ACTA ARITHMETICA
118.2 (2005)

Modular curves of composite level

by

ANDREAS ENGE (Palaiseau) and REINHARD SCHERTZ (Augsburg)

1. Motivation. The modular curves $X_0(N)$ have been studied intensively since they provide a link between modular and elliptic functions. Among other things, they parameterise pairs of elliptic curves with a cyclic isogeny of degree N between them. Topics of interest include the search for models with few or no singularities or with small coefficients. For instance, the question which curves $X_0(N)$ are hyperelliptic has been answered in [11] and complemented by concrete models in [12, 9, 16]. The factorisation pattern of these modular equations provides information on the rationality of isogenies and can thus be used to determine the L-function of elliptic curves over finite fields. In general, plane equations with nice properties are obtained by looking for two functions on $X_0(N)$ with suitable pole orders and determining a polynomial relationship between them. To link the modular equations to the pairs of isogenous elliptic curves they parameterise, one needs to exhibit a relationship with the modular invariant j, which requires considerable work in each case (see [5, 2]).

It is thus convenient to fix one of the functions as j and to consider $X_0(N)$ as a cover of $X_0(1)$, albeit this introduces further singularities. Equations for $X_0(N)/X_0(1)$ with small coefficients have been exhibited in [7] and [8, Chapter 5]; some ideas presented there go back to Atkin (see [2]). In the context of point counting on elliptic curves, it is most efficient to use curves of prime level N.

In this article we deal with an infinite family of modular curves $X_0(N)$ where N is composite of the simplest form, i.e. a product of two primes p_1 and p_2, which need not be distinct. Besides j, we also fix the second function generating the function field of $X_0(N)$ as a certain product of η-functions. This is motivated by the observation that the singular values of these functions at ideals of suitable orders in imaginary-quadratic number fields lie in the corresponding Hilbert and ring class fields [13]. The modular polynomials relating these functions and j can thus be used to explicitly determine

2000 *Mathematics Subject Classification*: 11F03, 14G35, 11G18.

elliptic curves with complex multiplication [4]. Moreover, the functions are computationally attractive because the corresponding class polynomials usually have small coefficients (see [3]). This is in accordance with the fact that the η products appear in Kronecker's limit formula for L-series of imaginary quadratic fields with ring class characters. In fact, the class number formulae derived by Meyer [6] show that these η quotients are in close correspondence to systems of fundamental units in ring class fields, so that they can be expected to provide in some sense "simple" algebraic numbers.

We show that the equations between j and the η products do indeed provide a model for the modular curve $X_0(N)$, and exhibit properties of the modular polynomials such as their degree in j and the values of certain coefficients.

2. The η products. Let $\Gamma = \mathrm{Sl}_2(\mathbb{Z})$ denote the full modular group, and for some positive integer N, let $\Gamma^0(N)$ be the congruence subgroup consisting of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ of determinant 1 such that $N \mid b$. Thus, $\Gamma = \Gamma^0(1)$. Denote by $\mathbb{C}_\Gamma$ resp. $\mathbb{C}_{\Gamma^0(N)}$ the fields of all modular functions invariant under Γ resp. $\Gamma^0(N)$, so that $\mathbb{C}_{\Gamma^0(N)}$ is the function field of $X_0(N)$ and $\mathbb{C}_\Gamma = \mathbb{C}(j)$ the function field of $X_0(1)$.

Throughout this article we denote by z a complex variable, by q its Fourier transform $q = q(z) = e^{2\pi i z}$ and by $q^{1/n}$ the nth root of q given by $e^{2\pi i z/n}$. In a similar vain, ζ_n stands for the canonical primitive nth root of unity $e^{2\pi i/n}$. Recall Dedekind's η-function, which is given by

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n) = q^{1/24} \Big(1 + \sum_{n=1}^{\infty} (-1)^n (q^{n(3n-1)/2} + q^{n(3n+1)/2})\Big),$$

and which is a modular form of weight 1/2.

Assume from now on, unless otherwise stated, that $N = p_1 p_2$ with p_1 and p_2 primes; here, $p_1 = p_2$ or $p_1 \in \{2, 3\}$ are possible choices. Let $s = 24/\gcd(24, (p_1 - 1)(p_2 - 1))$ be the integer measuring how far $(p_1 - 1)(p_2 - 1)$ is from being divisible by 24. We examine the function $\mathfrak{w}_{p_1,p_2}^s$ with

$$\mathfrak{w}_{p_1,p_2}(z) = \frac{\eta(z/p_1)\eta(z/p_2)}{\eta(z)\eta(z/p_1 p_2)}.$$

It is well known that $\mathfrak{w}_{p_1,p_2}$ is invariant under $\Gamma^0(N)$ (see [10, Theorem 1]). One may easily check this assertion once the transformation behaviour of η under Γ is known. The following result is taken from [14, Proposition 2]; a similar formula can be found in [1, p. 13].

