MATHEMATICS OF COMPUTATION
Volume 73, Number 246, Pages 869–880
S 0025-5718(03)01562-X
Article electronically published on June 17, 2003

ELLIPTIC CURVES WITH NONSPLIT MOD 11 REPRESENTATIONS

IMIN CHEN AND CHRIS CUMMINS

Abstract. We calculate explicitly the j-invariants of the elliptic curves corresponding to rational points on the modular curve $X_{ns}^{+}(11)$ by giving an expression defined over $\mathbb{Q}$ of the j-function in terms of the function field generators X and Y of the elliptic curve $X_{ns}^{+}(11)$. As a result we exhibit infinitely many elliptic curves over $\mathbb{Q}$ with nonsplit mod 11 representations.

1. Introduction

Let $X(p)$ denote the modular curve which classifies elliptic curves with full level p structure, where p is an odd prime. The group $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ acts on $X(p)$. Let $X_{ns}^{+}(p)$ denote the quotient of $X(p)$ by the normalizer of a nonsplit Cartan subgroup

$$\begin{aligned} N' &= \left\{ \begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix}, \begin{pmatrix} a & b\epsilon \\ -b & -a \end{pmatrix} \mid (a,b) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, (a,b) \neq (0,0) \right\} \\ &= C' \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} C', \end{aligned}$$

where ϵ is a quadratic nonresidue in $\mathbb{Z}/p\mathbb{Z}$ and

$$C' = \left\{ \begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix} \mid (a,b) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, (a,b) \neq (0,0) \right\}.$$

The subgroup N' has order $2(p^2-1)$.

The modular curve $X_{ns}^{+}(p)$ is defined over $\mathbb{Q}$, and its $\mathbb{Q}$-rational points correspond to elliptic curves $E|\mathbb{Q}$ with a specified level p structure $\phi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to E[p](\overline{\mathbb{Q}})$ such that the mod p representation $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ obtained by Galois action on the p-torsion points of E (with respect to ϕ) has image lying inside the subgroup N' above. We say such an $E|\mathbb{Q}$ has a nonsplit mod p representation.

The $\mathbb{Q}$-rational points of $X_{ns}^{+}(p)$ arise in the context of a question of Serre [11] which asks whether the mod p representations of non-CM elliptic curves defined over $\mathbb{Q}$ are always surjective for p greater than some absolute constant $c_{\mathbb{Q}}$. The modular curve $X_{ns}^{+}(p)$ represents the most difficult case of Serre's question, and it has resisted study using currently known techniques such the methods of Mazur [10] used in studying the modular curve $X_0(p)$. From current knowledge about the $\mathbb{Q}$-rational points on the modular curves arising from Serre's question, $c_{\mathbb{Q}} \geq 37$. However, due to the difficulty of determining the $\mathbb{Q}$-rational points on modular

Received by the editor May 2, 2002 and, in revised form, September 11, 2002.
2000 *Mathematics Subject Classification.* Primary 11G05; Secondary 14G05.
Research supported by NSERC.

curves associated to the normalizer of Cartan subgroups (both split and nonsplit cases), the true value of $c_{\mathbb{Q}}$ is currently unknown.

The modular curves $X_{ns}^{+}(p)$ have at least one $\mathbb{Q}$-rational point due to CM elliptic curves. For $p = 3, 5, 7$, the modular curve $X_{ns}^{+}(p)$ has genus 0 and is hence isomorphic to $\mathbb{P}^1|\mathbb{Q}$. An explicit determination of the natural covering maps $X_{ns}^{+}(p) \to X(1)$ to the j-line are known in these cases [2], [6], [13].

For $p = 11$, the modular curve $X_{ns}^{+}(p)$ is an elliptic curve. Using indirect methods, Ligozat [9] showed that $X_{ns}^{+}(11)$ is isomorphic over $\mathbb{Q}$ to the elliptic curve $Y^2 + Y = X^3 - X^2 - 7X + 10$ (labelled 121D in [1]). The Mordell-Weil group of this elliptic curve has rank 1 and is generated by the point $[4 : 5 : 1]$. Thus, there are infinitely many elliptic curves over $\mathbb{Q}$ whose 11-torsion points give rise to a nonsplit mod 11 representation.

In this paper, we explicitly determine the j-invariants of the elliptic curves corresponding to the $\mathbb{Q}$-rational points on $X_{ns}^{+}(11)$. In particular, we show the following computational result using Magma.

Theorem 1.1. *Let $P = [X : Y : 1]$ denote a $\mathbb{Q}$-rational point on the elliptic curve $X_{ns}^{+}(11)$ given in Weierstrass form as $Y^2 + Y = X^3 - X^2 - 7X + 10$. Let $(E|\mathbb{Q}, [\phi])$ denote an elliptic curve with nonsplit* mod 11 *representation corresponding to P. The j-invariant of $E|\mathbb{Q}$ is then given by*

$$j = \frac{B + CY}{A},$$

where $A = (X^5 - 119X^4 + 1381X^3 - 2642X^2 - 9313X + 19249)^{11}$ and $B, C \in \mathbb{Q}[X]$ are the polynomials of degrees 54, 53, *respectively, that are listed in the Appendix.*

