

EXPLICIT FORMULAS FOR THE MODULAR EQUATION

PAUL BAGINSKI AND ELENA FUCHS

ABSTRACT. We determine a linear time algorithm for calculating the modular equation $\Phi_N(X, J)$ for $N = p_1 p_2$, where p_1 and p_2 are distinct primes. We provide $N = 10$ as an example.

1. INTRODUCTION

Let $J(z)$ be the modular invariant of the elliptic curve $y^2 = 4x^3 - g_2(z)x - g_3(z)x$ over \mathbb{C} . Specifically, $J(z)$ is given by:

$$J(z) = 12^3 \frac{g_2^3(z)}{g_2^3(z) - 27g_3^2(z)}$$

where the denominator is nonzero.

The modular equation $\Phi_N(X, J) = 0$ provides an algebraic relation between $J(z)$ and $X = J(Nz)$ as roots of an irreducible polynomial Φ_N in two variables over \mathbb{C} . The polynomial $\Phi_N(X, J)$ is symmetric in the variables, and is of degree $\psi(N)$. Namely, $\Phi_N(X, J)$ is of the form

$$X^{\psi(N)} + J^{\psi(N)} + \sum_{0 \leq j \leq i < \psi(N)} C_{i,j} F_{i,j},$$

where $F_{i,j} = X^i J^j + X^j J^i$ and

$$\psi(N) = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

where the product is taken over the primes p in the prime factorization of N . All the coefficients of $X^i J^j$ are integers, thus $C_{i,j}$ is always an integer, except perhaps when $i = j$ in which case $C_{i,i}$ can be half of an integer.

The modular equation $\Phi_N(X, J) = 0$ has many useful applications in the theory of elliptic curves and number theory, among many other fields. Descriptions of these applications can be found in [1], [2], [3], and [12]. It is of great interest then to determine explicit formulas for Φ_N . Several methods have already been developed.

For arbitrary N , one can reduce the problem of calculating Φ_N to calculating Φ_p for all prime factors of p using the following theorem:

Theorem 1.1 ([11]). (1) If $N = n_1 n_2$ with n_1, n_2 relatively prime, then

$$\Psi_N(X, J) = \prod_{i=1}^{\psi(n_2)} \Psi_{n_1}(X, \xi_i)$$

where $\{\xi_i \mid i = 1, \dots, \psi(n_2)\}$ are the distinct roots of the polynomial $\Psi_{n_2}(X, J)$.

(2) If $N = p^e$ for some p prime and $e > 1$, then

$$\Psi_N(X, J) = \prod_{i=1}^{\psi(p^{e-1})} \Psi_p(X, \xi_i) / [\Psi_{p^{e-2}}(X, J)]^p$$

where $\{\xi_i \mid i = 1, \dots, \psi(p^{e-1})\}$ are the distinct roots of the polynomial $\Psi_{p^{e-1}}(X, J)$.

For practical application, this theorem can be somewhat cumbersome or even intractable, as it involves finding roots of polynomials of high degree. Therefore, there has been an effort to find alternate methods for explicitly calculating the coefficients of the modular equation.

Using the technique of cusp expansions, Yui[13] developed an algorithm for calculating the coefficients of Φ_p for p prime. Dutta Gupta and She ([4] and [5]) expanded upon this technique to create an algorithm for $N = p^2$ for primes p , and to analyze the case when $N = p^e$ for p prime and $e > 2$. Using a different methods, Ito ([7] and [8]) developed an algorithm for calculating the coefficients.

As far as precise computation, the modular equation has been explicitly calculated for the primes $p = 2, 3, 5, 7$, and 11 and can be found in [6] and [10]. Recently, Ito ([7] and [8]) determined Ψ_n for all $n \leq 56$.

In this paper, we will provide a general algorithm for calculating the coefficients of $\Phi_N(X, J)$ for $N = p_1 p_2$, the product of distinct primes. We will also show that this algorithm performs the calculation in linear time. The next section develops the necessary machinery for the algorithm, as well as describing and analyzing it. The other section deals with the exceptional case of $N = 6$.

2. GENERAL p_1 AND p_2

Let p_1 and p_2 be distinct primes with $p_1 > p_2$. Choose integers u and v such that $p_1 u + p_2 v = 1$.