THEOREM 1. *Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ be normalised such that $c \geq 0$, and $d > 0$ if $c = 0$. Write $c = \gamma 2^\lambda$ with γ odd; by convention, $\gamma = \lambda = 1$ if $c = 0$.*

Then

$$\eta(Mz) = \varepsilon(M)\sqrt{cz+d}\,\eta(z)$$

with $\Re(\sqrt{cz+d}) > 0$ *and*

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

Theorem 2. *$\mathfrak{w}_{p_1,p_2}$ is invariant under the Fricke–Atkin–Lehner involution w_N associated to the matrix $\left(\begin{smallmatrix}0 & -N\\ 1 & 0\end{smallmatrix}\right) \in \mathrm{Gl}_2(\mathbb{Z})$, i.e.,*

$$\mathfrak{w}_{p_1,p_2}\left(-\frac{N}{z}\right) = \mathfrak{w}_{p_1,p_2}(z).$$

Proof. We have

$$\mathfrak{w}_{p_1,p_2}\left(-\frac{N}{z}\right) = \frac{\eta(-p_2/z)\eta(-p_1/z)}{\eta(-p_1p_2/z)\eta(-1/z)} = \frac{\sqrt{z/p_2}\sqrt{z/p_1}}{\sqrt{z/p_1p_2}\sqrt{z}}\,\frac{\eta(z/p_2)\eta(z/p_1)}{\eta(z/p_1p_2)\eta(z)}$$

by Theorem 1. The choice of the complex square roots implies that this quantity indeed equals $\mathfrak{w}_{p_1,p_2}(z)$. ∎

To examine the modular polynomials relating $\mathfrak{w}_{p_1,p_2}^s$ and j, we need to know the conjugates of $\mathfrak{w}_{p_1,p_2}^s$ under the isomorphisms of $\mathbb{C}_{\Gamma^0(N)}/\mathbb{C}_\Gamma$; in other words, we need to know how unimodular transformations act on $\mathfrak{w}_{p_1,p_2}^s$, and an obvious approach is to study how they act on the components of $\mathfrak{w}_{p_1,p_2}^s$ given by $\eta(z/K)$ for $K \mid N$. In particular, the q-expansions of $\eta(z/K) \mid M$ for $M = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma$ play an important role. It is impossible, however, to derive them directly from the q-expansion of $\eta(z/K)$ since there is no general way of expressing $q(Mz) = e^{2\pi i(az+b)/(cz+d)}$ in terms of $q(z) = e^{2\pi iz}$ whenever $c \neq 0$. But using the transformation formula for η, we may obtain expressions from which the q-expansions are easily derived.

Theorem 3. *Let $K \in \mathbb{N}$ and $T = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma$ such that $c \geq 0$, and $d > 0$ if $c = 0$. Write*

$$ua + vKc = \delta = \gcd(a, Kc) = \gcd(a, K), \qquad U = \begin{pmatrix} a/\delta & -v\\ Kc/\delta & u\end{pmatrix}.$$

Then

$$\eta\left(\frac{Tz}{K}\right) = \varepsilon(U)\sqrt{\delta(cz+d)}\,\eta\left(\frac{\delta z + (ub + vKd)}{K/\delta}\right)$$

with $\varepsilon(U)$ as in Theorem 1.

Proof. Letting

$$R_0 = \begin{pmatrix}1 & 0\\ 0 & K\end{pmatrix}, \qquad R = \begin{pmatrix}\delta & ub+vKd\\ 0 & K/\delta\end{pmatrix},$$

one easily checks that $R_0 T = UR$ so that

$$\eta\left(\frac{Tz}{K}\right) = \eta(R_0 Tz) = \eta(URz).$$

An application of Theorem 1 yields the result. ∎

3. The modular polynomials. The modular polynomial associated to the function $\mathfrak{w}^s_{p_1,p_2} \in \mathbb{C}_{\Gamma^0(N)}$ is given by its characteristic polynomial (called "Hauptpolynom" in [1]) with respect to the field extension $\mathbb{C}_{\Gamma^0(N)}/\mathbb{C}_\Gamma$, i.e. by

$$\Phi_{p_1,p_2}(X) = \prod_{\sigma \in \mathrm{Iso}(\mathbb{C}_{\Gamma^0(N)}/\mathbb{C}_\Gamma)} (X - \sigma(\mathfrak{w}^s_{p_1,p_2})).$$

Notice that $\mathbb{C}_{\Gamma^0(N)}/\mathbb{C}_\Gamma$ is not a Galois extension, so that $\mathrm{Iso}(\mathbb{C}_{\Gamma^0(N)}/\mathbb{C}_\Gamma)$ is the set of embeddings of $\mathbb{C}_{\Gamma^0(N)}$ into the algebraic closure of $\mathbb{C}_\Gamma$. We call the $\sigma(\mathfrak{w}^s_{p_1,p_2})$ the *conjugates* of $\mathfrak{w}^s_{p_1,p_2}$. Furthermore, it is a priori not clear whether $\mathfrak{w}^s_{p_1,p_2}$ generates $\mathbb{C}_{\Gamma^0(N)}/\mathbb{C}_\Gamma$. We show in Theorem 8 that indeed it does, so that Φ_{p_1,p_2} is in fact the minimal polynomial of $\mathfrak{w}^s_{p_1,p_2}$. In principle, Φ_{p_1,p_2} is an element of $\mathbb{C}_\Gamma[X] = \mathbb{C}(j)[X]$. Since $\mathfrak{w}^s_{p_1,p_2}$ is holomorphic in the upper complex half plane (where η has neither zeroes nor poles) and its q-expansion is rational, Hasse's q-expansion principle implies that $\Phi_{p_1,p_2} \in \mathbb{Q}[j, X]$. In Theorem 7 we show that $\mathfrak{w}^s_{p_1,p_2}$ is entire, that is, the q-expansions of all of its conjugates have integral algebraic coefficients. Hence, the coefficients of the polynomial lie even in $\mathbb{Z}[j]$.

