ELLIPTIC FUNCTIONS AND EQUATIONS OF MODULAR CURVES

LEV A. BORISOV, PAUL E. GUNNELLS, AND SORIN POPESCU

Abstract. Let $p \geq 5$ be a prime. We show that the space of weight one Eisenstein series defines an embedding into $\mathbb{P}^{(p-3)/2}$ of the modular curve $X_1(p)$ for the congruence group $\Gamma_1(p)$ that is scheme-theoretically cut out by explicit quadratic equations.

1. Introduction

Modular curves are compactifications of quotients of the upper half plane $\mathfrak{H}$ by arithmetic groups $\Gamma \subset \mathrm{SL}_2(\mathbb{Q})$ acting on $\mathfrak{H}$ via Möbius transformations. The group varies depending on the type of polarization and, when appropriate, the choice of the level structure (see [15] for a full account). Since Γ is arithmetic, in other words commensurable with $\mathrm{SL}_2(\mathbb{Z})$, the quotient $\Gamma\backslash\mathfrak{H}$ is an open Riemann surface that can be compactified to the modular curve $X(\Gamma)$ by the addition of finitely many points (cusps).

Historically, several cases are of particular interest. The classical one is where Γ is the principal congruence subgroup $\Gamma(p) \subset \mathrm{SL}_2(\mathbb{Z})$ of level p, consisting of all matrices congruent to the identity matrix modulo an odd prime number p, and where the modular curve $X(p) := X(\Gamma(p))$ parameterizes elliptic curves with canonical level structure of order p (i.e. with fixed isomorphisms between their group of p-torsion points with the Weil pairing, and the abstract group $(\mathbb{Z}/p\mathbb{Z})^2$ with a certain standard symplectic paring). It is standard knowledge (see for instance [15], Section 1.6) that $X(1) = \mathbb{P}^1$, having one cusp, and that $X(p)$ has genus $(p^2-1)(p-6)/24+1$ and $(p^2-1)/2$ cusps if $p \geq 3$. Several natural embedded models of $X(p)$ have been extensively studied starting perhaps with Felix Klein ([11], [12]). The best understood model is the so-called z-modular curve in $\mathbb{P}^{(p-3)/2} = \mathbb{P}(V_-)$, which is essentially the image in the negative eigenspace of the Heisenberg involution, acting on $\mathbb{P}^{p-1}$, of the 0-section of the universal elliptic curve over $X(p)$ under a morphism whose restriction to each smooth fiber is induced by p times the origin of that elliptic curve. It is known that the z-modular curve is smooth [17], Théorème 10.6. The large symmetry group $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ of the z-modular curve accounts for interesting geometry and highly

Date: May 22, 2000.
1991 *Mathematics Subject Classification.* 11F11, 14G35, 14H52, 14H70.
Key words and phrases. modular forms, modular curves, elliptic functions.
The third author was partially supported by NSF grant DMS-9610205.

structured defining equations. When $p = 7$, the z-modular curve in $\mathbb{P}^2$ is defined by Klein's quartic $x_0^3x_1 + x_1^3x_2 + x_2^3x_0 = 0$, whose automorphisms group $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$ has maximal possible order for its genus [11], [17] (see also [9], Example 2.10). For $p = 11$, the z-modular curve in $\mathbb{P}^4$ is defined by the 4×4-minors of the Hessian of the unique $\mathrm{PSL}_2(\mathbb{Z}/11\mathbb{Z})$-invariant cubic hypersurface $W \subset \mathbb{P}^4$ given by the equation $v^2w + w^2x + x^2y + y^2z + z^2v = 0$. We refer for these and other beautiful facts about the geometry of $X(11)$ to [12], pp. 153-156, [7], [1], [10]. In general, one has the following beautiful picture (cf. [1], Theorem 19.7, p. 56): There exists a $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$-equivariant isomorphism $\Phi : S^2(V_-) \cong \Lambda^2(V_+)$, where $V_\pm$ denote the $\pm$-eigenspaces of the Heisenberg involution, such that by means of Φ the z-curve coincides with ${\nu_2}^{-1}(\mathrm{Gr}(2, V_+))$, where $\mathrm{Gr}(2, V_+) \subset \mathbb{P}(\Lambda^2(V_+))$ denotes the Plücker embedding of the Grassmannian of 2-dimensional linear subspaces in V_+, and $\nu_2 : \mathbb{P}(V_-) \to \mathbb{P}(S^2(V_-))$ denotes the quadratic Veronese embedding. See also [9], Corollary 2.9 and Example 2.10, and [10], §2, and proof and discussion before of Lemma 2.1, for a different approach to this description of the z-curve. It is conjectured that the z-modular curve is linearly normal and that the rank 2 vector bundle corresponding to the embedding into $\mathrm{Gr}(2, V_+)$ is stable (see [1], [6] for details).

In this paper we investigate natural equations for $X_1(p) := X(\Gamma_1(p))$, the modular curve for the congruence subgroup $\Gamma_1(p)$ of matrices satisfying

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod p \right\},$$

where $p \geq 3$ is a prime. Our point of view is quite different from the one described above for $X(p)$—our embedding uses certain modular forms of weight one, whereas the embedding of the z-modular curve uses forms of weight $(p-3)/(2p-12)$. It would be very interesting to somehow relate these two approaches.

In our case the modular curve $X_1(p)$ parameterizes elliptic curves with a choice of non-trivial p-torsion point. Furthermore, $X_1(p)$ is a smooth curve of genus $(p-5)(p-7)/24$ with $(p-1)$ cusps for $p \geq 5$ (see [15]). We consider in this paper the linear system on $X_1(p)$ defined by weight one Eisenstein series, and show that it defines an embedding of $X_1(p)$ into $\mathbb{P}^{(p-3)/2}$ (see Corollary 2.2). Our main result is an explicit description of the equations defining this embedding:

Theorem 4.5. *Let $p \geq 5$ be a prime number. The space of weight one Eisenstein series defines an embedding of the modular curve $X_1(p) \subset \mathbb{P}^{(p-3)/2}$ that is scheme-theoretically cut out by the quadratic equations*

$$\begin{aligned} (p-4)(s_as_b + s_bs_c + s_cs_a) =& 2s_a^2 + 2s_b^2 + 2s_c^2 - \frac{4}{p-2}\sum_{k\neq 0} s_k^2 \\ &+ \sum_{k\neq 0,a} s_ks_{a-k} + \sum_{k\neq 0,b} s_ks_{b-k} + \sum_{k\neq 0,c} s_ks_{c-k}, \end{aligned}$$

for all $a, b, c \in (\mathbb{Z}/p\mathbb{Z})^*$ *with* $a+b+c=0$, *where* $\{s_a\}_{a\in(\mathbb{Z}/p\mathbb{Z})^*}$ *is a suitable system of coordinates with* $s_{-a} = -s_a$.