The method used in determining the j-function explicitly as an element of $\mathbb{Q}(X, Y)$ consists of first exhibiting two functions $x, y \in \mathbb{C}(X, Y)$ with poles supported at the cusp ∞. These functions x, y are constructed from Siegel functions and have known q-expansions. This allows one to compute the j-function explicitly as an element of $\mathbb{C}(x, y)$. However, since the cusp $\infty \in X_{ns}^{+}(11)(\mathbb{C})$ is not defined over $\mathbb{Q}$, it is necessary to translate the coordinate functions x, y using the group law on the elliptic curve to new coordinate functions x', y' with poles supported at a known $\mathbb{Q}$-rational point on $X_{ns}^{+}(11)$ (for example, a CM-point). It is then possible to relate x', y' to X, Y, and to finally express the j-function explicitly as an element of $\mathbb{Q}(X, Y)$.

2. Klein forms and Siegel functions

This section gives a short introduction to the theory of Klein forms and Siegel functions, following [7], Chapter 2, §1, closely. More complete definitions and proofs can be found there.

Let L be a lattice in $\mathbb{C}$ and let $\mathfrak{f}(z, L)$ denote the Klein form attached to L. This is a function which takes as arguments a complex number z and a lattice L in $\mathbb{C}$. It is of degree 1; that is, $\mathfrak{f}(\lambda z, \lambda L) = \lambda \mathfrak{f}(z, L)$.

Let $W = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathbb{C}^2$ be a vector whose components are linearly independent over $\mathbb{R}$. Let $L = L(W) = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, and $z = z(a, W) = a_1\omega_1 + a_2\omega_2$, where $a = (a_1, a_2) \in \mathbb{R} \times \mathbb{R}$. Define a function which takes as arguments $a \in \mathbb{R} \times \mathbb{R}$ and $W \in \mathbb{C}^2$ whose components are linearly independent over $\mathbb{R}$ by $\mathfrak{f}_a(W) \equiv \mathfrak{f}(z, L)$. The function $\mathfrak{f}_a(W)$ has the following properties.

K0. $\mathfrak{f}_a(\lambda W) = \lambda \mathfrak{f}_a(W)$.

K1. For $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $\mathfrak{f}_a(\gamma W) = \mathfrak{f}_{a\gamma}(W)$.

K2. If $b = (b_1, b_2) \in \mathbb{Z} \times \mathbb{Z}$, then

$$\mathfrak{f}_{a+b}(W) = \epsilon(a,b)\mathfrak{f}_a(W),$$

where $\epsilon(a,b) = (-1)^{b_1b_2+b_1+b_2} e^{-\pi i(b_1a_2-b_2a_1)}$.

Let $\mathfrak{H}$ denote the complex upper half-plane. Let $\tau \in \mathfrak{H}$ and define $\mathfrak{f}_a(\tau) \equiv \mathfrak{f}_a(W_\tau)$, where $W_\tau = \begin{pmatrix} \tau \\ 1 \end{pmatrix}$. From properties **K0** and **K1** we see that for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, we have

$$\begin{aligned}
\mathfrak{f}_{a\gamma}(\tau) &= \mathfrak{f}_{a\gamma}(W_\tau) \\
&= \mathfrak{f}_a(\gamma W_\tau) \\
&= \mathfrak{f}_a\left(\begin{pmatrix} a\tau + b \\ c\tau + d \end{pmatrix}\right) \\
&= \mathfrak{f}_a\left((c\tau + d)\begin{pmatrix} \frac{a\tau+b}{c\tau+d} \\ 1 \end{pmatrix}\right) \\
&= (c\tau + d)\mathfrak{f}_a\left(\begin{pmatrix} \frac{a\tau+b}{c\tau+d} \\ 1 \end{pmatrix}\right) \\
&= (c\tau + d)\mathfrak{f}_a(\gamma(\tau)).
\end{aligned}$$

Let $f : \mathfrak{H} \to \mathbb{C}$ be a function. For $k \in \mathbb{Z}$, the action of the k-th stroke operator for $\gamma \in \mathrm{SL}_2(\mathbb{R})$ on f is defined by

$$(f_{|_{k,\gamma}})(\tau) = f(\gamma(\tau))j(\gamma,\tau)^{-k},$$

where $j(\gamma,\tau) = (c\tau + d)$. Note that $(f_1f_2)_{|_{k,\gamma}} = f_{1|_{k_1,\gamma}} f_{2|_{k_2,\gamma}}$ as long as $k_1 + k_2 = k$, and $f_{|_{k,\delta\gamma}} = f_{|_{k,\delta}} f_{|_{k,\gamma}}$. The above calculation shows that $\mathfrak{f}_{a|_{-1,\gamma}} = \mathfrak{f}_{a\gamma}$.