To study the modular polynomial Φ_{p_1,p_2}, we need an explicit description of the isomorphisms of $\mathbb{C}_{\Gamma^0(N)}/\mathbb{C}(j)$. For this purpose, according to [1], we introduce the set $\mathcal{M}_N$ of primitive integral 2×2 matrices of determinant N together with the equivalence relation $\sim_\Gamma$ given by $R \sim_\Gamma R'$ if $\Gamma R = \Gamma R'$ for $R, R' \in \mathcal{M}_N$. For the time being, we may lift the restrictions imposed on N.

Let $R_0 \in \mathcal{M}_N$ be fixed and let

$$R_i = \begin{pmatrix} a_i & b_i \\ 0 & d_i \end{pmatrix}, \quad i = 1, \ldots, \psi(N) = N \prod_{p \mid N,\, p \,\mathrm{prime}} \left(1 + \frac{1}{p}\right),$$

be the matrices in $\mathcal{M}_N$ with $a_i > 0$, $a_i d_i = N$, $\gcd(a_i, b_i, d_i) = 1$ and $0 \le b_i < d_i$. Then the R_i, $i \ge 1$, form a set of representatives of $\mathcal{M}_N$ modulo $\sim_\Gamma$. Since Γ acts transitively from the right on the classes of $\mathcal{M}_N$, there are unimodular matrices T_i and U_i such that $U_i R_i = R_0 T_i$, and the $R_0 T_i$ form an alternative set of representatives of $\mathcal{M}_N$ modulo $\sim_\Gamma$. If $g(z)$ is a modular function invariant under $R_0^{-1} \Gamma R_0 \cap \Gamma$, then its conjugates under the isomorphisms of $\mathbb{C}_{R_0^{-1}\Gamma R_0 \cap \Gamma}/\mathbb{C}(j)$ are given by the $g(T_i z)$, $i = 1, \ldots, \psi(N)$.

The matrices T_i and U_i may be computed as follows: Determine k_i and $\delta_i = -b_i + k_i a_i$ such that $\gcd(\delta_i, d_i) = 1$. This is possible since the arithmetic progression $(-b_i + ka_i)_{k\geq 0}$ contains infinitely many primes multiplied by $\gcd(a_i, b_i)$, and $\gcd(a_i, b_i)$ is coprime to d_i. Use the extended Euclidean algorithm to obtain α_i, $\beta_i \in \mathbb{Z}$ such that $\alpha_i\delta_i - \beta_i d_i = 1$. Then

$$U_i = \begin{pmatrix} \alpha_i & \beta_i \\ d_i & \delta_i \end{pmatrix}, \quad T_i = \begin{pmatrix} \alpha_i a_i & \alpha_i a_i k_i - 1 \\ 1 & k_i \end{pmatrix}.$$

So far, the description is completely generic and depends neither on N nor on the particular choice of R_0. Notice that $R_0 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & N \end{smallmatrix}\right)$ leads to $R_0^{-1}\Gamma R_0 \cap \Gamma = \Gamma^0(N)$, the case we are interested in. The factorisation of N is now needed to determine the possible values of the a_i and d_i, so from now on we assume again that N is the product of two primes p_1 and p_2. As a first step towards an explicit description of the conjugates of $\mathfrak{w}^s_{p_1,p_2}$, we provide a closed description for the matrices T_i introduced above.

Theorem 4. *Let $N = p_1p_2$ with p_1 and p_2 prime and $R_0 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & N \end{smallmatrix}\right)$. Then a set of representatives of $\mathcal{M}_N$ modulo $\sim_\Gamma$ is given by the R_0T with $T \in \mathcal{T}$, where $\mathcal{T}$ is defined as follows*:

- *for $p_1 \neq p_2$ and $u, v \in \mathbb{Z}$ such that $up_1 + vp_2 = 1$:*

$$\begin{aligned} \mathcal{T} = &\left\{\begin{pmatrix} 1 & \nu \\ 0 & 1 \end{pmatrix} : 0 \leq \nu < N\right\} \cup \left\{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right\} \\ &\cup \left\{\begin{pmatrix} \nu p_1 & -1 \\ 1 & 0 \end{pmatrix} : 1 \leq \nu < p_2\right\} \cup \left\{\begin{pmatrix} \nu p_2 & -1 \\ 1 & 0 \end{pmatrix} : 1 \leq \nu < p_1\right\} \\ &\cup \left\{\begin{pmatrix} up_1 & -vp_2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} vp_2 & -up_1 \\ 1 & 1 \end{pmatrix}\right\}; \end{aligned}$$

- *for $p_1 = p_2 = p$:*

$$\begin{aligned} \mathcal{T} = &\left\{\begin{pmatrix} 1 & \nu \\ 0 & 1 \end{pmatrix} : 0 \leq \nu < N\right\} \cup \left\{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right\} \\ &\cup \left\{\begin{pmatrix} \nu p & -1 \\ 1 & 0 \end{pmatrix} : 1 \leq \nu < p\right\}. \end{aligned}$$

Proof. We use the notation and consider the system of representatives introduced above, omitting the subscripts i for convenience. For $R = \left(\begin{smallmatrix} 1 & \nu \\ 0 & N \end{smallmatrix}\right)$, $0 \leq \nu < N$, put $U = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and obtain $UR = R_0T$ with $T = \left(\begin{smallmatrix} 1 & \nu \\ 0 & 1 \end{smallmatrix}\right)$. For $R = \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$, put $U = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and obtain $T = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

The further matrices depend on the factorisation of N. For $R = \left(\begin{smallmatrix} p_1 & b \\ 0 & p_2 \end{smallmatrix}\right)$, $1 \leq b < p_2$, choose $k = 0$, $\delta = -b$, $\alpha = \nu = -b^{-1} \bmod p_2 \in \{1, \dots, p_2 - 1\}$. Then $T = \left(\begin{smallmatrix} \nu p_1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, and as b varies over $\{1, \dots, p_2 - 1\}$, so does ν. If $p_1 = p_2$, there are no more matrices to consider.