Consider $\Gamma = SL(2, \mathbb{Z})$ and the subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \equiv 0 \pmod{N} \right\}$$

It is well-known that $J(z)$ is invariant under the natural group action of Γ on the upper half-plane. Namely

$$J(z) = J\left(\frac{az + b}{cz + d}\right)$$

for any matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. A simple consequence of this fact is that $J(Nz)$ is invariant under the subgroup $\Gamma_0(N)$ of Γ .

By Proposition 9.3 in [9], we have that $[\Gamma : \Gamma_0(N)] = \psi(N)$. Therefore, when p_1 and p_2 are distinct primes, we have that $[\Gamma : \Gamma_0(p_1 p_2)] = (p_1 + 1)(p_2 + 1)$.

Lemma 2.1. *A complete set of left-coset representatives β_i of $\Gamma_0(p_1 p_2)$ in Γ is:*

$$\begin{aligned} & \left\{ \begin{pmatrix} j & 1 \\ -1 & 0 \end{pmatrix} \mid 0 \leq j < p_1 p_2 \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ p_1 k & 1 \end{pmatrix} \mid 0 \leq k < p_2 \right\} \cup \\ & \left\{ \begin{pmatrix} 1 & 0 \\ p_1 k & 1 \end{pmatrix} \mid 0 \leq k < p_2 \right\} \cup \left\{ \begin{pmatrix} p_1 & -v \\ p_2 & u \end{pmatrix}, \begin{pmatrix} p_2 & -u \\ p_1 & v \end{pmatrix} \right\} \end{aligned}$$

Proof. Left to the reader.

Lemma 2.2. *The cusps of $\Gamma_0(p_1p_2)$ are*

$$\left\{0, \infty, \frac{-u}{p_2}, \frac{-v}{p_1}\right\} \cup \left\{\frac{-1}{p_1k} \mid 0 < k < p_2\right\} \cup \left\{\frac{-1}{p_2k} \mid 0 < k < p_1\right\}$$

Proof. By the discussion on page 262 of [9], the cusps are given by $\beta_j^{-1}(\infty)$, where the β_j run over our left-coset representatives of $\Gamma_0(p_1p_2)$ in Γ . \square

Given any modular function f of $\Gamma_0(p_1p_2)$, we may perform a Fourier expansion of f around the cusp ∞ with respect to $q = e^{2\pi iz}$. We also may perform an expansion of f around any other cusp x in terms of the expansion at ∞ . Namely, if $\beta \in SL(2, \mathbb{Z})$ is such that $\beta^{-1}(\infty) = x$, then we define the expansion of f at x to be the expansion of $f(\beta^{-1}(z))$ at ∞ . It can be shown that this expansion is independent of the choice of the coset representative β .

When one performs the expansion of f at $x \neq \infty$, the resulting expansion is given in powers of $q_{p_1p_2} = e^{2\pi iz/p_1p_2}$, and hence is periodic in p_1p_2 . It can occur, that for a given cusp x , every modular function f has an expansion at x which is periodic in some period less than p_1p_2 . Thus, we define the **width** of the cusp x to be the least positive integer w which acts as a period for the expansions at x of all modular functions f of $\Gamma_0(p_1p_2)$. The following proposition permits explicit calculation of the width of a cusp.

Proposition 2.3. *Let $\beta^{-1}(\infty)$ be a cusp of $\Gamma_0(p_1p_2)$, where $\beta \in SL(2, \mathbb{Z})$. Then there exists a unique primitive matrix $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ such that $ad = p_1p_2$, $0 \leq b < d$, and $\text{GCD}(a, b, d) = 1$ with*

$$\begin{pmatrix} p_1p_2 & 0 \\ 0 & 1 \end{pmatrix} \beta^{-1} = \gamma \alpha$$

for some $\gamma \in SL(2, \mathbb{Z})$. Moreover, the width of the cusp $\beta^{-1}(\infty)$ is d .

Proof. For a proof, see Proposition 9.4 of [9].

We will now perform expansions of J and $X = J(p_1p_2z)$ at the cusps ∞ and $-v/p_1$. The expansions will be in terms of q and $q_r = e^{2\pi iz/p_2}$, respectively.

