Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9

Noam D. Elkies

Abstract. Let $E$ be an elliptic curve over $\mathbb{Q}$, and $\rho_l: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}_l)$ its $l$-adic Galois representation. Serre observed in 1968 [2] IV, 3.4, Lemma 3 that for $l \geq 5$ there is no proper closed subgroup of $\text{SL}_2(\mathbb{Z}_l)$ that maps surjectively onto $\text{SL}_2(\mathbb{Z}/l\mathbb{Z})$, and concluded that if $\rho_l$ is surjective mod $l$ then it is surjective onto $\text{GL}_2(\mathbb{Z}_l)$. We show that this no longer holds for $l = 3$ by describing a modular curve $\mathcal{X}_9$ of genus 0 parametrizing elliptic curves for which $\rho_3$ is not surjective mod 9 but generically surjective mod 3. The curve $\mathcal{X}_9$ is defined over $\mathbb{Q}$, and the modular cover $\mathcal{X}_9 \to X(1)$ has degree 27, so $\mathcal{X}_9$ is rational because 27 is odd. We exhibit an explicit rational function $f \in \mathbb{Q}(x)$ of degree 27 that realizes this cover. We show that for every $x \in \mathbb{P}^1(\mathbb{Q})$, other than the two rational solutions of $f(x) = 0$, the elliptic curves with $j$-invariant $f(x)$ have $\rho_3$ surjective mod 3 but not mod 9. We determine all nonzero integral values of $f(x)$, and exhibit several elliptic curves satisfying our condition on $\rho_3$, of which the simplest are the curves $Y^2 = X^3 - 27X - 42$ and $Y^2 + Y = X^3 - 135X - 604$ of conductors 1944 = $2^33^5$ and 6075 = $3^55^2$ respectively.

0. Introduction. Let $E$ be an elliptic curve over $\mathbb{Q}$, and $\rho_l: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}_l)$ its $l$-adic Galois representation. Serre observed in 1968 [2] IV, 3.4, Lemma 3 that for $l \geq 5$ there is no proper closed subgroup of $\text{SL}_2(\mathbb{Z}_l)$ that maps surjectively onto $\text{SL}_2(\mathbb{Z}/l\mathbb{Z})$, and concluded that if $\rho_l$ is surjective mod $l$ then it is surjective onto $\text{GL}_2(\mathbb{Z}_l)$. He noted [2] IV, 3.4, Exercise 3 that for $l = 3$ there exists a subgroup $G \subset \text{SL}_2(\mathbb{Z}/9\mathbb{Z})$ such that the restriction to $G$ of the reduction-mod-3 map $\text{SL}_2(\mathbb{Z}/9\mathbb{Z}) \to \text{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is an isomorphism. The preimage of $G$ in $\text{SL}_2(\mathbb{Z}_9)$ is then a proper closed subgroup that maps surjectively to $\text{SL}_2(\mathbb{Z}/3\mathbb{Z})$. This suggests that there could be curves $E$ for which $G$ is the image of $\rho_3$ mod 9, making $\rho_3$ surjective mod 3 but not mod 9. Serre does not raise this question explicitly, and it does not seem to have been addressed elsewhere in the literature; I thank Grigor Grigorov for drawing my attention to it. In this paper we answer the question by showing that there exist infinitely many $j \in \mathbb{Q}$ for which an elliptic curve of $j$-invariant $j$ must have $\rho_3$ surjective mod 3 but not mod 9. The simplest examples are $j = 4374$, $j = 419904$, and $j = -44789760$. In general $j$ is the value of a rational function $f(x)$ of degree 27 at all but finitely many $x \in \mathbb{P}^1(\mathbb{Q})$.

Such curves $E$ are parametrized by a modular curve $\mathcal{X}_9 = X(9)/G$. The natural cover $\mathcal{X}_9 \to X(1)$ has degree 27, and our rational function $f$ arises as the pullback to $\mathcal{X}_9$ of the degree-1 function $j$ on $X(1)$. It is easy to check from the Riemann-Hurwitz formula that $\mathcal{X}_9$ has genus zero. The challenge is to prove that $\mathcal{X}_9$ is defined over $\mathbb{Q}$ and to compute $f(x)$ for some choice of rational coordinate $x$ on $\mathcal{X}_9$. (Once $\mathcal{X}_9$ is known to be defined over $\mathbb{Q}$, it is automatically isomorphic with $\mathbb{P}^1$ over $\mathbb{Q}$, because it supports the rational function $j$ of odd degree.) We prove the rationality in section 1, and compute $x$ using products of Siegel functions in section 2. Such products are modular.

