatrix} \mu p_1 & -1 \\ 1 & 0 \end{pmatrix}$	$C_{2,\nu}(z) = \phi^{\theta_2(\nu)}\varepsilon_2 \frac{\eta(p_1(z+\nu))\eta(\frac{z+\nu}{p_2})}{\eta(z+\nu)\eta\left(\frac{p_1(z+\nu)}{p_2}\right)}$, $0 \le \nu < p_2$
$M_{2,0} = \begin{pmatrix} up_1 & -vp_2 \\ 1 & 1 \end{pmatrix}$	

Also,

$$\varepsilon_2 = \begin{cases} \left(\dfrac{p_1}{p_2}\right) & \text{if } p_2 \neq 2, \\ 1 & \text{if } p_2 = 2. \end{cases}$$

For $i \in \{1,2\}$, the functions $C_{i,\nu}$ have order r/p_i and leading term $\phi^{\theta_i(\nu)}\varepsilon_i\zeta_{p_i}^{\nu r}$.

When $p_1 = p_2 = p$, we must consider the following $p-1$ conjugate functions:

matrix	$\mathfrak{w}_{p,p} \circ M$
$M_\mu = \begin{pmatrix} \mu p & -1 \\ 1 & 0 \end{pmatrix}$	$C_\nu(z) = \sqrt{p}\,\varepsilon(\nu)\zeta_{24}^{\theta(\nu)} \frac{\eta(pz)^2}{\eta(z)\eta(z+\nu/p)}$, $1 \le \nu < p$

where $1 = -\mu\nu + vp$, $\varepsilon(\nu) = \left(\frac{-\nu}{p}\right)$ if p is odd (resp. 1 when $p=2$) and

$$\theta(\nu) = \begin{cases} p\nu(1-\mu^2) + (-3p+2+v)\mu - 3 + 3p & \text{if } p \text{ is odd}, \\ 0 & \text{if } p = 2. \end{cases}$$

Moreover, $C_\nu(z)$ has order $(p-1)/12$ and leading coefficient

$$\sqrt{p}\,\varepsilon(\nu)\zeta_{24p}^{p\theta(\nu)-\nu}.$$

Proof. The cases of the A_ν matrices and of B are treated without difficulty, as in [7]. The value of $\mathcal{Q}(M)$ is 1, unless we are dealing with the

case $p_1 = p_2 = p$. The computations for the C matrices involve non-zero exponents for ζ_{24}.

Case $p_1 \neq p_2$. Following [7], we first prove the result for $C_{2,\nu}$ when $\nu > 0$. Iterate over $1 \leq \mu < p_2$ and define $\nu = -(\mu p_1)^{-1} \bmod p_2 \in \{1, \ldots, p_2 - 1\}$, $v_2 = (1 + \mu\nu p_1)/p_2$. Note that $\nu \mapsto \mu$ is an involution and the corresponding v_2's are equal. Moreover, iterating over $1 \leq \mu < p_2$ is the same as iterating over $1 \leq \nu < p_2$. We find

$$\mathcal{N}(M_{2,\mu}) = \frac{\eta(p_1 z)\eta((z+\nu)/p_2)}{\eta(z)\eta(p_1(z+\nu)/p_2)} = \zeta_{24}^{\nu(1-p_1)} \frac{\eta(p_1(z+\nu))\eta((z+\nu)/p_2)}{\eta(z+\nu)\eta(p_1(z+\nu)/p_2)}.$$

(a) Assume first $p_2 \neq 2$. We compute $\mathrm{Jac}(M_{2,\mu}) = \left(\frac{p_1}{p_2}\right)$, and the total exponent of ζ_{24} is

$$\begin{aligned}
&\nu(1-p_1) + \mathcal{E}(M_{2,\mu}) \\
&\qquad = (p_1 - 1)(p_2 \nu p_1 \mu^2 + p_2 \nu + 2\mu p_2 - \mu v_2 - \nu - \mu) \\
&\qquad = (p_1 - 1)\big((p_2 - 1)(\nu\mu^2 p_1 + \nu + 2\mu) + \mu(1 - v_2 + \mu\nu p_1)\big) \\
&\qquad = (p_1 - 1)(p_2 - 1)(\nu\mu^2 p_1 + \nu + 2\mu + \mu v_2) \\
&\qquad = (p_1 - 1)(p_2 - 1)\big(\mu((p_2 + 1)v_2 + 1) + \nu\big)
\end{aligned}$$

where we have used $p_2 v_2 = 1 + \mu\nu p_1$ twice.

When $p_2 = 2$, we find $\mathrm{Jac}(M_{2,\mu}) = 1$ and the total exponent of ζ_{24} is

$$\nu(1-p_1) + \mathcal{E}(M_{2,\mu}) = (p_1 - 1)\big(3p_1\mu^2(\nu + 1) + \mu(3\mu - 1) + \nu\big)/2.$$

Since ν is odd, we have $\mu = 1$ and the exponent reduces to

$$(p_1 - 1)(3p_1 + 2)(\nu + 1)/2.$$

(b) For $C_{2,0}$,

$$\mathcal{N}(M_{2,0}) = \frac{\eta(p_1(z+1))\eta(z/p_2)}{\eta(z+1)\eta(p_1 z/p_2)} = \zeta_{24}^{p_1 - 1} \frac{\eta(z/p_2)\eta(p_1 z)}{\eta(z)\eta(p_1 z/p_2)}.$$

Assume first $p_2 \neq 2$. Then $\mathrm{Jac}(M_{2,0}) = \left(\frac{p_1}{p_2}\right)$ and the exponent of ζ_{24} is

$$\begin{aligned}
p_1 - 1 + \mathcal{E}(M_{2,0}) &= -(p_1 - 1)\big((p_2 - 1)(p_1 u^2 - 2u + 1) + u(p_1 u + v - 1)\big) \\
&= -24r(p_1 u^2 - 2u + 1 - uv) = 24r(uv(p_2 + 1) + u - 1).
\end{aligned}$$

When $p_2 = 2$, we find $\mathrm{Jac}(M_{2,0}) = 1$ and the total exponent of ζ_{24} is

$$(p_1 - 1)(3u + 2)(u - 1)/2.$$

Case $p_1 = p_2 = p$. In all cases,

$$\mathcal{N}(M_\mu) = \sqrt{p} \frac{\eta(pz)^2}{\eta(z)\eta(z + \nu/p)}$$

where $1 = -\mu\nu + vp$.

When $p \neq 2$, we find $\mathrm{Jac}(M_\mu) = \left(\frac{\mu}{p}\right)$ and the exponent given by $\theta(\nu)$. When $p = 2$, $\mathrm{Jac}(M_\mu) = 1$ and the exponent given by $v - 1 = 0$. ∎

4.3. Action of T and S. This section is devoted to the proofs of the actions of T and S on our basic functions as stated in the following two propositions.

PROPOSITION 4.4.

(i) $B \circ T = \phi^{-1} B$.
(ii) *For* $0 \leq \nu < N-1$, *we have* $A_\nu \circ T = A_{\nu+1}$ *and* $A_{N-1} \circ T = \phi^{-1} A_0$.
(iii) *For* $0 \leq \nu < p_2 - 1$, $C_{2,\nu} \circ T = \phi^{\theta_2(\nu)-\theta_2(\nu+1)} C_{2,\nu+1}$; *moreover,* $C_{2,p_2-1} \circ T = \phi^{\theta_2(p_2-1)-\theta_2(0)+1} C_{2,0}$.
(iv) *For* $1 \leq \nu < p$, $C_\nu \circ T = \zeta_{24}^{2p-2} C_\nu$.

Proof. (i), (ii) and (iv) are direct applications of Theorem 2.3.