The function $J(z)$ has a well known q -expansion at ∞ given by:

$$(2.1) \quad J(z) = \frac{1}{q} \sum_{j=0}^{\infty} a_j q^j = \frac{1}{q} + 744 + 196884q + \dots$$

Consequently, at ∞ we have that the expansion of $X = J(p_1p_2z)$ is

$$(2.2) \quad X = \frac{1}{q^{p_1p_2}} \sum_{j=0}^{\infty} a_j q^{p_1p_2j}.$$

At the other cusp, J has the same q -expansion, since J is $SL(2, \mathbb{Z})$ invariant. However, when rewritten in terms of q_r , we obtain that the expansion at $-v/p_1$ is

given by:

$$(2.3) \quad J(z) = \frac{1}{q_r^{p_2}} \sum_{j=0}^{\infty} a_j q_r^{p_2 j}.$$

Proposition 2.4. *The q_r expansion of X at the cusp $-v/p_1$ is given by:*

$$(2.4) \quad X(z) = \frac{1}{q_r^{p_1}} \sum_{j=0}^{\infty} a_j q_r^{p_1 j}$$

Proof. The expansion of X at $\frac{-v}{p_1}$ is given by the expansion of $X \circ \beta^{-1}$ at ∞ , where $\beta = \begin{pmatrix} p_2 & -u \\ p_1 & v \end{pmatrix}$. Thus, determining the matrices involved in the identity in Proposition 2.3, we obtain:

$$\begin{aligned} X \circ \beta^{-1}(z) &= J \left(\begin{pmatrix} p_1 p_2 & 0 \\ 0 & 1 \end{pmatrix} \circ \begin{pmatrix} v & u \\ -p_1 & p_2 \end{pmatrix} (z) \right) \\ &= J \left(\begin{pmatrix} p_2 v & p_1 u \\ -1 & 1 \end{pmatrix} \circ \begin{pmatrix} p_1 & 0 \\ 0 & p_2 \end{pmatrix} (z) \right) \\ &= J \left(\begin{pmatrix} p_1 & 0 \\ 0 & p_2 \end{pmatrix} (z) \right) \\ &= J \left(\frac{p_1 z}{p_2} \right) \\ &= \frac{1}{e^{2\pi i p_1 z / p_2}} \sum_{j=0}^{\infty} a_j (e^{2\pi i p_1 z / p_2})^j \\ &= \frac{1}{q_r^{p_1}} \sum_{j=0}^{\infty} a_j q_r^{p_1 j} \end{aligned}$$

□

We collect the relevant information into the following table:

cusps	∞	$-v/p_1$
width	1	p_2
order of pole of J	1	p_1
leading coefficient of J	1	1
order of pole of X	$p_1 p_2$	p_2
leading coefficient of X	1	1
order of pole of $X^{\psi(p_1 p_2)} + J^{\psi(p_1 p_2)}$	$\psi(p_1 p_2) p_1 p_2$	$\psi(p_1 p_2) p_2$
leading coefficient of $X^{\psi(p_1 p_2)} + J^{\psi(p_1 p_2)}$	1	1
order of pole of $F_{i,j}$ ($i > j$)	$p_1 p_2 i + j$	$p_1 i + p_2 j$
leading coefficient of $F_{i,j}$	1	1
order of pole of $F_{i,i}$	$i(p_1 p_2 + 1)$	$i(p_1 + p_2)$
leading coefficient of $F_{i,i}$	2	2

We will use the expansions at ∞ and $-v/p_1$ for our analysis. If one considers the modular equation

$$X^{\psi(p_1 p_2)} + J^{\psi(p_1 p_2)} = \sum_{0 \leq j \leq i < \psi(p_1 p_2)} -C_{i,j} F_{i,j}$$

in these expansions, we get a system of linear equations corresponding to the coefficients of powers of q (respectively q_r). Namely, if we equate the coefficients of q^{-k} on both sides of the modular equation, we obtain the equation $d_k = s_k$, where $d_k \in \mathbb{Q}$ and s_k is a linear combination of the $C_{i,j}$. Similarly, if we equate the coefficients of q_r^{-k} in the $-v/p_1$ expansion of the modular equation, we obtain the linear equation $e_k = t_k$, where $e_k \in \mathbb{Q}$ and t_k is a linear combination of the $C_{i,j}$.