The Siegel function $g_a(\tau)$ is a function on $\mathfrak{H}$ defined as $g_a(\tau) = \mathfrak{f}_a(\tau)\Delta(\tau)^{\frac{1}{12}}$, where $\Delta(\tau)^{\frac{1}{12}} = \eta(\tau)^2$ and $\eta(\tau)^2 = q^{\frac{1}{12}} \prod_{n=1}^{\infty}(1 - q^n)^2$. If $0 \neq a' \in \mathbb{Q} \times \mathbb{Q}$, then by property **K2**, $\mathfrak{f}_a(\tau) = \epsilon \mathfrak{f}_c(\tau)$, where $c = (c_1, c_2)$ satisfies $0 \leq c_i < 1$ and ϵ is a root of unity. Let $q = q_\tau = e^{2\pi i\tau}$ and $q_z = e^{2\pi iz}$. The Siegel function $g_a(\tau)$ can be expressed in terms of q as follows:

$$g_a(\tau) = -q^{\frac{1}{2}B_2(a_1)} e^{2\pi i a_2(a_1-1)/2}(1 - q_z)\prod_{n=1}^{\infty}(1 - q^n q_z)(1 - q^n/q_z),$$

where $B_2(x) = x^2 - x + \frac{1}{6}$ and $z = a_1\tau + a_2$. If $0 \leq a_i < 1$, then the lowest power of q occurring in $g_a(\tau)$ is $B_2(a_1)$.

In the next section we will need the following condition, due to Kubert [8], for the product of Klein forms to be an automorphic form for $\Gamma(N)$.

Theorem 2.1. *Let N be odd. Let $f = \prod_r \mathfrak{f}^{m_r}_{(r_1/N, r_2/N)}$ be a finite product of Klein forms, where $r = (r_1, r_2) \in \mathbb{Z} \times \mathbb{Z}$. If*

$$\sum_r m_r r_1^2 \equiv \sum_r m_r r_2^2 \equiv \sum_r m_r r_1 r_2 \equiv 0 \pmod{N},$$

then f is an automorphic form for $\Gamma(N)$.

Proof. Theorem 4.1 in Chapter 3 of [7] □

This condition is called **QUAD(N)odd** in [7].

3. Method of calculation

For $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, let $\overline{\gamma}$ be its reduction modulo 11. Let $SN' = N' \cap \mathrm{SL}_2(\mathbb{Z}/11\mathbb{Z})$. Consider the congruence subgroup given by

$$\Gamma_{ns}^{+}(11) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \overline{\gamma} \in SN'\}.$$

As Riemann surfaces we have that $X_{ns}^{+}(11)(\mathbb{C}) \cong \Gamma_{ns}^{+}(11)\backslash\mathfrak{H}^*$ [5]. We can regard $\infty \in \Gamma_{ns}^{+}(11)\backslash\mathfrak{H}^* \cong X_{ns}^{+}(11)(\mathbb{C})$ as a $\mathbb{C}$-point of $X_{ns}^{+}(11)$. In fact, it is known ([12], A.5) that ∞ is $\mathbb{Q}(\zeta_{11})^{+}$-rational, where $\mathbb{Q}(\zeta_{11})^{+}$ denotes $\mathbb{R} \cap \mathbb{Q}(\zeta_{11})$.

Proposition 3.1. *Let $\Gamma^*(11) = \pm I \cdot \Gamma(11)$, where $\Gamma(11)$ is the principal congruence subgroup of level 11. Let Ω be a complete set of inequivalent coset representatives for $\Gamma^*(11)\backslash\Gamma_{ns}^{+}(11)$. For $a \in \mathbb{Q} \times \mathbb{Q}$, define*

$$u_a(\tau) = \prod_{\gamma \in \Omega} g_{a\gamma}(\tau).$$

Now let

$$\begin{aligned} x &= \theta_x \cdot u_{(5/11,0)}(\tau), \\ y &= \theta_y \cdot u_{(5/11,0)}(\tau)/u_{(3/11,0)}(\tau), \end{aligned}$$

where $\theta_x, \theta_y \in \mathbb{C}$ are constants (depending on Ω) chosen so that the leading terms in the q-expansions of x, y are 1.

1. *The functions x, y are independent of the choice of Ω.*
2. *The functions x, y are automorphic functions for the group $\Gamma_{ns}^{+}(11)$, i.e., they lie in the function field $\mathbb{C}(X_{ns}^{+}(11))$ of $X_{ns}^{+}(11)$*
3. *The functions x and y only have poles at the cusp ∞ of orders 2 and 3, respectively, so that $\mathbb{C}(x, y) = \mathbb{C}(X_{ns}^{+}(11))$.*
4. *The functions x, y satisfy the Weierstrass equation*

```
y^2 + (2*z^9 + 2*z^8 + 2*z^7 + 2*z^6 + 2*z^5 + 2*z^4
                                 + 2*z^3 + 2*z^2 + 2)*x*y
+ (-2*z^9 - 2*z^8 - z^7 - z^4 - 2*z^3 - 2*z^2)*y
= x^3 + (2*z^9 + 2*z^8 + 2*z^7 + 2*z^4 + 2*z^3 + 2*z^2)*x^2
+ (-2*z^9 - 3*z^8 - z^7 + z^6 + z^5 - z^4 - 3*z^3
                                            - 2*z^2 + 2)*x,
```

where $z = \zeta_{11}$ is a primitive 11-th root of unity. Let $E \cong_{\mathbb{Q}(\zeta_{11})} X_{ns}^{+}(11)$ denote the elliptic curve over $\mathbb{Q}(\zeta_{11})$ defined by this Weierstrass equation. Thus, $x, y \in \mathbb{Q}(\zeta_{11})(X_{ns}^{+}(11))$.