For $p_1 \neq p_2$, the T corresponding to $R = \left(\begin{smallmatrix} p_2 & b \\ 0 & p_1 \end{smallmatrix}\right)$, $1 \leq b < p_1$, are obtained by symmetry. If $R = \left(\begin{smallmatrix} p_1 & 0 \\ 0 & p_2 \end{smallmatrix}\right)$, let $k = 1$, $\delta = p_1$, $\alpha = u$, which yields $T = \left(\begin{smallmatrix} up_1 & -vp_2 \\ 1 & 1 \end{smallmatrix}\right)$. Similarly, $T = \left(\begin{smallmatrix} vp_2 & -up_1 \\ 1 & 1 \end{smallmatrix}\right)$ is obtained from $R = \left(\begin{smallmatrix} p_2 & 0 \\ 0 & p_1 \end{smallmatrix}\right)$. ■

To state the main result on the conjugates of $\mathfrak{w}_{p_1,p_2}^s$, we need some additional notation.

Definition 5. If $g(z) = \sum_{k=k_0}^{\infty} a_k q^{k/N}$ with $q = e^{2\pi i z}$, $a_k \in \mathbb{C}$ and $a_{k_0} \neq 0$, is a modular function, we denote by

$$\operatorname{ord}(g) = \frac{k_0}{N}$$

its order at infinity and by

$$l(g) = a_{k_0}$$

its leading coefficient.

Notice that the order of j at infinity is -1, so that the order of a polynomial in j is nothing but its negative degree, and the notions of leading coefficients coincide.

Combining the results of Theorems 4 and 3, we obtain the conjugates of $\mathfrak{w}_{p_1,p_2}$ together with their explicit q-expansions, of which we retain only the orders and the leading coefficients.

Theorem 6. *Let $N = p_1 p_2$ with p_1 and p_2 prime. Then the conjugates of $\mathfrak{w}_{p_1,p_2}^s$ under the isomorphisms of $\mathbb{C}_{\Gamma^0(N)}/\mathbb{C}(j)$, their orders and their leading coefficients are given as follows*:

- *For $p_1 \neq p_2$*:

Conjugate	ord	l
$\mathfrak{w}_{p_1,p_2}^s(z+\nu),\ 0 \leq \nu < N$	$-\frac{s(p_1-1)(p_2-1)}{24p_1p_2}$	$\zeta_N^{-\nu s(p_1-1)(p_2-1)/24}$
$\mathfrak{w}_{p_1,p_2}^s(Nz)$	$-\frac{s(p_1-1)(p_2-1)}{24}$	1
$\left(\left(\frac{p_2}{p_1}\right)\frac{\eta(\frac{z+\nu}{p_1})\eta(p_2(z+\nu))}{\eta(z+\nu)\eta(\frac{p_2(z+\nu)}{p_1})}\right)^s,\ 0 \leq \nu < p_1$	$\frac{s(p_1-1)(p_2-1)}{24p_1}$	$\left(\frac{p_2}{p_1}\right)^s \zeta_{p_1}^{-\nu s(p_1-1)(p_2-1)/24}$
$\left(\left(\frac{p_1}{p_2}\right)\frac{\eta(p_1(z+\nu))\eta(\frac{z+\nu}{p_2})}{\eta(z+\nu)\eta(\frac{p_1(z+\nu)}{p_2})}\right)^s,\ 0 \leq \nu < p_2$	$\frac{s(p_1-1)(p_2-1)}{24p_2}$	$\left(\frac{p_1}{p_2}\right)^s \zeta_{p_2}^{-\nu s(p_1-1)(p_2-1)/24}$

- *For $p_1 = p_2 = p$*:

Conjugate	ord	l
$\mathfrak{w}_{p_1,p_2}^s(z+\nu),\ 0 \leq \nu < N$	$-\frac{s(p-1)^2}{24p^2}$	$\zeta_N^{-\nu s(p-1)^2/24}$
$\mathfrak{w}_{p_1,p_2}^s(Nz)$	$-\frac{s(p-1)^2}{24}$	1
$\sqrt{p}^s\varepsilon(\nu)\left(\frac{\eta(pz)^2}{\eta(z)\eta(z+k\nu/p)}\right)^s,\ 1 \leq \nu < p$	$\frac{s(p-1)}{12}$	$\sqrt{p}^s\varepsilon(\nu)\zeta_p^{-s'\nu}$

with $\varepsilon(\nu) = \left(\frac{3\nu}{p}\right)$ *if* $p \equiv 1 \pmod 4$, $\varepsilon(\nu) = 1$ *if* $p = 2$, $\varepsilon(\nu) = -1$ *otherwise*; $k = 1$ *for* $p = 2$, $k = 4$ *for* $p = 3$, $k = 24$ *otherwise*; $s' = 1$ *for* $p \in \{2, 3\}$, $s' = s$ *otherwise.*