We now will describe precisely which $C_{i,j}$ appear in s_k and t_k for various k . Clearly, $C_{i,j}$ appears in s_k (respectively, t_k) precisely when $F_{i,j}$ has a nonzero coefficient for q^{-k} (q_r^{-k}) in the expansion at ∞ ($-v/p_1$). Examining the expansions of $F_{i,j}$ yields the following proposition:

Proposition 2.5. *For $k \geq 0$,*

- (1) s_k contains $C_{i,j}$ precisely if there are $m \geq 0$ and $m' \geq 0$ such that $k = p_1 p_2 (i - m) + (j - m')$ or $k = p_1 p_2 (j - m') + (i - m)$.
- (2) t_k contains $C_{i,j}$ precisely if there are $m \geq 0$ and $m' \geq 0$ such that $k = p_1 (i - m) + p_2 (j - m')$ or $k = p_1 (j - m') + p_2 (i - m)$.

Proof. This easily follows from considering the cusp expansions. □

An immediate consequence of this proposition is the following observation: if one has solved all the equations $s_k = d_k$ for $k > K$, then to solve $s_K = d_K$, one need only consider the $C_{i,j}$ which appear in s_K but do not appear in s_k for any $k > K$. We call such $C_{i,j}$ **debutantes**. Since $j \leq i$, the debutantes appearing in s_K will be precisely those such that $K = p_1 p_2 i + j$ and $j \leq i$. We may also consider debuts of $C_{i,j}$ for each t_K and observe that the debutantes appearing in t_K are precisely those $C_{i,j}$ such that $K = p_1 i + p_2 j$ and $j \leq i$. Though there can be several debutantes appearing in each t_k , the number of debutantes appearing in each s_k has a favorable description.

Lemma 2.6. *For each $p_1 p_2 (\psi(p_1 p_2) - 1) + \psi(p_1 p_2) - 1 \geq k \geq 0$, there are at most two $C_{i,j}$ such that $k = p_1 p_2 i + j$. In other words, there are at most two debutantes in s_k . Specifically, if $k = p_1 p_2 i + j$ with $p_1 p_2 + 1 \leq i \leq p_1 p_2 + p_1 + p_2$ and $0 \leq j \leq i - p_1 p_2 - 1$, then there are two debutantes; otherwise, there is only one.*

Proof. We must have $0 \leq j \leq i \leq \psi(p_1 p_2) - 1 = p_1 p_2 + p_1 + p_2$. If $k < p_1 p_2$ there is clearly only one valid representation in terms of i and j , so assume $k \geq p_1 p_2$. Each such k can have at most the following two representations: $k = p_1 p_2 i + j$ and $k = p_1 p_2 (i - 1) + (j + p_1 p_2)$, where $0 \leq j < p_1 p_2$. These correspond to $C_{i,j}$ and $C_{i-1, j+p_1 p_2}$. Since we also require $j \leq i$ for each $C_{i,j}$, both representations are valid precisely when $i - 1 \geq j + p_1 p_2$. But this holds precisely when $p_1 p_2 + p_1 + p_2 \geq i \geq p_1 p_2 + 1$ and $i - p_1 p_2 - 1 \geq j \geq 0$, since $j \geq 0$. □

Lemma 2.7. *Given $K = (p_1 + p_2)L$ for some $p_1p_2 + p_1 > L \geq p_1p_2$, assume that all equations $t_k = e_k$ have been solved for $k > K$ and all equations $s_k = d_k$ have been solved for $k \geq p_1p_2(L + p_2 + 2)$. Let λ be the greatest integer less than $L + p_2$ such that there is $p_1p_2 \leq \gamma \leq \lambda$ with $p_1\lambda + p_2\gamma \leq K < p_1\lambda + p_2\gamma + p_2$. Then each s_k contains at most one uncalculated debutante for every $k > p_1p_2\lambda + \gamma$.*

Proof. Note that $L \leq \lambda$ since $Lp_1 + p_1p_2^2 \leq K$. Also note that by our assumption on the s_k , all the $C_{i,j}$ have been calculated for $i \geq L + p_2 + 2$.