In contrast with the conjectural picture for $X(p)$, our embedding $X_1(p) \subset \mathbb{P}^{(p-3)/2}$ is in general neither linearly nor quadratically normal. In fact, the failure of linear or quadratic normality reflects the existence of certain modular forms (see Remark 4.6 for the precise statement).

The equations of $X_1(p)$ can be greatly simplified by considering a related embedding of $X_1(p)$ into the weighted projective space $\mathbb{P}(1, \ldots, 1, 2, \ldots, 2)$ with $(p-1)/2$ variables s_a of weight one and symmetry as above, and with $(p-1)/2$ variables t_a of weight two and symmetry $t_{-a} = t_a$:

Theorem 4.4. *The quadratic relations*

$$s_a s_b + s_b s_c + s_c s_a + t_a + t_b + t_c = 0,$$

for all $a, b, c \in (\mathbb{Z}/p\mathbb{Z})^*$ *with* $a+b+c=0$, *scheme-theoretically cut out the modular curve* $X_1(p) \subset \mathbb{P}(1, \ldots, 1, 2, \ldots, 2)$.

The paper is structured as follows. In Section 2 we recall first results from [2] and [3] concerning modular forms for $\Gamma_1(p)$, then show that weight one Eisenstein series define an embedding of the modular curve and compute equations vanishing on the image of this embedding (Proposition 2.4). In Section 3 we introduce a system of differential equations (2) that mimics the system satisfied by elliptic functions with poles of order one along a subgroup of order p. We construct Laurent series solutions to this system, and show that they satisfy the defining quadratic equations of a (possibly degenerate) elliptic normal curve in $\mathbb{P}^{p-1}$. Finally, in Section 4 we use a deformation argument to show that a deformation of the solutions of the system of differential equations leads to a deformation of elliptic curve, thus eventually showing that the equations in Theorem 4.5 cut out scheme-theoretically the modular curve.

It is worth mentioning that the elliptic functions appearing in this paper can be interpreted as discrete versions of the solutions of the associative Yang-Baxter equation that was introduced in a recent paper of Polishchuk [**?**].

Acknowledgements. It is a pleasure to thank Igor Krichever and Pavel Etingof for useful discussions. We are also grateful to Dan Grayson and Mike Stillman for *Macaulay2* [8], which helped us to carefully check the structure of the equations described in this paper.

2. Embedding modular curves by Eisenstein series of weight one

Let p be a natural number, and let $\Gamma_1(p)$ be as in Section 1. For any positive integer r, let $\mathscr{M}_r(p) := \mathscr{M}_r(\Gamma_1(p))$ be the $\mathbb{C}$-vector space of weight r holomorphic modular forms for $\Gamma_1(p)$.

Most results of this section hold with minor modifications for non-prime levels, but for simplicity we consider only odd prime levels p. Let

$$\vartheta(z,\tau) = q^{\frac{1}{8}}(2\sin\pi z)\prod_{l=1}^{\infty}(1-q^l)\prod_{l=1}^{\infty}(1-q^l\mathrm{e}^{2\pi\mathrm{i}z})(1-q^l\mathrm{e}^{-2\pi\mathrm{i}z}),$$

be the Jacobi theta function, where $q=\mathrm{e}^{2\pi\mathrm{i}\tau}$ (cf. [5]). As a theta function with characteristic this is $\vartheta_{1,1}(z,\tau)$ (cf. [14]). The following functions on the upper half plane

$$s_a(\tau) := \frac{1}{2\pi\mathrm{i}}\frac{d}{dz}\ln\vartheta(z,\tau)|_{z=a/p} = \frac{\xi^a+1}{2(\xi^a-1)} - \sum_d q^d\sum_{k|d}(\xi^{ka}-\xi^{-ka}),$$

where $\xi=\mathrm{e}^{2\pi\mathrm{i}/p}$ and a is an integer with $a\neq 0 \bmod p$, are modular forms of weight one with respect to the group $\Gamma_1(p)$ (see for instance [13]). In fact, $s_a = s_{a+p}$ and thus we will regard the subscripts a as elements of $(\mathbb{Z}/p\mathbb{Z})^*$. Moreover it follows directly from the definition that $s_{-a}=-s_a$. Notice that each $s_a(\tau)$ is an Eisenstein series. Our notation here differs slightly from that of [2], [3] and [4]. What we denote by s_a here was called $s_{a/p}$ in those papers. We will need the following results:

Theorem 2.1. ([2], [3], [4]) *The subring $\mathscr{T}_*(p)\subset\mathscr{M}_*(p)$ generated by the s_a is Hecke-stable. Moreover, for weights $k\geq 3$ we have $\mathscr{T}_k(p)=\mathscr{M}_k(p)$, while for weight two $\mathscr{T}_2(p)$ is the direct sum of the space of Eisenstein series and the span of Hecke eigenforms of analytic rank zero.*

Corollary 2.2. *The map $X_1(p)\to\mathbb{P}^{(p-3)/2}$ that sends τ to $\{s_a(\tau)\}$ defines a closed embedding of $X_1(p)$ into $\mathbb{P}^{(p-3)/2}$.*

Remark 2.3. One may prove directly this corollary without using the calculations in [4]. For instance, to show that the map defined by the weight one forms s_a separates points, different from the cusps, one reconstructs the values of $s^{(k)}_{a/p}$, in the notation of [2], up to a scaling factor c^k. This allows reconstruction of the elliptic functions

$$\frac{\vartheta(a/p-cz,\tau)\vartheta_z(0,\tau)}{\vartheta(-cz,\tau)\vartheta(a/p,\tau)} = \exp(\sum_{k\geq 1}(2\pi\mathrm{i}z)^k\frac{s^{(k)}_{a/p}}{k!}).$$

Their poles and zeros determine uniquely up to scaling a lattice Λ in $\mathbb{C}$ together with an element of order p in $\mathbb{C}/\Lambda$. Therefore, $\{s_a\}_{a\in(\mathbb{Z}/p\mathbb{Z})^*}$ determine uniquely a point of $X_1(p)$. We leave the details to the reader.

Since the s_a's define an embedding, we will abuse notation and denote in the sequel the image of the embedding of the modular curve in $\mathbb{P}^{(p-3)/2}$ simply by $X_1(p)$.