(iii) For $0 \leq \nu < p_2 - 1$, one has $C_{2,\nu} \circ T = \phi^{\theta_2(\nu)-\theta_2(\nu+1)} C_{2,\nu+1}$. For $\nu = p_2 - 1$,

$$\begin{aligned} C_{2,p_2-1} \circ T &= \phi^{\theta_2(p_2-1)} \varepsilon_2 \frac{\eta\left(\frac{z+p_2}{p_2}\right)\eta(p_1(z+p_2))}{\eta(z+p_2)\eta\left(\frac{p_1(z+p_2)}{p_2}\right)} \\ &= \phi^{\theta_2(p_2-1)} \varepsilon_2 \frac{\eta\left(\frac{z}{p_2}+1\right)\eta(p_1 z + N)}{\eta(z+p_2)\eta\left(\frac{p_1 z}{p_2}+p_1\right)} \\ &= \phi^{\theta_2(p_2-1)} \varepsilon_2 \zeta_{24}^{1+N-p_1-p_2} \frac{\eta\left(\frac{z}{p_2}\right)\eta(p_1 z)}{\eta(z)\eta\left(\frac{p_1 z}{p_2}\right)} \\ &= \phi^{1+\theta_2(p_2-1)-\theta_2(0)} C_{2,0}. \ ∎ \end{aligned}$$

PROPOSITION 4.5. *For all primes* p_1 *and* p_2, *one has:*

(i) $(A_0, B) \circ S = (B, A_0)$.
(ii) *When* $0 < \nu < p_1 p_2$ *and* $\gcd(\nu, p_1 p_2) = 1$,

$$A_\nu \circ S = \phi^{\theta_3(\nu)} A_\omega$$

where $1 = -\omega\nu + v_{12}(p_1 p_2)$ *and*

$$\theta_3(\nu) = \begin{cases} -\omega\nu^2 - 2\nu + \omega + 3 + \nu v_{12} & \text{if } p_2 \neq 2, \\ \omega + \nu(v_{12}(1-2p_1)+2) & \text{if } p_2 = 2. \end{cases}$$

Suppose from now on that $p_1 \neq p_2$. *The following hold:*

(iii) *When* $0 < \nu = p_1 \rho < p_1 p_2$,

$$A_\nu \circ S = \phi^{\theta_4(\rho)} C_{2,\varpi}$$

where $1 = -\varpi\nu + wp_2$, *and*

$$\theta_4(\rho) = \begin{cases} -\theta_2(\varpi) + \rho(w(p_2+1)+1) + \varpi & \text{if } p_2 \neq 2, \\ -\theta_2(\varpi) + 3\frac{p_1+1}{2}\rho^2 + \rho(3w-2) + \varpi & \text{if } p_2 = 2. \end{cases}$$

(iv) *When* $0 < \nu < p_2$, *we have* $\mu \equiv -1/(\nu p_1) \bmod p_2$ *and*

$$C_{2,\nu} \circ S = A_{\mu p_1}.$$

(v) *We have*

$$C_{2,0} \circ S = C_{1,0} \times \begin{cases} \phi^{-2\theta_1(0)} & \text{if } p_2 \neq 2, \\ \phi^{-\theta_1(0)+(u^2 p_1(p_1+1)/2+(1-u)/2)} & \text{if } p_2 = 2. \end{cases}$$

Proof. (i) We first get

$$w_{p_1,p_2} \circ (T^\nu \circ S) = w_{p_1,p_2} \circ \begin{pmatrix} \nu & -1 \\ 1 & 0 \end{pmatrix}$$

and the case $\nu = 0$ yields immediately $A_0 \circ S = B$. On the other hand, we also have the reassuring result that

$$B \circ S = \mathfrak{w}_{p_1,p_2}(-N/z) = \mathfrak{w}_{p_1,p_2}(z) = A_0(z).$$

(ii) When $\gcd(\nu, p_1p_2) = 1$, we write $1 = -\omega\nu + v_{12}(p_1p_2)$, and find

$$\mathcal{N}(M_{2,\mu} \circ S) = \frac{\eta((z+\omega)/p_1)\eta((z+\omega)/p_2)}{\eta(z)\eta((z+\omega)/(p_1p_2))} = \zeta_{24}^{\omega} A_\omega.$$

When $p_2 \neq 2$, $\mathrm{Jac}(M_{2,\mu} \circ S) = 1$ and the total exponent of ζ_{24} is

$$\begin{aligned} &\omega + \mathcal{E}(M_{2,\mu} \circ S) \\ &\quad = -\omega\nu^2(24r-1) + \nu\big(-48r + 1 + v_{12}(1-p_1-p_2)\big) + 24r(\omega+3) \\ &\quad = 24r(-\omega\nu^2 - 2\nu + \omega + 3) + \nu\big(\omega\nu + 1 + v_{12}(1-p_1-p_2)\big) \\ &\quad = 24r(-\omega\nu^2 - 2\nu + \omega + 3 + \nu v_{12}) = 24r\theta_3(\nu). \end{aligned}$$

When $p_2 = 2$, we also have $\mathrm{Jac}(M_{2,\mu} \circ S) = 1$ and the exponent of ζ_{24} becomes

$$(p_1 - 1)\big(\omega + \nu(v_{12}(1-2p_1)+2)\big).$$

Similar computations show that the result also holds for $p_1 = p_2 = 2$.

(iii) Suppose now that $\nu = \rho p_1$, $1 \leq \rho < p_2$. We write $1 = -\varpi\nu + wp_2$. In all cases

$$\begin{aligned} \mathcal{N}(M_{2,\mu} \circ S) &= \frac{\eta(p_1 z)\eta((z+\varpi)/p_2)}{\eta(z)\eta(p_1(z+\varpi)/p_2)} \\ &= \zeta_{24}^{-p_1\varpi+\varpi} \frac{\eta(p_1(z+\varpi))\eta((z+\varpi)/p_2)}{\eta(z+\varpi)\eta(p_1(z+\varpi)/p_2)} \\ &= \zeta_{24}^{-p_1\varpi+\varpi} (\phi^{-\theta_2(\varpi)} \varepsilon_2 C_{2,\varpi}). \end{aligned}$$

Assume $p_2 \neq 2$. We get $\mathrm{Jac}(M_{2,\mu} \circ S) = \left(\frac{p_1}{p_2}\right)$. The partial exponent is given by

$$\begin{aligned}
&-\varpi(p_1-1) + \mathcal{E}(M_{2,\mu} \circ S) \\
&\qquad = (p_1-1)\big(p_2 p_1 \varpi \rho^2 + (-w+2p_2-1)\rho + (p_2-1)\varpi\big) \\
&\qquad = (p_1-1)\big(p_2 \rho(p_1 \rho \varpi) + (-w+2p_2-1)\rho + (p_2-1)\varpi\big) \\
&\qquad = (p_1-1)\big(p_2 \rho(w p_2 - 1) + (-w+2p_2-1)\rho + (p_2-1)\varpi\big) \\
&\qquad = (p_1-1)(p_2-1)\big(\rho(w(p_2+1)+1) + \varpi\big),
\end{aligned}$$

yielding the final result.