Proof. Let us first derive the explicit formulae for the conjugates. We have to consider the functions

$$\mathfrak{w}_{p_1,p_2}^s(Tz) = \left(\frac{\eta\left(\frac{Tz}{K_1}\right)\eta\left(\frac{Tz}{K_2}\right)}{\eta\left(\frac{Tz}{K_3}\right)\eta\left(\frac{Tz}{K_4}\right)}\right)^s$$

with $K_1 = p_1$, $K_2 = p_2$, $K_3 = 1$, $K_4 = p_1p_2$ and T being one of the matrices of Theorem 4. We adopt the notations of Theorem 3 and its proof and designate by the subscript $i \in \{1, \ldots, 4\}$ the values corresponding to the term $\eta\left(\frac{Tz}{K_i}\right)$. Then

$$\mathfrak{w}_{p_1,p_2}^s(Tz) = \varepsilon\left(\sqrt{\frac{\delta_1\delta_2}{\delta_3\delta_4}}\right)^s \left(\frac{\eta(R_1z)\eta(R_2z)}{\eta(R_3z)\eta(R_4z)}\right)^s$$

with

$$\varepsilon = \left(\frac{\varepsilon(U_1)\varepsilon(U_2)}{\varepsilon(U_3)\varepsilon(U_4)}\right)^s.$$

Notice that the factors $\sqrt{cz+d}$ cancel since there are as many factors in the numerator as in the denominator. Furthermore,

$$\begin{aligned}\sqrt{\frac{\delta_1\delta_2}{\delta_3\delta_4}} &= \sqrt{\frac{\gcd(a,p_1)\gcd(a,p_2)}{\gcd(a,p_1p_2)}}\\ &= \begin{cases}\sqrt{p} & \text{for } p_1 = p_2 = p \text{ and } \gcd(a,p^2) = p,\\ 1 & \text{otherwise.}\end{cases}\end{aligned}$$

For $T = \left(\begin{smallmatrix}1 & \nu\\ 0 & 1\end{smallmatrix}\right)$, the conjugates $\mathfrak{w}_{p_1,p_2}^s(Tz)$ already have the desired form. If $T = \left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$, then $U_i = T$ independently of i and $R_i = \left(\begin{smallmatrix}K_i & 0\\ 0 & 1\end{smallmatrix}\right)$, which yields $\mathfrak{w}_{p_1,p_2}^s(Nz)$. The further conjugates require several case distinctions.

Case 1: $p_1 \neq p_2$. Let

$$T = \begin{pmatrix}\nu p_1 & -1\\ 1 & 0\end{pmatrix} \quad \text{with } 1 \leq \nu < p_2.$$

Then $\delta_1 = \delta_4 = p_1$, $\delta_2 = \delta_3 = 1$. Let $\mu = -(\nu p_1)^{-1} \bmod p_2 \in \{1, \ldots, p_2 - 1\}$, $u_2 = u_3 = -\mu$, $u_1 = u_4 = -p_1\mu$, $v_2 = v_4 = (1 + p_1\mu\nu)/p_2$, $v_1 = v_3 = p_2v_2$. We then have

$$R_1 = \begin{pmatrix}p_1 & p_1\mu\\ 0 & 1\end{pmatrix},\ R_2 = \begin{pmatrix}1 & \mu\\ 0 & p_2\end{pmatrix},\ R_3 = \begin{pmatrix}1 & \mu\\ 0 & 1\end{pmatrix},\ R_4 = \begin{pmatrix}p_1 & p_1\mu\\ 0 & p_2\end{pmatrix},$$

$$U_1 = \begin{pmatrix} \nu & -p_2 v_2 \\ 1 & -p_1 \mu \end{pmatrix}, \qquad U_2 = \begin{pmatrix} \nu p_1 & -v_2 \\ p_2 & -\mu \end{pmatrix},$$

$$U_3 = \begin{pmatrix} \nu p_1 & -p_2 v_2 \\ 1 & -\mu \end{pmatrix}, \quad U_4 = \begin{pmatrix} \nu & -v_2 \\ p_2 & -p_1 \mu \end{pmatrix}.$$

(a) Let $p_2 \neq 2$. Then the product of the Legendre symbols contributing to ε is

$$\left(\frac{\left(\frac{\nu}{1}\right)\left(\frac{\nu p_1}{p_2}\right)}{\left(\frac{\nu p_1}{1}\right)\left(\frac{\nu}{p_2}\right)} \right)^s = \left(\frac{p_1}{p_2}\right)^s.$$

Considering only the first term in the exponent of the 24th root of unity, we obtain

$$\zeta_{24}^{\nu s(-p_2 v_2 - p_1 v_2 + p_1 p_2 v_2 + v_2)} = \zeta_{24}^{\nu v_2 s(p_1 - 1)(p_2 - 1)} = 1$$

since $24 \mid s(p_1 - 1)(p_2 - 1)$. Similar considerations for the further terms in the exponent show that the 24th root of unity vanishes completely.

(b) If $p_2 = 2$, then the γ_i and λ_i corresponding to the matrices U_i (cf. Theorem 1) are given by $\gamma_1 = \gamma_2 = \gamma_3 = \gamma_4 = 1$, $\lambda_1 = \lambda_3 = 0$ and $\lambda_2 = \lambda_4 = 1$. The product of Legendre symbols is now trivially 1 and equals $\left(\frac{p_1}{p_2}\right)^s$ since either $2 \mid s$ or $8 \mid p_1 - 1 = (p_1 - 1)(p_2 - 1)$. The terms in the exponent of the 24th root of unity having to do with γ or λ, which did not occur in the previous case, lead to

$$\zeta_{24}^{3s((\nu-1)+(\nu p_1 - 1)-(\nu p_1 - 1)-(\nu - 1))} = 1$$

and

$$\zeta_{24}^{\frac{3}{2}s((\nu^2 p_1^2 - 1)-(\nu^2 - 1))} = \zeta_8^{\nu^2 s(p_1 - 1)(p_1 + 1)/2} = 1$$

since $8 \mid s(p_1 - 1)$.

