

FUNCTIONS AND DIFFERENTIALS ON THE NON-SPLIT CARTAN MODULAR CURVE OF LEVEL 11

JULIO FERNÁNDEZ AND JOSEP GONZÁLEZ

ABSTRACT. The genus 4 modular curve $X_{ns}(11)$ attached to a non-split Cartan group of level 11 admits a model defined over \mathbb{Q} . We compute generators for its function field in terms of Siegel modular functions. We also show that its Jacobian is isomorphic over \mathbb{Q} to the new part of the Jacobian of the classical modular curve $X_0(121)$.

INTRODUCTION

When making computations on the modular curve attached to a congruence subgroup Γ of level N containing $\Gamma_1(N)$, one counts on the \mathbb{Q} -rationality of the cusp at infinity. Moreover, several well-known classical modular tools, such as the Dedekind η -function, are then available, together with explicit methods to find a basis for the vector space of weight 2 cuspforms, that is, a basis of regular differentials on the curve. Any such cuspform $f(\tau)$ has period 1 on the complex upper half-plane, hence admits a Fourier expansion in $e^{2\pi i\tau}$, and, furthermore, the minimal field of definition for $f(\tau)$ is the number field generated by its Fourier coefficients. All of this provides some crucial help in order to compute generators for the function fields of the curve and its quotients. See, for instance, [Gon91], [Shi95], [Gal96], [BGGP05], [Gon12].

By contrast, this kind of computation becomes more complicated and laborious whenever Γ does not contain $\Gamma_1(N)$. This article is meant to serve as an explicit example in which Γ is the congruence subgroup corresponding to a non-split Cartan group of level $N=11$. The attached modular curve $X_{ns}(11)$ has genus 4 and is not hyperelliptic. Though it is defined over \mathbb{Q} , its cusps are not. Even worse, for a function on the curve, its minimal field of definition does not necessarily coincide with the number field generated by its Fourier coefficients. The interest on the modular curves $X_{ns}(N)$ is closely related to the class number one problem and comes from the classification in [Ser72] of the cases in which the Galois representation attached to the N -torsion of an elliptic curve is not surjective.

An equation for $X_{ns}(11)$ is derived in [DFGS14] from a certain elliptic quotient $X_{ns}^+(11)$ which was first handled in [Lig77]. This is done by combining a result of [Bar10] on the ramification locus of the modular j -function together with an expression given in [Hal98] for this function in terms of the Weierstrass coordinates of $X_{ns}^+(11)$. The proof relies strongly on the fact that this elliptic curve has trivial rational 2-torsion.

Received by the editor December 3, 2014 and, in revised form, June 10, 2015.

2010 *Mathematics Subject Classification*. Primary 11F46, 14G35, 14Q05; Secondary 14H45, 11F03.

The authors were partially supported by DGICYT Grant MTM2015-66180-R.

Through a different method not using that proof, in Section 2 we compute generators for the function field of $X_{ns}(11)$ satisfying the equation given in [DFGS14]. They can be explicitly given in terms of *modular units*, that is, of modular functions with cuspidal divisor. For that purpose, we devote Section 1 to the function field of the modular curve $X_{ns}(p)$ for an odd prime p . We include there a partial result on the characterization of modular units for this curve showing, in particular, how to construct such kinds of functions from certain products of Siegel functions which are naturally attached to its cusps. The key reference in this approach is [KL81].

The rest of the paper can be regarded as a by-product, being ultimately connected with modular coverings of curves. A basis of regular differentials for $X_{ns}(11)$ can be obtained from the functions in Section 2 to produce a period matrix for the Jacobian of the curve. According to [Che98], this Jacobian is isogenous over \mathbb{Q} to the new part of the Jacobian of the genus 6 modular curve $X_0(121)$. In Section 3 we show computationally that these two abelian varieties are in fact isomorphic over \mathbb{Q} and, nevertheless, $X_0(121)$ is not a covering of $X_{ns}(11)$.

1. MODULAR UNITS ON THE CURVES $X_{ns}(p)$ AND $X_{ns}^+(p)$

Let p be an odd prime. A non-split Cartan group of level p is a subgroup of $GL_2(\mathbb{F}_p)$ in the conjugacy class of

$$\left\{ \begin{pmatrix} m & \alpha n \\ n & m \end{pmatrix} \mid (0, 0) \neq (m, n) \in \mathbb{F}_p^2 \right\}$$

for any non-square α in \mathbb{F}_p^* . It is isomorphic to the multiplicative group of \mathbb{F}_{p^2} . The above matrix group and its normalizer in $GL_2(\mathbb{F}_p)$ define, as shown in [Lig77] or [Maz77], respective canonical curves $X_{ns}(p)$ and $X_{ns}^+(p)$ defined over \mathbb{Q} , along with projections

$$X(p) \xrightarrow{\pi} X_{ns}(p) \xrightarrow{\pi^+} X_{ns}^+(p) \xrightarrow{j} X(1),$$

where $X(p)$ is the modular curve attached to the congruence subgroup $\Gamma(p)$, that is, to the kernel of the mod p reduction map $SL_2(\mathbb{Z}) \rightarrow SL_2(\mathbb{F}_p)$. The map π^+ has degree 2 and is defined over \mathbb{Q} . In other words, $X_{ns}^+(p) = X_{ns}(p)/\langle w \rangle$ for an involution w of $X_{ns}(p)$ defined over \mathbb{Q} . This involution is conjectured to be the only non-trivial automorphism of $X_{ns}(p)$ if $p > 11$. As for the maps π and j , they have degrees $(p + 1)/2$ and $p(p - 1)/2$, respectively. We refer to [Bar10], where formulas for the genus and the number of cusps for these modular curves are given.

An explicit description of the cusps is required for our purposes. There is a bijection between the set of cusps of $X(p)$ and the quotient set of $\mathbb{F}_p^2 \setminus \{(0, 0)\}$ by the equivalence relation identifying a pair (m, n) with the pair $(-m, -n)$. This bijection comes from the reduction mod p of integer coordinates, taken to be coprime, for every point in $\mathbb{P}^1(\mathbb{Q})$. For $k = 1, \dots, (p - 1)/2$, let P_k denote the image by π of the cusp represented by the pair $(k, 0)$. The cuspidal points on $X_{ns}(p)$ are then $P_1, \dots, P_{(p-1)/2}, wP_1, \dots, wP_{(p-1)/2}$. On the above canonical model for $X_{ns}^+(p)$, the set of cusps is a Galois orbit defined over the maximal real subfield of the p -th cyclotomic extension of \mathbb{Q} . Each of these cusps has two preimages on $X_{ns}(p)$ which are switched by the involution w , and the set of cusps on $X_{ns}(p)$ is a Galois orbit defined over the p -th cyclotomic extension of \mathbb{Q} [Ser89].

The main reference in what follows is [KL81]. Let us fix the p -th root of unity $\zeta := e^{2\pi i/p}$ and, for τ in the complex upper half-plane, let us take $q_* := e^{2\pi i\tau/p}$ as local parameter of level p at infinity. The set of modular functions of level p whose Fourier q_* -expansion has coefficients in $\mathbb{Q}(\zeta)$ can be naturally identified with the function field of the modular curve $X(p)$ over that cyclotomic extension. Any such function can be uniquely normalized by a suitable constant so that the first non-zero coefficient of its Fourier q_* -expansion is 1.

To every pair of integers $Q = (m, n)$ representing a cusp of $X(p)$ through the above mod p parameterization, one can attach the Siegel function

$$S_Q(\tau) := \zeta^{n(m/p-1)/2} q_*^{p/2 B_2(m/p)} (1 - \zeta^n q_*^m) \prod_{\ell \geq 1} (1 - \zeta^n q_*^{p\ell+m})(1 - \zeta^{-n} q_*^{p\ell-m}),$$

where $B_2(x) = x^2 - x + 1/6$ is the second Bernoulli polynomial. The power S_Q^{12p} becomes a function on $X(p)$ whose divisor has support in the set of cusps and can be explicitly given: the order at a cusp represented by a pair (m', n') is $6p^2 B_2((m m' + n n')/p)$, where one regards the sum $m m' + n n'$ reduced mod p . Every product of Siegel functions whose divisor has integer coefficients lies in the function field of $X(p)$ over $\mathbb{Q}(\zeta)$. Conversely, every modular unit on $X(p)$ can be explicitly written, up to a non-zero multiplicative constant, as a product of Siegel functions.

For any two pairs of integers Q and Q' representing the same cusp of $X(p)$, the quotient $S_{Q'}/S_Q$ is a $2p$ -th root of unity. Indeed, there exists a matrix μ in $\Gamma(p)$ such that $Q = \pm Q\mu$, and then the quotient $S_{Q\mu}/S_Q$ is a p -th root of unity by Theorem 1.1 in [KL81]. Moreover, one can check the relation $S_{-Q} = -S_Q$. In particular, any modular function which is obtained as a product of Siegel functions does not depend, once it is normalized, on the chosen representatives for the corresponding cusps of $X(p)$.