Proof. (1) If $\delta \in \Gamma(11)$, $\gamma \in \Gamma_{ns}^{+}(11)$, then $\mathfrak{f}_{a\delta\gamma}(\tau) = \mathfrak{f}_{a|_{-1,\delta\gamma}}(\tau) = \epsilon(\delta)\mathfrak{f}_{a|_{-1,\gamma}}(\tau) = \epsilon(\delta)\mathfrak{f}_{a\gamma}(\tau)$, where $\epsilon(\delta)$ is an 11-th root of unity (see the argument in (2)). Also, $\mathfrak{f}_{a|_{-1,-I}}(\tau) = -\mathfrak{f}_a(\tau)$. Thus, we see that a different choice of a complete set of inequivalent coset representatives for Ω will only result in changing u_a by a scalar factor which is a 22-nd root of unity. As we scale x and y so they have leading term 1, the resulting x and y are then independent of the choice of coset representatives Ω.

(2) Consider the following elements of $SN' \leq \mathrm{SL}_2(\mathbb{Z}/11\mathbb{Z})$:

$$\bar{\sigma} = \begin{pmatrix} 3 & 5 \\ 6 & 3 \end{pmatrix},$$
$$\bar{s} = \begin{pmatrix} 1 & 8 \\ 8 & 10 \end{pmatrix}.$$

It can be verified that $\bar{\sigma}$ has order 12, $\bar{s}$ has order 4, and that $\langle \bar{\sigma} \rangle \cap \langle \bar{\tau} \rangle = \{\pm I\}$. In addition, $\bar{s}^{-1}\bar{\sigma}\bar{s} = \bar{\sigma}^{-1}$. Thus, $\bar{\Omega} = \left\{ \bar{\sigma}^i, \bar{s}\bar{\sigma}^i \mid i = 0, \ldots, 5 \right\}$ forms a complete set of inequivalent coset representatives for $\{\pm I\} \backslash SN'$.

Let σ and s be lifts of $\bar{\sigma}$ and $\bar{s}$ to $\mathrm{SL}_2(\mathbb{Z})$. Let $\Omega = \left\{ \sigma^i, s\sigma^i \mid i = 0, \ldots, 5 \right\}$. This is a complete set of inequivalent coset representatives for $\Gamma^*(11) \backslash \Gamma^+_{ns}(11)$. We work with this fixed set of coset representatives for convenience in later arguments.

Let a have denominator 11. Consider the function

$$\begin{aligned} u_a(\tau) &= \prod_{\gamma \in \Omega} g_{a\gamma}(\tau) \\ &= \Delta(\tau) \prod_{\gamma \in \Omega} \mathfrak{f}_{a\gamma}(\tau), \end{aligned}$$

where the last equality follows from the fact that there are 12 elements in Ω. Let $h_a(\tau) = \prod_{\gamma \in \Omega} \mathfrak{f}_{a\gamma}(\tau)$.

The condition **QUAD(N)odd** is satisfied by the product defining $h_a(\tau)$ for $N = 11$; so, by Theorem 2.1, $h_a(\tau)$ is an automorphic form for $\Gamma(11)$ of weight -12. This can be verified by using the explicit form of the subgroup N' given in the introduction and the fact that $\sum_{\alpha,\beta \in \mathbb{Z}/p\mathbb{Z}} \alpha^2 = \sum_{\alpha,\beta \in \mathbb{Z}/p\mathbb{Z}} \alpha\beta = \sum_{\alpha,\beta \in \mathbb{Z}/p\mathbb{Z}} \beta^2 = 0$.

Since $\mathfrak{f}_{a|_{-1,-I}}(\tau) = -\mathfrak{f}_a(\tau)$, we see that $h_a(\tau)$ is an automorphic form of weight -12 for $\Gamma^*(11)$, as there are an even number of elements in Ω. Thus, $u_a(\tau)$ is an automorphic function for $\Gamma^*(11)$.

By Theorem 1.1 in Chapter 2 of [7], $\mathfrak{f}_a(\tau)^{11}$ is an automorphic form for $\Gamma(11)$ of weight -11. Thus, for $\gamma \in \Gamma(11)$

$$\begin{aligned} \mathfrak{f}^{11}_{a}{}_{|_{-11,\gamma}} &= \left(\mathfrak{f}_{a|_{-1,\gamma}} \right)^{11} \\ &= \mathfrak{f}_a^{11}. \end{aligned}$$

Thus for $\gamma \in \Gamma(11)$ we have $\mathfrak{f}_{a|_{-1,\gamma}} = \epsilon(\gamma)\mathfrak{f}_a$, where ϵ is an 11-th root of unity.