1 Supported in part by NSF grants DMS-0200687 and DMS-0501029.
units on $X(N)$ with known $q$-expansions; since the cusps of $\mathcal{X}_9$ are not rational we must also find a fractional linear transformation over $\mathcal{Q}$ that takes the modular unit to a function $x$ defined over $\mathcal{Q}$. In section 3 we discuss elliptic curves $E$ with $j$-invariants obtained by specializing $f$, and use explicit computation of curves $X(9)/H$ with $H \subset G$ to show that all such curves with $x \in \mathcal{P}_1(\mathcal{Q})$ satisfy our condition on $\rho_3$ except for those with $j = 0$. Finally in section 4 we determine the finite set $f(\mathcal{P}_1(\mathcal{Q})) \cap \mathcal{Z}$, and exhibit some specific elliptic curves $E$ whose $j$-invariants are these integral values.

1. The group $G$ and the curve $\mathcal{X}_9$. The group $\text{SL}_2(\mathcal{Z}/3\mathcal{Z})$ is generated by

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

the images mod 3 of the standard generators of $\text{SL}_2(\mathcal{Z})$. These generators of $\text{SL}_2(\mathcal{Z}/3\mathcal{Z})$ satisfy

$$S^2 = (ST)^3 = -I, \quad T^3 = I.$$ 

To lift $\text{SL}_2(\mathcal{Z}/3\mathcal{Z})$ to a subgroup $G$ of $\text{SL}_2(\mathcal{Z}/9\mathcal{Z})$, it is enough to lift $S, T$ to matrices mod 9 satisfying the same relations[2]. A direct search finds 27 such lifts $\tilde{S}, \tilde{T}$, all equivalent under conjugation in $\text{SL}_2(\mathcal{Z}/9\mathcal{Z})$. These yield 27 choices of lift of $\text{PSL}_2(\mathcal{Z}/3\mathcal{Z})$ to a subgroup $G/\{ \pm 1 \}$ of $\text{PSL}_2(\mathcal{Z}/9\mathcal{Z}) = \text{Aut}(X(9))$, all conjugate in $\text{Aut}(X(9))$. Hence the quotients of $X(9)$ by these subgroups are all equivalent under $\text{Aut}(X(9))$. We choose

$$\tilde{S} = \begin{pmatrix} 0 & 2 \\ 4 & 0 \end{pmatrix}, \quad \tilde{T} = \begin{pmatrix} 4 & 1 \\ -3 & 4 \end{pmatrix},$$

and set $G = \langle \tilde{S}, \tilde{T} \rangle \subset \text{SL}_2(\mathcal{Z}/9\mathcal{Z})$ and $\mathcal{X}_9 = X(9)/(G/\{ \pm 1 \})$.

We can then calculate the genus of $\mathcal{X}_9$ by applying the Riemann-Hurwitz formula either to the quotient map $X(9) \rightarrow \mathcal{X}_9$, using the fact that $X(9)$ has genus 10, or to the covering map $\mathcal{X}_9 \rightarrow X(1)$. In the quotient map, each of the three involutions in $G$ has six fixed points, and each of the four 3-element subgroups has three; thus the ramification divisor has degree $3 \cdot 6 + 4 \cdot 6 = 42 = 2|G| + 2(10 - 1)$, whence $\mathcal{X}_9$ has genus 0. The covering map has degree 27 and is unramified except above the cusp $j = \infty$ and the elliptic points $j = 0, j = 1728$. We find that these points have preimages with multiplicities $9^3, 3^61^3$, and $12^21^3$ respectively (using $m^c$ as a standard shorthand for $c$ preimages of multiplicity $m$). Hence the ramification divisor has degree $3 \cdot 8 + 8 \cdot 2 + 12 = 52 = 2(27 - 1)$, so again we conclude that $\mathcal{X}_9$ has genus 0.