Consider $C_{\lambda+1+i,j}$ for $0 < i$ and $0 \leq j \leq \lambda + 1 + i$. By Lemma 2.6, $C_{\lambda+1+i,j}$ is the sole debutante appearing in $s_{p_1p_2(\lambda+1+i)+j}$ when $j > \lambda + i - p_1p_2$. When $0 \leq j \leq \lambda + i - p_1p_2$, there are two debutantes: $C_{\lambda+1+i,j}$ and $C_{\lambda+i,j+p_1p_2}$.

Assume $\lambda < L + p_2 - 1$. Then, by the maximality of λ , we have that $p_1(\lambda + i) + p_1p_2^2 > K$ for any $i > 0$. So for any $i > 0$ we have $p_1(\lambda + i) + p_2(j + p_1p_2) > K$ and so $C_{\lambda+i,j+p_1p_2}$ appears in one of the t_k which had already been solved. If, on the other hand, $\lambda = L + p_2 - 1$, then:

$$\begin{aligned} p_1(\lambda + i) + p_2(j + p_1p_2) &\geq p_1(L + p_2) + p_2(j + p_1p_2) \\ &= p_1L + p_2(p_1p_2 + p_1) + jp_2 \\ &> p_1L + p_2L + yp_2 \\ &\geq K \end{aligned}$$

so again we have that $C_{\lambda+i,j+p_1p_2}$ appears in one of the t_k which had already been solved.

Thus, we have handled all the s_k for $k \geq p_1p_2(\lambda + 2)$. Now, let us consider the s_k for $p_1p_2(\lambda + 2) > k > p_1p_2\lambda + \gamma$. Since $\gamma \geq p_1p_2$, all these s_k have a debutante of the form $C_{\lambda+1,j}$ where $\lambda + 1 \geq j > \gamma - p_1p_2$. Using Lemma 2.6, we see that $C_{\lambda+1,j}$ is the sole debutante if $j > \lambda - p_1p_2$. So assume that $j \leq \lambda - p_1p_2$. Then the two debutantes which appear in $s_{p_1p_2(\lambda+1)+j}$ are $C_{\lambda+1,j}$ and $C_{\lambda,j+p_1p_2}$. But, we have

$$p_1\lambda + p_2(j + p_1p_2) \geq p_1\lambda + p_2(\gamma + 1) > K$$

so $C_{\lambda,j+p_1p_2}$ appears in one of the t_k which have already been solved. \square

Lemma 2.8. *Given $K = (p_1 + p_2)L$ for some $p_1p_2 > L \geq p_1p_2 - p_2$, assume that all equations $t_k = e_k$ have been solved for $k > K$. Then each s_k contains at most one uncalculated debutante for every $k \geq 0$.*

Proof. By Proposition 2.6, there are two debutantes appearing in s_k precisely when $k = p_1p_2i + j$ with $p_1p_2 + 1 \leq i \leq p_1p_2 + p_1 + p_2$ and $0 \leq j \leq i - p_1p_2 - 1$. In this case, we have that the debutantes are $C_{i,j}$ and $C_{i-1,j+p_1p_2}$. We claim that $C_{i-1,j+p_1p_2}$ appears in one of the t_k which had already been solved. Indeed:

$$p_1(i - 1) + p_2(j + p_1p_2) \geq (p_1 + p_2)p_1p_2 > (p_1 + p_2)L = K$$

so $C_{i-1,j+p_1p_2}$ had already been calculated. \square

Lemma 2.9. *Assume $p_1p_2 \neq 6$. Let $K = p_1p_2x + y$ with $p_1p_2 + 1 \leq x \leq p_1p_2 + p_1 + p_2$ and $0 \leq y \leq x - p_1p_2 - 1$ be given and assume all the $s_k = d_k$ have been solved for $k > K$. Then for $k > (p_1 + p_2)(x - p_2)$ the equation $t_k = e_k$ contains at most one debutante which has not been calculated.*

Proof. Since all the equations $s_k = d_k$ have been solved for $k > K$, we know that the following $C_{i,j}$ have been calculated:

- (1) for all $i > x + 1$ and all $j \geq 0$;
- (2) for $i = x + 1$ and all $j > y$;
- (3) for $i = x$ and all $j > y + p_1 p_2$.