Thus whether p_1 equals 2 or not, $\varepsilon = \left(\frac{p_1}{p_2}\right)^s$.

When ν varies over $\{1, \ldots, p_2 - 1\}$, so does μ, and we obtain indeed the conjugates of the fourth line for $\nu \neq 0$. The further conjugates in this case are derived similarly.

CASE 2: $p_1 = p_2 = p$. Let

$$T = \begin{pmatrix} \nu p & -1 \\ 1 & 0 \end{pmatrix} \quad \text{with } 1 \leq \nu < p.$$

Then $\delta_1 = \delta_2 = \delta_4 = p$, $\delta_3 = 1$,

$$U_1 = U_2 = \begin{pmatrix} \nu & -1 \\ 1 & 0 \end{pmatrix}, \quad U_3 = \begin{pmatrix} \nu p & -1 \\ 1 & 0 \end{pmatrix}, \quad U_4 = \begin{pmatrix} \nu & -v_4 \\ p & u_4 \end{pmatrix},$$

$$R_1 = R_2 = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \quad R_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad R_4 = \begin{pmatrix} p & -u_4 \\ 0 & p \end{pmatrix}.$$

Here, u_4 is an inverse of ν modulo p and $v_4 = (1 - u_4\nu)/p$. A complication is introduced by the fact that for an arbitrary choice of u_4, the root of unity may not cancel. We thus have to take into account an additional constraint modulo 24, which will be dealt with later.

(a) Let $p \notin \{2, 3\}$. Then the Legendre symbols in ε multiply to yield $\left(\frac{\nu}{p}\right)^s$. The exponent of the root of unity is computed as

$$s(3(p-1) - 3p\nu + 2\nu + v_4\nu - pu_4 + p\nu(u_4\nu)).$$

After replacing $u_4\nu$ by $1 - v_4 p$, it becomes

$$(3 - 2\nu)s(p-1) - v_4\nu s(p^2 - 1) - psu_4 \equiv 3s(p-1) - psu_4 \pmod{24}$$

since $12 \mid s(p-1)$ and $24 \mid s(p^2 - 1)$. We may choose $u_4 = -24\mu$ with $\mu \in \{1, \ldots, p-1\}$ and $u_4 \equiv \nu^{-1} \pmod{p}$. Then the term $-psu_4$ vanishes, and we obtain

$$\varepsilon = \left(\frac{\nu}{p}\right)^s (-1)^{s(p-1)/4}.$$

If $p \equiv 3 \pmod{4}$, then $2 \parallel s$ and $\varepsilon = -1$. If $p \equiv 1 \pmod{4}$, then $2 \nmid s$, $(-1)^{(p-1)/4} = \left(\frac{2}{p}\right)$ and

$$\varepsilon = \left(\frac{2\nu}{p}\right)^s = \left(\frac{-2\nu^{-1}}{p}\right) = \left(\frac{48\mu}{p}\right) = \left(\frac{3\mu}{p}\right).$$

The result on the conjugates follows since together with ν, also μ varies over $\{1, \ldots, p-1\}$.

(b) For $p = 3$, we have $s = 6$ and may choose $u_4 = -4\mu$ with $\mu \in \{1, \ldots, p-1\}$ and $\mu \equiv \nu^{-1} \pmod{p}$. Then the term $-psu_4$ in the exponent vanishes again, and we obtain $\varepsilon = -1$.

(c) For $p = 2$, we have $s = 24$ and trivially $\varepsilon = 1$.

The assertions on the orders and leading coefficients are now readily derived from the facts that $\operatorname{ord}(\eta) = \frac{1}{24}$, $l(\eta) = 1$ and $q\left(\frac{az+b}{d}\right) = e^{2\pi i(az+b)/d} = \zeta_d^b q(z)^{a/d}$. ∎

Following [15], we denote by $\mathcal{F}_N$ the set of modular functions of level N all conjugates of which have q-expansions with coordinates in $\mathbb{Q}(\zeta_N)$.

Theorem 7. *Under the assumptions of Theorem* 6, *the function* $\mathfrak{w}_{p_1,p_2}^s$ *lies in* $\mathcal{F}_N$. *Furthermore*, $\Phi_{p_1,p_2} \in \mathbb{Z}[j, X]$.

Proof. Concerning membership in $\mathcal{F}_N$, by Theorem 6, all conjugates satisfy the required condition on their q-expansions except for possibly the last set of conjugates in the case $p_1 = p_2 = p$. Noticing that $q(z + k\nu/p)^{s/24} = \zeta_p^{sk\nu/24} q^{1/24}$ and $24 \mid sk$, the only possible obstacle comes from $\sqrt{p}^s$ for s odd. But then $p \equiv 1 \pmod{4}$, and $\sqrt{p} \in \mathbb{Z}[\zeta_p]$.

A closer examination shows that the q-expansion coefficients of the conjugates even lie in $\mathbb{Z}[\zeta_N]$ since $l(\eta) = 1$. In particular, $\mathfrak{w}_{p_1,p_2}^s$ is entire. As it is furthermore holomorphic and has a rational q-expansion, Hasse's principle proves that $\Phi_{p_1,p_2} \in \mathbb{Z}[j, X]$. ∎

THEOREM 8. *Under the assumptions of Theorem* 6, *the polynomial* Φ_{p_1,p_2} *is an affine model for the modular curve* $X_0(N)$.