In particular, each of the cusps of $X(9)$ has trivial stabilizer in $G$. To explain this, note that the stabilizer in $\text{PSL}_2(\mathcal{Z}/9\mathcal{Z})$ of each cusp of $X(9)$ is conjugate to the group of matrices $\{ \pm (1,1) \}$; if $G$ had a nontrivial intersection with this group then $G$ would contain $\{ \pm (1,3) \}$, contradicting the requirement that the reduction map $G \rightarrow \text{PSL}_2(\mathcal{Z}/3\mathcal{Z})$ be bijective. It follows that $\mathcal{X}_9$ has $27/9 = 3$ cusps.

---

[2] Warning: This approach to lifting $\text{SL}_2(\mathcal{Z}/n\mathcal{Z})$ works only for $n \leq 5$ (including $n = 4$), where $\langle s, t \mid s^2 = (st)^3 = t^n = 1 \rangle$ is a presentation of $\text{PSL}_2(\mathcal{Z}/n\mathcal{Z})$. For $n > 5$ more relations must be checked.
To obtain a model of $\mathcal{X}_9$ defined over $\mathbb{Q}$, we must extend $G$ to a group $G' \subset \text{GL}_2(\mathbb{Z}/9\mathbb{Z})$ such that $G' \triangleright G$ and the determinant map $G'/G \to (\mathbb{Z}/9\mathbb{Z})^\ast$ is an isomorphism. For the preimages of the squares in $(\mathbb{Z}/9\mathbb{Z})^\ast$ we use the invertible multiples of the identity (recall that $-I$ is already in $G$). It remains to lift $\pm\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ from $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ to $\text{GL}_2(\mathbb{Z}/9\mathbb{Z})$, and we calculate that the unique choice that normalizes $G$ is $\pm\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Together with the invertible scalar matrices this yields a unique extension $G'$ satisfying our conditions, and thus a unique structure for $\mathcal{X}_9$ as a modular curve over $\mathbb{Q}$.

In general, even if a curve of genus 0 is known to be defined over $\mathbb{Q}$ it need not be isomorphic with $\mathbb{P}^1(\mathbb{Q})$. But in our case the curve supports $\mathbb{Q}$-rational divisors of odd degree (such as the preimage of the cusp, or indeed the preimage of any rational point on $X(1)$, so $\mathcal{X}_9$ must be isomorphic with $\mathbb{P}^1(\mathbb{Q})$. In the next section we choose an isomorphism, and compute $j$ as a rational function of a rational coordinate on $\mathcal{X}_9$.

While $\mathcal{X}_9$ is defined over $\mathbb{Q}$, its three cusps are not rational. More precisely, they are conjugate over the cyclic cubic extension $K := \mathbb{Q}(\zeta + \zeta^{-1})$, where $\zeta = e^{2\pi i/9}$, a primitive 9th root of unity. To see this, we check that $G'$ contains an element $\pm\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for $a = \pm 1$ (when $b = 0$) but no other $a \in (\mathbb{Z}/9\mathbb{Z})^\ast$. (Since $G'$ contains $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, it is enough to check this for $a = 4$ and $a = 7$, and then we can multiply by the scalar matrix $a^{-1} \in G'$ to reduce to the corresponding statement for $G$.) Thus the subgroup of $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ that fixes the cusp $i\infty$ consists of the images of $\pm 1$ under the standard identification of $(\mathbb{Z}/9\mathbb{Z})^\ast$ with $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Hence that cusp is defined over $K$ but not over $\mathbb{Q}$, and its conjugates under $\text{Gal}(K/\mathbb{Q})$ must be the other two cusps of $\mathcal{X}_9$.

The fact that the cusps of $\mathcal{X}_9$ are not rational will make our computation of rational functions on $\mathcal{X}_9$ somewhat trickier: we can still expand these functions in powers of $q$, but the coefficients will in general be contained only in $K$, not in $\mathbb{Q}$, even for a function in $\mathbb{Q}(\mathcal{X}_9)$.