Theorem 1.1. *For $k = 1, \dots, (p - 1)/2$, let g_k and h_k be the products of Siegel functions S_Q for Q running over a system of representatives for the set of cusps $\pi^{-1}(P_k)$ and $\pi^{-1}(wP_k)$, respectively, and let also r_k and s_k be integers such that*

$$F := \prod_{k=1}^{(p-1)/2} g_k^{r_k} h_k^{s_k}$$

is a function on $X(p)$. Then, the following hold:

- (i) F is a function on $X_{ns}(p)$ if, and only if, $\sum_{k=1}^{(p-1)/2} (r_k + s_k) \equiv 0 \pmod{2}$.

This is necessarily satisfied whenever $p \not\equiv 7 \pmod{8}$.

- (ii) If $r_k = s_k$ for $k=1, \dots, (p - 1)/2$, then F is a function on $X_{ns}^+(p)$.

Proof. The hypothesis on the function F implies the congruence

$$(1.1) \quad \frac{p+1}{2} \sum_{k=1}^{(p-1)/2} (r_k + s_k) \equiv 0 \pmod{12}$$

by Theorem 5.2 in [KL81]. This relation plays an important role in the proof.

Let $\Gamma_{ns}(p)$ and $\Gamma_{ns}^+(p)$ be the congruence subgroups of $SL_2(\mathbb{Z})$ defining the modular curves $X_{ns}(p)$ and $X_{ns}^+(p)$. The group $\Gamma_{ns}(p)$ has index 2 in $\Gamma_{ns}^+(p)$ and contains

the matrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, whereas $\Gamma(p)$ does not. Let us fix any matrix $\rho \in \Gamma_{ns}(p)$ whose class in the cyclic quotient $\Gamma_{ns}(p)/\Gamma(p)$ is a generator. Since the order of this group is $p + 1$, the matrix $\theta := -\rho^{(p+1)/2}$ must lie in $\Gamma(p)$, and this is used later in the proof. The action of $\text{SL}_2(\mathbb{Z})$ on the upper half-plane embeds the dihedral quotient $\Gamma_{ns}^+(p)/\pm \Gamma(p)$ onto the subgroup of automorphisms of $X(p)$ fixing $X_{ns}^+(p)$. Let us also take any matrix $\varpi \in \Gamma_{ns}^+(p)$ not lying in $\Gamma_{ns}(p)$, that is, inducing the modular involution w on $X_{ns}(p)$. Though it is not needed for the proof, the reduction mod p of such a matrix ϖ can be made explicit: it is of the form

$$\begin{pmatrix} m & \alpha n \\ -n & -m \end{pmatrix},$$

with α non-square in \mathbb{F}_p^* . We also use below the fact that the matrix $v := -\varpi^2$ lies in $\Gamma(p)$.

The proof consists in determining conditions which guarantee the invariance of F under the automorphisms of $X(p)$ induced by ρ and ϖ . For every pair of integers Q representing a cusp of $X(p)$ and every matrix μ in the full modular group $\text{SL}_2(\mathbb{Z})$, one has a relation of the form

$$S_Q(\mu(\tau)) = \xi_\mu S_{Q\mu}(\tau)$$

for some 12-th root of unity ξ_μ depending only on μ . This follows from the action of $\text{SL}_2(\mathbb{Z})$ on the classical Dedekind η -function, on the one hand, and any Klein form, on the other hand; for the latter we refer to property **K1** in [KL81]. In view of (1.1), the knowledge of ξ_μ is irrelevant when checking whether F is invariant under the action of a given matrix μ .

Since the statement does not depend on the set of representatives in \mathbb{Z}^2 for the cusps of $X(p)$, we choose both in part (i) and in part (ii) a suitable set \mathcal{P} in order to handle the products of Siegel functions. To this end, we must introduce some further notation. For $k=1, \dots, (p-1)/2$, let us fix two pairs of integers Q_k and \widehat{Q}_k representing cusps of $X(p)$ in $\pi^{-1}(P_k)$ and $\pi^{-1}(wP_k)$, respectively, and let us define

$$\begin{aligned} \mathcal{P}_k &:= \{Q_k \rho^\ell \mid 0 \leq \ell < (p+1)/2\}, \\ \widehat{\mathcal{P}}_k &:= \{\widehat{Q}_k \rho^\ell \mid 0 \leq \ell < (p+1)/2\}, \\ \widetilde{\mathcal{P}}_k &:= \{Q \varpi \mid Q \in \mathcal{P}_k\}. \end{aligned}$$

Part (i) of the statement gives an equivalent condition for F to remain fixed by the automorphism of $X(p)$ defined by the class of ρ in $\Gamma_{ns}(p)/\pm \Gamma(p)$. The divisor of F is invariant under the action of $\Gamma_{ns}(p)$, and all automorphisms of $X(p)$ are defined over $\mathbb{Q}(\zeta)$. In particular, the quotient $F(\rho(\tau)) / F(\tau)$ is a root of unity in $\mathbb{Q}(\zeta)$. As a matter of fact, it can only be ± 1 because its order must divide $(p+1)/2$. Let us now take

$$\mathcal{P} = \bigsqcup_{k=1}^{(p-1)/2} \mathcal{P}_k \sqcup \widehat{\mathcal{P}}_k$$

as a system of representatives for the cusps of $X(p)$, and consider the products

$$g_k = \prod_{Q \in \mathcal{P}_k} S_Q, \quad h_k = \prod_{Q \in \widehat{\mathcal{P}}_k} S_Q, \quad \rho g_k = \prod_{Q \in \mathcal{P}_k} S_{Q\rho}, \quad \rho h_k = \prod_{Q \in \widehat{\mathcal{P}}_k} S_{Q\rho}.$$

Then, the quotients

$$\frac{\rho g_k}{g_k} = \prod_{\ell=0}^{(p-1)/2} \frac{S_{Q_k \rho^{\ell+1}}}{S_{Q_k \rho^\ell}} = \frac{-S_{Q_k \theta}}{S_{Q_k}}$$

and

$$\frac{\rho h_k}{h_k} = \prod_{\ell=0}^{(p-1)/2} \frac{S_{\widehat{Q}_k \rho^{\ell+1}}}{S_{\widehat{Q}_k \rho^\ell}} = \frac{-S_{\widehat{Q}_k \theta}}{S_{\widehat{Q}_k}}$$

are non-trivial $2p$ -th roots of unity of even order. This is the key point for the rest of the computation: specifically, and for some integer a ,

$$\begin{aligned} F(\rho(\tau)) &= \prod_{k=1}^{(p-1)/2} g_k(\rho(\tau))^{r_k} h_k(\rho(\tau))^{s_k} = \prod_{k=1}^{(p-1)/2} \rho g_k(\tau)^{r_k} \rho h_k(\tau)^{s_k} \\ &= (-1)^\chi \zeta^a F(\tau), \end{aligned}$$

with $\chi = \sum_{k=1}^{(p-1)/2} (r_k + s_k)$. The root of unity ζ^a must be 1 because $F(\rho(\tau)) = \pm F(\tau)$.

Thus, F is fixed by ρ if, and only if, χ is even. This is satisfied for $p \not\equiv 7 \pmod{8}$ due to (1.1).

Let us now prove (ii). If $r_k = s_k$ for $k = 1, \dots, (p-1)/2$, then F is a function on $X_{ns}(p)$ by (i). We then need to show that the involution w fixes F , that is, $F(\varpi(\tau)) = F(\tau)$. Since the divisor of F is now also invariant under the action of $\Gamma_{ns}^+(p)$, one can assure $F(\varpi(\tau)) = \varepsilon F(\tau)$ with $\varepsilon = \pm 1$. Let us modify the above choice for the set \mathcal{P} by replacing $\widehat{\mathcal{P}}_k$ with $\widetilde{\mathcal{P}}_k$, and consider the analogous products

$$g_k = \prod_{Q \in \mathcal{P}_k} S_Q, \quad h_k = \prod_{Q \in \widetilde{\mathcal{P}}_k} S_Q, \quad \varpi g_k = \prod_{Q \in \mathcal{P}_k} S_{Q\varpi}, \quad \varpi h_k = \prod_{Q \in \widetilde{\mathcal{P}}_k} S_{Q\varpi}.$$

Then,

$$\frac{\varpi g_k \varpi h_k}{g_k h_k} = \frac{\varpi h_k}{g_k} = \prod_{Q \in \mathcal{P}_k} \frac{S_{Q\varpi^2}}{S_Q} = \prod_{Q \in \mathcal{P}_k} \frac{-S_{Q\varpi}}{S_Q} = (-1)^{(p+1)/2} \zeta^{b_k}$$

for some integers b_k which are not needed either: indeed, a computation along the lines of that in the proof of part (i) yields $\varepsilon = (-1)^\psi$ with $\psi = \frac{p+1}{2} \sum_{k=1}^{(p-1)/2} r_k$.