Pick $k > (p_1 + p_2)(x - p_2)$. In order for t_k to have any debutantes, we need $k = p_1 \alpha + p_2 \beta$ for some $p_1 p_2 + p_1 + p_2 \geq \alpha \geq \beta \geq 0$. Pick the least such α for which there is a β satisfying the conditions. Note that $\alpha > x - p_2$ since $\alpha \geq \beta$ and $k > (p_1 + p_2)(x - p_2)$. Every $C_{i,j}$ which appears in t_k must be of the form $C_{\alpha+p_2 f, \beta-p_1 f}$ for $f \geq 0$ (f cannot be negative by the minimality of α). Since $\alpha > x - p_2$, for every $f > 0$ we have that $\alpha + f p_2 > x$.

Case 1: $\alpha > x - p_2 + 1$. Then $\alpha + f p_2 > x + 1$ for every $f > 0$ and thus every $C_{\alpha+f p_2, \beta-f p_1}$ has been calculated, save perhaps $C_{\alpha, \beta}$. Therefore there is at most one debutante in t_k which has not been calculated.

Case 2: $\alpha = x - p_2 + 1$. For $f > 1$, $\alpha + f p_2 > x + 1$ and thus $C_{\alpha+f p_2, \beta-f p_1}$ has been calculated, whereas for $f = 1$, $\alpha + f p_2 = x + 1$. If $\beta - p_1 > y$, then $C_{\alpha+p_2, \beta-p_1}$ has already been calculated, and so $C_{\alpha+f p_2, \beta-f p_1}$ has been calculated for every f except maybe $f = 0$. But since $k = p_1(x - p_2 + 1) + p_2 \beta > (p_1 + p_2)(x - p_2)$, we have that $p_2 \beta > p_2(x - p_2) - p_1$. Since $y < x - p_1 p_2$, we have $\beta - p_1 > y$ if $p_2(\beta - p_1) \geq p_2(x - p_1 p_2)$. But $p_2(\beta - p_1) > p_2(x - p_2) - p_1 - p_1 p_2$, so $\beta - p_1 > y$ if $p_2(x - p_2) - p_1 - p_1 p_2 \geq p_2(x - p_1 p_2)$. This inequality reduces to showing that $p_2^2(p_1 - 1) \geq p_1(p_2 + 1)$, or equivalently, $1 - 1/p_1 \geq 1/p_2 + 1/p_2^2$. Since $p_1 > p_2$ and $p_1 p_2 \neq 6$, this inequality holds and therefore $\beta - p_1 > y$ and so $C_{\alpha+p_2, \beta-p_1}$ had already been calculated. \square

Theorem 2.10. *For $p_1 p_2 \neq 6$, the coefficients $C_{i,j}$ of the modular polynomial $\Phi_{p_1 p_2}(X, J)$ can be calculated in linear time.*

Proof. Recall our earlier observation that if all the $s_k = d_k$ have been solved for $k > K$, then to solve $s_K = d_K$, one needs only consider the debutantes appearing in this equation. In particular, if one also has some of the $t_k = e_k$ solved, then one only needs to solve for the uncalculated debutantes in order to solve $s_K = d_K$. The same statement holds with t swapped for s and e swapped with d . Our algorithm will arrange the equations $s_k = d_k$ and $t_k = e_k$ in such an order so that if all the previous linear equations have been solved, then there is at most one uncalculated debutante in the current linear equation. In this manner, we have arranged the linear equations $s_k = d_k$ and $t_k = e_k$ in order to create a lower triangular matrix to solve for the $C_{i,j}$. Our algorithm will only utilize the equations $s_k = d_k$ for $0 \leq k \leq (p_1 p_2 + 1)(\psi(p_1 p_2) - 1)$ and $t_k = e_k$ for $p_1 p_2 - p_2 \leq k \leq p_1(\psi(p_1 p_2) - 1) + p_2(\psi(p_1 p_2) - 1)$. Thus, the total number of linear equations used in the lower triangular matrix is:

$$\begin{aligned} \psi(p_1 p_2)(p_1 p_2 + p_1 + p_2 + 1) - 2p_1 p_2 + p_2 + 1 &\leq \psi(p_1 p_2)(p_1 p_2 + p_1 + p_2 + 1) \\ &= \psi(p_1 p_2)(p_1 + 1)(p_2 + 1) \\ &= \psi(p_1 p_2)^2 \end{aligned}$$

Since there are a total of $\psi(p_1 p_2)(\psi(p_1 p_2) + 1)/2$ many $C_{i,j}$ to solve for, this algorithm will clearly run in linear time with respect to the number of $C_{i,j}$.