2. Computing $x$ and $f(x)$. For $\tau$ in the upper half-plane $\mathcal{H}$, let $q = e^{2\pi i\tau}$ as usual, and let $q_9 = e^{2\pi i\tau/9}$, a local parameter for $X(9)$ and $\mathcal{X}_9$ at the cusp $\tau = i\infty$, with $q = q_9^3$. The curve $X(3)$ has genus zero with rational coordinate

$$H_3 = \left(\frac{\eta(\tau/3)}{\eta(3\tau)}\right)^3 + 3 = q_9^{-3}(1 + 5q - 7q^2 + 3q^3 + 15q^4 - 32q^5 + \cdots);$$

the curve $X(9)$ is a $(\mathbb{Z}/3\mathbb{Z})^3$ cover of $X(3)$ whose function field is obtained from $\mathbb{C}(H_3)$ by adjoining cube roots of $H - 3$, $\zeta^3 H - 3$, and $\zeta^{-3} H - 3$. The group $\text{PSL}_2(\mathbb{Z}/3\mathbb{Z})$ acts on $X(3)$ by the fractional linear transformations of $H$ that permute $\{\infty, 3\zeta, 3\zeta^2, 3\zeta^{-2}, 3\zeta^{-3}\}$, which are the transformations that preserve $j = H^3((H^3+216)/(H^3-27))^3$. (Recall that we set $\zeta = e^{2\pi i/9}$, so 1 and $\zeta^{\pm 3}$ are the cube roots of unity.) To compute $\mathcal{X}_9$, we may lift these transformations to elements of $G$ in the group $\text{PSL}_2(\mathbb{Z}/9\mathbb{Z})$ of automorphisms of $X(9)$ and look for a rational function $x$ of degree 1 on the quotient $\mathcal{X}_9 = X(9)/G$. We could try to find $x$ using our above description of the function field of $X(9)$ as a $(\mathbb{Z}/3\mathbb{Z})^3$ extension of $\mathbb{C}(H_3)$, but this seemed like an unpleasant project. Instead we use modular units on $X(9)$, that is, modular functions whose divisors are supported on the cusps.
For integers $a, b$ we have a function $s_{a,b}$ on $\mathcal{H}$ defined by

$$s(a, b) = q_9^\alpha (1 - \zeta^b q_9^a) \prod_{n=1}^{\infty} (1 - \zeta^b q_9^{9n+a})(1 - \zeta^{-b} q_9^{9n-a}),$$

where $\alpha = (a^2 / 9 + a - 9/6)/2 = 18B_2(a/9)$. This is a modular unit, namely the “Siegel function” of [4] p.29 with parameters $(a/9, b/9)$, multiplied by a power of $-\zeta$ that is irrelevant for our purpose. Taking $N = 9$ in [4] p.68, Thm. 4.1, we see that a product $F = \prod r s(a_r, b_r)^{m_r}$ of such functions is a modular function on $X(9)$ if and only if the $(a_r, b_r)$ and $m_r$ satisfy the “quadratic relations”

$$\sum_r m_r a_r^2 = \sum_r m_r b_r^2 = \sum_r m_r a_r b_r = 0 \mod 9.$$

Note that this condition depends only on the $(a_r, b_r) \mod 9$, and is invariant under changing $(a_r, b_r)$ to $(-a_r, -b_r)$ for some $r$; Indeed $s(-a, -b)$ is a scalar multiple of $s(a, b)$, as is $s(a', b')$ if $(a', b') \equiv (a, b) \mod 9$.

The pairs $\{(a, b), (-a, -b)\} \in (\mathbb{Z}/9\mathbb{Z})^2$ with at least one of $a, b$ not divisible by 3 correspond bijectively with the cusps of $X(9)$: the cusps are orbits of $\Gamma(9)$ acting on $\mathbb{P}^1(\mathbb{Q})$, and if $\gcd(a, b) = \gcd(a', b') = 1$ for some integers $a, b, a', b'$ then $a/b$ and $a'/b'$ are in the same orbit if and only if $(a', b') \equiv (a, b) \mod 9$. This labeling is consistent with the action of $\text{PSL}_2(\mathbb{Z}/9\mathbb{Z})$ on cusps, and dual to its action on the modular units $s(a, b)$ (up to $\mu_{18}$ factors). We choose one of the three orbits of the action of $G/\{\pm 1\}$ on the cusps of $X(9)$, and take $(a_r, b_r)$ corresponding to the twelve cusps in the orbit. We check that these satisfy the quadratic relations with $m_r = 1$, so the product $F$ of the twelve functions $S(a_r, b_r)$ is a modular function on $X(9)$ whose divisor is invariant under $G$.