Let $g \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$\begin{aligned} h_{a|_{-12,g}} &= \left(\prod_{\gamma \in \Omega} \mathfrak{f}_{a\gamma} \right)_{|_{-12,g}} \\ &= \prod_{\gamma \in \Omega} \left(\mathfrak{f}_{a|_{-1,\gamma}|_{-1,g}} \right) \\ &= \prod_{\gamma \in \Omega} \mathfrak{f}_{a|_{-1,\gamma g}}. \end{aligned}$$

Let σ_g denote the permutation of the coset representatives in Ω obtained by multiplication on the left by g, written so it acts from the right in exponential notation. It has the property that $\gamma g = \delta(\gamma, g) \cdot \gamma^{\sigma_g}$, where $\delta(\gamma, g) \in \Gamma^*(11)$, $\gamma \in \Omega$. Let $\epsilon(g, \gamma)$ be the 22-nd root of unity such that $\mathfrak{f}_{a|_{-1,\gamma g}} = \epsilon(\gamma, g)\mathfrak{f}_{a|_{-1,\gamma^{\sigma_g}}}$. Note that if

$\delta(\gamma, g) \in \Gamma(11)$, then $\epsilon(\gamma, g)$ is an 11-th root of unity; otherwise it is the negative of an 11-th root of unity. We then have that

$$\begin{aligned}\prod_{\gamma\in\Omega} \mathfrak{f}_{a|_{-1,\gamma g}} &= \prod_{\gamma\in\Omega} \epsilon(\gamma, g)\mathfrak{f}_{a|_{-1,\gamma^{\sigma} g}} \\ &= \epsilon(g)h_a,\end{aligned}$$

where $\epsilon(g) = \prod_{\gamma\in\Omega} \epsilon(\gamma, g)$.

If $\bar{g} = \bar{\sigma}^j$, then

$$\begin{aligned}\bar{\sigma}^i\bar{g} &= \bar{\sigma}^{i+j}, \\ \bar{s}\bar{\sigma}^i\bar{g} &= \bar{s}\bar{\sigma}^{i+j},\end{aligned}$$

so that

$$\begin{aligned}\sigma^i g &= \delta\sigma^{i+j}, \\ s\sigma^i g &= \delta' s\sigma^{i+j},\end{aligned}$$

for some $\delta, \delta' \in \Gamma(11)$. Thus, we see that all the $\epsilon(\gamma, g)$'s are in fact 11-th roots of unity, so $\epsilon(g)$ is an 11-th root of unity.

Similarly, if $\bar{g} = \bar{s}\bar{\sigma}^j$, then

$$\begin{aligned}\bar{\sigma}^i\bar{g} &= \bar{s}\bar{\sigma}^{j-i}, \\ \bar{s}\bar{\sigma}^i\bar{g} &= \bar{s}^2\bar{\sigma}^{j-i} = -\bar{\sigma}^{j-i},\end{aligned}$$

so that

$$\begin{aligned}\sigma^i g &= \delta s\sigma^{j-i}, \\ s\sigma^i g &= \delta' s^2\sigma^{j-i} = -\delta'\sigma^{j-i},\end{aligned}$$

for some $\delta, \delta' \in \Gamma(11)$. Thus, we see that there are an even number of $\epsilon(\gamma, g)$'s which are the negatives of an 11-th root of unity, so that $\epsilon(g)$ is in fact an 11-th root of unity.

Thus, $u_{a|_{0,g}} = \epsilon(g)u_a$, where $\epsilon(g)$ is an 11-th root of unity. We can then define a homomorphism from $G = \{\pm I\}\backslash SN'$ to $\mathbb{C}^\times$ given by

$$\begin{aligned}\rho : G &\to \mathbb{C}^\times, \\ g &\mapsto \epsilon(g).\end{aligned}$$

This one-dimensional representation takes on values which must be both 11-th and 12-th roots of unity (as G has order 12), so is in fact trivial.

We have thus shown that $u_a(\tau) = \prod_{\gamma\in\Omega} g_{a\gamma}(\tau)$ is an automorphic function for $\Gamma_{ns}^{+}(11)$, at least when we take Ω to be the particular choice of coset representatives given at the beginning of this proof. The result then follows for any choice of coset representatives, thanks to the remark in (1).

(3) The fact that x and y have poles of order 2 and 3, respectively, only at ∞ can be seen from the explicit q-expansions of x and y as calculated by Magma (see the Appendix). Note from [7], Chapter 2, Theorem 1.2, that $g_a(\tau)$ has neither zeroes nor poles on the upper half-plane.

To calculate the q-expansion of $g_{a\gamma}(\tau)$, we calculate the q-expansion of $g_c(\tau)$, where $c = a\gamma - b$ and $b \in \mathbb{Z} \times \mathbb{Z}$ is chosen so that $c = (c_1, c_2)$ satisfies $0 \leq c_i < 1$. Since $g_c(\tau)$ differs from $g_a(\tau)$ by a root of unity, this does not affect the final q-expansions of the x and y we obtain.

(4) Since we know $X_{ns}^+(11)$ has genus 1, and x and y have poles supported at ∞ of order 2 and 3 respectively, x and y should satisfy a Weierstrass equation. Using the explicit q-expansions of x and y (which are elements of the ring $R = \mathbb{Q}(\zeta_{11})((q^{1/11})))$, we used Magma to solve for $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}(\zeta_{11})$ such that $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ in the ring R. This amounts to solving a linear system over the field $\mathbb{Q}(\zeta_{11})$, i.e., one considers the above equation over R to a specified order of precision in $q^{1/11}$ such that the resulting linear system over $\mathbb{Q}(\zeta_{11})$ has a 1-dimensional solution space. □

The j-invariant of $121D$ is -32768. We confirmed using Magma that the j-invariant of E is also -32768, so $E \cong_{\mathbb{C}} X_{ns}^+(11)$, as predicted by theory. Since $j \in \mathbb{Q}(\zeta_{11})(x, y)$, the function j is expressible in the form

$$j = \frac{b + cy}{a} \tag{1}$$

for $a, b, c \in \mathbb{Q}(\zeta_{11})[x]$.