The Algorithm:

Step 1. We begin with the ∞ expansion, and consider the linear equation

$$s_{(p_1 p_2 + 1)(\psi(p_1 p_2) - 1)} = d_{(p_1 p_2 + 1)(\psi(p_1 p_2) - 1)}$$

which, as our table shows, corresponds to the first nonzero coefficients in the q -expansion of the modular equation about ∞ . By Proposition 2.5, this linear equation will have only one variable $C_{\psi(p_1 p_2) - 1, \psi(p_1 p_2) - 1}$, which we calculate. Set $K = p_1 p_2 (\psi(p_1 p_2) - 1) + p_1 + p_2 - 1$. Then by Lemma 2.6, there will be only one debutante for every $k > K$, and therefore we are able to solve all these $s_k = d_k$. Note that by this lemma, s_K will have two debutantes.

Step 2. We have that $K = p_1 p_2 x + y$ with $p_1 p_2 + 1 \leq x \leq p_1 p_2 + p_1 + p_2$ and $0 \leq y \leq x - p_1 p_2 - 1$. Therefore, we may apply Lemma 2.9 to conclude that for every $k > (p_1 + p_2)(x - p_2)$, the equation $t_k = d_k$ has only one uncalculated debutante. Solve all these equations. If $x - 2 < p_1 p_2$, then go to Step 4. Otherwise, go to Step 3.

Step 3. Since $x - 2 \geq p_1 p_2$, we may use Lemma 2.7 to select a suitable λ and γ with $x - 2 \leq \lambda < x - 2 + p_2$ and $p_1 p_2 \leq \gamma \leq \lambda$ and such that for every $k > p_1 p_2 \lambda + \gamma$, s_k has at most one uncalculated debutante. Solve all of these s_k , set $K = p_1 p_2 \lambda + \gamma$ and repeat Step 2. Note that K can be rewritten as $p_1 p_2 (\lambda + 1) + (\gamma - p_1 p_2)$ in order to satisfy the conditions for Step 2.

Step 4. Since $x - 2 < p_1 p_2$ but $x \geq p_1 p_2 + 1$ we know that $x - 2 \geq p_1 p_2 - p_2$. Therefore we may use Lemma 2.8 to conclude that every s_k contains at most one uncalculated debutante for every $k \geq 0$. Thus, we may solve all the remaining equations and determine the remaining $C_{i,j}$. \square

3. THE CASE $p_1 p_2 = 6$

The statement of the algorithm proposed in Theorem 2.10 concerns only $p_1 p_2 \neq 6$. One can easily observe that the case $p_1 p_2 = 6$ does not adhere to the behavior predicted by our algorithm. However, the general method of alternating between the two cusp expansions still allows for a linear time technique for solving the coefficients $C_{i,j}$. We explicitly describe this method below.

The table reprinted for $p_1 p_2 = 6$ becomes:

cusp	∞	$-2/3$
width	1	2
order of pole of J	1	3
leading coefficient of J	1	1
order of pole of X	6	2
leading coefficient of X	1	1
order of pole of $X^{12} + J^{12}$	72	24
leading coefficient of $X^{\psi(p_1 p_2)} + J^{\psi(p_1 p_2)}$	1	1
order of pole of $F_{i,j}$ ($i > j$)	$6i + j$	$3i + 2j$
leading coefficient of $F_{i,j}$	1	1
order of pole of $F_{i,i}$	$7i$	$5i$
leading coefficient of $F_{i,i}$	2	2

Now consider the modular equation

$$X^{12} + J^{12} = - \sum_{0 \leq j \leq i \leq 11} C_{i,j} F_{i,j}$$

We omit the actual calculation of the coefficients $C_{i,j}$, as it is of more interest to us to rather locate the values k at which two uncalculated debutantes appear in s_k or t_k . In this manner we are able to determine where to switch from one cusp expansion to another.