There is then a homomorphism $\chi : G \to \mathbb{C}^*$ such that $F(g(\tau)) = \chi(g)F(\tau)$ for all $g \in G$ and $\tau \in \mathcal{H}$. We claim that $\chi$ is trivial. Indeed, if it were nontrivial we could take for $g$ a 3-cycle in $G$, and for $\tau$ a preimage of a fixed point on $X(9)$ of $g$, and conclude that $\tau$ is a zero or pole of $F$, which is impossible because $\tau$ is not a cusp. Therefore $\chi$ is trivial as claimed, whence $F$ descends to a function on $\mathcal{X}_9$ whose only poles or zeros are at the cusps.

We find that $F$ has a simple pole at one cusp, a simple zero at another, and neither zero nor pole at the third. In particular, $F$ is a function of degree 1 on $\mathcal{X}_9$. Choosing the orbit of $(a, b) = (1, 0)$, corresponding to the cusp $i\infty$, we find that $F$ has a pole at that cusp, and calculate the $q$-expansion

$$F = q_9^{-1} - 1 + c_1 q_9 + c_1^2 q_9^2 + (c_2 + 2) q_9^3 + c_3 q_9^4 + \cdots,$$

where $c_m := \zeta^m + \zeta^{-m}$, a unit in $K$. The $q$-expansions of the products corresponding to the other two orbits then let us recognize those products as fractional linear transformations of $F$, namely $1/(F - c_2 + 1)$ and $(1 - c_2)/F$.

It follows that $F$ takes the values 0 and $1 - c_2$ on the other two cusps of $\mathcal{X}_9$. Therefore $j$, considered as a rational function of $F$, must have its poles at $F = 0, 1 - c_2, \infty,$
each with multiplicity 9. Indeed we compute that \( F^3(F - c_2 + 1)^3 j \) is a polynomial of degree 27 in \( F \) to the accuracy allowed by our \( q \)-expansions (which extend far enough beyond the constant term of that polynomial to provide a sanity check on our computations).

It remains to find a fractional linear transformation with coefficients in \( K \) that, when applied to \( F \), yields a coordinate \( x \) on \( \mathcal{Z}_9 \) such that \( j \in \mathbb{Q}(x) \). Thus \( x \) must map the three cusps to a \( \text{Gal}(K/\mathbb{Q}) \) orbit in \( K \). We may choose any ordered orbit, and then \( x \) is determined uniquely, because \( \text{PGL}_2 \) acts simply 3-transitively on \( \mathbb{P}^1 \). (The order must be consistent with the Galois action on the cusps.) We then apply a \( \text{PGL}_2(\mathbb{Q}) \) transformation so that the map \( \mathcal{Z}_9 \to X(1) \) is represented by a rational function with small coefficients. This leads us to

\[
\begin{align*}
x &= \frac{-c_1 F + 1 - c_2}{F - c_1 + 3(1 - c_2)} \\
&= -c_1 + (2c_2 + c_4)q_9 + 3(1 - c_1)q_9^2 + (6 - 7c_1 + c_2)q_9^3 + (15 - 16c_1 + 7c_2)q_9^4 \cdots,
\end{align*}
\]

when \( j = f(x) \) with

\[
\begin{align*}
f(x) &= -3^7(x^2 - 1)^3(x^6 + 3x^5 + 6x^4 + x^3 - 3x^2 + 12x + 16)^3(2x^3 + 3x^2 - 3x - 5) \\
&= 1728 - \frac{3^2 A(x) B^2(x)(2x^3 - 3x^2 + 4)}{(x^3 - 3x - 1)^9},
\end{align*}
\]

where \( A(x), B(x) \) are the sextic polynomials

\[
\begin{align*}
A(x) &= x^6 + 6x^5 + 4x^3 + 12x^2 - 18x - 23, \\
B(x) &= 7x^6 + 24x^5 + 18x^4 - 26x^3 - 33x^2 + 18x + 28.
\end{align*}
\]

3. The elliptic curves parametrized by \( \mathcal{Z}_9 \). Now let \( E/\mathbb{Q} \) be an elliptic curve with \( j \)-invariant \( f(x) \) for some \( x \in \mathbb{P}^1(\mathbb{Q}) \). Assume that its 3-adic Galois representation \( \rho_3 \) is surjective mod 3. Then its image mod 9 is a conjugate of the proper subgroup \( G' \) of \( \text{GL}_3(\mathbb{Z}/9\mathbb{Z}) \), because this image is contained in \( G \) and its determinant maps surjectively to \( \mathbb{Z}_3^* \). In particular, \( \rho_3 \) is surjective mod 3 but not mod 9, as desired.