Proof. It suffices to show that $\mathfrak{w}_{p_1,p_2}^s$ generates $\mathbb{C}_{\Gamma^0(N)}/\mathbb{C}(j)$, i.e. that Φ_{p_1,p_2} is the minimal polynomial of $\mathfrak{w}_{p_1,p_2}^s$. In any case, Φ_{p_1,p_2} is a power of the minimal polynomial. By Theorem 6, $\mathfrak{w}_{p_1,p_2}^s(Nz)$ is a simple root of Φ_{p_1,p_2} since it is the only root of order $-s(p_1-1)(p_2-1)/24$. This observation finishes the proof. ∎

Theorem 6 also allows us to determine certain terms of Φ_{p_1,p_2}.

THEOREM 9. *Under the assumptions of Theorem* 6, Φ_{p_1,p_2}, *seen as a polynomial in* j *with coefficients in* $\mathbb{Z}[X]$, *has degree* $s(p_1-1)(p_2-1)/12$. *Its leading term is* $X^{p_1+p_2}$ *for* $p_1 \neq p_2$ *and* X^{p-1} *for* $p_1 = p_2 = p$. *Seen as a polynomial in* X *with coefficients in* $\mathbb{Z}[j]$, *it has constant term* 1 *for* $p_1 \neq p_2$ *and* $p^{s(p-1)/2}$ *for* $p_1 = p_2 = p$.

Proof. The coefficient $e_{\psi(N)-i}$ of $X^{\psi(N)-i}$ in Φ_{p_1,p_2} is (up to sign) the elementary symmetric function of degree i in the conjugates of $\mathfrak{w}_{p_1,p_2}^s$. By Theorem 6, there are N conjugates of order $-s(p_1-1)(p_2-1)/24N$ and one conjugate of order $-s(p_1-1)(p_2-1)/24$, while all others have positive orders. Thus,

$$\begin{aligned}\operatorname{ord}(e_{\psi(N)-i}) &\geq -N\,\frac{s(p_1-1)(p_2-1)}{24N} - \frac{s(p_1-1)(p_2-1)}{24}\\ &= -\frac{s(p_1-1)(p_2-1)}{12}\end{aligned}$$

by the triangle inequality. If $i < N+1$, then no term contains all conjugates of negative order; if $i > N+1$, then each term contains a conjugate of positive order. Hence, in these cases the above inequality is strict. If $i = N+1$, however, then the term in $e_{\psi(N)-i}$ corresponding to the product of the conjugates of negative orders has the exact order $-s(p_1-1)(p_2-1)/12$, and all others have larger orders. This shows that $\operatorname{ord}(e_{\psi(N)-1}) = -s(p_1-1)(p_2-1)/12$ and

$$l(e_{\psi(N)-1}) = (-1)^{N+1}\Big(\prod_{\nu=0}^{N-1}\zeta_N^\nu\Big)^{-s(p_1-1)(p_2-1)/24} = 1.$$

Now the remark after Definition 5 implies the assertion on the degree in j.

Concerning the constant coefficient e_0, it equals the product of all conjugates since $\psi(N)$ is even, and Theorem 6 shows that it is of order 0 and its leading coefficient is $\big(\big(\frac{p_1}{p_2}\big)^{p_1}\big(\frac{p_2}{p_1}\big)^{p_2}\big)^s = 1$ if $p_1 \neq p_2$ and $(\sqrt{p})^{s(p-1)}\prod_{\nu=1}^{p}\varepsilon(\nu)$ $= p^{s(p-1)/2}$ if $p_1 = p_2 = p$. ∎

4. Examples and conclusion. Using the explicit description of the conjugates of the modular functions given in Theorem 6, one can compute the modular polynomials following the standard approach, described for instance in [7] and [8, Chapter 5], for modular curves of prime level. The basic idea is to replace the conjugates by their q-expansions, to compute the coefficients of the modular polynomials as Laurent series in q and to rewrite them as polynomials in j. We developed a different approach, based on evaluating the conjugates in several complex arguments and polynomial interpolation, which will be described in detail in a forthcoming article.

As a first example, consider the smallest polynomial obtained with $p_1, p_2 \notin \{2,3\}$:

$$\begin{aligned}
\Phi_{5,7} = {} & X^{48} + (-j + 708)X^{47} + (35j + 171402)X^{46} \\
& + (-525j + 15185504)X^{45} + (4340j + 248865015)X^{44} \\
& + (-20825j + 1763984952)X^{43} + (52507j + 6992359702)X^{42} \\
& + (-22260j + 19325688804)X^{41} + (-243035j + 42055238451)X^{40} \\
& + (596085j + 70108209360)X^{39} + (-272090j + 108345969504)X^{38} \\
& + (-671132j + 121198179480)X^{37} + (969290j + 155029457048)X^{36} \\
& + (-1612065j + 97918126080)X^{35} + (2493785j + 141722714700)X^{34} \\
& + (647290j - 1509796288)X^{33} + (-3217739j + 108236157813)X^{32} \\
& + (3033590j - 93954247716)X^{31} + (-5781615j + 91135898154)X^{30} \\
& + (1744085j - 108382009680)X^{29} + (1645840j + 66862445601)X^{28} \\
& + (-2260650j - 66642524048)X^{27} + (6807810j + 38019611082)X^{26} \\
& + (-2737140j - 28638526644)X^{25} + (2182740j + 17438539150)X^{24} \\
& + (-125335j - 8820058716)X^{23} + (-1729889j + 5404139562)X^{22} \\
& + (1024275j - 1967888032)X^{21} + (-1121960j + 1183191681)X^{20} \\
& + (395675j - 370697040)X^{19} + (-54915j + 103145994)X^{18} \\
& + (15582j - 42145404)X^{17} + (34755j - 15703947)X^{16} \\
& + (-6475j - 3186512)X^{15} + (1120j - 4585140)X^{14} \\
& + (-176j + 1313040)X^{13} + (j^2 - 1486j - 38632)X^{12} \\
& + (-7j + 399000)X^{11} + (-19j + 211104)X^{10} + (-9j + 6771)X^{8} \\
& + (8j - 6084)X^{7} + (7j - 5258)X^{6} + (j - 792)X^{5} - 105X^{4} + 16X^{3} \\
& + 42X^{2} + 12X + 1.
\end{aligned}$$

The degree of the polynomial in j is indeed 2 and the unique appearance of j^2 is in front of $X^{12} = X^{p_1+p_2}$ as predicted by Theorem 9.