Again by (1.1), ψ is always even. □

2. THE FUNCTION FIELD OF $X_{ns}(11)$

From now on, we stick to the case $p=11$, namely, to the only prime p for which $X_{ns}^+(p)$ has genus 1. As a matter of fact, $X_{ns}^+(11)$ is an elliptic curve. A Weierstrass equation for $X_{ns}^+(11)$ was determined in [Lig77]:

$$(2.1) \quad y^2 + y = x^3 - x^2 - 7x + 10.$$

It has conductor 121 and label B1 in [Cre97]. Its Mordell-Weil group is infinite and generated by the point $P := (4, -6)$. So $X_{ns}^+(11)$, as an algebraic curve, has infinitely many automorphisms defined over \mathbb{Q} . They are generated by the elliptic involution

$$(x, y) \longmapsto (x, -1 - y)$$

and the translation-by- P map

$$(x, y) \mapsto \left(\frac{4x^2 + x - 2 + 11y}{(x - 4)^2}, \frac{(2x^2 + 17x - 34 + 11y)(1 - 3x)}{(x - 4)^3} \right).$$

Among the corresponding infinitely many pairs of functions in $\mathbb{Q}(X_{ns}^+(11))$ satisfying (2.1), in this section we compute functions for which the projection

$$j : X_{ns}^+(11) \longrightarrow X(1)$$

is given by the rational function

$$(2.2) \quad \begin{aligned} j(x, y) = & (7x^2 + 16x - 44 + (x + 18)y)^2 (4x^3 + x^2 - 24x - 11 - (x^2 + 3x + 5)y)^{11} \\ & (11(y - 5)(x^2 + 3x - 6)(3x^2 - 3x - 14 - (2x + 3)y))^3 \\ & ((12x^3 + 28x^2 - 41x - 62 + (3x^2 + 20x + 37)y)(x^3 + 4x^2 + x + 22 - (3x - 1)y))^3 \\ & (x + 2)^{-12} (x - 4)^{-14} (x^5 - 9x^4 - 16x^3 + 53x^2 + 37x - 23)^{-11} \end{aligned}$$

obtained through the above translation from the expression for j in Section 2.2 of [Hal98]. This fixes the j -invariants of the points on $X_{ns}^+(11)$ corresponding to the origin O in equation (2.1) and to the point P , namely, $j(O) = 2^3 3^3 11^3$ and $j(P) = -2^{15} 5^3 3$.

The bielliptic curve $X_{ns}(11)$ has genus 4. We note that Proposition 1 in [Ogg74] implies that it is not hyperelliptic. The equation derived in [DFGS14] for this curve, as a degree 2 covering of the elliptic curve $X_{ns}^+(11)$, is

$$(2.3) \quad t^2 = -(4x^3 + 7x^2 - 6x + 19).$$

In particular, the curve admits an *exotic* involution besides the involution w defining the quotient $X_{ns}^+(11)$. The main result in [DFGS14] shows that the full automorphism group is generated by these two involutions. Our goal here is to compute generators X, Y, T for the function field of $X_{ns}(11)$ satisfying the equations (2.1) and (2.3). We show how they can be made explicit from Siegel functions of level 11.

Let us fix the 11-th root of unity $\zeta := e^{2\pi i/11}$ together with the generator $\epsilon := \zeta + \zeta^{-1}$ for the maximal real subfield of $\mathbb{Q}(\zeta)$. As in Section 1, π and π^+ stand for the projections

$$\pi : X(11) \longrightarrow X_{ns}(11), \quad \pi^+ : X_{ns}(11) \longrightarrow X_{ns}^+(11),$$

and, for $k = 1, \dots, 5$, P_k denotes the image by π of the cusp represented by the pair $(k, 0)$. The cuspidal points on $X_{ns}(11)$ are then $P_1, \dots, P_5, wP_1, \dots, wP_5$. They all have ramification index 11 over $X(1)$, are defined over $\mathbb{Q}(\zeta)$ and are transitively permuted by the Galois group of this extension over \mathbb{Q} . The cuspidal points on $X_{ns}^+(11)$ are $\pi^+(P_1), \dots, \pi^+(P_5)$ and their minimal field of definition is $\mathbb{Q}(\epsilon)$.

The first step in our computations follows from Theorem 1.1 and a routine application of the procedure in [KL81] for producing modular units of prime level, as summarized in Section 1.

Lemma 2.1. *There are exactly two normalized modular units \tilde{X}, \tilde{Y} on $X_{ns}^+(11)$ having degree at most 3 and only a pole at $\pi^+(P)$. There are exactly two normalized modular units \tilde{U}, \tilde{V} on $X_{ns}(11)$ which are not functions on $X_{ns}^+(11)$ and have only*

poles at P_1 and wP_1 of order 5. Specifically, the functions $\tilde{X}, \tilde{Y}, \tilde{U}, \tilde{V}$ have divisors

$$\begin{aligned} \operatorname{div}(\tilde{X}) &= (\pi^+(P_3)) + (\pi^+(P_3)) - 2(\pi^+(P_1)), \\ \operatorname{div}(\tilde{Y}) &= (\pi^+(P_3)) + 2(\pi^+(P_2)) - 3(\pi^+(P_1)), \\ \operatorname{div}(\tilde{U}) &= 4(P_2) + (P_4) + 5(P_3) - 5(P_1) - 5(wP_1), \\ \operatorname{div}(\tilde{V}) &= 4(wP_2) + (wP_4) + 5(wP_3) - 5(P_1) - 5(wP_1), \end{aligned}$$

and they are respectively given, up to multiplication by elements in $\mathbb{Q}(\epsilon)$, by

$$g_5 h_5, \quad \frac{g_5 h_5}{g_3 h_3}, \quad \frac{g_5^2 h_5}{h_2 g_3 h_3^2 g_4}, \quad \frac{g_5 h_5^2}{g_2 g_3^2 h_3 h_4},$$

where g_k and h_k stand for the products of Siegel functions S_Q for Q running over a system of representatives for the set of cusps $\pi^{-1}(P_k)$ and $\pi^{-1}(wP_k)$, respectively.

The functions in Lemma 2.1 satisfy the relations

$$\begin{aligned} &\tilde{Y}^2 - 2\epsilon \tilde{X} \tilde{Y} + (2 + 6\epsilon + 2\epsilon^2 - 2\epsilon^3 - \epsilon^4) \tilde{Y} \\ &= \tilde{X}^3 - 2(3\epsilon + 3\epsilon^2 - \epsilon^3 - \epsilon^4) \tilde{X}^2 + (3 + 11\epsilon + 5\epsilon^2 - 4\epsilon^3 - 2\epsilon^4) \tilde{X}, \\ (2.4) \quad &\tilde{U} \tilde{V} = \tilde{Y}^2 (\tilde{X}^2 - (1 - 3\epsilon + \epsilon^3) \tilde{Y} + (1 - 2\epsilon - 3\epsilon^2 + \epsilon^3 + \epsilon^4) \tilde{X}). \end{aligned}$$

This can be checked from their Fourier q_* -expansions. Specifically, since both terms in each equality are functions on $X_{ns}^+(11)$ having exactly a pole at infinity, only their Fourier coefficients up to the constant term need to be compared.

Proposition 2.1. *With the notation in Lemma 2.1, consider the functions*

$$\begin{aligned} \hat{X} &:= 5 - 5\epsilon - 7\epsilon^2 + 2\epsilon^3 + 2\epsilon^4 + (12 - 7\epsilon - 12\epsilon^2 + 3\epsilon^3 + 3\epsilon^4) \tilde{X}, \\ \hat{Y} &:= -12 + 3\epsilon + 10\epsilon^2 - \epsilon^3 - 2\epsilon^4 - (13 - 7\epsilon - 20\epsilon^2 + 5\epsilon^3 + 6\epsilon^4) \tilde{X} \\ &\quad - (46 - 19\epsilon - 57\epsilon^2 + 7\epsilon^3 + 13\epsilon^4) \tilde{Y} \end{aligned}$$

and the constants

$$\begin{aligned} \alpha_2 &:= 11\epsilon + 6\epsilon^2 - 4\epsilon^3 - 2\epsilon^4, & \kappa_3 &:= -4 - 26\epsilon - 19\epsilon^2 + 10\epsilon^3 + 7\epsilon^4, \\ \alpha_1 &:= 21 + 66\epsilon + 25\epsilon^2 - 24\epsilon^3 - 12\epsilon^4, & \kappa_2 &:= -200 - 722\epsilon - 313\epsilon^2 + 259\epsilon^3 + 133\epsilon^4, \\ \alpha_0 &:= 17 - 103\epsilon - 61\epsilon^2 + 38\epsilon^3 + 21\epsilon^4, & \kappa_1 &:= 208 + 1062\epsilon + 633\epsilon^2 - 396\epsilon^3 - 245\epsilon^4, \\ \delta_1 &:= 77 + 242\epsilon + 99\epsilon^2 - 88\epsilon^3 - 44\epsilon^4, & \kappa_0 &:= 534 + 1499\epsilon + 425\epsilon^2 - 516\epsilon^3 - 210\epsilon^4, \\ \delta_0 &:= 187 + 517\epsilon + 264\epsilon^2 - 187\epsilon^3 - 110\epsilon^4, & \beta &:= -7 - 52\epsilon - 38\epsilon^2 + 20\epsilon^3 + 14\epsilon^4. \end{aligned}$$