By specifying maximal degrees for a, b, c, one can solve the linear system corresponding to the equation $aj = b + cy$ over R using a specified order of precision in $q^{1/11}$. We found the minimal maximal degrees for a, b, c which gave nontrivial solution spaces using a specified order of precision in $q^{1/11}$. With these maximal degrees, we then increased the order of precision in $q^{1/11}$ until the solution space of the linear system was 1-dimensional. We omit giving the values of a, b, c, which are of degrees $33, 38, 37$, respectively.

Since $X_{ns}^+(11)$ is an elliptic curve over $\mathbb{Q}$ with Weierstrass equation $Y^2 + Y = X^3 - X^2 - 7X + 10$, there are functions X and Y in the function field $\mathbb{Q}(X_{ns}^+(11))$ satisfying this equation such that $\mathbb{Q}(X, Y) = \mathbb{Q}(X_{ns}^+(p))$. Since $j \in \mathbb{Q}(X_{ns}^+(11))$, j is expressible in the form

$$j = \frac{B + CY}{A}$$

where $A, B, C \in \mathbb{Q}[X]$.

Our objective is to find $A, B, C \in \mathbb{Q}[X]$ explicitly. To do this, we relate the functions x, y to X, Y. The functions $x, y \in \mathbb{Q}(\zeta_{11})(X_{ns}^+(11))$ have poles at ∞. However, the point ∞ of $X_{ns}^+(11)$ is only defined over $\mathbb{Q}(\zeta_{11})^+$ [4], and X, Y should have poles at a point O which is $\mathbb{Q}$-rational.

Lemma 3.2. *Let $E|\mathbb{Q}$ denote an elliptic curve with CM by a maximal order $\mathcal{O}$ in an imaginary quadratic field with class number 1 in which p is inert. Then there is a choice of $\phi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to E[p](\overline{\mathbb{Q}})$ such that $(E, [\phi])$ corresponds to a $\mathbb{Q}$-rational point on $X_{ns}^+(p)$.*

Proof. Cf. [12], A.5 □

Corollary 3.3. *Let E be an elliptic curve with CM by $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ or $\mathbb{Z}[\sqrt{-1}]$ (corresponding to j-invariant 0 or 1728, respectively). Then $(E, [\phi])$ from the lemma above corresponds to a $\mathbb{Q}$-rational point on $X_{ns}^+(11)$.*

Let $P \in X_{ns}^{+}(11)(\mathbb{Q})$ be the point as in the corollary which corresponds to an elliptic curve with CM by $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$. Similarly, let $Q \in X_{ns}^{+}(11)(\mathbb{Q})$ be the point which corresponds to an elliptic curve with CM by $\mathbb{Z}[\sqrt{-1}]$. Both P, Q can be regarded in $E(\mathbb{Q}(\zeta_{11}))$ under the isomorphism $E \cong_{\mathbb{Q}(\zeta_{11})} X_{ns}^{+}(11)$.

By translation under the group law on $X_{ns}^{+}(11)$, we may assume without loss of generality that $O = P$. Let $[x' : y' : 1] = [x : y : 1] - [x(P) : y(P) : 1]$. Then x', y' still satisfy the Weierstrass equation (E), but now have poles at P instead of ∞.

Since x', y' and X, Y are two different Weierstrass models for $X_{ns}^{+}(11)|\mathbb{Q}(\zeta_{11})$ with poles at $O = P$, there is a relation

$$\begin{aligned} X &= u^2 x' + r, \\ Y &= u^3 y' + u^2 s x' + t, \end{aligned}$$

for some $u, r, s, t \in \mathbb{Q}(\zeta_{11})$, by uniqueness of Weierstrass models. The values of u, r, s, t can be determined, as the Weierstrass models have known coefficients (the ambiguity in sign in u is due to the extra automorphism -1). Thus, one can now obtain the (now formal) q-expansion of X, Y. Using a method similar to expressing j in terms of x, y, one can then express j in terms of X, Y.

To determine the values of $x(P), y(P)$, we used the following method. Plugging in $j = 0$ in relation (1) and solving for x subject to the equation satisfied by x, y, we obtained 5 possible distinct values for $x(P) \in \mathbb{Q}(\zeta_{11})$, given below with multiplicity:

```
<z^3 + z^2, 3>,
<z^6 + z^5 + 1, 11>,
<-z^9 - z^8 - z^7 - z^4 - z^3 - z^2, 11>,
<-z^9 + z^8 + z^7 - z^6 - z^5 + z^4 + z^3 - z^2 + 2, 1>,
<z^9 + z^8, 3>.
```

To determine which choice of $x(P)$ is correct, we first computed the possibilities for $x(Q)$ in a similar fashion:

```
<z^6 + z^5 + 1, 11>,
<-z^8 - z^7 - z^6 - z^5 - z^4 - z^3 + 1, 1>,
<-z^9 - z^ 8 - z^7 - z^4 - z^3 - z^2, 11>.
```