Notice that from a geometric point of view, this equation is certainly not optimal: It is known from [11] that the modular curve of level 35 is hyperelliptic of genus 3. While our equation confirms the hyperellipticity, it has (affine) singularities, which is reflected by the fact that its degree in X exceeds 8. Furthermore, its coefficients are considerably larger than those of the model in [12, 16]. This kind of behaviour appears to be unavoidable as long as we choose j as separating variable, which is important for applications in which one wishes to relate the modular polynomial to concrete equations of elliptic curves (e.g., the determination of the number of rational isogenies or the construction of elliptic curves with complex multiplication [4]).

As another example, we provide the curve of level 9:

$$\begin{aligned}\Phi_{3,3} = {} & X^{12} + (-j + 684)X^{11} + (54j + 158058)X^{10} \\ & + (-1053j + 12812940)X^9 + (8712j + 111071655)X^8 \\ & + (-24948j + 350544024)X^7 + (-13608j + 428079276)X^6 \\ & + (74088j + 137660472)X^5 + (31104j + 29200095)X^4 \\ & + (-7291j + 3832380)X^3 + (j^2 - 1494j + 361098)X^2 \\ & + (-27j + 20412)X + 729.\end{aligned}$$

This curve is of genus 0, but its degree in j is not 1. So unlike the rational curves of level 2 obtained by Weber's functions, this equation does not yield a rational expression for j in terms of the second function on $X_0(N)$. Notice that by Theorem 9, the degree of our modular polynomials in j is always even. This is correlated with the fact that the $\mathfrak{w}^s_{p_1,p_2}$ are invariant under the Fricke–Atkin–Lehner involution as shown in Theorem 7, whence they are functions on $X_0^+(N)$. This could be used to factor the extension $\mathbb{C}(\mathfrak{w}^s_{p_1,p_2}, j)/\mathbb{C}(\mathfrak{w}^s_{p_1,p_2})$ through $X_0^+(N)$, an approach that deserves further studying.

Acknowledgements. We thank François Morain, whose interest in this work was a great motivation for our research. The first author gratefully acknowledges the support through a fellowship within the postdoctoral programme of the German Academic Exchange Service (DAAD). His research was partially supported by the French Ministry of Research — ACI Cryptologie.

References

[1] M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, in: Enzyklop. d. math. Wissenschaften, Volume I 2, Heft 10, Teubner, Stuttgart, 2nd ed., 1958.

[2] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, in: D. A. Buell and J. T. Teitelbaum (eds.), Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin, Stud. Adv. Math. 7, Amer. Math. Soc., 1998, 21–76.

[3] A. Enge and F. Morain, *Comparing invariants for class fields of imaginary quadratic fields*, in: C. Fieker and D. R. Kohel (eds.), Algorithmic Number Theory—ANTS-V, Lecture Notes in Comput. Sci. 2369, Springer, Berlin, 2002, 252–266.

[4] A. Enge and R. Schertz, *Constructing elliptic curves over finite fields using double eta-quotients*, J. Théor. Nombres Bordeaux 16 (2005), 555–568.

[5] T. Hibino and N. Murabayashi, *Modular equations of hyperelliptic $X_0(N)$ and an application*, Acta Arith. 82 (1997), 279–291.

[6] C. Meyer, *Die Berechnung der Klassenzahl abelscher Körper über quadratischen Zahlkörpern*, Akademie-Verlag, Berlin, 1957.

[7] 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.

[8] V. Müller, *Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei*, Dissertation, Univ. des Saarlandes, Saarbrücken, 1995.

[9] N. Murabayashi, *On normal forms of modular curves of genus* 2, Osaka J. Math. 29 (1992), 405–418.

[10] M. Newman, *Construction and application of a class of modular functions* (II), Proc. London Math. Soc. (3) 9 (1959), 373–387.

[11] A. P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France 102 (1974), 449–462.

[12] J. G. Rovira, *Equations of hyperelliptic modular curves*, Ann. Inst. Fourier (Grenoble) 41 (1991), 779–795.

[13] R. Schertz, *Zur expliziten Berechnung von Ganzheitsbasen in Strahlklassenkörpern über einem imaginär-quadratischen Zahlkörper*, J. Number Theory 34 (1990), 41–53.

[14] —, *Weber's class invariants revisited*, J. Théor. Nombres Bordeaux 14 (2002), 325–343.

[15] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton Univ. Press, 1971.

[16] M. Shimura, *Defining equations of modular curves $X_0(N)$*, Tokyo J. Math. 18 (1995), 443–456.

INRIA Futurs & LIX (CNRS/UMR 7161)
École polytechnique
91128 Palaiseau Cedex, France
E-mail: enge@lix.polytechnique.fr

Institut für Mathematik
Universität Augsburg
86135 Augsburg, Germany
E-mail: schertz@math.uni-augsburg.de

Received on 28.10.2003
and in revised form on 2.11.2004 (4652)