The following proposition follows easily from Lemma 4.8 in [2] for $N=2$, and Propositions 4.7 and 4.8 in [3]:

Proposition 2.4. *The weight two modular forms*

$$t_a(\tau) := \frac{1}{2}(2\pi \mathrm{i})^{-2}\left(\frac{\vartheta_{zz}(a/p,\tau)}{\vartheta(a/p,\tau)} - \frac{\vartheta_{zzz}(0,\tau)}{3\vartheta_z(0,\tau)}\right) = \frac{1}{12} - \sum_{d>0} q^d \sum_{k|d} \frac{d}{k}(\xi^{ak}+\xi^{-ak}),$$

where $a \in (\mathbb{Z}/p\mathbb{Z})^*$, satisfy the following quadratic relations

$$s_a s_b + s_b s_c + s_c s_a + t_a + t_b + t_c = 0 \tag{1}$$

for every triple of numbers $a, b, c \in (\mathbb{Z}/p\mathbb{Z})^*$ with $a+b+c=0$. In particular, the symmetry of the s_a's implies $t_{-a} = t_a$.

In fact the set of equations (1) allows one to express $\{t_a\}$ in terms of $\{s_a\}$, and thus gives rise to degree two relations involving only $\{s_a\}$. The goal of this paper is to show that these relations cut out the curve $X_1(p)$ scheme-theoretically.

We will need the following results in the remaining two sections. First of all, notice that the group $(\mathbb{Z}/p\mathbb{Z})^*$ acts on s_a and t_a by $s_a \rightsquigarrow s_{ak}$, $t_a \rightsquigarrow t_{ak}$. Moreover, the action of the Fricke involution (see for example [13]) on $X_1(p)$ also lifts to an action w_p on $\{s_a\}$ and $\{t_a\}$:

Proposition 2.5. *The Fricke involution w_p acts on the ring $\mathbb{C}[s_1, \dots, s_{p-1}, t_1, \dots, t_{p-1}]$ as follows:*

$$w_p(s_a) = (-p)^{-1/2} \sum_{k=1}^{p-1} \xi^{ka} s_k,$$

$$w_p(t_a) = (-p)^{-1} \sum_{k=1}^{p-1} \xi^{ka}(-s_k^2 + 2t_k).$$

This transformation preserves the subscheme cut out by the quadratic equations (1) and the symmetry relations on s and t.

Proof. If $a+b+c=0$, where $a, b, c \neq 0$, then

$$\begin{aligned}
&(-p)w_p(s_a s_b + s_b s_c + s_c s_a + t_a + t_b + t_c) = \\
&\quad = \sum_{k,l\neq 0} (\xi^{ka+lb} + \xi^{-la+(k-l)b} + \xi^{(l-k)a-kb}) s_k s_l + \sum_{k\neq 0} (\xi^{ka}+\xi^{kb}+\xi^{kc})(-s_k^2+2t_k) \\
&\quad = -\sum_{\substack{k,l\neq 0\\ k\neq l}} \xi^{ka+lb}(s_{-k}s_l + s_{-k}s_{k-l} + s_l s_{k-l} + t_{-k} + t_l + t_{k-l}).
\end{aligned}$$

The fact that w_p is indeed the Fricke involution follows from the details of the calculation in [2]. □

In what follows we shall also need a description of the cusps of $X_1(p)$.

Proposition 2.6. *There are $p-1$ cusps on $X_1(p)$. They can all be obtained by the action of $(\mathbb{Z}/p\mathbb{Z})^*$ and w_p from the point with coordinates*

$$s_a = \lambda(1-\frac{2a}{p}),\ 1\le a\le p-1.$$

Proof. Every cusp on $X_1(p)$ can be obtained from $i\infty$ by means of $(\mathbb{Z}/p\mathbb{Z})^*$ and the Fricke involution. It remains to recall now the value of $s_a(\tau)$ at $\tau=0$, which is computed by means of the Fricke involution. □

3. Differential equations and quadratic relations

We start by analyzing the system of quadratic equations (1), where $\{s_a, t_a\}$ will be now considered as free variables rather than functions on the upper half-plane. To each solution of this system we will associate a curve in $\mathbb{P}^{p-1}$ that, as we will see in Section 4, turns out to be a $\mathbb{Z}/p\mathbb{Z}$-equivariant elliptic normal curve, or a degeneration thereof. The main idea is to set up a suitable system of differential equations that mimics the system satisfied by the elliptic functions

$$z \longmapsto \frac{\vartheta(a/p-z,\tau)\vartheta_z(0,\tau)}{\vartheta(-z,\tau)\vartheta(a/p,\tau)}.$$

We then construct Laurent series solutions to these equations, and show that they satisfy certain quadratic relations (see (4), (5) bellow) that are the defining equations of an "elliptic" normal curve in $\mathbb{P}^{p-1}$.

Definition 3.1. For each solution $\{s_a, t_a\}$ of the quadratic relations (1) we introduce the system of ordinary differential equations for functions $r_a(z)$, $a\in(\mathbb{Z}/p\mathbb{Z})^*$:

$$\frac{dr_a}{dz} = -\frac{1}{p-2}\Big(\sum_{k\neq 0,a} r_k r_{a-k} + 2r_a s_a\Big). \tag{2}$$

We will be looking for solutions with a pole of order one at $z=0$:

Definition 3.2. A solution $\{\hat r_a\}$, $a\in(\mathbb{Z}/p\mathbb{Z})^*$ of the system (2) with Laurent series expansion

$$\hat r_a(z) = \frac{1}{z} + s_a + t_a z + \cdots$$

will be called a *standard solution* of this system of differential equations. Such a solution will be interpreted as an element $\hat r = \sum_{a=0}^{p-1} \hat r_a \xi^a$ in $\mathbb{C}[\xi]/(\xi^p-1)[[z,z^{-1}]]$, where now $\hat r_0$ is defined to be 1.