Then,

$$X = \frac{\alpha_2 \hat{X}^2 + \alpha_1 \hat{X} + \alpha_0 + \beta \hat{Y}}{(\hat{X} - 11\epsilon - 6\epsilon^2 + 4\epsilon^3 + 2\epsilon^4)^2}$$

and

$$Y = \frac{\kappa_3 \hat{X}^3 + \kappa_2 \hat{X}^2 + \kappa_1 \hat{X} + \kappa_0 + (\delta_1 \hat{X} + \delta_0) \hat{Y}}{(\hat{X} - 11\epsilon - 6\epsilon^2 + 4\epsilon^3 + 2\epsilon^4)^3}$$

are the generators of the function field $\mathbb{Q}(X_{ns}^+(11))$ satisfying the relations (2.1) and (2.2). Their values at the cusps are

$$\begin{aligned} X(P_1) &= 11\epsilon + 6\epsilon^2 - 4\epsilon^3 - 2\epsilon^4, & Y(P_1) &= -4 - 26\epsilon - 19\epsilon^2 + 10\epsilon^3 + 7\epsilon^4, \\ X(P_2) &= 10 - 3\epsilon - 10\epsilon^2 + \epsilon^3 + 2\epsilon^4, & Y(P_2) &= -29 + 13\epsilon + 37\epsilon^2 - 5\epsilon^3 - 9\epsilon^4, \\ X(P_3) &= -3 - 4\epsilon + 11\epsilon^2 + \epsilon^3 - 3\epsilon^4, & Y(P_3) &= 2 + 17\epsilon - 21\epsilon^2 - 4\epsilon^3 + 6\epsilon^4, \\ X(P_4) &= 2 - 2\epsilon - 5\epsilon^2 + 2\epsilon^3 + 2\epsilon^4, & Y(P_4) &= -\epsilon - 2\epsilon^2 - 3\epsilon^3 - \epsilon^4, \\ X(P_5) &= -2\epsilon - 2\epsilon^2 + \epsilon^4, & Y(P_5) &= 1 - 3\epsilon + 5\epsilon^2 + 2\epsilon^3 - 3\epsilon^4, \end{aligned}$$

where $X(P_k), Y(P_k)$ is an abuse of notation for $X(\pi^+(P_k)), Y(\pi^+(P_k))$, respectively. The first coefficients of their Fourier q_* -expansions are as follows:

q_*^ℓ	X	Y
1	$11\epsilon + 6\epsilon^2 - 4\epsilon^3 - 2\epsilon^4$	$-4 - 26\epsilon - 19\epsilon^2 + 10\epsilon^3 + 7\epsilon^4$
q_*	$12 + 54\epsilon + 22\epsilon^2 - 19\epsilon^3 - 9\epsilon^4$	$-62 - 239\epsilon - 115\epsilon^2 + 86\epsilon^3 + 47\epsilon^4$
q_*^2	$58 + 237\epsilon + 113\epsilon^2 - 86\epsilon^3 - 46\epsilon^4$	$-352 - 1463\epsilon - 704\epsilon^2 + 528\epsilon^3 + 286\epsilon^4$
q_*^3	$232 + 968\epsilon + 477\epsilon^2 - 351\epsilon^3 - 192\epsilon^4$	$-1763 - 7441\epsilon - 3640\epsilon^2 + 2691\epsilon^3 + 1469\epsilon^4$
q_*^4	$889 + 3760\epsilon + 1854\epsilon^2 - 1362\epsilon^3 - 746\epsilon^4$	$-8158 - 34317\epsilon - 16835\epsilon^2 + 12417\epsilon^3 + 6790\epsilon^4$

Proof. From the Weierstrass equation given in (2.4), \widehat{X} and \widehat{Y} can be checked to satisfy

$$\widehat{Y}^2 + \widehat{Y} = \widehat{X}^3 - \widehat{X}^2 - 7\widehat{X} + 10.$$

They are functions in $\mathbb{Q}(\zeta)(X_{ns}^+(11))$ with a pole at the cusp $\pi^+(P_1)$ of order 2 and 3, respectively. This means that their relation with X and Y must be given, up to the elliptic involution, by translation by $\pi^+(P_1)$, namely,

$$(X, Y) = (\widehat{X}, \widehat{Y}) + (X(P_1), Y(P_1)) \text{ or } (X, Y) = (\widehat{X}, -1 - \widehat{Y}) + (X(P_1), Y(P_1)),$$

where the addition sign stands for the group law in the Weierstrass equation (2.1). The exact relation turns out to be of the second type and holds for

$$X(P_1) = 11\epsilon + 6\epsilon^2 - 4\epsilon^3 - 2\epsilon^4, \quad Y(P_1) = -4 - 26\epsilon - 19\epsilon^2 + 10\epsilon^3 + 7\epsilon^4.$$

Indeed, it is uniquely determined from the values that the functions $X, Y, \widehat{X}, \widehat{Y}$ take at the other cuspidal points. On the one hand, each of these points is a zero of either $\widetilde{X}, \widetilde{Y}$ or $\widetilde{U}\widetilde{V}$, so that the relations in (2.4) lead to the following values:

$$\begin{aligned} \widehat{X}(P_2) &= -2 + \epsilon + 5\epsilon^2 - \epsilon^4, & \widehat{Y}(P_2) &= -4 + 2\epsilon + 5\epsilon^2 - 2\epsilon^3 - 2\epsilon^4, \\ \widehat{X}(P_3) &= 5 - 5\epsilon - 7\epsilon^2 + 2\epsilon^3 + 2\epsilon^4, & \widehat{Y}(P_3) &= -12 + 3\epsilon + 10\epsilon^2 - \epsilon^3 - 2\epsilon^4, \\ \widehat{X}(P_4) &= 1 - 2\epsilon + 3\epsilon^2 - \epsilon^4, & \widehat{Y}(P_4) &= -2 - 4\epsilon + 11\epsilon^2 + \epsilon^3 - 3\epsilon^4, \\ \widehat{X}(P_5) &= 5 - 5\epsilon - 7\epsilon^2 + 2\epsilon^3 + 2\epsilon^4, & \widehat{Y}(P_5) &= 11 - 3\epsilon - 10\epsilon^2 + \epsilon^3 + 2\epsilon^4. \end{aligned}$$

On the other hand, the cusps on $X_{ns}^+(11)$ have ramification index 11 over $X(1)$ and are transitively permuted by the Galois group of $\mathbb{Q}(\epsilon)$ over \mathbb{Q} . Thus, the expression (2.2) yields

$$X(P_k) = -2z - 2z^2 + z^4, \quad Y(P_k) = 1 - 3z + 5z^2 + 2z^3 - 3z^4,$$

for z lying in the set

$$\{\epsilon, -2 + \epsilon^2, 2 - 4\epsilon^2 + \epsilon^4, -3\epsilon + \epsilon^3, -1 + 2\epsilon + 3\epsilon^2 - \epsilon^3 - \epsilon^4\}$$

of Galois conjugates of ϵ . The way in which z runs over this set for $k = 1, \dots, 5$ is the only one making the values $\widehat{X}(P_k), \widehat{Y}(P_k)$ match with the values $X(P_k), Y(P_k)$ through one of the two possible relations above. \square

Remark 2.1. The relations

$$(X, Y) = (\widehat{X}, -1 - \widehat{Y}) + (X(P_1), Y(P_1)) \quad \text{and} \quad (\widehat{X}, \widehat{Y}) = (X, -1 - Y) + (X(P_1), Y(P_1))$$

are equivalent. This means that the expressions for X and Y as rational functions on \widehat{X}, \widehat{Y} are the same as the expressions for \widehat{X} and \widehat{Y} , respectively, as rational functions on X, Y . These expressions can thus be seen as an involution on $X_{ns}^+(11)$ defined over $\mathbb{Q}(\epsilon)$.

Proposition 2.2. *With the notation in Lemma 2.1 and Proposition 2.1, consider the function*

$$\widehat{T} := \widetilde{U} + \frac{1}{11} (8 + 17\epsilon - 21\epsilon^2 - 4\epsilon^3 + 6\epsilon^4) \widetilde{V}$$

and let \overline{T} be the trace of $(X - 11\epsilon - 6\epsilon^2 + 4\epsilon^3 + 2\epsilon^4)^5 \widehat{T}$ from the function field $\mathbb{Q}(\zeta)(X_{ns}(11))$ to the subextension $\mathbb{Q}(\sqrt{-11})(X_{ns}(11))$. Then, the function

$$T := \frac{\overline{T}}{\sqrt{-11} (1458X^3 + 12640X^2 - 56666X + 59141 - (107X^2 + 7296X - 5508)Y)}$$

generates $\mathbb{Q}(X_{ns}(11))$ over $\mathbb{Q}(X_{ns}^+(11))$ and satisfies the equation (2.3) along with X . The first coefficients of its Fourier q_* -expansion are as follows:

q_*^ℓ	$T/\sqrt{-11}$
1	$-5 - 17\epsilon - 10\epsilon^2 + 6\epsilon^3 + 4\epsilon^4$
q_*	$-34 - 152\epsilon - 78\epsilon^2 + 55\epsilon^3 + 31\epsilon^4$
q_*^2	$-214 - 903\epsilon - 441\epsilon^2 + 326\epsilon^3 + 178\epsilon^4$
q_*^3	$-1088 - 4550\epsilon - 2215\epsilon^2 + 1645\epsilon^3 + 896\epsilon^4$