When $p_2 = 2$, we find $\mathrm{Jac}(M_{2,\mu} \circ S) = 1$ and

$$-\varpi(p_1-1) + \mathcal{E}(M_{2,\mu} \circ S) = (p_1-1)\left(\rho(3w-2) + 3\frac{p_1+1}{2}\rho^2 + \varpi\right).$$

(iv) For $1 \leq \nu < p_2$, we compute $\mu \equiv -1/(\nu p_1) \bmod p_2$ and

$$\begin{aligned}
C_{2,\nu} \circ S &= \mathfrak{w}_{p_1,p_2} \circ \begin{pmatrix} \mu p_1 & -1 \\ 1 & 0 \end{pmatrix} \circ S \\
&= \frac{\eta((z+p_1\mu)/p_1)\eta((z+p_1\mu)/p_2)}{\eta(z+p_1\mu)\eta((z+p_1\mu)/(p_1p_2))} = A_{p_1\mu}.
\end{aligned}$$

(v) In all cases, we compute

$$\begin{aligned}
\mathrm{Jac}(M \circ S)\mathcal{N}(M \circ S) &= \left(\frac{p_2}{p_1}\right)\frac{\eta(z/p_1)\eta(p_2 z - p_2)}{\eta(z-1)\eta(p_2 z/p_1)} \\
&= \left(\frac{p_2}{p_1}\right)\zeta_{24}^{1-p_2}\frac{\eta(z/p_1)\eta(p_2 z)}{\eta(z)\eta(p_2 z/p_1)}.
\end{aligned}$$

When $p_2 \neq 2$, this yields

$$\mathrm{Jac}(M \circ S)\mathcal{N}(M \circ S) = \zeta_{24}^{1-p_2}\phi^{-\theta_1(0)}C_{1,0}.$$

The exponent of ζ_{24} is

$$\begin{aligned}
1 - p_2 + \mathcal{E}(M \circ S) &= (p_2-1)\big(p_1 p_2 v^2 + (u+1-2p_1)v + p_1 - 1\big) \\
&= (p_1-1)(p_2-1)\big(-uv(p_1+1) - v + 1\big) \\
&= 24r\big(-uv(p_1+1) - v + 1\big) = -24r\theta_1(0),
\end{aligned}$$

so that $C_{2,0} \circ S = \phi^{-2\theta_1(0)}C_{1,0}$.

When $p_2 = 2$, the exponent of ζ_{24} becomes

$$-1 + \mathcal{E}(M \circ S) = (p_1-1)\left(u^2 p_1 \frac{p_1+1}{2} + \frac{1-u}{2}\right),$$

so that the final value is

$$\phi^{-\theta_1(0)+(u^2p_1(p_1+1)/2+(1-u)/2)}C_{1,0}. \ \blacksquare$$

PROPOSITION 4.6. *Suppose that $p_1 = p_2 = p$. Then:*

(i) *When $\nu = \rho p$, $1 \le \rho < p$, set $1 = -\varpi\rho + wp$. Then $A_\nu \circ S = C_\varpi$.*

(ii) *For all p, and all $1 \le \nu < p$, one has $C_\nu \circ S = A_{\mu p}$ where $\mu \equiv -1/\nu \bmod p$.*

Proof. (i) When $p \neq 2$,

$$\begin{aligned} A_\nu \circ S &= \sqrt{p}\left(\frac{\rho}{p}\right)\frac{\eta(pz)^2}{\eta(z)\eta(z+\varpi/p)}\zeta_{24}^{-\rho^2 p\varpi+(-3p+2+w)\rho+p\varpi-3+3p} \\ &= \sqrt{p}\left(\frac{-\varpi}{p}\right)\left((1/\sqrt{p})\varepsilon(\varpi)\zeta_{24}^{-\theta(\varpi)}C_\varpi\right)\zeta_{24}^{-\rho^2 p\varpi+(-3p+2+w)\rho+p\varpi-3+3p} \\ &= \zeta_{24}^{-\rho^2 p\varpi+(-3p+2+w)\rho+p\varpi-3+3p-\theta(\varpi)}C_\varpi = C_\varpi \end{aligned}$$

using $\theta(\varpi) = p\varpi(1-\rho^2) + (-3p+2+w)\rho - 3 + 3p$.

When $p = 2$, we have $\rho = 1$, implying $\varpi = w = 1$ and

$$A_2 \circ S = \sqrt{2}\,\zeta_{24}^{w-1}\frac{\eta(2z)^2}{\eta(z)\eta(z+\varpi/2)} = \zeta_{24}^{-\theta(2)}C_1 = C_1.$$

(ii) In all cases, we get

$$C_\nu \circ S = \frac{\eta((z+p\mu)/p)^2}{\eta(z+p\mu)\eta((z+p\mu)/p^2)} = A_{\mu p}. \ \blacksquare$$

4.4. Finding invariant functions. The idea is simple. Using the explicit actions given above, we need to find suitable modifications of the functions B, A_ν, $C_{1,\nu}$, $C_{2,\nu}$ such that the action of T and S on any power sum coincides with the action on γ_2, γ_3 or the product $\gamma_2\gamma_3$, as given in Section 4.3.

Note that $B^e \circ T = \zeta_{24}^{-24re}B^e$. Write $re = t/\delta$ and observe that this fraction is irreducible (s being prime to t implies δ is). This leads to setting $\chi = \phi^{-e} = \zeta_{24}^{-24re} = \zeta_\delta^{-t}$, a primitive δth root of unity.

The aim of this section is to prove the following theorem from which Theorem 4.1 will follow.

THEOREM 4.7. *Under the assumptions of Theorem* 4.1*, define the functions*

$$\begin{gathered} A'_\nu = \chi^{\alpha_0-\nu}A_\nu^e, \quad B' = B^e; \\ C'_{1,\nu} = \chi^{\theta_1(\nu)-\nu}C_{1,\nu}^e, \quad C'_{2,\nu} = \chi^{\theta_2(\nu)-\nu}C_{2,\nu}^e; \\ C'_\nu = \chi^\mu C_\nu^e, \end{gathered}$$

where $\mu \equiv -1/\nu \bmod p$ and

$$\alpha_0 = \begin{cases} 1 & \text{if } \delta = 2, \\ 0 & \text{if } \delta = 3, \\ 3 & \text{if } \delta = 6, \end{cases}$$

making $\chi^{\alpha_0} = (-1)^{\delta+1} = \chi^{-\alpha_0} = \chi^{-3}$. *Then, for all integers* k, *the quantity*

$$\mathcal{S}_k = B'^k + \sum_{\nu=0}^{N-1} A_\nu'^k + \sum_{\nu=0}^{p_1-1} C_{1,\nu}'^k + \sum_{\nu=0}^{p_2-1} C_{2,\nu}'^k = B'^k + \mathcal{S}_{A,k} + \mathcal{S}_{C_1,k} + \mathcal{S}_{C_2,k}$$

satisfies $\mathcal{S}_k \circ (T,S) = (\chi^k, \chi^{\alpha_0 k})\mathcal{S}_k$.

With these notations, we have

PROPOSITION 4.8. *The following hold:*

(a) $B' \circ T = \chi B'$.
(b) $\{A'_\nu\}_\nu \circ T = \{\chi A'_\nu\}_\nu$.
(c) $\{C'_{i,\nu}\}_\nu \circ T = \{\chi C'_{i,\nu}\}_\nu$.
(d) *For all* ν, $C'_\nu \circ T = \chi C'_\nu$.

Proof. (a) and (c) follow easily from Proposition 4.4.

(b) We first obtain $A^e_{N-1} \circ T = \chi A^e_0$. Let us explain where the choice A'_ν comes from. For some function α to be specified later, set $A'_\nu = \chi^{\alpha(\nu)} A^e_\nu$, so that

$$A'_\nu \circ T = \chi^{\alpha(\nu)} A^e_{\nu+1} = \chi^{\alpha(\nu)-\alpha(\nu+1)} A'_{\nu+1},$$
$$A'_{N-1} \circ T = \chi^{\alpha(N-1)} \chi A^e_0 = \chi^{\alpha(N-1)+1-\alpha(0)} A'_0.$$

We must find α such that

$$\alpha(\nu) - \alpha(\nu+1) \equiv 1 \bmod \delta, \qquad 0 \le \nu < N-1,$$

and

$$\alpha(N-1) - \alpha(0) + 1 \equiv 1 \bmod \delta.$$

The first set of equations gives us $\alpha(\nu) \equiv \alpha(0) - \nu \bmod \delta$ and the second $\alpha(0) - (N-1) \equiv \alpha(0) \bmod \delta$, which is possible only when $N \equiv 1 \bmod \delta$. Setting $\alpha_0 = \alpha(0)$ yields the result.