Proposition 3.3. *Standard solutions exist and are unique. They are convergent in a small punctured disc around $z=0$ in the sense of convergence of functions with values in $\mathbb{C}[\xi]/(\xi^p-1)$.*

Proof. Observe first that the relations among $\{s_a, t_a\}$ imply that $\hat{r}$ satisfies the differential equations up to first order in z. More explicitly, by summing (1) up for all triples $(k, a-k, -a)$ and using the fact that $\sum_{k\neq 0} s_k = 0$, we obtain the necessary relation

$$-(p-2)t_a = \sum_{k\neq 0,a} s_k s_{a-k} + \sum_{k\neq 0,a} (t_k + t_a) + 2s_a^2. \tag{3}$$

On the other hand, the differential equations lead to recursive relations on the coefficients $\hat{r}_{a,n}$ of $\hat{r}_a = \sum_n \hat{r}_{a,n} z^k$ of the form

$$n\hat{r}_{a,n} = -\frac{1}{p-2}\Big(\sum_{k\neq 0,a} \hat{r}_{k,n} + \hat{r}_{a-k,n} + \sum_{k\neq 0,a}\sum_{d=0}^{n-1} \hat{r}_{k,d}\hat{r}_{a-k,n-1-d} + 2s_a\hat{r}_{a,n-1}\Big)$$

Observe now that these linear equations define $\hat{r}_{a,n}$ uniquely. Moreover, it is straightforward to show by induction that $|\hat{r}_{a,n}| \leq c^n$ for some constant c. This follows since the inverse of the matrix defining the above recursion is $\frac{1}{n}\mathbf{id} + O(1)$ as $n \to \infty$. Thus the convergence of the series follows, and this concludes the proof. We remark that the constant c depends on $\{s_a, t_a\}$. $\square$

We will now introduce free variables $r_0, \dots, r_{p-1}$ to study the algebraic relations satisfied by the $\hat{r}_a(z)$. These free variables should not be confused with the complex-valued functions in Definition 3.1.

Definition 3.4. We introduce now the following two sets of relations in the polynomial ring $\mathbb{C}[r_0, \dots, r_{p-1}]$.

(4)

$$R_{a,b,c,d} := r_a r_b - r_c r_d - r_0 r_{a+b}(s_a + s_b - s_c - s_d),\ a+b = c+d \neq 0,\ a,b,c,d \neq 0,$$

and

$$R_{a,b,-a,-b} := r_a r_{-a} - r_b r_{-b} - r_0^2(-s_a^2 + 2t_a + s_b^2 - 2t_b),\ a,b \neq 0. \tag{5}$$

These relations define an homogeneous ideal $I_{s,t}$ in the ring $\mathbb{C}[r_0, r_1, \dots, r_{p-1}]$. The goal of the rest of the section is to calculate the Hilbert function of $\mathbb{C}[r_0, r_1, \dots, r_{p-1}]/I_{s,t}$.

Proposition 3.5. *For all $n > 0$,*

$$\dim_{\mathbb{C}}\big(\mathbb{C}[r_0, r_1, \dots, r_{p-1}]/I_{s,t}\big)_n \leq np.$$

The dimension of the zero graded component is one.

Proof. Observe that this ring is $\mathbb{Z}/p\mathbb{Z}$-graded by the subscripts of r_a. The quadratic relations (4) and (5) imply that the dimension of each $\mathbb{Z}/p\mathbb{Z}$-graded component of $\big(\mathbb{C}[r_0, r_1, \dots, r_{p-1}]/I_{s,t}\big)_n$ is at most n. Indeed, a spanning set is constructed inductively by multiplying the previous spanning set by r_0 and by adding any monomial of the correct $\mathbb{Z}/p\mathbb{Z}$-weight that does not contain r_0. We need to show that modulo r_0 any two monomials with the same $\mathbb{Z}/p\mathbb{Z}$-weight are equivalent. We use induction on the degree and the number of equal factors. If one monomial is $r_{a_1} r_{a_2} \cdots$ and the other one is $r_{b_1}r_{b_2}\cdots$, then we may reduce the first monomial to $r_{b_1}r_{a_1+a_2-b_1}\cdots$ unless $b_1 = a_1 + a_2$. This argument shows that the only difficulty could occur in the case of monomials r_a^n and r_b^n with $2a = b$ and $2b = a$. However, this is not possible for $p > 3$. □

We will now show that $\hat r$ satisfies the quadratic relations (4) and (5).

Proposition 3.6. *Define $\hat R_{a,b,c,d}(z)$, for $a+b = c+d,\ a,b,c,d \neq 0$ by*

$$\hat R_{a,b,c,d}(z) = \hat r_a \hat r_b - \hat r_c \hat r_d - \hat r_0 \hat r_{a+b}(s_a + s_b - s_c - s_d),\ a+b \neq 0,$$

$$\hat R_{a,b,-a,-b}(z) = \hat r_a \hat r_{-a} - \hat r_b \hat r_{-b} - \hat r_0^2(-s_a^2 + 2t_a + s_b^2 - 2t_b).$$

Then $\hat R_{a,b,c,d}(z) \equiv 0$.

Proof. The differential equations for the $\hat r$'s imply the following differential equations for the $\hat R$'s:

$$\frac{d\hat R_{a,b,c,d}}{dz} = -\frac{1}{p-2}\Big(\sum_{k\neq 0,a,c,a+b} \hat r_k \hat R_{a-k,b,c-k,d} + \sum_{k\neq 0,b,d,a+b} \hat r_k \hat R_{b-k,a,d-k,c}$$
$$+ \hat r_{a+b}(\hat R_{a,-a,c,-c} + \hat R_{b,-b,d,-d}) + (s_a + s_b + s_c + s_d)\hat R_{a,b,c,d}\Big),$$

$$\frac{d\hat R_{a,b,-a,-b}}{dz} = -\frac{1}{p-2}\sum_{k\neq 0,a,b} \hat r_k(\hat R_{-a,a-k,-b,b-k} + \hat R_{a,-a+k,b,-b+k}).$$

To derive the first set of differential equations, we use the formula for the derivatives of $\hat r$ and then collect terms with the common factor $\hat r_k$ (where k is the index of summation in equation (2)). We then split off products of $\hat r_k$ and $\hat R$ to get

$$(2-p)\frac{d\hat R_{a,b,c,d}}{dz} = \sum_{k\neq 0,a,c,a+b} \hat r_k \hat R_{a-k,b,c-k,d} + \sum_{k\neq 0,b,d,a+b} \hat r_k \hat R_{b-k,a,d-k,c}$$
$$+ \sum_{k\neq 0,a,c,a+b} \hat r_k \hat r_{a+b-k}(s_{a-k} + s_b - s_{c-k} - s_d) + \sum_{k\neq 0,b,d,a+b} \hat r_k \hat r_{a+b-k}(s_{b-k} + s_a - s_{d-k} - s_c)$$
$$- \sum_{k\neq 0,a+b} \hat r_k \hat r_{a+b-k}(s_a + s_b - s_c - s_d) + \hat r_{a+b}(\hat r_a \hat r_{-a} + \hat r_b \hat r_{-b} - \hat r_c \hat r_{-c} - \hat r_d \hat r_{-d})$$
$$+ 2\hat r_a \hat r_b(s_a + s_b) - 2\hat r_c \hat r_d(s_c + s_d) - 2\hat r_{a+b}s_{a+b}(s_a + s_b - s_c - s_d).$$

We observe that the sums that contain $\hat r_k \hat r_{a+b-k}$ would cancel if the summation were over all $k \neq 0, a+b$, since $k \rightsquigarrow a+b-k$ results in $a-k \rightsquigarrow k-b$, $c-k \rightsquigarrow k-d$. Thus one may reduce all the terms to $\hat r_{a+b}$ modulo $\hat R$. The fact that $\{s_a, t_a\}$ satisfy equations (1) insures that the coefficient of $\hat r_{a+b}$ vanishes. The differential equations for $\hat R_{a,-a,b,-b}$ are treated similarly.