Proof. The functions \widetilde{V} and $\widetilde{U}w$ have the same divisor, so $\widetilde{U}w = c\widetilde{V}$ for some constant c . This constant can be computed using that $\widetilde{U} + c\widetilde{V}$, which is a function in $\mathbb{Q}(\zeta)(X_{ns}^+(11))$ with only a pole of order 5 at the cusp $\pi^+(P_1)$, must be a polynomial in \widetilde{X} and \widetilde{Y} . Specifically, from the Fourier q_* -expansions of these functions one obtains

$$(2.5) \quad \widetilde{U} + c\widetilde{V} = d_2\widetilde{X}^2 + d_1\widetilde{X} + d_0 + (e_1\widetilde{X} + e_0)\widetilde{Y}$$

for

$$\begin{aligned} 11c &= -8 - 17\epsilon + 21\epsilon^2 + 4\epsilon^3 - 6\epsilon^4, & 11d_2 &= -21 + 9\epsilon - 15\epsilon^2 + 5\epsilon^3 + 9\epsilon^4, \\ 11e_1 &= 3 - 17\epsilon + 21\epsilon^2 + 4\epsilon^3 - 6\epsilon^4, & 11d_1 &= -13 + 4\epsilon + 52\epsilon^2 - 10\epsilon^3 - 18\epsilon^4, \\ 11e_0 &= -25 - 71\epsilon + 45\epsilon^2 + 29\epsilon^3 - 5\epsilon^4, & 11d_0 &= 17 + 76\epsilon + 31\epsilon^2 - 25\epsilon^3 - 12\epsilon^4. \end{aligned}$$

The function $\widehat{T} = \widetilde{U} - c\widetilde{V}$ keeps the same polar part as $\widetilde{U}, \widetilde{V}$ and satisfies $\widehat{T}w = -\widehat{T}$, so its square must also be a polynomial in $\widetilde{X}, \widetilde{Y}$, hence in \widehat{X}, \widehat{Y} . The relations given in Proposition 2.1 and Remark 2.1 between \widehat{X}, \widehat{Y} and X, Y lead to an identity of the form

$$(2.6) \quad \left((X - 11\epsilon - 6\epsilon^2 + 4\epsilon^3 + 2\epsilon^4)^5 \widehat{T} \right)^2 = \frac{1}{11} (4X^3 + 7X^2 - 6X + 19) (f_1(X) + f_2(X)Y)^2$$

for certain polynomials $f_1(x), f_2(x)$ in $\mathbb{Z}[\epsilon][x]$ of respective degrees 3 and 2 (see Remark 2.2).

Let us take the trace \overline{T} of $(X - 11\epsilon - 6\epsilon^2 + 4\epsilon^3 + 2\epsilon^4)^5 \widehat{T}$ to $\mathbb{Q}(\sqrt{-11})(X_{ns}(11))$. Since X is defined over \mathbb{Q} , it suffices to compute the conjugate functions $\sigma^\ell \widetilde{U}$ and $\sigma^\ell \widetilde{V}$ for $\ell = 1, \dots, 4$, where σ is the automorphism of the Galois extension $\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{-11})$ sending ζ to ζ^9 , hence ϵ to $\epsilon^2 - 2$. To that end, one can first derive $\sigma^\ell \widetilde{X}$ and $\sigma^\ell \widetilde{Y}$ as rational functions on X and Y with coefficients in $\mathbb{Q}(\epsilon)$. This is a straightforward application of Proposition 2.1 and Remark 2.1.

Note that the values at the cusps given in Proposition 2.1 imply

$$\begin{aligned} \pi^+(\sigma P_1) &= \pi^+(P_4), & \pi^+(\sigma P_4) &= \pi^+(P_5), & \pi^+(\sigma P_5) &= \pi^+(P_2), \\ \pi^+(\sigma P_2) &= \pi^+(P_3), & \pi^+(\sigma P_3) &= \pi^+(P_1). \end{aligned}$$

Of course, this agrees with the formula (3.6.1) in [Lig77], and the same permutation can be checked to hold for the cusps P_1, \dots, P_5 . Then, the information on Siegel functions in Section 1 leading to Lemma 2.1 yields these expressions:

$$\begin{aligned} \sigma \widetilde{U} &= \nu_1 \frac{g_4^2 h_4}{h_5 g_2 h_2^2 g_1}, & \sigma \widetilde{V} &= \vartheta_1 \frac{g_4 h_4^2}{g_5 g_2^2 h_2 h_1}, \\ \sigma^2 \widetilde{U} &= \nu_2 \frac{g_1^2 h_1}{h_4 g_5 h_5^2 g_3}, & \sigma^2 \widetilde{V} &= \vartheta_2 \frac{g_1 h_1^2}{g_4 g_5^2 h_5 h_3}, \\ \sigma^3 \widetilde{U} &= \nu_3 \frac{g_3^2 h_3}{h_1 g_4 h_4^2 g_2}, & \sigma^3 \widetilde{V} &= \vartheta_3 \frac{g_3 h_3^2}{g_1 g_4^2 h_4 h_2}, \\ \sigma^4 \widetilde{U} &= \nu_4 \frac{g_2^2 h_2}{h_3 g_1 h_1^2 g_5}, & \sigma^4 \widetilde{V} &= \vartheta_4 \frac{g_2 h_2^2}{g_3 g_1^2 h_1 h_5}, \end{aligned}$$

where ν_ℓ and ϑ_ℓ are constants which can be determined from the conjugate functions $\sigma^\ell \widetilde{X}, \sigma^\ell \widetilde{Y}$ and the relation (2.5). They are displayed in the following table:

ℓ	ν_ℓ	ϑ_ℓ
1	$2 + 7\epsilon - \epsilon^2 - 8\epsilon^3 - 3\epsilon^4$	$\epsilon^2 - \epsilon^3 - \epsilon^4$
2	$-1 + 2\epsilon^2 - \epsilon^3$	$4\epsilon + \epsilon^2 - 2\epsilon^3$
3	$10 - 3\epsilon - 12\epsilon^2 + \epsilon^3 + 3\epsilon^4$	$-27 + 15\epsilon + 33\epsilon^2 - 8\epsilon^3 - 6\epsilon^4$
4	$-2\epsilon + 10\epsilon^2 - 3\epsilon^4$	$2 + 3\epsilon - 10\epsilon^2 + 3\epsilon^4$

Finally, one obtains the equality

$$\begin{aligned} \overline{T}^2 = 11 (4X^3 + 7X^2 - 6X + 19) & (1458X^3 + 12640X^2 - 56666X + 59141 \\ & - (107X^2 + 7296X - 5508)Y)^2 \end{aligned}$$

from the Fourier q_* -expansions of \overline{T} , X and Y . □

Remark 2.2. Two polynomials $f_1(x), f_2(x)$ satisfying (2.6) can be explicitly given:

$$\begin{aligned} f_1(x) = & (-3468 - 14558\epsilon - 7094\epsilon^2 + 5265\epsilon^3 + 2866\epsilon^4) x^3 \\ & + (-30028 - 126111\epsilon - 61527\epsilon^2 + 45617\epsilon^3 + 24848\epsilon^4) x^2 \\ & + (134152 + 563914\epsilon + 276359\epsilon^2 - 204056\epsilon^3 - 111479\epsilon^4) x \\ & + 139612 - 587393\epsilon - 288873\epsilon^2 + 212613\epsilon^3 + 116417\epsilon^4, \\ f_2(x) = & (251 + 1054\epsilon + 522\epsilon^2 - 382\epsilon^3 - 210\epsilon^4) x^2 \\ & + (17231 + 72451\epsilon + 35622\epsilon^2 - 26226\epsilon^3 - 14358\epsilon^4) x \\ & - 13166 - 55263\epsilon - 26705\epsilon^2 + 19969\epsilon^3 + 10808\epsilon^4. \end{aligned}$$

Note that the function

$$\sqrt{-11} \frac{(X - 11\epsilon - 6\epsilon^2 + 4\epsilon^3 + 2\epsilon^4)^5 \widehat{T}}{f_1(X) + f_2(X)Y}$$

generates $\mathbb{Q}(\zeta)(X_{ns}(11))$ over $\mathbb{Q}(\zeta)(X_{ns}^+(11))$. Its norm to $\mathbb{Q}(\sqrt{-11})(X_{ns}(11))$ is, up to sign, the generator for $\mathbb{Q}(X_{ns}(11))$ over $\mathbb{Q}(X_{ns}^+(11))$ given by $(4X^3 + 7X^2 - 6X + 19)^2 T$. The point in taking the trace \overline{T} rather than the norm of the function $(X - 11\epsilon - 6\epsilon^2 + 4\epsilon^3 + 2\epsilon^4)^5 \widehat{T}$ as a generator is the much simpler expression for its square inside $\mathbb{Q}[X, Y]$.

Remark 2.3. The trace \overline{T} , hence also the generator T , can be explicitly given in terms of Siegel functions from the data in the proof of Proposition 2.2 and in the statements of Proposition 2.1 and Lemma 2.1.

Remark 2.4. The proof of Proposition 2.2 is in fact an alternative explicit way of deducing the equation (2.3). Indeed, the square of the trace \overline{T} is defined over \mathbb{Q} ; hence either ${}^{\varsigma}\overline{T} = \overline{T}$ or ${}^{\varsigma}\overline{T} = -\overline{T}$ must hold for the complex conjugation ς . In the first case, \overline{T} would already be defined over \mathbb{Q} and the minimal field of definition for its values at the cusps should necessarily be $\mathbb{Q}(\zeta)$. But all the values of the function $11(4X^3 + 7X^2 - 6X + 19)$ at the cusps can be computed from those given in Proposition 2.1 and can be checked to be squares in $\mathbb{Q}(\epsilon)$. So $\overline{T}/\sqrt{-11}$ lies in $\mathbb{Q}(X_{ns}(11))$.