(d) Proposition 4.4 gives us $C'_\nu \circ T = \zeta_{24}^{2e(p-1)} C'_\nu$. A glance at Table 2 shows that $p^2 - 1 \equiv 0 \bmod (24/e)$, which implies $2e(p-1) \equiv -(p-1)^2 e \bmod 24$ and therefore $\zeta_{24}^{2e(p-1)} = \chi$. ∎

The actual value of α is in fact dictated by the other invariance properties that follow.

REMARK. This proposition shows at the same time that we cannot expect any nice T-action when $N \not\equiv 1 \bmod \delta$.

Let us turn our attention to the S-action on our candidate functions, using the notations of Proposition 4.5.

PROPOSITION 4.9.

(i) $(B', A'_0) \circ S = \chi^{\alpha_0}(A'_0, B')$.
(ii) *When* $\gcd(\nu, p_1 p_2) = 1$, $A'_\nu \circ S = \chi^{\alpha_0} A'_\omega$.

(iii) *For* $\nu = p_1\rho$, $A'_\nu \circ S = \chi^{\alpha_0} C'_{2,\varpi}$.
(iv) *For* $1 \le \nu < p_2$, $\mu \equiv -1/(\nu p_1) \bmod p_2$ *and* $C'_{2,\nu} \circ S = \chi^{\alpha_0} A'_{\mu p_1}$.
(v) $C'_{2,0} \circ S = \chi^{\alpha_0} C'_{1,0}$.
(vi) *For* $\nu = \rho p$, $1 \le \rho < p$, *set* $1 = -\varpi\rho + wp$. *For all* p, $A'_\nu \circ S = \chi^{\alpha_0} C'_\varpi$.
(vii) *For* $1 \le \nu < p$, *setting* $\mu \equiv -1/\nu \bmod p$, *we have* $C'_\nu \circ S = \chi^{\alpha_0} A'_{\mu p}$.

Proof. (i) We have $B' \circ S = \chi^{-\alpha_0} A'_0$ and $A'_0 \circ S = \chi^{\alpha_0} B'$, and the result follows from $\chi^{-\alpha_0} = \chi\alpha_0$.

(ii) Proposition 4.5 can be rewritten

$$A'_\nu \circ S = \chi^{\omega-\nu-\theta_3(\nu)} A'_\omega$$

and we simplify the exponent using $1 = -\omega\nu + v_{12} \bmod \delta$, which leads to

$$A'_\nu \circ S = A'_\omega \begin{cases} \chi^{-3} & \text{if } p_2 \neq 2, \\ \chi^{\nu(-3+v_{12}(2p_1-1))} & \text{if } p_2 = 2. \end{cases}$$

When $p_2 \neq 2$, we use $\chi^{-3} = \chi^{\alpha_0}$. The case $p_2 = 2$ can occur only for $\delta = 3$, in which case $p_1 \equiv -1 \bmod 3$ and the exponent of χ is 0.

(iii) For $\nu = \rho p_1$ we use $1 = -\varpi\nu + wp_2$ to get

$$A^e_\nu \circ S = \chi^{-\theta_4(\rho)} C^e_{2,\varpi},$$

so that

$$\chi^{-\alpha_0+\nu} A'_\nu \circ S = \chi^{-\theta_4(\rho)} \chi^{\varpi-\theta_2(\varpi)} C'_{2,\varpi},$$

and we simplify:

$$-\theta_4(\rho) - \theta_2(\varpi) + \alpha_0 + \varpi - \nu.$$

Using the definition of θ_4, we get

$$A'_\nu \circ S = C'_{2,\varpi} \begin{cases} \chi^{\alpha_0-\rho((p_2+1)w+p_1+1)} & \text{if } p_2 \neq 2, \\ \chi^{\alpha_0-\rho((3\frac{p_1+1}{2})\rho+p_1+3w-2)} & \text{if } p_2 = 2, \end{cases}$$

and we conclude using $p_i \equiv -1 \bmod \delta$.

(iv) For $1 \le \nu < p_2$, we compute $\mu \equiv -1/(\nu p_1) \bmod p_2$ and

$$C'_{2,\nu} \circ S = \chi^{\theta_2(\nu)-\nu} A^e_{\mu p_1} = \chi^{\theta_2(\nu)-\nu-\alpha_0+\mu p_1} A'_{\mu p_1}.$$

Simplifying the exponent gives

$$C'_{2,\nu} \circ S = A'_{\mu p_1} \begin{cases} \chi^{-\alpha_0+\mu((p_2+1)v_2+p_1+1)} & \text{if } p_2 \neq 2, \\ \chi^{-\alpha_0+4p_1+1} & \text{if } p_2 = 2, \end{cases}$$

where for $p_2 = 2$, we used $\nu = \mu = 1$. We conclude as in (iii).

(v) When $p_2 \neq 2$, we start from

$$C^e_{2,0} \circ S = \chi^{2\theta_1(0)} C^e_{1,0},$$

which yields

$$\chi^{-\theta_2(0)} C'_{2,0} \circ S = \chi^{\theta_1(0)} C'_{1,0},$$

so

$$C'_{2,0} \circ S = \chi^{\theta_1(0)+\theta_2(0)} C'_{1,0},$$

and the exponent is

$$uv(p_1 + p_2 + 2) + u + v - 2.$$

This quantity is $\equiv u + v - 2 \bmod \delta$ since $p_i \equiv -1 \bmod \delta$. Moreover $1 \equiv p_1(u + v) \bmod \delta$ and finally the exponent is $-3 \bmod \delta$.

When $p_2 = 2$, we have

$$\chi^{-\theta_2(0)} C'_{2,0} \circ S = \chi^{-(u^2 p_1 \frac{p_1+1}{2} + \frac{1-u}{2})} C'_{1,0},$$

so

$$C'_{2,0} \circ S = \chi^{-\frac{(p_1^2+p_1-3)u^2-3}{2}} C'_{1,0},$$

and this is χ^0 since this can only happen when $\delta = 3$.

(vi) Since $1 = -\varpi\rho + wp$, we can write

$$A'_\nu \circ S = \chi^{\alpha_0-\nu-\kappa(\varpi)} C'_\varpi,$$

and the result comes from the definition of κ.

(vii) We have $C^e_\nu \circ S = A^e_{\mu p}$, so that

$$C'_\nu \circ S = \chi^{\kappa(\nu)} \chi^{-\alpha_0+\mu p} A'_{\mu p},$$

and we conclude as in (vi). ∎

4.5. Properties of the modular equation. From the preceding sections, we see that

$$\Phi(F) = (F - B') \prod_{\nu=0}^{N-1} (F - A'_\nu) \prod_{\nu=0}^{p_1-1} (F - C'_{1,\nu}) \prod_{\nu=0}^{p_2-1} (F - C'_{2,\nu})$$

is a modular equation whose coefficients can be expressed in terms of j, γ_2 or γ_3 depending on the value of δ. Before doing this, we may express these coefficients as Puiseux series.

PROPOSITION 4.10. *With the usual notations:*

(a) *the coefficient of smallest order of* Φ *is* q^{-2re}*;*
(b) *the trace has order* re*;*
(c) *when* $p_1 \neq p_2$, $\Phi(0) = 1$*;*
(d) *when* $p_1 = p_2 = p$, $\Phi(0) = (-p)^{e(p-1)/2}$ *when* p *is odd and* 2^4 *when* $p = 2$.