One can check that the equations on $\{s_a\}$ and $\{t_a\}$ imply that $\hat R$ is zero to the order z^0. The vanishing of other Laurent coefficients of $\hat R(z)$ is proved by induction on the degree of z. It is easy to see that the recursion matrix is invertible starting from the coefficients at z^2, because the diagonal entries dominate the rows. The case of the coefficients by z^1 is handled separately as follows.

It is easy to see that $\hat{r}_a(z) = 1/z + s_a + t_a z + u_a z^2 + \cdots$, where

$$u_a = \frac{1}{(p-3)}(\sum_{k\neq 0,a} s_{k-a}t_k - s_a t_a).$$

To show that the coefficient of $\hat{R}_{a,b,c,d}$ at z^1 is zero, it is enough to show

$$s_a t_b + s_b t_a - (s_a + s_b)t_{a+b} + u_a + u_b + 2u_{a+b} = 0 \tag{6}$$

for all $a, b \neq 0$ such that $a + b \neq 0$. To prove this, for every $k \neq 0, -a, b$, we use the relations (1) for triples $(-k-a, k, a)$, $(k-b, -k, b)$, and $(-k+b, k+a, -a-b)$ multiplied by $(s_{k-b} + s_b)$, $(s_{k+a} + s_a)$, and $(s_a + s_b)$ respectively to get

$$\begin{aligned}
&s_a s_{a+b}(s_{k+a} - s_{k-b}) + s_a s_b(s_{k-b} - s_{k+a}) + s_b s_{a+b}(s_{k+a} - s_{k-b}) \\
&- (s_a + s_b)t_{a+b} + s_a t_b + s_b t_a + (s_a + s_b)t_k - s_a t_{k+a} - s_b t_{k-b} \\
&+ s_{k-b}t_k + s_{k-b}t_{k+a} + s_{k-b}t_a - s_{k+a}t_k - s_{k+a}t_{k-b} - s_{k+a}t_b = 0.
\end{aligned}$$

We then sum the above equations for all $k \neq 0, -a, b$. Finally we use $\sum_{k\neq 0} s_k = 0$ and the relation (1) for $(a, b, -a-b)$ to get

$$\begin{aligned}
s_a t_a + s_b t_b + 2s_{a+b}t_{a+b} =& (p-3)(s_a t_b + s_b t_a - (s_a + s_b)t_{a+b}) \\
&+ \sum_{k\neq 0,b} s_{k-b}t_k + \sum_{k\neq 0,a} s_{k-a}t_k + 2\sum_{k\neq 0,a+b} s_{k-a-b}t_k,
\end{aligned}$$

which is equation (6) above. To finish the proof, observe now that the differential equations for $\hat{R}_{a,-a,b,-b}$ imply that it vanishes to the order z^1 as long as all $\hat{R}_{a,b,c,d}$ with $a + b = c + d \neq 0$ vanish. Alternatively, observe that $\hat{R}_{a,-a,b,-b}(z)$ is even, because $\hat{r}_a(-z) = -\hat{r}_{-a}(z)$. □

Theorem 3.7. *For all $n > 0$,*

$$\dim_{\mathbb{C}}\big(\mathbb{C}[r_0, r_1, \ldots, r_{p-1}]/I_{s,t}\big)_n = np.$$

In other words, the Hilbert function of this ring is the same as the Hilbert function of the homogeneous coordinate of an elliptic normal curve of degree p in $\mathbb{P}^{p-1}$.

Proof. By Proposition 3.6 we can use $\hat{r}$ to map $\mathbb{C}[r_0, r_1, \ldots, r_{p-1}]/I_{s,t}$ to $\mathbb{C}[\xi]/(\xi^p - 1)[[z, z^{-1}]]$. We observe that each $\mathbb{Z}/p\mathbb{Z}$-graded component of degree n is mapped onto a space of dimension at least n, because polynomials of degree n in $\hat{r}$ and fixed $\mathbb{Z}/p\mathbb{Z}$-grading can have an arbitrary singular part in their Laurent expansions. The only exception is the zero graded component, where the coefficient by z^{-1} cannot be chosen freely (in fact, it is always zero), but $\hat{r}_0^n$ allows us to freely choose the constant term. This provides a lower bound on the Hilbert function, which together with Proposition 3.5 finishes the proof. □

4. The modular curve

As a first step to proving our main result, we show the following:

Theorem 4.1. *The quadratic relations* (1) *on* s_a *and* t_a *cut out set-theoretically the modular curve* $X_1(p) \subset \mathbb{P}(1, \dots, 1, 2, \dots, 2)$.

Proof. Let $\{s_a, t_a\}$ be a solution to the system (1). Then the results of Section 3 allow us to define a dimension one subscheme C of $\mathbb{P}^{p-1}$ cut out by the ideal $I_{s,t}$. Notice that points p_k, $k = 0, \dots, p-1$ with coordinates $(w_k^1 : w_k^2 : \dots : w_k^{p-1} : 0)$, where $w_k = \exp(2\pi i k/p)$, lie on C. Moreover, $\hat{r}$ defines a map from the disjoint union of the neighborhoods of p non-singular points in $\mathbb{C}$ to C. As a result, the embedding

$$\mathbb{C}[r_0, r_1, \dots, r_{p-1}]/I_{s,t} \to \mathbb{C}[\xi]/(\xi^p - 1)[[z, z^{-1}]]$$

factors through

$$\mathbb{C}[r_0, r_1, \dots, r_{p-1}]/I_{s,t} \to \mathbb{C}[r_0, r_1, \dots, r_{p-1}]/J_{s,t},$$

where $J_{s,t}$ is the defining ideal of the reduced irreducible components of C that pass through points p_k. Indeed, a map to $\mathbb{C}[\xi]/(\xi^p-1)[[z, z^{-1}]]$ is determined by a collection of p maps to the ring of usual Laurent series, which is an integral domain. This shows that $I_{s,t} = J_{s,t}$. In particular, C is reduced and has no isolated closed points.