3. THE JACOBIAN OF $X_{ns}(11)$

In this section we exploit the equations (2.1), (2.3) and the regular differentials on the modular curve $X_0(121)$ to make explicit an isomorphism defined over \mathbb{Q} between the new part of its Jacobian and the Jacobian $J_{ns}(11)$ of the curve $X_{ns}(11)$. First, we need to recall some concepts and tools.

An abelian variety $\bar{\mathcal{A}}$ is an *optimal quotient* of an abelian variety \mathcal{A} over a number field K if there is a surjective morphism $\bar{\pi}: \mathcal{A} \rightarrow \bar{\mathcal{A}}$ defined over K with connected kernel. In such a case, $\bar{\mathcal{A}}$ is determined by the pull-back $\bar{\pi}^*(\Omega_{\bar{\mathcal{A}}/K}^1)$ of the

regular differentials defined over K . Any basis $\omega_1, \dots, \omega_n$ of this K -vector space yields a lattice for $\bar{\mathcal{A}}$ as a complex torus by taking in \mathbb{C}^n the elements of the form

$$\left(\int_{\gamma} \omega_1, \dots, \int_{\gamma} \omega_n \right),$$

for γ running over the homology group $H_1(\mathcal{A}, \mathbb{Z})$. For any surjective morphism $\pi: \mathcal{A} \rightarrow \mathcal{B}$ of abelian varieties defined over K , there exists a morphism $\bar{\pi}: \mathcal{A} \rightarrow \bar{\mathcal{A}}$ onto an optimal quotient along with an isogeny $\lambda: \bar{\mathcal{A}} \rightarrow \mathcal{B}$, both defined over K , making commutative the following diagram:

$$\begin{array}{ccc} \mathcal{A} & & \\ \bar{\pi} \downarrow & \searrow \pi & \\ \bar{\mathcal{A}} & \xrightarrow{\lambda} & \mathcal{B} \end{array}$$

Whenever \mathcal{A} is the Jacobian of a curve \mathcal{C} defined over K and \mathcal{B} is an elliptic curve, there is a morphism $\phi: \mathcal{C} \rightarrow \mathcal{B}$ defined over K inducing π ; hence there exists a non-constant morphism $\bar{\phi}: \mathcal{C} \rightarrow \bar{\mathcal{A}}$ for which the diagram

(3.1)
$$\begin{array}{ccc} \mathcal{C} & & \\ \bar{\phi} \downarrow & \searrow \phi & \\ \bar{\mathcal{A}} & \xrightarrow{\lambda} & \mathcal{B} \end{array}$$

also holds.

We need to consider the classical modular setting $\mathcal{C} = X_0(N)$. The *new part* $J_0(N)^{\text{new}}$ of the Jacobian $J_0(N)$ is the optimal quotient defined as follows. Take the usual local parameter $q := e^{2\pi i\tau}$ for τ in the complex upper half-plane, so that the space $S_2(\Gamma_0(N))$ of weight 2 cuspforms can be seen, through their Fourier q -expansions, inside the \mathbb{C} -vector space $\mathbb{C}[[q]]$. The map $h(q) \mapsto h(q) dq/q$ yields an isomorphism from $S_2(\Gamma_0(N))$ to the space of regular differentials $\Omega^1_{X_0(N)/\mathbb{C}}$ such that $\Omega^1_{X_0(N)/\mathbb{Q}}$ is the image of the \mathbb{Q} -vector space of rational cuspforms, $S_2(\Gamma_0(N)) \cap \mathbb{Q}[[q]]$. The abelian variety $J_0(N)^{\text{new}}$ corresponds to the subspace $S_2(\Gamma_0(N))^{\text{new}} \cap \mathbb{Q}[[q]]$ which is orthogonal to the subspace of oldforms with respect to the Petersson product.

Let us now focus on the genus 6 curve $X_0(121)$ and its Jacobian $J_0(121)$. There are exactly four \mathbb{Q} -isogeny classes of elliptic curves with conductor 121. They can be represented by the Weierstrass models

(3.2)
$$\begin{aligned} E_A : \quad & y^2 + xy + y = x^3 + x^2 - 30x - 76, \\ E_B : \quad & y^2 + y = x^3 - x^2 - 7x + 10, \\ E_C : \quad & y^2 + xy = x^3 + x^2 - 2x - 7, \\ E_D : \quad & y^2 + y = x^3 - x^2 - 40x - 221, \end{aligned}$$

with respective labels $A1, B1, C1, D1$ in Cremona's tables [Cre97]. These four elliptic curves are optimal quotients of $J_0(121)$ and $J_0(121)^{\text{new}}$ over \mathbb{Q} . Each of them admits a non-constant morphism from $X_0(121)$ defined over \mathbb{Q} such that the pull-back of the invariant differential is, up to sign, the regular differential on $X_0(121)$ corresponding to the normalized newform in $S_2(\Gamma_0(121))$ attached to the \mathbb{Q} -isogeny

class of the elliptic curve. Let f_A, f_B, f_C, f_D denote these newforms. Thus, the sets

$$\Lambda_A := \left\{ \int_{\gamma} f_A(q) \frac{dq}{q} \right\}, \quad \Lambda_B := \left\{ \int_{\gamma} f_B(q) \frac{dq}{q} \right\},$$

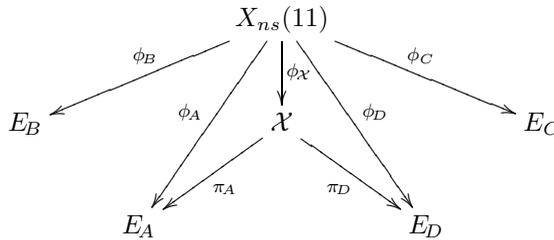
$$\Lambda_C := \left\{ \int_{\gamma} f_C(q) \frac{dq}{q} \right\}, \quad \Lambda_D := \left\{ \int_{\gamma} f_D(q) \frac{dq}{q} \right\},$$

for γ running over the homology group $H_1(X_0(121), \mathbb{Z})$, are the lattices corresponding to the elliptic curves E_A, E_B, E_C, E_D , respectively.

By Section 8 in [Che98], $J_0(121)^{\text{new}}$ is isogenous over \mathbb{Q} to the Jacobian $J_{ns}(11)$. In order to show this explicitly, we exploit the basis for the space of regular differentials $\Omega^1_{X_{ns}(11)/\mathbb{Q}}$ which was used in [DFGS14] to prove that the automorphism group of $X_{ns}(11)$ is isomorphic to Klein’s four group. The quotients of the curve by the involutions in this group are the elliptic curves E_B, E_C and the genus 2 curve given by the equation

$$(3.3) \quad \mathcal{X} : y^2 = -(4x^3 - 4x^2 - 28x + 41)(4x^3 + 7x^2 - 6x + 19).$$

One has a commutative diagram



with degree 2 morphisms ϕ_B, ϕ_X, ϕ_C and degree 3 morphisms π_A, π_D which, on the models for these curves given by (2.1), (2.3), (3.2) and (3.3), are defined as follows:

$$\phi_B(x, y, t) = (x, y),$$

$$\phi_X(x, y, t) = (x, (2y + 1)t),$$

$$\phi_C(x, y, t) = (-x - 1, (t + x + 1)/2),$$

$$\pi_A(x, y) = \left(\frac{-13x^3 + 13x^2 + 102x - 147}{4x^3 - 4x^2 - 28x + 41}, \frac{(-8x^3 + 19x^2 - 10x + 6)y}{2(4x^3 - 4x^2 - 28x + 41)^2} + \frac{9x^3 - 9x^2 - 74x + 106}{2(4x^3 - 4x^2 - 28x + 41)} \right),$$

$$\pi_D(x, y) = \left(\frac{27x^3 + 138x^2 - 101x - 749}{4x^3 + 7x^2 - 6x + 19}, \frac{121(x^3 - x^2 - 29x - 53)y}{2(4x^3 + 7x^2 - 6x + 19)^2} - \frac{1}{2} \right).$$

We claim that the elliptic curves E_A, E_B, E_C, E_D are also optimal quotients of $J_{ns}(11)$ over \mathbb{Q} . Indeed, it suffices to replace the morphism ϕ in (3.1) with each of $\phi_A, \phi_B, \phi_C, \phi_D$ and take into account that neither E_A nor E_D admits an isogeny of degree 2 or 3 defined over \mathbb{Q} to another elliptic curve; see Table 1 in [Cre97]. This fact suggests that $J_0(121)^{\text{new}}$ and $J_{ns}(11)$ could be isomorphic.

Theorem 3.1. *The abelian variety $J_0(121)^{\text{new}}$ is isomorphic over \mathbb{Q} to $J_{ns}(11)$. Moreover, there exists an isogeny*

$$J_{ns}(11) \longrightarrow E_A \times E_B \times E_C \times E_D$$

defined over \mathbb{Q} with kernel isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4 \times (\mathbb{Z}/3\mathbb{Z})^2$.

Proof. By computational means, we produce period matrices Ω_{new} and Ω_{ns} for the abelian varieties $J_0(121)^{\text{new}}$ and $J_{ns}(11)$, respectively, such that

$$(3.4) \quad \Omega_{ns} \mathcal{M} = \mathcal{N} \Omega_{\text{new}}$$

for some matrices $\mathcal{M} \in \text{GL}_8(\mathbb{Z})$ and $\mathcal{N} \in \text{GL}_4(\mathbb{Q})$. This relation amounts to the first part of the statement.