For each choice of $x(P), y(P), x(Q), y(Q)$, we checked if $X(Q), Y(Q)$ was $\mathbb{Q}$-rational. There was only one choice of (P, Q) for which this property held, namely

```
x(P) = -z^9 + z^8 + z^7 - z^6 - z^5 + z^4 + z^3 - z^2 + 2,
x(Q) = -z^8 - z^7 - z^6 - z^5 - z^4 - z^3 + 1.
```

4. Some examples of elliptic curves with nonsplit mod 11 representations

As an application, we can now determine the j-invariants of the elliptic curves corresponding to the $\mathbb{Q}$-rational points of $X_{ns}^{+}(11)$. Let $R = [4 : 5 : 1]$ be the generator of the Mordell-Weil group of $X_{ns}^{+}(11)$ over $\mathbb{Q}$. Here are examples of the

j-invariants of the elliptic curves corresponding to some multiples of R:

$$\begin{aligned}
3R :& j = 2^4 3^3 5^3 17^6 41^3 71^3 89^3 167^3 313^3 / 23^{11} 197^{11} \text{ (non-CM)},\\
2R :& j = 2^3 3^9 5^3 11^3 17^6 29^3 53^3 191^3 / 769^{11} \text{ (non-CM)},\\
R :& j = -640320^3 \text{ (CM by } -163),\\
O :& j = 0 \text{ (CM by } -3),\\
-R :& j = 1728 \text{ (CM by } -4),\\
-2R :& j = -5280^3 \text{ (CM by } -67),\\
-3R :& j = 54000 \text{ (CM by } -12),\\
-4R :& j = 66^3 \text{ (CM by } -16),\\
-5R :& j = -12288000 \text{ (CM by } -27),\\
-6R :& j = 2^8 3^3 5^6 11^3 53^3 / 23^{11} \text{ (non-CM)},\\
-7R :& j = -2^9 3^3 5^3 13^1 71^3 181^3 / 43^{11} \text{ (non-CM)}.
\end{aligned}$$

For each of the non-CM j-invariants indicated above, the following table gives a corresponding elliptic curve with small conductor N_E and the discriminant d_K of the quadratic field K associated to its projectively dihedral mod 11 representation. This was determined using the information about K given in [11] and the congruences which $a_p(E)$ should satisfy (i.e., for $p \nmid N_E \cdot 11$, p inert in K, $a_p(E) \equiv 0 \pmod{11}$) (cf. also [3]).

	E	d_K	N_E
3R	$y^2 = x^3$ $-6461935725764314856079747552315 35x$ $+19813780048239074375628018028202424203478982531558$	-3208243	$2^2 23^1 59^2 197^1 54377^2$
2R	$y^2 = x^3$ $+370507764651148661222565x$ $+1942350668351402409019671053342936 14$	-171924	$2^5 3^2 769^1 14327^2$
-6R	$y^2 = x^3 + 26366175x + 454085948673$	-67	$2^2 3^2 23^1 67^2$
-7R	$y^2 = x^3 - 6682520x - 39157150032$	-4	$2^5 13^2 43^1$

5. Acknowledgments

The first author would like to thank MSRI for his visit there in October–December 2000, where this work began, and also to thank N. Yui for comments and suggestions.

6. Appendix

The q-expansions of the functions x and y in Proposition 2.1, where $q = e^{2\pi i\tau}$:

```
x = q^(-2/11) + -z^9 - z^2 + (-z^7 - z^4)*q^(1/11) + (-z^8 - z^6
    - z^5 - z^3 + 1)*q^(2/11) + (z^9 - z^7 + z^6 + z^5 - z^4
    + z^2 - 1)*q^(3/11) + (-z^9 - z^7 - z^4 - z^2 - 1)*q^(4/11)
    + (z^9 - 3*z^8 - 2*z^7 - 2*z^6 - 2*z^5 - 2*z^4 - 3*z^3 + z^2
    - 2)*q^(5/11) + (2*z^9 + z^8 + z^3 + 2*z^2 + 4)*q^(6/11)
    + (-2*z^9 - 2*z^2 - 2)*q^(7/11) + (-4*z^9 - 2*z^8 - z^7 - 4*z^6
    - 4*z^5 - z^4 - 2*z^3 - 4*z^2 - 3)*q^(8/11) + (2*z^8 - 4*z^6
    - 4*z^5 + 2*z^3 + 10)*q^(9/11) + (-3*z^8 + z^7 - 3*z^6 - 3*z^5
    + z^4 - 3*z^3)*q^(10/11) + O(q),
y = q^(-3/11) + (-z^9 - z^8 - z^7 - z^6 - z^5 - z^4 - z^3 - z^2 - 1)
    *q^(-2/11) + (z^8 + z^7 + z^4 + z^3 + 1)*q^(-1/11) + 2*z^9 + z^8
    + z^6 + z^5 + z^3 + 2*z^2 + 1 + (-2*z^9 - 2*z^8 - z^7 - 4*z^6
    - 4*z^5 - z^4 - 2*z^3 - 2*z^2 - 1)*q^(1/11) + (-z^8 - 5*z^7
    - 5*z^4 - z^3 - 3)*q^(2/11) + (2*z^9 + z^8 + 3*z^7 + 2*z^6
    + 2*z^5 + 3*z^4 + z^3 + 2*z^2 + 4)*q^(3/11) + (3*z^9 - 7*z^8
    - 5*z^7 - 3*z^6 - 3*z^5 - 5*z^4 - 7*z^3 + 3*z^2 - 5)*q^(4/11)
    + (-6*z^9 + z^8 - 9*z^7 - 7*z^6 - 7*z^5 - 9*z^4 + z^3 - 6*z^2
    + 2)*q^(5/11) + (-z^9 - 4*z^8 - 2*z^7 - 2*z^6 - 2*z^5 - 2*z^4
     - 4*z^3 - z^2 - 7)*q^(6/11) + (4*z^9 + 12*z^7 - z^6 - z^5
    + 12*z^4 + 4*z^2 + 12)*q^(7/11) + (-7*z^9 + 4*z^8 - 12*z^7
    - 13*z^6 - 13*z^5 - 12*z^4 + 4*z^3 - 7*z^2 + 16)*q^(8/11)
    + (-24*z^9 - 18*z^8 - 15*z^7 - 30*z^6 - 30*z^5 - 15*z^4
    - 18*z^3 - 24*z^2 - 21)*q^(9/11) + (2*z^9 + 11*z^8 + 21*z^7
    + 5*z^6 + 5*z^5 + 21*z^4 + 11*z^3 + 2*z^2 + 23)*q^(10/11)
    + O(q).
```