Proof. (a) The coefficient of smallest order comes from the coefficient of $F^{\psi(N)-N-1}$ which has the order of $B' \prod_{\nu=0}^{N-1} A'_\nu$, that is,

$$-re + \sum_{\nu=0}^{N-1} \frac{-re}{N} = -2re.$$

When $p_1 \neq p_2$, $\psi(N) - N - 1 = p_1 + p_2$; when $p_1 = p_2 = p$, this is $p - 1$. Note that all other terms have orders strictly less than this bound.

As an example, when $s = e$, the degree of the equation in J is $2rs$ and the corresponding term is $J^{2rs}F^{\psi(N)-N-1}$.

Moreover

$$\begin{aligned} B' \prod_{\nu=0}^{N-1} A'_\nu &= \Big(\prod_{\nu=0}^{N-1} \chi^{\alpha_0-\nu}\Big)\zeta_N^{-reN(N-1)/2} q^{-2re}(1+\cdots) \\ &= \chi^{N\alpha_0-N(N-1)/2}\zeta_{24N}^{-24reN(N-1)/2} q^{-2re}(1+\cdots) \\ &= \chi^{\alpha_0-N(N-1)/2}\zeta_{24N}^{-24reN(N-1)/2} q^{-2re}(1+\cdots), \end{aligned}$$

using $N \equiv 1 \bmod \delta$. When N is odd, this reduces to

$$\chi^{\alpha_0-N(N-1)/2+(N-1)/2} q^{-2re}(1+\cdots) = \chi^{\alpha_0-(N-1)^2/2} q^{-2re}(1+\cdots).$$

(b) The dominant term in the sum of the conjugates is that of B', namely q^{-re}.

(c) For $p_1 \neq p_2$,

$$\begin{aligned} \prod_{\nu=0}^{p_2-1} C'_{2,\nu} &= \prod_{\nu=0}^{p_2-1} \chi^{\theta_2(\nu)-\nu}\chi^{-\theta_2(\nu)}\varepsilon_2^e \zeta_{p_2}^{\nu re} q^{er/p_2}(1+\cdots) \\ &= \chi^{-p_2(p_2-1)/2}\varepsilon_2^{p_2 e}\zeta_{p_2}^{rep_2(p_2-1)/2} q^{er}(1+\cdots). \end{aligned}$$

Multiplying all together, we find the norm to be of valuation 0, hence a constant

$$\begin{aligned} \vartheta &= \chi^{\alpha_0-N(N-1)/2}\zeta_{24N}^{-24reN(N-1)/2} \\ &\quad \cdot \chi^{-p_1(p_1-1)/2}\varepsilon_1^{p_1 e}\zeta_{p_1}^{rep_1(p_1-1)/2}\chi^{-p_2(p_2-1)/2}\varepsilon_2^{p_2 e}\zeta_{p_2}^{rep_2(p_2-1)/2} \\ &= (\varepsilon_1^{p_1}\varepsilon_2^{p_2})^e \chi^{\alpha_0-N(N-1)/2-p_1(p_1-1)/2-p_2(p_2-1)/2}\zeta_{24N}^{-24reN((N-1)/2-(p_1+p_2-2)/2)}. \end{aligned}$$

When $p_2 = 2$ (with p_1 odd), we have $\delta = 3$ always, meaning $\alpha_0 = 0$ and $N \equiv 1 \bmod 3$. Therefore, noting that e is always even,

$$\vartheta = \left(\frac{2}{p_1}\right)^{p_1 e} \chi^1 \zeta_{24N}^{-24reN(p_1-1)/2} = \chi^{(p_1+1)/2} = 1$$

since $p_1 \equiv -1 \bmod 3$.

When $p_2 \neq 2$, both p_i being odd, we may use the quadratic reciprocity law to find

$$\begin{aligned} \vartheta &= (-1)^{e(p_1-1)(p_2-1)/4}\chi^{\alpha_0-N(N-1)/2-p_1(p_1-1)/2-p_2(p_2-1)/2} \\ &\quad \cdot \zeta_{24N}^{-24reN((N-1)/2-(p_1+p_2-2)/2)}. \end{aligned}$$

Since $p_1 + p_2 - 2$ is even, we obtain

$$\begin{aligned}\vartheta &= \zeta_{24}^{3(24re)}\chi^{\alpha_0 - N(N-1)/2 - p_1(p_1-1)/2 - p_2(p_2-1)/2 + (N-1)/2 - (p_1+p_2-2)/2}\\ &= \chi^{\alpha_0 - 3 - N(N-1)/2 - p_1(p_1-1)/2 - p_2(p_2-1)/2 + (N-1)/2 - (p_1+p_2-2)/2}\\ &= \chi^{-N(N-1)/2 - p_1(p_1-1)/2 - p_2(p_2-1)/2 + (N-1)/2 - (p_1+p_2-2)/2},\end{aligned}$$

and by inspection, this is always 1.

(d) When $p_1 = p_2 = p$, we get

$$\begin{aligned}\prod_{\nu=1}^{p-1} C'_\nu &= \prod_{\nu=1}^{p-1} \chi^{\kappa(\nu)} p^{e/2} \varepsilon(\nu)^e \zeta_{24}^{e\theta(\nu)} \zeta_{24p}^{-e\nu} q^{e(p-1)/12}(1 + \cdots)\\ &= \chi^{p(p-1)/2} p^{e(p-1)/2} \Big(\prod_{\nu=1}^{p-1} \varepsilon(\nu)\Big)^e \zeta_{24}^{e\sum_{\nu=1}^{p-1}\theta(\nu)} \zeta_{24p}^{-ep(p-1)/2} q^{2er}(1 + \cdots).\end{aligned}$$

The quantity $\prod_{\nu=1}^{p-1} \varepsilon(\nu)$ is 1 for $p = 2$; when p is odd,

$$\prod_{\nu=1}^{p-1} \varepsilon(\nu) = \left(\frac{(-1)^{p-1}(p-1)!}{p}\right) = \left(\frac{-1}{p}\right)$$

using Wilson's theorem.

When $p = 2$, $e = 8$, $\delta = 3$, we find

$$\begin{aligned}\vartheta &= \chi^{\alpha_0 - N(N-1)/2} \zeta_{24N}^{-24reN(N-1)/2} \chi^{p(p-1)/2} p^{e(p-1)/2} \zeta_{24}^{e\sum_{\nu=1}^{p-1}\theta(\nu)} \zeta_{24p}^{-ep(p-1)/2}\\ &= \chi^{0-6} \zeta_{96}^{-8\cdot 4\cdot 3/2} \chi^1 2^4 \zeta_{48}^{-8} = 2^4.\end{aligned}$$

When p is odd,

$$\begin{aligned}\vartheta = \left(\frac{-1}{p}\right)^e &\chi^{\alpha_0 - N(N-1)/2 + p(p-1)/2} p^{e(p-1)/2}\\ &\cdot \zeta_{24N}^{-24reN(N-1)/2} \zeta_{24}^{e(-(p-1)/2 + \sum_{\nu=1}^{p-1}\theta(\nu))}.\end{aligned}$$