To make the computations easy, we choose in both cases a suitable basis of regular differentials. Specifically, the directions of each basis are the pull-backs to $J_0(121)^{\text{new}}$ or to $J_{ns}(11)$, respectively, of the spaces $\Omega_{E_A/\mathbb{Q}}^1, \Omega_{E_B/\mathbb{Q}}^1, \Omega_{E_C/\mathbb{Q}}^1, \Omega_{E_D/\mathbb{Q}}^1$. Moreover, the elements in each basis yield, by integration over the homology group of the respective abelian variety, the above elliptic lattices $\Lambda_A, \Lambda_B, \Lambda_C, \Lambda_D$. This is possible due to the fact that the elliptic curves E_A, E_B, E_C, E_D are optimal quotients of both abelian varieties over \mathbb{Q} . The elements of such bases are then determined up to sign, and the lattices Λ_{new} and Λ_{ns} of $J_0(121)^{\text{new}}$ and $J_{ns}(11)$, respectively, defined by these bases are both contained in the lattice

$$\Lambda_A \times \Lambda_B \times \Lambda_C \times \Lambda_D$$

attached to the abelian variety $E_A \times E_B \times E_C \times E_D$.

The obvious basis of regular differentials to be taken for $J_0(121)^{\text{new}}$ is the one corresponding to the newforms f_A, f_B, f_C, f_D . A basis for $H_1(X_0(121), \mathbb{Z})$ can be explicitly given as a set of modular symbols. The following subset provides a basis for the new part:

$$\begin{aligned} \gamma_1 &= \{0, 3/52\}, & \gamma_2 &= \{0, 4/97\}, & \gamma_3 &= \{0, 19/92\}, & \gamma_4 &= \{0, 59/119\}, \\ \gamma_5 &= \{0, 8/57\}, & \gamma_6 &= \{0, 11/74\}, & \gamma_7 &= \{0, 3/28\}, & \gamma_8 &= \{0, 11/37\}. \end{aligned}$$

One can then compute the period matrix attached to these data:

$$\Omega_{\text{new}} := \begin{pmatrix} \int_{\gamma_1} f_A(q) \frac{dq}{q} & \cdots & \cdots & \int_{\gamma_8} f_A(q) \frac{dq}{q} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \int_{\gamma_1} f_D(q) \frac{dq}{q} & \cdots & \cdots & \int_{\gamma_8} f_D(q) \frac{dq}{q} \end{pmatrix}.$$

Its columns regarded in \mathbb{C}^4 are a \mathbb{Z} -basis for Λ_{new} . A \mathbb{Z} -basis for each of the elliptic lattices $\Lambda_A, \Lambda_B, \Lambda_C, \Lambda_D$ can also be computed, and the quotient group $(\Lambda_A \times \Lambda_B \times \Lambda_C \times \Lambda_D) / \Lambda_{\text{new}}$ is then checked to be isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/6\mathbb{Z})^2$, which implies the second part of the statement.

As for the basis of regular differentials on $X_{ns}(11)$, we multiply by suitable constants the invariant differentials of the elliptic quotients and then take the corresponding pull-backs:

$$\begin{aligned} \omega_A &:= \phi_A^* \left(\frac{4 dx}{2y + x + 1} \right), & \omega_B &:= \phi_B^* \left(\frac{4 dx}{2y + 1} \right), \\ \omega_C &:= \phi_C^* \left(\frac{4 dx}{2y + x} \right), & \omega_D &:= \phi_D^* \left(\frac{-4 dx}{2y + 1} \right), \end{aligned}$$

that is to say,

$$\begin{aligned} \omega_A &:= \frac{44 dX}{(2Y + 1)T}, & \omega_B &:= \frac{4 dX}{2Y + 1}, \\ \omega_C &:= \frac{-4 dX}{T}, & \omega_D &:= \frac{4(3X - 1) dX}{(2Y + 1)T}, \end{aligned}$$

where X, Y, T are the functions in Propositions 2.1 and 2.2. In order to compute a period matrix, we need to express these differentials in terms of a plane (singular) model for the curve, which can be derived from the equations (2.1) and (2.3). Specifically, we take T and $Z := (2Y + 1)T$ as generators of the function field over \mathbb{Q} , so that

$$X = \frac{12T^4 + 187T^2 + Z^2}{4(T^4 - 11T^2 + Z^2)}.$$

Thus, from the relation $TdT = -(6X^2 + 7X - 3)dX$ one obtains

$$\omega_C = \frac{32(T^4 - 11T^2 + Z^2)^2}{(18T^4 + 121T^2 + 7Z^2)(32T^4 + 605T^2 - Z^2)} dT$$

and

$$\omega_A = \frac{-11T}{Z} \omega_C, \quad \omega_B = \frac{-T^2}{Z} \omega_C, \quad \omega_D = \frac{-T(32T^4 + 605T^2 - Z^2)}{4Z(T^4 - 11T^2 + Z^2)} \omega_C.$$

One can then produce, using algebraic computational software such as *Maple*, a period matrix Ω_{ns} attached to this basis of regular differentials. The proof concludes by checking that the matrix

$$\mathcal{M} := \begin{pmatrix} \operatorname{Re}(\Omega_{ns}) \\ \operatorname{Im}(\Omega_{ns}) \end{pmatrix}^{-1} \begin{pmatrix} \operatorname{Re}(\Omega_{\text{new}}) \\ \operatorname{Im}(\Omega_{\text{new}}) \end{pmatrix}$$

lies in $\operatorname{GL}_8(\mathbb{Z})$ and, thus, satisfies (3.4) for \mathcal{N} equal to the identity matrix. □

Remark 3.1. Though it is not needed for the proof, it can also be checked from the period matrix Ω_{ns} that the quotient $(\Lambda_A \times \Lambda_B \times \Lambda_C \times \Lambda_D)/\Lambda_{ns}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/6\mathbb{Z})^2$. Furthermore, the lattice $\Lambda_{\mathcal{X}}$ of the Jacobian $\operatorname{Jac}(\mathcal{X})$, defined by the regular differentials whose pull-backs by $\phi_{\mathcal{X}}$ are $\omega_A, \omega_B, \omega_C, \omega_D$, is a sublattice of $\Lambda_A \times \Lambda_D$ with quotient isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$. Thus, there is an isogeny

$$J_{ns}(11) \longrightarrow \operatorname{Jac}(\mathcal{X}) \times E_B \times E_C$$

defined over \mathbb{Q} with kernel isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$.

Remark 3.2. The normalized weight 2 cuspforms corresponding to the pull-backs of the spaces $\Omega_{E_A/\mathbb{Q}}^1, \Omega_{E_B/\mathbb{Q}}^1, \Omega_{E_C/\mathbb{Q}}^1, \Omega_{E_D/\mathbb{Q}}^1$ by the morphisms $\phi_A, \phi_B, \phi_C, \phi_D$, respectively, are canonically defined by the regular differentials $\omega_A, \omega_B, \omega_C, \omega_D$ of $X_{ns}(11)$ in the proof of Theorem 3.1. The first coefficients of their Fourier q_* -expansions

can be computed from the expressions given in Propositions 2.1 and 2.2 for the generators X, Y, T of the function field of the curve:

q_*^ℓ	$\frac{\sqrt{-11}}{4(\epsilon-2)^2} (3 - \epsilon^2)(1 + \epsilon - \epsilon^2) \omega_A \frac{q_*}{dq_*}$	$\frac{\sqrt{-11}}{4(\epsilon-2)^4} (11 + \epsilon - 22\epsilon^2 + 2\epsilon^3 + 5\epsilon^4) \omega_C \frac{q_*}{dq_*}$
q_*	1	1
q_*^2	$-8\epsilon - 6\epsilon^2 + 3\epsilon^3 + 2\epsilon^4$	$2\epsilon - \epsilon^3$
q_*^3	$-2(-2 - 8\epsilon - 5\epsilon^2 + 3\epsilon^3 + 2\epsilon^4)$	$2(-2 + 2\epsilon + \epsilon^2 - \epsilon^3)$
q_*^4	$-6\epsilon - 3\epsilon^2 + 2\epsilon^3 + \epsilon^4$	$2 - 3\epsilon^2 + \epsilon^4$
q_*^5	$-3 - 6\epsilon - 2\epsilon^2 + 2\epsilon^3 + \epsilon^4$	$3 - 4\epsilon^2 + \epsilon^4$
q_*^6	$2(-3 - 6\epsilon - 2\epsilon^2 + 2\epsilon^3 + \epsilon^4)$	$2(-3 + 4\epsilon^2 - \epsilon^4)$
q_*^ℓ	$\frac{-11}{4(\epsilon-2)} (2 - \epsilon - 3\epsilon^2 + \epsilon^4) \omega_B \frac{q_*}{dq_*}$	$\frac{\sqrt{-11}}{4} \epsilon(1 - \epsilon)(1 + \epsilon)(2 + \epsilon) \omega_D \frac{q_*}{dq_*}$
q_*	1	1
q_*^2	0	$2(-4\epsilon + 3\epsilon^3 + \epsilon^4)$
q_*^3	$-3 + 3\epsilon + 4\epsilon^2 - \epsilon^3 - \epsilon^4$	$1 + \epsilon - 2\epsilon^2 - 3\epsilon^3 - \epsilon^4$
q_*^4	$2(2 - 4\epsilon^2 + \epsilon^4)$	$2(-2\epsilon^3 - \epsilon^4)$
q_*^5	$-3(-2 + \epsilon + \epsilon^2)$	$3\epsilon + \epsilon^2 - 4\epsilon^3 - 2\epsilon^4$
q_*^6	0	$2(3\epsilon + \epsilon^2 - 4\epsilon^3 - 2\epsilon^4)$

Note that the cuspforms provided by the pull-backs of the invariant differentials of the elliptic curves E_A, E_B, E_C, E_D are not normalized: the leading coefficient in each case is, up to 4 times a unit in $\mathbb{Z}[\zeta]$, a power of a generator of the prime ideal over 11. The corresponding normalized cuspforms, as it happens for the functions X, Y and $T/\sqrt{-11}$, have Fourier coefficients in $\mathbb{Q}(\epsilon)$. It may be that this property holds for all primes $p \geq 11$, namely, that there exists a basis of $\Omega_{X_{ns}(p)/\mathbb{Q}}^1$ whose corresponding weight 2 normalized cuspforms have Fourier coefficients in the maximal real subfield of the p -th cyclotomic extension of \mathbb{Q} .