The polynomials A, B, C of Theorem 1.1:

```
A = (X^5 - 119*X^4 + 1381*X^3 - 2642*X^2 - 9313*X + 19249)^11,

B = (-98387520*X^54 - 220438794499*X^53 - 53420217837899*X^52
+ 6338048458979853*X^51 + 71475058557035848*X^50
- 4429159788731198073*X^49 + 32427115856565021423337*X^48
- 123595289334495611502045*X^47
+ 2465220203610361958991252*X^46
+ 4714178266732077504326779*X^45
- 223043130380136743147858654 3*X^44
+ 923321461306906881425179746 63*X^43
- 2507289782484853611270309175397*X^42
+ 5335969780947520724506055736 3937*X^41
- 942047948418627104106931499116639*X^40
+ 14114007315932826893573283384330808*X^39
- 18369044731752236666885484019765 1161*X^38
+ 2171510861410311795157039184686867406*X^37
- 24911038397772665326423913919305711163*X^36
+ 291169675293150416804617731761995291067*X^35
- 3415529427584012398564140280662798038067*X^34
+ 37855207962015462701067289499903775336771*X^33
- 374992775331213422799775513202374746471447*X^32
+ 3207001025188524833125521692358292634027949*X^31
- 23141471939301096287187426104081929791336253*X^30
+ 137360034469063724618182923106280369775169352*X^29
- 638617861348315025223322860571024211741905470*X^28
+ 2013006888766112251485827113833063752292822797*X^27
- 11668204576301833742662357648796837248247307 53*X^26
- 35448755737371974992340224606099228330400359378*X^25
+ 281145492835905205314154378132072415664685281266*X^24
- 1275116642123942750922015094862993429873903104392*X^23
+ 3568711769977516712360325915844869782908014276967*X^22
- 27265071788664773805740481436443251943201308842 62*X^21 -
- 31447406024550699683476578355464224641763394892606*X^20
```

[4] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In P. Deligne and W. Kuyk, editors, *Modular Functions of One Variable II*, number 349 in Lecture Notes in Mathematics, pages 143–316. Springer-Verlag, 1972. MR **49:**2762

[5] N. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves*. Number 108 in Annals of Mathematics Studies. Princeton University Press, 1985. MR **86i:**11024

[6] M.A. Kenku. A note on the integral points of a modular curve of level 7. *Mathematika*, 32:45–48, 1985. MR **87d:**11040

[7] D. Kubert and S. Lang. *Modular Units*, volume 244 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1981. MR **84h:**12009

[8] Daniel Kubert. Quadratic relations for generators of units in the modular function field. *Math. Ann.*, 225(1):1–20, 1977. MR **55:**5536

[9] G. Ligozat. Courbes modulaires de niveau 11. In J.P. Serre and D.B. Zagier, editors, *Modular Functions of One Variable V*, number 601 in Lecture Notes in Mathematics, pages 149–237. Springer-Verlag, 1977. MR **57:**3079

[10] B. Mazur. Rational isogenies of prime degree. *Inventiones mathematicae*, 44:129–162, 1978. MR **80h:**14022

[11] J.P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Mathematicae*, 15:259–331, 1972. MR **52:**8126

[12] J.P. Serre. *Lectures on the Mordell-Weil Theorem*. Number E15 in Aspects of Mathematics. Friedr, Vieweg & Sohn, Braunschweig, 1989. MR **90e:**11086

[13] C.L. Siegel. Zum Beweise des Starkschen Satzes. *Inventiones Mathematicae*, 5:180–191, 1968. MR **37:**4045

Department of Mathematics, Simon Fraser University, Burnaby, British Columbia, Canada, V5A 1S6
E-mail address: ichen@math.sfu.ca

Department of Mathematics and Statistics, Concordia University, Montreal, Quebec, Canada, H3G 1M8
E-mail address: cummins@mathstat.concordia.ca