We claim that the mod-3 condition on \( \rho_3 \) is satisfied by except at \( x = \pm 1 \), the points at which \( f(x) = 0 \), the \( j \)-invariant of an elliptic curve with complex multiplication.

For any elliptic curve \( E/\mathbb{Q} \), the representation \( \rho_3 \) is surjective mod 3 if and only if the intersection of its image in \( \text{PGL}_2(\mathbb{Z}/3\mathbb{Z}) \) with \( \text{PSL}_2(\mathbb{Z}/3\mathbb{Z}) \) is contained in the 4-element normal subgroup or in a cyclic subgroup of order 3. In the former case, the \( j \)-invariant \( j_E \) of \( E \) is a cube, and this necessary condition is also sufficient unless \( j_E = 0 \). If \( f(x) \neq 0 \) then \( f(x) \) is a cube if and only if \( 3(2x^3 + 3x^2 - 3x - 5) = z^3 \) for some \( z \in \mathbb{Q} \). This curve of genus 1 has no rational points due to a 3-adic obstruction: we have

\[
2x^3 + 3x^2 - 3x - 5 = 3(x + 1)^3 - (x + 2)^3,
\]

so the 3-adic valuation of \( 3(2x^3 + 3x^2 - 3x - 5) \) is never divisible by 3. Thus \( f(x) \) is never a nonzero cube. The latter case holds if and only if \( E \) admits a rational
3-isogeny. Such \( x \) are parametrized by a curve \( \mathcal{X}'_g = \mathcal{X}_g/\langle T \rangle \), the quotient of \( X(9) \) by a 3-cycle in \( G \). This curve has genus 3, so there are only finitely many such \( x \) by Mordell-Faltings. For a general curve of genus 3 it is not known how to provably list all the rational points. But here we are lucky: we can give a rational map of degree 3 from \( \mathcal{X}'_g \) to the elliptic curve \( Y^2 + Y = X^3 \), which is known to have rank zero. Pulling back each of this curve’s three rational points to \( \mathcal{X}'_g \) then yields a set of \( \mathbb{Q} \)-rational points that must contain all the \( \mathbb{Q} \)-rational ones. To complete the proof of our claim we shall observe that there are only two \( \mathbb{Q} \)-rational points, one for each of \( x = \pm 1 \).

A simple model for \( \mathcal{X}'_g \) is
\[
3z_2^3 = z_1(z_1^3 + 3z_1^2 - 6z_1 + 1),
\]
and the map to \( Y^2 + Y = X^3 \) can be given by
\[
(X : Y : 1) = (z_1(z_1 + 1)z_2 : 3z_1^2 : z_2^3).
\]
The rational points on \( \mathcal{X}'_g \) are \((0, 0)\) and the point at infinity. The equation (1) for \( \mathcal{X}'_g \) shows that this curve has an automorphism \( \sigma \) of order 3 that fixes \( z_1 \) and multiplies \( z_2 \) by a cube root of unity. This automorphism arises from the element \( 3T - 2 = (1, 1, 1) \) of \( \text{PSL}_2(\mathbb{Z}/9\mathbb{Z}) \), which commutes with \( T \) and thus descends from \( \text{Aut}(X(9)) \) to an automorphism of \( \mathcal{X}'_g \). The quotient of \( \mathcal{X}'_g \) by \( \langle \sigma \rangle \) is the \( z_1 \)-line, which covers the \( j \)-line \( X(1) \) with degree 36 and the curve \( X_0(3) \) with degree 9. The latter map can be realized by the rational function \( 27((z_1^3 + 3z_1^2 - 6z_1 + 1)/(z_1^3 - 6z_1^2 + 3z_1 + 1))^3 \).