Now,

$$\begin{aligned}\sum_{\nu=1}^{p-1} \theta(\nu) &= \sum_{\nu=1}^{p-1} p\nu(1-\mu^2) + (-3p + 2 + v)\mu - 3 + 3p\\ &= (p - 3p + 2)S_0 + 3(p-1)^2 + \sum_{\nu=1}^{p-1} -p\nu\mu^2 + v\mu\end{aligned}$$

where $S_0 = \sum_{\nu=1}^{p-1} \nu$. Using $1 = -\mu\nu + vp$, the sum becomes

$$\sum_{\nu=1}^{p-1} p\mu(1 - vp) + v\mu = \sum_{\nu=1}^{p-1} \mu(p - vp^2 + v) \equiv pS_0 \bmod 24$$

in all cases: when $p > 3$, $p^2 \equiv 1 \bmod 24$; when $p = 3$, $\nu = 1$ (resp. $\nu = -1$) leads to $\mu = -1$, $v = 0$ (resp. $\mu = 1$, $v = 0$). Therefore, the exponent of ζ_{24} is

$$\equiv e\big(-(p-1)/2 + (-p+2)S_0 + 3(p-1)^2\big) \equiv -e(p-7)(p-1)^2/2 \bmod 24,$$

so that

$$\begin{aligned}\vartheta &= \left(\frac{-1}{p}\right)^e p^{e(p-1)/2} \zeta_{24N}^{-24reN(N-1)/2} \chi^{\alpha_0 - N(N-1)/2 + p(p-1)/2} \zeta_{24}^{-e(p-1)^2(p-7)/2} \\ &= \left(\frac{-1}{p}\right)^e p^{e(p-1)/2} \chi^{\alpha_0 + (N-1)/2 - N(N-1)/2 + p(p-1)/2 + (p-7)/2} \\ &= \left(\frac{-1}{p}\right)^e p^{e(p-1)/2} \chi^{\alpha_0 - (p^4 - 3p^2 - 8)/2}.\end{aligned}$$

For instance, when $p = 3$, $e = 3$, $\delta = 2$, we find $\vartheta = (-1)3^3(-1)^{1-31} = -3^3$. More generally, as soon as $p > 3$,

$$\vartheta = \left(\frac{-1}{p}\right)^e p^{e(p-1)/2} \chi^{\alpha_0 - 3} = \left(\frac{-1}{p}\right)^e p^{e(p-1)/2}$$

since $p^2 \equiv 1 \bmod 24$ and the fact already used that $\chi^{\alpha_0} = \chi^{-3}$. ∎

4.6. Computing the modular equations using series expansions. There are a variety of methods to compute modular equations. For large computations, it is possible to use suitably modified versions of [4] or [2]. Also, we can use resultants in the same spirit as in the remark at the end of Section 3, noting that $\mathfrak{w}_{p_1,p_2}^s = (\mathfrak{w}_{p_1}(z)/\mathfrak{w}_{p_1}(z/p_2))^s$.

Here, we content ourselves with the use of series expansions and nice formulas that can help us for small cases. Also, this will add new properties to our equations.

Looking carefully at the expression for $\mathcal{S}_k$, we see that the terms in C_1, C_2 or C cannot contribute to the modular equation, since they have positive order. Therefore, we need only consider the expansions of B'^k and $\mathcal{S}_{A,k}$. Doing this, we see that the useful terms for $\mathcal{S}_{A,k}$ are for $j \le -ktN'/N$. Since $B'^k = q^{-rek}(1 + \cdots)$ and $1 \le k \le \psi(N)$, we need at least $re\psi(N)$ terms in the last coefficient. Since B' is the product and quotient of very sparse series, it might be worthwhile to compute its powers by successive applications of special routines handling this kind of computations. It is possible to compute nice formulas for the $\mathcal{S}_{A,k}$, in the spirit of the ones to come, but we do not need them.

A second algorithm consists in grouping

$$\Phi(F) = P_B(F)P_A(F)P_{C_1}(F)P_{C_2}(F)$$

and to compute P_A (resp. P_{C_1} and P_{C_2}) via its power sums that are given in the preceding propositions.

Inspired by the approach of Section 3.2, the third algorithm uses the reciprocal polynomial, whose power sums will depend on the $C'_{1,\nu}$ and $C'_{2,\nu}$ only:

$$\Sigma_k = \sum_{\nu=0}^{p_2-1} \frac{1}{C'^k_{2,\nu}} + \sum_{\nu=0}^{p_1-1} \frac{1}{C'^k_{1,\nu}},$$

which is a process involving p_1+p_2. We will prove two useful results (Propositions 4.11 and 4.12 below) to help us compute these quantities.

PROPOSITION 4.11. *For all integers $k \neq 0$,*

$$\mathcal{S}_{C_2,k} = p_2 \varepsilon_2^{ke} q^{kt/\delta} \sum_{j \geq ktp'_2/p_2} c_{k,jp_2-ktp'_2} q^j,$$

where $(p_2+1)/\delta = p'_2$ and the $c_{k,i}$ are explicitly given in the proof.

Proof. Put $w = q^{1/p_2}$, $\zeta = \zeta_{p_2}$ and write

$$\begin{aligned}\frac{\eta(p_1 z)\eta\left(\frac{z}{p_2}\right)}{\eta(z)\eta\left(\frac{p_1 z}{p_2}\right)} &= \frac{(w^{p_1p_2/24}(1+\sum_{i=1}^{\infty} a_i w^{p_1p_2 i}))(w^{1/24}(1+\sum_{i=1}^{\infty} a_i w^i))}{w^{p_2/24}(1+\sum_{i=1}^{\infty} a_i w^{p_2 i}) w^{p_1/24}(1+\sum_{i=1}^{\infty} a_i w^{p_1 i})} \\ &= w^r \mathcal{C}_{12}(w)\end{aligned}$$

with $\mathcal{C}_{12}(q) = 1 + \cdots \in \mathbb{Z}[[q]]$ (which is symmetrical in p_1 and p_2), which yields

$$C'_{2,\nu} = \chi^{\theta_2(\nu)-\nu} \chi^{-\theta_2(\nu)} \varepsilon_2^e (w\zeta^\nu)^{re} \mathcal{C}_{12}(w\zeta^\nu)^e,$$

$$\mathcal{S}_{C_2,k} = \varepsilon_2^{ke} w^{kre} \sum_{\nu=0}^{p_2-1} \chi^{-k\nu} \zeta^{kre\nu} \mathcal{C}_{12}(w\zeta^\nu)^{ek}.$$

Writing $\mathcal{C}_{12}(w)^{ek} = \sum_{i=0}^{\infty} c_{k,i} w^i$ (note this is valid irrespective of the sign of k), the inner sum becomes

$$\sum_{i=0}^{\infty} c_{k,i} w^i \sum_{\nu=0}^{p_2-1} (\chi^{-k} \zeta^{kre+i})^\nu,$$

in which the root of unity is

$$\chi^{-k}\zeta^{kre} = \zeta_{24}^{24kre}\zeta^{kre} = \zeta_{24p_2}^{24krep_2+24kre} = \zeta_{24p_2}^{24kre(p_2+1)}.$$

Now, we use the fact that $p_2 \equiv -1 \bmod \delta$, so that $re(p_2+1) = tp'_2$ where $p'_2 = (p_2+1)/\delta$. The above sum is now

$$\begin{aligned}\sum_{i=0}^{\infty} c_{k,i} w^i \sum_{\nu=0}^{p_2-1} (\zeta^{ktp'_2+i})^\nu &= p_2 \sum_{i \equiv -ktp'_2 \bmod p_2}^{\infty} c_{k,i} w^i \\ &= p_2 w^{-ktp'_2} \sum_{j \geq ktp'_2/p_2} c_{k,jp_2-ktp'_2} q^j,\end{aligned}$$

leading to the result. ∎

PROPOSITION 4.12. *In case $p_1 = p_2 = p$, for all $k \neq 0$,*

$$\mathcal{S}_{C,k} \in \left(q^{-1/24}\frac{\eta(pz)^2}{\eta(z)}\right)^{ek} \mathbb{Z}[[q]] = q^{Kk/\delta}\mathbb{Z}[[q]],$$

where all series are specified in the proof.