Suppose now that C is singular. Let $p = (\rho_0 : \dots : \rho_{p-1})$ be a singular point on C. We will first consider the case $\rho_0 \neq 0$, which we can normalize to get $\rho_0 = 1$. Let $p_\epsilon = (1 : \rho_1 + \epsilon u_1 : \dots : \rho_{p-1} + \epsilon u_{p-1})$ be a $\mathbb{C}[\epsilon]/\epsilon^2$-point of C that reduces to p. Set up the differential equations (2) for power series $\widetilde{r}_a(z) = (\rho_a + \epsilon u_a) + O(z)$. The argument of Proposition 3.6 can be extended to the power series over the ring of dual numbers. Unless the solutions $\widetilde{r}_a$ are constant, this allows one to move a $\mathbb{C}[\epsilon]/\epsilon^2$-point to a nearby location on C, which is impossible since C is reduced. Therefore, the solution $\widetilde{r}_a$ must be constant, which implies

$$0 = -\frac{1}{p-2}\Big(\sum_{k \neq 0, a} \rho_k \rho_{a-k} + 2\rho_a s_a\Big). \tag{7}$$

Lemma 4.2. *If the point* p *satisfies the equation* (7), *then* $\{s_a, t_a\}$ *correspond to a cusp of* $X_1(p)$.

Proof. For each $a, b, a+b \neq 0$ let

$$x_{a+b} := \rho_a \rho_b - \rho_{a+b}(s_a + s_b).$$

Observe that because of relation (4), x_{a+b} depends on the sum $a+b$ only. Equation (7) then implies $x_a = 0$ for all $a \neq 0$. As a consequence, we have

$$\rho_a \rho_b = \rho_{a+b}(s_a + s_b) \tag{8}$$

for all $a, b, a+b \neq 0$. There are now two cases to consider.

Case 1. One of the ρ_a, $a \neq 0$ is zero. If any other ρ_b is non-zero, then the above equation for a triple $b, b, 2b \neq 0$ implies $\rho_{2b} \neq 0$. Then the above equation for $b, 2b, 3b$

gives $\rho_{3b} \neq 0$ and so on. Eventually we get $\rho_a \neq 0$, which is a contradiction. Therefore $\rho_a = 0$ for all $a \neq 0$.

Relations (5) now imply that for all $a, b \neq 0$,

$$s_a^2 - 2t_a = s_b^2 - 2t_b.$$

Let us denote by $x = s_a^2 - 2t_b$. Then relations (1) become

$$(s_a + s_b + s_c)^2 = 3x$$

for all $a, b, c \neq 0, a + b + c = 0$. We may scale $\{s_a\}$ so that $3x = 1$ to get

$$s_a + s_b + s_c = \pm 1, \qquad a, b, c \neq 0, \quad a + b + c = 0.$$

It is easy to see that for any given choice of signs, either there is no solution, or the solution is unique and rational.

The action of $(\mathbb{Z}/p\mathbb{Z})^*$ allows us to assume that s_1 is the biggest of all s_a. We have $2s_1 - s_2 = \pm 1$, therefore $s_1 \leq 1$. Since $s_{p-1} = -s_1$, s_1 must be positive, so $2s_1 - s_2 = 1$ and $s_1 \leq 1$. Therefore $|s_a| \leq 1$ for all a. For every $a = 2, \ldots, p-2$ we have

$$s_1 + s_a - s_{a+1} = \pm 1.$$

If the right hand side is -1, then we have $1 + s_1 = s_{a+1} - s_a$, which can happen only if $s_1 = 1$, $s_{a+1} = 1$, and $s_a = -1$. This implies $2 + s_{a-1} = \pm 1$, so $s_{a-1} = -1$. Then analogously $s_{a-2} = -1$, and so eventually we get $s_1 = -1$, a contradiction. Therefore, we have $s_{a+1} = s_a + s_1 - 1$ for all $a = 1, \ldots, p-2$. Together with $s_{p-1} = -s_1$ this forces

$$s_k = 1 - \frac{2k}{p},$$

which means that $\{s_a\}$ has values corresponding to one of the cusps of $X_1(p)$.

Case 2. All ρ_a are non-zero. Then all $s_a + s_b$ are non-zero for $a + b \neq 0$. Denote by $x_a = -\rho_a/\rho_{-a}$. Notice that $x_a x_b = x_{a+b}$ for all a, b, when we set $x_0 = 1$. Therefore, $x_a = w^a$ where w is a p-th root of unity. We can multiply each ρ_a by w_1^a where w_1 is an appropriately chosen p-th root of unity to reduce ourselves to the case $x_a = 1$. So now we have $\rho_{-a} = -\rho_a$. For every $a + b + c = 0$, $a, b, c \neq 0$ consider now the equations (8)

$$\rho_a \rho_b = -\rho_c(s_a + s_b), \quad \rho_c \rho_a = -\rho_b(s_c + s_a).$$

They imply $\rho_a^2 = (s_a + s_b)(s_a + s_c)$, so $s_a s_b + s_b s_c + s_a s_c$ depends on a only. Now the quadratic relations (1) imply that $t_a + t_b + t_c$ depends on a only, if $a + b + c = 0 \bmod p$. This easily yields that all t_k are the same. If we act on this set of $\{s_k, t_k\}$ by the Fricke involution, see Section 2, we get $\{s_k, t_k\}$ for which all $s_a^2 - 2t_a$ are the same. Then the argument of case 1 finishes the proof of the lemma. □

Proof of Theorem 4.1 *continued.* Returning to the case of the singular point p with $\rho_0 = 0$, observe that the equations (4) and (5) imply that the point is one of the points p_k. Similar arguments show then that it has to be nonsingular.

Because of the equality $I_{s,t} = J_{s,t}$ and the presence of the $\mathbb{Z}/p\mathbb{Z}$ action, either C is a smooth curve of degree p and genus one, or it consists of p lines. In the latter case, the Hilbert function together with the symmetry forces the lines to form a p-gon. In particular it has singularities, which implies that $\{s_a, t_a\}$ corresponds then to a cusp of the modular curve.