It follows from Theorem 3.1 that $J_{ns}(11)$ is an optimal quotient of $J_0(121)$. Nevertheless, the Riemann-Hurwitz formula implies that $X_{ns}(11)$ does not admit a non-constant morphism from $X_0(121)$. Let us finish by giving a less obvious result: neither does its genus 2 quotient \mathcal{X} . This is related to the *modularity* of curves over $\overline{\mathbb{Q}}$.

A curve \mathcal{C} defined over a number field L is called *modular over L* if there exists a non-constant morphism $\pi: X(N) \rightarrow \mathcal{C}$ defined over L for some integer N . In that case, the curve \mathcal{C} is also covered by the modular curve $X_1(N^2)$, though not necessarily over L . See, for instance, the appendix in [Maz91]. Both $X_{ns}(11)$ and \mathcal{X} admit then a non-constant morphism from $X_1(121)$. Let us also show that any such morphism cannot be defined over the quadratic field $K = \mathbb{Q}(\sqrt{-11})$.

Proposition 3.1. *The curves $X_{ns}(11)$ and \mathcal{X} have no points defined over K .*

Proof. It suffices to prove the statement for \mathcal{X} . The origin O of E_A is the only rational point on this elliptic curve; see [Cre97]. Take P in $E_A(K)$. Then $P + \varsigma P$ lies in $E_A(\mathbb{Q})$, where ς stands for the complex conjugation. So $\varsigma P = -P$, which means that P defines a rational point on the twist of E_A by K . On this twist, which

has conductor 121 and label $C2$ in [Cre97], the origin is also the only rational point. Hence P must be O . Since the preimages of O under the map $\pi_{\mathbb{A}}: \mathcal{X} \rightarrow E_A$ are not defined over K , the result follows. \square

Proposition 3.2. *All endomorphisms of $J_0(121)$ are defined over K .*

Proof. The Jacobian $J_0(121)$ is isogenous over \mathbb{Q} to the product of elliptic curves

$$E_A \times E_B \times E_C \times E_D \times J_0(11)^2.$$

The elliptic curve E_B is the only one in this product having complex multiplication (by the ring of integers of K). As noted in the proof of Proposition 3.1, E_A is isogenous to E_C over K . The same holds for E_D and $J_0(11)$. Specifically, the twist of E_D by K is the elliptic curve with conductor 11 and label $A3$ in [Cre97]. Since none of the curves in the \mathbb{Q} -isogeny class of E_A is isomorphic to a curve in the \mathbb{Q} -isogeny class of E_D , these two elliptic curves cannot be isogenous. Hence the splitting of $J_0(121)$ over $\overline{\mathbb{Q}}$ is

$$E_A^2 \times E_B \times E_D^3$$

and it is defined over K . The endomorphisms of E_B are defined over K , so the result follows. \square

Corollary 3.1. *Any curve \mathcal{C} of genus $g > 1$ defined over K which can be covered by $X_0(121)$ admits a non-constant morphism $X_0(121) \rightarrow \mathcal{C}$ defined over K .*

Proof. For a non-constant morphism $\pi: X_0(121) \rightarrow \mathcal{C}$ defined over $\overline{\mathbb{Q}}$, Proposition 3.2 implies that

$$\pi^*(\Omega_{\mathcal{C}/\overline{\mathbb{Q}}}^1) \cap \Omega_{X_0(121)/K}^1$$

is a K -vector space of dimension g . The results in Section 2 of [BGGP05] show then that there exist functions in $K(X_0(121))$ which generate the function field of \mathcal{C} over K . \square

Corollary 3.2. *The curves $X_{ns}(11)$ and \mathcal{X} cannot be covered by $X_1(M)$ over K , for any M , nor by $X_0(121)$ over $\overline{\mathbb{Q}}$.*

Proof. Since the cusp at infinity on both $X_1(M)$ and $X_0(121)$ is defined over \mathbb{Q} , the result follows from Proposition 3.1 and Corollary 3.1. \square

ACKNOWLEDGEMENTS

The authors thank the referee for a stimulating report and for pointing them towards the completion of some details, which led to the result in Section 1.

REFERENCES

- [Bar10] B. Baran, *Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem*, J. Number Theory **130** (2010), no. 12, 2753–2772, DOI 10.1016/j.jnt.2010.06.005. MR2684496 (2011i:11083)
- [BGGP05] M. H. Baker, E. González-Jiménez, J. González, and B. Poonen, *Finiteness results for modular curves of genus at least 2*, Amer. J. Math. **127** (2005), no. 6, 1325–1387. MR2183527 (2006i:11065)
- [Che98] I. Chen, *The Jacobians of non-split Cartan modular curves*, Proc. London Math. Soc. (3) **77** (1998), no. 1, 1–38, DOI 10.1112/S0024611598000392. MR1625491 (99m:11068)
- [Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed. Cambridge University Press, Cambridge, 1997. MR1628193 (99e:11068)

- [DFGS14] V. Dose, J. Fernández, J. González, and R. Schoof, *The automorphism group of the non-split Cartan modular curve of level 11*, *J. Algebra* **417** (2014), 95–102, DOI 10.1016/j.jalgebra.2014.05.036. MR3244639
- [Gal96] S. Galbraith, *Equations for modular curves*, PhD thesis, University of Oxford, 1996.
- [Gon91] J. González Rovira, *Equations of hyperelliptic modular curves* (English, with French summary), *Ann. Inst. Fourier (Grenoble)* **41** (1991), no. 4, 779–795. MR1150566 (93g:11064)
- [Gon12] J. González, *Equations of bielliptic modular curves*, *JP J. Algebra Number Theory Appl.* **27** (2012), no. 1, 45–60. MR3086199
- [Hal98] E. Halberstadt, *Sur la courbe modulaire $X_{nd\acute{e}p}(11)$* (French, with English and French summaries), *Experiment. Math.* **7** (1998), no. 2, 163–174. MR1677158 (99m:11062)
- [KL81] D. S. Kubert and S. Lang, *Modular units*, *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science]*, vol. 244, Springer-Verlag, New York-Berlin, 1981. MR648603 (84h:12009)
- [Lig77] G. Ligozat, *Courbes modulaires de niveau 11* (French), *Modular functions of one variable, V* (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), *Lecture Notes in Math.* vol. 601, Springer, Berlin, 1977, pp. 149–237. MR0463118 (57 #3079)
- [Maz77] B. Mazur, *Rational points on modular curves*, *Modular functions of one variable, V* (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), *Lecture Notes in Math.* vol. 601, Springer, Berlin, 1977, pp. 107–148. MR0450283 (56 #8579)
- [Maz91] B. Mazur, *Number theory as gadfly*, *Amer. Math. Monthly* **98** (1991), no. 7, 593–610, DOI 10.2307/2324924. MR1121312 (92f:11077)
- [Ogg74] A. P. Ogg, *Hyperelliptic modular curves*, *Bull. Soc. Math. France* **102** (1974), 449–462. MR0364259 (51 #514)
- [Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* (French), *Invent. Math.* **15** (1972), no. 4, 259–331. MR0387283 (52 #8126)
- [Ser89] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, *Aspects of Mathematics*, E15, Friedr. Vieweg & Sohn, Braunschweig, 1989. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. MR1002324 (90e:11086)
- [Shi95] M. Shimura, *Defining equations of modular curves $X_0(N)$* , *Tokyo J. Math.* **18** (1995), no. 2, 443–456, DOI 10.3836/tjm/1270043475. MR1363479 (96j:11085)

DEPARTAMENT DE MATEMÀTIQUES, UNIVERSITAT POLITÈCNICA DE CATALUNYA, EPSEVG,
 AVINGUDA VÍCTOR BALAGUER 1, 08800 VILANOVA I LA GELTRÚ, SPAIN
E-mail address: julio.fernandez.g@upc.edu

DEPARTAMENT DE MATEMÀTIQUES, UNIVERSITAT POLITÈCNICA DE CATALUNYA, EPSEVG,
 AVINGUDA VÍCTOR BALAGUER 1, 08800 VILANOVA I LA GELTRÚ, SPAIN
E-mail address: josep.gonzalez@upc.edu