Proof. One uses $\zeta = \zeta_p$ in

$$\begin{aligned}\mathcal{S}_{C,k} &= p^{ek/2}\left(\frac{\eta(pz)^2}{\eta(z)}\right)^{ek} \sum_{\nu=1}^{p-1} \varepsilon(\nu)^{ek} \frac{\chi^{k\kappa(\nu)}\zeta_{24}^{ek\theta(\nu)}}{\eta(z+\nu/p)^{ek}} \\ &= p^{ek/2}\left(\frac{\eta(pz)^2}{\eta(z)}\right)^{ek} \sum_{\nu=1}^{p-1} \varepsilon(\nu)^{ek} q^{-ek/24}\zeta^{-ek\nu/24} \frac{\chi^{k\kappa(\nu)}\zeta_{24}^{ek\theta(\nu)}}{(1+\sum_{i=1}^{\infty} a_i q^i \zeta^{i\nu})^{ek}} \\ &= p^{ek/2}\left(q^{-1/24}\frac{\eta(pz)^2}{\eta(z)}\right)^{ek} \sum_{\nu=1}^{p-1} \varepsilon(\nu)^{ek}\chi^{k\kappa(\nu)}\zeta_{24}^{ek\theta(\nu)}\zeta^{-ek\nu/24}\mathcal{C}(q\zeta^{\nu})^{ek}\end{aligned}$$

where

$$\mathcal{C}(q) = \frac{1}{1+\sum_{i=1}^{\infty} a_i q^i}.$$

Writing $\mathcal{C}(q)^{ek} = \sum_{i=0}^{\infty} c_{k,i} q^i$ (same remark on the sign of k), the inner sum of the preceding relation is now

$$\begin{aligned}(4.1)\qquad &\sum_{\nu=1}^{p-1} \varepsilon(\nu)^{ek}\chi^{k\kappa(\nu)}\zeta_{24}^{ek\theta(\nu)}\zeta^{-ek\nu/24} \sum_{i=0}^{\infty} c_{k,i}(q\zeta^{\nu})^i \\ &\qquad = \sum_{i=0}^{\infty} c_{k,i} q^i \sum_{\nu=1}^{p-1} \varepsilon(\nu)^{ek}\chi^{k\kappa(\nu)}\zeta_{24}^{ek\theta(\nu)}(\zeta^{-ek/24}\zeta^i)^{\nu}.\end{aligned}$$

Let us treat the case $p = 2$ first, with $e = 8$. We get

$$\begin{aligned}\mathcal{S}_{C,k} &= 2^{4k}\left(\frac{q^{-1/24}\eta(2z)^2}{\eta(z)}\right)^{8k} \sum_{i=0}^{\infty} c_{k,i} q^i (\zeta_2^{-k}\zeta_2^i) \\ &= (-2^4)^k \left(q^{-1/24}\frac{\eta(2z)^2}{\eta(z)}\right)^{8k} \sum_{i=0}^{\infty} c_{k,i}(-q)^i.\end{aligned}$$

For p odd, the root of unity in the inner sum of (4.1) is

$$\varepsilon(\nu)^{ek}\zeta_{24p}^{ek(p(-(p-1)^2\kappa(\nu)+\theta(\nu))-\nu)}(\zeta^i)^{\nu},$$

the exponent of ζ_{24p} being

$$p\big(-(p-1)^2\mu + p\nu(1-\mu^2) + (-3p+2+v)\mu - 3 + 3p\big) - \nu.$$

When $p = 3$ and $e = 3$, we find

$$\zeta_{24}^{k(-32\mu+8\nu-8\nu\mu^2+18)} = (\zeta_{12}^{-16\mu+4\nu-4\nu\mu^2+9})^k = (\zeta_4^3\zeta_3^\nu)^k,$$

leading to

$$\mathcal{S}_{C,k} = 3^{3k/2}\zeta_4^{3k}\left(q^{-1/24}\frac{\eta(3z)^2}{\eta(z)}\right)^{3k}\sum_{i=0}^{\infty}c_{k,i}q^i\sum_{\nu=1}^{2}\varepsilon(\nu)^k(\zeta_3^{i+k})^\nu.$$

When k is even, this boils down to

$$\begin{aligned}\mathcal{S}_{C,k} &= (-3)^{3k/2}\left(q^{-1/24}\frac{\eta(3z)^2}{\eta(z)}\right)^{3k}\Big(2\sum_{i\equiv -k \bmod 3}c_{k,i}q^i - \sum_{i\not\equiv -k \bmod 3}c_{k,i}q^i\Big)\\ &= (-3)^{3k/2}\left(q^{-1/24}\frac{\eta(3z)^2}{\eta(z)}\right)^{3k}\Big(3\sum_{i\equiv -k \bmod 3}c_{k,i}q^i - \sum_{i=0}^{\infty}c_{k,i}q^i\Big).\end{aligned}$$

When k is odd,

$$\mathcal{S}_{C,k} = 3^{3k/2}\zeta_4^{3k}\left(q^{-1/24}\frac{\eta(3z)^2}{\eta(z)}\right)^{3k}\sum_{i=0}^{\infty}c_{k,i}q^i\sum_{\nu=1}^{2}\varepsilon(\nu)^k(\zeta_3^{i+k})^\nu$$

and

$$\begin{aligned}\sum_{\nu=1}^{2}\varepsilon(\nu)^k(\zeta_3^{i+k})^\nu &= -\zeta_3^{i+k} + \zeta_3^{2(i+k)}\\ &= \begin{cases}0 & \text{if } i+k \equiv 0 \bmod 3,\\ (-1)^{(i+k) \bmod 3}\sqrt{-3} & \text{otherwise,}\end{cases}\end{aligned}$$

which yields

$$\mathcal{S}_{C,k} = (-3)^{(3k+1)/2}\left(q^{-1/24}\frac{\eta(3z)^2}{\eta(z)}\right)^{3k}\sum_{i+k\not\equiv 0 \bmod 3}^{\infty}(-1)^{(i+k) \bmod 3}c_{k,i}q^i.$$

When $p > 3$, we get

$$\begin{aligned}&(\zeta_{24}^{-(p-1)^2\mu+p\nu(1-\mu^2)+(-3p+2+v)\mu-3+3p})^{ek}(\zeta_{24p}^{-ek+24i})^\nu\\ &\qquad = (\zeta_{24}^{(\nu-\nu\mu^2-\mu+3)p+\mu v-3})^{ek}(\zeta_{24p}^{-ek+24i})^\nu,\end{aligned}$$

using $p^2 \equiv 1 \bmod 24$. We simplify this as

$$(\zeta_{24}^{p(\nu+3)-3})^{ek}(\zeta_{24p}^{-ek+24i})^\nu = \zeta_8^{ek(p-1)}(\zeta_{24p}^{ek(p^2-1)+24i})^\nu.$$

Write $p^2 - 1 = 24p'$ to obtain

$$\zeta_8^{ek(p-1)}(\zeta_p^{ekp'+i})^\nu.$$

When k is even, this gives

$$\begin{aligned}\mathcal{S}_{C,k} &= p^{ek/2}\zeta_8^{ek(p-1)}\left(q^{-1/24}\frac{\eta(pz)^2}{\eta(z)}\right)^{ek}\sum_{i=0}^{\infty}c_{k,i}q^i\sum_{\nu=1}^{p-1}(\zeta_p^{ekp'+i})^\nu\\ &= p^{ek/2}\zeta_8^{ek(p-1)}\left(q^{-1/24}\frac{\eta(pz)^2}{\eta(z)}\right)^{ek}\\ &\quad\cdot\Big((p-1)\sum_{i+ekp'\equiv 0 \bmod p}^{\infty}c_{k,i}q^i-\sum_{i+ekp'\not\equiv 0 \bmod p}c_{k,i}q^i\Big)\\ &= p^{ek/2}\zeta_8^{ek(p-1)}\left(q^{-1/24}\frac{\eta(pz)^2}{\eta(z)}\right)^{ek}\Big(p\sum_{i+ekp'\equiv 0 \bmod p}^{\infty}c_{k,i}q^i-\sum_{i=0}^{\infty}c_{k,i}q^i\Big).\end{aligned}$$