- The expansion at ∞ allows us to go down to $k = 71$, solving explicitly for $C_{11,11}$, $C_{11,10}$, $C_{11,9}$, $C_{11,8}$, $C_{11,7}$, $C_{11,6}$, and $C_{11,5}$.
- We then must switch to the expansion at $-2/3$ and go down to $k = 42$, solving for $C_{10,10}$, $C_{10,9}$, $C_{10,8}$, $C_{10,7}$, $C_{10,6}$, $C_{9,9}$, and $C_{9,8}$.
- Switching back to the expansion at ∞ , we go down to $k = 62$, and solve for $C_{11,4}$, $C_{11,3}$, $C_{11,2}$, $C_{11,1}$, $C_{11,0}$, $C_{10,5}$, $C_{10,4}$, $C_{10,3}$, and $C_{10,2}$.
- Switching again to the expansion at $-2/3$, we go down to $k = 36$ and solve for $C_{9,7}$, $C_{9,6}$, $C_{9,5}$, $C_{8,8}$, $C_{8,7}$, and $C_{8,6}$.
- Returning to the expansion at ∞ , we descend to $k = 50$, solving for $C_{10,1}$, $C_{10,0}$, $C_{9,5}$, $C_{9,4}$, $C_{9,3}$, $C_{9,2}$, $C_{9,1}$, $C_{9,0}$, $C_{8,5}$, $C_{8,4}$, $C_{8,3}$, and $C_{8,2}$ along the way.
- Switching to the expansion at $-2/3$, we go down to $k = 27$ and solve for $C_{7,7}$, $C_{7,6}$, $C_{7,5}$, $C_{7,4}$, $C_{7,3}$, $C_{6,6}$, and $C_{6,5}$.
- Finally, we make our last switch to the expansion at ∞ and determine the rest of the $C_{i,j}$, as there is only one debutante per s_k for $k < 50$.

REFERENCES

- [1] K. Barre-Sirieix, G. Diaz, F. Gramain, G. Philibert, *Une preuve de la conjecture de Mahler-Manin*, Invent. Math. **124** (1996), No. 1-3, 1-9.
- [2] H. Cohn, **Introduction to the Construction of Class Fields**, Cambridge University Press, 1985.
- [3] D. Cox, **Primes of the form $X^2 + nY^2$** , John Wiley and Sons, 1989.
- [4] S. Dutta Gupta, X. She, *On explicit formulas for the modular equation*, Rocky Mountain J. Math. **31** (2001), no. 1, 185-195.
- [5] S. Dutta Gupta, X. She, *On the computation of the modular equation*, Adv. Stud. Contemp. Math. (Kyungshang) **4** (2001), no. 1, 43-54.
- [6] O. Herrmann, *Über die Berechnung der Fourierkoeffizienten der Funktion $j(\tau)$* , J. Reine Angew. Math. **274/275** (1975), 187-195.
- [7] H. Ito, *Computation of the modular equation* Proc. Japan Acad. Ser. A Math. Sci. **71** (1995), no. 3, 48-50.
- [8] H. Ito, *Computation of modular equation II* Mem. College Ed. Akita Univ. Natur. Sci. No. 52 (1997), 1-10.
- [9] A. Knapp, **Elliptic Curves**, Princeton University Press, 1992.
- [10] E. Kaltofen, N. Yui, *On the modular equation of order 11*, in Third MACSYMA User's Conference, Proceedings, General Electric, (1984), 472-485.
- [11] S. Lang, **Elliptic Functions**, Addison Wesley, 1973.
- [12] G. Shimura, **Introduction to Arithmetic Theory of Automorphic Functions**, Princeton University Press, 1971.
- [13] N. Yui, *Explicit Form of Modular Equation*, J. Reine Angew. Math. **299-300** (1978), 185-200.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA AT BERKELEY
E-mail address: paulb2@andrew.cmu.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA AT BERKELEY
E-mail address: `lenfuchs@uclink.berkeley.edu`