So C is an elliptic curve with a $\mathbb{Z}/p\mathbb{Z}$-action which permutes the points p_k. Therefore, these points form a subgroup S of order p on C. Observe now that the embedding of C by the r_a's is given by the complete linear system $H^0(\mathcal{O}_C(S))$. Because the r_a's are eigenvectors of the $\mathbb{Z}/p\mathbb{Z}$-action, we get

$$\frac{r_a}{r_0} = \lambda_a \frac{\vartheta(a/p - z, \tau)\vartheta_z(0,\tau)}{\vartheta(-z,\tau)\vartheta(a/p,\tau)},$$

where ϑ denotes the Jacobi theta function and z is a uniformizing parameter on the universal cover of the elliptic curve C such that the points p_k lift to $\frac{k}{p} + \mathbb{Z}$. Since all the coefficients of the products $r_a r_b$ in the relations (4) and (5) are one, all λ_a are equal to one. Then the s_a's can be uniquely determined from the equations (4) up to a multiplicative constant. More precisely, we rescale the s_a's and r_a's to get $r_0 = 1$. Then for any two solutions $\{s'_a\}$ and $\{s''_a\}$ their componentwise difference $\{\widetilde{s}_a\}$ satisfies $\widetilde{s}_a + \widetilde{s}_b = \widetilde{s}_c + \widetilde{s}_d$ whenever $a + b = c + d \bmod p$. This together with the symmetries of the $\widetilde{s}_a$'s yields $\widetilde{s}_a = 0$. It remains to observe now that $s_a = \partial_z \log \vartheta(a/p, \tau)$ is a solution to (4). This finishes the proof. □

Corollary 4.3. *The system of differential equations* (2) *has a solution in elliptic functions with poles of order one along a subgroup of order p if and only if $\{s_a, t_a\}$ satisfy the quadratic relations* (1) *and do not correspond to a cusp.*

Finally we prove now the main result of the paper:

Theorem 4.4. *The quadratic relations* (1) *on s_a and t_a cut out scheme-theoretically the modular curve $X_1(p) \subset \mathbb{P}(1, \dots, 1, 2, \dots, 2)$.*

Proof. We need to show that the scheme $\widetilde{X}_1(p) \subset \mathbb{P}(1, \dots, 1, 2, \dots, 2)$ cut out by these quadratic relations is smooth. Let $\{s_a, t_a\}$ be a closed point of $\widetilde{X}_1(p)$ that is not a cusp. Let $\{s_a : t_a\}_\epsilon$ be a $\mathbb{C}[\epsilon]/\epsilon^2$-point of $\widetilde{X}_1(p)$ that reduces to $\{s_a : t_a\}$. Even though s_a and t_a are defined only up to homothety (multiplication by λ and λ^2, respectively), we shall make a choice and fix a solution as a set of numbers.

Then the quadratic relations (4) and (5) define an elliptic curve C embedded into $\mathbb{P}^{p-1}$ by a complete linear system of degree p. A $\mathbb{C}[\epsilon]/\epsilon^2$-point defines a deformation of the homogeneous coordinate ring of this embedding. In fact, one can set up the system of differential equations on $\hat{r}_a(z)$ that will now take values in $\mathbb{C}[\epsilon]/\epsilon^2$ instead of $\mathbb{C}$. Then its solutions will satisfy the quadratic relations and will define a map from $(\mathbb{C}[\epsilon]/\epsilon^2)[r_0, \dots, r_{p-1}]/I_{s,t}$ to the ring of Laurent series with coefficients in the dual numbers. As before one shows that the dimension of $((\mathbb{C}[\epsilon]/\epsilon^2)[r_0, \dots, r_{p-1}]/I_{s,t})_n$

over $\mathbb{C}$ is $2pn$ and that it is a free module over $\mathbb{C}[\epsilon]/\epsilon^2$ with a monomial basis as in Proposition 3.5.

Therefore we have a $\mathbb{Z}/p\mathbb{Z}$-equivariant deformation of the embedding of an elliptic normal curve in $\mathbb{P}^{p-1}$. Moreover the p-torsion points x_k, $k = 0, \dots, p-1$ with coordinates $(r_0 : \dots : r_{p-1}) = (0 : \xi^k : \xi^{2k} : \dots : \xi^{(p-1)k})$, where $\xi = \exp(2\pi \mathrm{i}/p)$ are fixed under this deformation.

Such $\mathbb{Z}/p\mathbb{Z}$-equivariant embedded deformations are parameterized by elements of

$$H^0(N_{C|\mathbb{P}^{p-1}} \otimes \mathcal{I}_{\{x_0,\dots,x_{p-1}\}})^{\mathbb{Z}/p\mathbb{Z}} = H^0(N_{C|\mathbb{P}^{p-1}}(-1))^{\mathbb{Z}/p\mathbb{Z}},$$

where $N_{C|\mathbb{P}^{p-1}}$ is the normal bundle of $C \subset \mathbb{P}^{p-1}$. An easy calculation shows that this space is 2-dimensional. Therefore all such deformations come either from the scaling of the s_a's and t_a's, or from deformations along the modular curve. This shows that the scheme cut out by the quadratic equations in (1) is nonsingular except possibly at the cusps.

Thus it remains to show that in the neighborhood of the cusps the quadratic relations (1) cut out a smooth curve. The action of $(\mathbb{Z}/p\mathbb{Z})^*$ and the Fricke involution allows one to consider only the case

$$s_a = 1 - \frac{2a}{p}, \quad t_a = s_a^2 - \frac{1}{3}.$$

It suffices to calculate the dimension of the tangent space at this point. Denote the coordinates in the tangent space at this point in $\mathbb{C}^{p-1}$ by $ds_a, dt_a,\ a = 1, \dots, p-1$ with $ds_{p-a} = -ds_a$ and $dt_{-a} = d_{t_a}$. Equations (1) yield in this tangent space

$$(ds_a + ds_b + ds_c) = (d\hat{t}_a + d\hat{t}_b + d\hat{t}_c)$$

for $a, b, c \in \{1, \dots, p-1\}$ with $a+b+c = p$, where $d\hat{t}_k = -dt_k + s_k ds_k$. Two solutions are easy to see, namely

$$ds_k = s_k, \quad dt_k = 2t_k$$

and

$$ds_k = \delta_k^1 - \delta_k^{p-1}, \quad d\hat{t}_k = 2\delta_k^1 + 2\delta_k^{p-1},$$

where δ is the Kronecker delta function. By subtracting a linear combination of these solutions one can reduce any other solution to the case $ds_1 = d\hat{t}_1 = 0$. For every $a = 1, \dots, p-2$ we get

$$ds_a - ds_{a+1} = d\hat{t}_a + d\hat{t}_{a+1}$$

which implies $ds_2 = -d\hat{t}_2$ and

$$ds_k = -2d\hat{t}_2 - 2d\hat{t}_3 - \dots - 2d\hat{t}_{k-1} - d\hat{t}_k, \quad k = 3, \dots, p-1.$$