When k is odd, noting that e is always odd from Table 2, the sum is

$$\mathcal{S}_{C,k} = p^{ek/2}\zeta_8^{ek(p-1)}\left(q^{-1/24}\frac{\eta(pz)^2}{\eta(z)}\right)^{ek}\sum_{i=0}^{\infty}c_{k,i}q^i\sum_{\nu=1}^{p-1}\varepsilon(\nu)(\zeta_p^{i+ekp'})^\nu.$$

But $\sum_{\nu=1}^{p-1}\varepsilon(\nu)(\zeta_p^{i+ekp'})^\nu = 0$ when $i+ekp'\equiv 0 \bmod p$ since there are the same number of quadratic residues and quadratic non-residues modulo p. When $i+ekp'\not\equiv 0 \bmod p$, $\zeta_p^{i+ekp'}$ is a primitive pth root of unity. Remember that [9, Ch. 6]

$$\sum_{x\text{ residue}}\zeta_p^x-\sum_{x\text{ non-residue}}\zeta_p^x=\sqrt{\left(\frac{-1}{p}\right)p}.$$

Let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. If u is an integer, then

$$\sum_{x\text{ residue}}(\zeta_p^{g^u})^x-\sum_{x\text{ non-residue}}(\zeta_p^{g^u})^x=(-1)^u\sqrt{\left(\frac{-1}{p}\right)p}.$$

When $i+ekp'\not\equiv 0 \bmod p$, we set $\Omega(i+ekp')=u$ such that $g^u\equiv i+ekp' \bmod p$. Then

$$\begin{aligned}\mathcal{S}_{C,k} &= \left(\frac{-1}{p}\right)\sqrt{\left(\frac{-1}{p}\right)}\,\zeta_8^{ek(p-1)}p^{(ek+1)/2}\left(q^{-1/24}\frac{\eta(pz)^2}{\eta(z)}\right)^{ek}\\ &\quad\cdot\sum_{i=0,\,i+ekp'\not\equiv 0 \bmod p}^{\infty}(-1)^{\Omega(i+ekp')}c_{k,i}q^i.\end{aligned}$$

When $p\equiv 1 \bmod 4$, the first terms simplify to $\zeta_2^{ek(p-1)/4}=(-1)^{(p-1)/4}$; when $p\equiv 3 \bmod 4$, we get $-\zeta_8^{2+ek(p-1)}=-\zeta_4^{1+ek(p-1)/2}=(-1)^{(3+ek(p-1)/2)/2}$.

As a last point, the dominant term of $\mathcal{S}_{C,k}$ is $q^{ke(p-1)/12}$. When $p=2$ and $e=8$, this is $2k/3$, whereas $re=1/3$; when $p=3$, $e=3$, we get $k/2$, whereas $re=1/2$. For $p>3$, we have $e=1$ and we compare $(p-1)/12$ and

$re = (p-1)/2 \cdot (p-1)/12$. Looking at the valuation of 2 and 3, we deduce that $re = t/\delta$ and $(p-1)/12 = p'/\delta$. ∎

4.7. Tables of equations for double η-quotients. We compute

$$\begin{aligned}\Phi[\mathfrak{w}_{2,2}^{24}](X,J) = {} & X^6 + (-J+624)X^5 + (96J+129840)X^4 \\ & + (-2352J+9018880)X^3 + (10495J+2077440)X^2 \\ & + (J^2-1488J+159744)X + 4096,\end{aligned}$$

whereas

$$\Phi[\mathfrak{w}_{2,2}^{8}](F,G_2) = F^6 - G_2F^5 + 208F^3 + 31G_2F^2 + G_2^2F + 16.$$

More examples are

$$\begin{aligned}\Phi[\mathfrak{w}_{3,3}^{3}](F,G_3) = {} & F^{12} - G_3F^{11} - 522F^{10} + 27G_3F^9 - 10557F^8 - 162G_3F^7 \\ & - 14076F^6 - 18G_3F^5 - 9801F^4 + 163G_3F^3 \\ & + (486 - G_3^2)F^2 - 9G_3F - 27,\end{aligned}$$

$$\begin{aligned}\Phi[\mathfrak{w}_{3,7}](F,G_3) = {} & F^{32} - G_3F^{31} - 514F^{30} + 21G_3F^{29} - 12585F^{28} \\ & - 147G_3F^{27} - 25158F^{26} + 322G_3F^{25} - 5103F^{24} \\ & + 378G_3F^{23} + 80556F^{22} - 1638G_3F^{21} - 21994F^{20} \\ & - 28136F^{18} + 1620G_3F^{17} + 25650F^{16} - 252G_3F^{15} \\ & - 3944F^{14} - 322G_3F^{13} - 14938F^{12} + 22G_3F^{11} \\ & - (G_3^2 - 2940)F^{10} - 10G_3F^9 + 1953F^8 + G_3F^7 \\ & - 462F^6 + 7G_3F^5 + 15F^4 - G_3F^3 - 10F^2 + 1.\end{aligned}$$

5. Conclusion. We have studied modular equations involving γ_2 and γ_3 for double η-quotients. As a result, more compact modular equations can be stored and used, with application to the SEA algorithm (see for instance [11]), or CM computations, as motivated for instance by [14] (see [12]).

It seems natural to conjecture that more general functions can exhibit the same properties. Experiments can be conducted on Newman functions, using for instance the resultant approach, leading to new instances of the theorems. This will be described in another article.

Acknowledgements. The author wishes to thank the referee for his/her precise remarks that made the article clearer.

References

[1] J. A. Antoniadis, *Über die Berechnung von Multiplikatorgleichungen*, Acta Arith. 43 (1984), 253–272.

[2] R. Bröker, K. Lauter, and A. V. Sutherland, *Modular polynomials via isogeny volcanoes*, Math. Comp. 81 (2012), 1201–1231.
[3] D. A. Cox, *Primes of the Form $x^2 + ny^2$*, Wiley, 1989.
[4] A. Enge, *Computing modular polynomials in quasi-linear time*, Math. Comp. 78 (2009), 1809–1824.
[5] A. Enge and F. Morain, *Generalized Weber functions*, http://hal.inria.fr/inria-00385608/, 2009.
[6] A. Enge and R. Schertz, *Constructing elliptic curves over finite fields using double eta-quotients*, J. Théor. Nombres Bordeaux 16 (2004), 555–568.
[7] A. Enge and R. Schertz, *Modular curves of composite level*, Acta Arith. 181 (2005), 129–141.
[8] A. Enneper, *Elliptische Functionen – Theorie und Geschichte*, 2nd ed., Louis Nebert, 1890.
[9] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Grad. Texts in Math. 84, Springer, 1982.
[10] L. Kiepert, *Über Theilung und Transformation der elliptischen Funktionen*, Math. Ann. 26 (1886), 369–454.
[11] F. Morain, *Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques*, J. Théor. Nombres Bordeaux 7 (1995), 255–282.
[12] F. Morain, *Implementation notes concerning the Rubin–Silverberg algorithms*, in preparation.
[13] M. Newman, *Construction and application of a class of modular functions*, Proc. London Math. Soc. 3 (1957), 334–350.
[14] K. Rubin and A. Silverberg, *Choosing the correct elliptic curve in the CM method*, Math. Comp. 79 (2010), 545–561.
[15] H. Weber, *Lehrbuch der Algebra, Vol. III*, Chelsea Publ., New York, 1908.

François Morain
INRIA Saclay–Île-de-France & Laboratoire d'Informatique (CNRS/UMR 7161)
École polytechnique
F-91128 Palaiseau, France
E-mail: morain@lix.polytechnique.fr

Received on 23.7.2012
and in revised form on 25.7.2013 (7137)