On the other hand, for every $a = 1, \dots, p-3$ one has

$$ds_2 + ds_a - ds_{a+2} = d\hat{t}_2 + d\hat{t}_a + d\hat{t}_{a+2}$$

which now implies

$$d\hat{t}_2 = d\hat{t}_{a+1}.$$

Because $ds_{p-1} = 0$, we deduce that $d\hat{t}_2 = 0$, and then that all ds_k and dt_k must be zero. Thus the dimension of the tangent space is one, after we mod out by the rescaling factor. □

Corollary 4.5. *The embedding of $X_1(p)$ into $\mathbb{P}^{(p-3)/2}$ induced by the weight one modular forms $\{s_a\}$ is scheme-theoretically cut out by quadrics obtained by eliminating the t's from the equations* (1). *Explicitly, $X_1(p)$ is cut out by the quadratic relations*

$$(p-4)(s_a s_b + s_b s_c + s_c s_a) = 2s_a^2 + 2s_b^2 + 2s_c^2 - \frac{4}{p-2}\sum_{k\neq 0} s_k^2 + \sum_{k\neq 0,a} s_k s_{a-k} + \sum_{k\neq 0,b} s_k s_{b-k} + \sum_{k\neq 0,c} s_k s_{c-k},$$

for all $a, b, c \in (\mathbb{Z}/p\mathbb{Z})^*$ with $a+b+c=0$.

Proof. This is immediate by using relations (3) to eliminate all t_a's in (1). Details are left to the reader. □

Remark 4.6. 1) The embedding $X_1(p)$ into $\mathbb{P}^{(p-3)/2}$ is generally not linearly normal. This is due to the existence of weight one cusp forms, and such forms are never in the span of $\{s_a(\tau)\}$. This first happens at $p = 23$, see [16]. Moreover, $X_1(23)$ is a projection of a canonical curve.

2) Furthermore, the embedding is not quadratically normal in general, due to the existence of Hecke eigenforms of positive analytic rank, see [3]. The first occurrence is at $p = 37$. The stability of the bundle of rank $(p-3)/2$, which is the kernel of the natural evaluation map, would imply through the known Koszul techniques a bound on the number of Hecke eigenforms of non-zero analytic rank, which is linear in p.

3) The quadratic relations (1) do not always generate the ideal of the embedding in degrees three or more. Macaulay [8] calculations show that this first happens at $p = 43$.

References

[1] A. Adler and S. Ramanan, *Moduli of abelian varieties*, Lecture Notes in Math., **1644**, Springer, Berlin, 1996.

[2] L. A. Borisov and P. E. Gunnells, *Toric varieties and modular forms*, Invent. Math., to appear, preprint `math.NT/9908138`.

[3] L. A. Borisov and P. E. Gunnells, *Toric modular forms and nonvanishing of L-functions*, J. Reine. Angew. Math., to appear, preprint `math.NT/9910141`.

[4] L. A. Borisov and P. E. Gunnells, *Toric modular forms of higher weight*, in preparation.

[5] K. Chandrasekharan, *Elliptic functions*, Fundamental Principles of Mathematical Sciences, **281**, Springer-Verlag, Berlin-New York, 1985.

[6] I. V. Dolgachev, *Invariant stable bundles over modular curves $X(p)$*, in *Recent progress in algebra (Taejon/Seoul, 1997)*, 65–99, Contemp. Math., **224**, Amer. Math. Soc., Providence, RI, 1999.

[7] W. L. Edge, *Klein's encounter with the simple group of order 660*, Proc. London Math. Soc. **24** (1972), 647–668.

[8] D. Grayson and M. Stillman, *Macaulay 2: A computer program designed to support computations in algebraic geometry and computer algebra.* Source and object code available from `http://www.math.uiuc.edu/Macaulay2/`.

[9] M. Gross and S. Popescu, *Equations of* $(1,d)$*-polarized abelian surfaces*, Math. Ann. **310** (1998), no. 2, 333–377.

[10] M. Gross and S. Popescu, *The moduli space of* $(1,11)$*-polarized abelian surfaces is unirational*, Compositio Math. (2000), to appear, preprint `math.AG/9902017`.

[11] F. Klein, *Über transformationen siebenter Ordnung der elliptischen Funktionen* (1878/79), Abhandlung **LXXXIV**, in *Gesammelte Werke*, Bd. **III**, Springer, Berlin 1924.

[12] F. Klein, *Über die Transformation elfter Ordnung der elliptischen Funktionen*, Math. Ann. **15** (1879), reprinted in *Ges. Math. Abh., Bd.* **III**, *art.* **LXXXVI**, *pp. 140-168.*

[13] S. Lang, *Introduction to modular forms*, Springer-Verlag, 1976.

[14] D. Mumford, *Tata lectures on theta I*, with the assistance of C. Musili, M. Nori, E. Previato and M. Stillman. Progress in Mathematics, **28**, Birkhäuser Boston, Inc., Boston, Mass., 1983.

[15] A. Polishchuk, *Classical Yang-Baxter equation and the* A_∞*-constraint*, preprint `math.AG/0008156`.

[16] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Reprint of the 1971 original, Princeton Univ. Press, Princeton, NJ, 1994.

[17] H. M. Stark, *Class fields and modular forms of weight one,* in *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, 277–287. Lecture Notes in Math., **601**, Springer, Berlin, 1977.

[18] J. Vélu, *Courbes elliptiques munies d'un sous-groupe* $\mathbb{Z}/n\mathbb{Z} \times \mu_n$. Bull. Soc. Math. France Mém. No. **57**, (1978), 5–152.

Department of Mathematics, Columbia University, New York, NY 10027
E-mail address: `lborisov@math.columbia.edu`
URL: `http://www.math.columbia.edu/~lborisov`

Department of Mathematics and Computer Science, Rutgers University, Newark, NJ 07102–1811
E-mail address: `gunnells@andromeda.rutgers.edu`

Department of Mathematics, Columbia University, New York, NY 10027, State University of New York at Stony Brook, Stony Brook, NY 11794-3651
E-mail address: `psorin@math.columbia.edu, sorin@math.sunysb.edu`
URL: `http://www.math.columbia.edu/~psorin/, http://www.math.sunysb.edu/~sorin/`