We next outline the computation of the model (1) and the map (2). We begin with the modular units
\[
s(1, 0)s(4, 6)s(4, 3), \quad s(4, 0)s(7, 6)s(7, 3), \quad s(7, 0)s(1, 6)s(1, 3).
\]
The first of these corresponds to the orbit of the cusp \( i\infty \) under the 3-cycle \( T \), and the others are obtained by multiplying \( \{1, 0 \}, \{4, 6 \}, \{4, 3 \} \) by 4 and 7 mod 9. We calculate that these products do not satisfy the quadratic relations, but the quotient of any two of them does, giving a rational function of degree 3 on \( \mathcal{X}'_g \). Using the \( q \)-expansions we find that the three functions in (3) are linearly dependent, and thus that their pairwise quotients are all related by fractional linear transformations over \( K \). As we did for \( x \), we find two linear combinations of the functions in (3) whose quotient is a degree-3 function on \( \mathcal{X}'_g \) defined over \( \mathbb{Q} \). We call this function
\[
y = -c_2 + (c_4 - c_2 + 3)q_0 + (3c_4 - 6c_7 + 9)q_0^2 + (10c_4 - 22c_7 + 27)q_0^3 \cdots,
\]
and use the \( q \)-expansions to find the coefficients of a polynomial identity \( P(x, y) = 0 \) of bidegree \( (3, 4) \) in \( (x, y) \).

This is a model for \( \mathcal{X}'_g \) in \( \mathbb{P}^1 \times \mathbb{P}^1 \), but it is not smooth. We find that it has three double points, at \( x = y = -c_1, -c_2, -c_4 \). Thus the holomorphic differentials on \( \mathcal{X}'_g \) are the forms \( Q(x, y)dx/P_y \) for \( Q \) in the 3-dimensional space of polynomials of bidegree \( (1, 2) \) that vanish at the three singularities. We interpret these as modular cuspforms of
weight 2 on $\mathcal{X}_4^2$ by writing $q\,dx/dq$ in place of $dx$, and find a basis for the space of such cuspforms:

\[
\begin{align*}
\varphi_1 &= c_4q - 3q^3 - 2c_2q^4 - c_1q^7 + 6q^{12} + 5c_2q^{13} + 4c_1q^{16} - 7c_4q^{19} + 3q^{21} \cdots, \\
\varphi_2 &= q + (c_4 - c_1)q^2 + q^4 + (2c_2 + c_4)q^5 + 2q^7 + (c_2 + c_4)q^8 - 3q^{10} \cdots, \\
\varphi_3 &= (c_4 - c_2)q - 3q^2 + (c_2 - c_1)q^4 + 3q^5 + (2c_1 - 2c_4)q^7 + 3q^8 + (3c_2 - 3c_4)q^{10} \cdots.
\end{align*}
\]

The affine model (1) is then obtained by taking $(z_1 : z_2 : 1) = (\varphi_2 + \varphi_1 : \varphi_3 : 2\varphi_2 - \varphi_3)$. The map (2) was obtained by integrating the CM form $\varphi_1$; it can also be seen in (1) by writing the cubic factor as $(z_1 + 1)^3 - 9z_1$.

4. Numerical examples. Besides $f(\pm 1) = 0$, there are seven other integers obtained by evaluating $f(x)$ at points of $P^1(\mathbb{Q})$ of small height. For each of those, we list $x$, $f(x)$, and one of the elliptic curves $E$ of $j$-invariant $f(x)$ and minimal conductor $N$:

| $x$ | $j = f(x)$ | $E$ | $N$ |
|-----|-------------|-----|-----|
| 1/0 | 4374        | $[0, 0, 0, -27, -42]$ | $2^{3}3^{5}$ |
| -2  | 419904      | $[0, 0, 0, -162, 792]$ | $2^{3}3^{5}$ |
| 0   | -44789760   | $[0, 0, 1, -135, -604]$ | $3^{5}5^{2}$ |
| -1/2| 15786448344 | $[0, 0, 0, -5427, 153882]$ | $2^{5}3^{5}$ |
| 2   | 2499251858304 | $[0, 0, 0, -201042, 34695912]$ | $2^{8}3^{5}17^{2}$ |
| -3/2| -9251041526500 | $[0, 0, 0, -1126035, 459913278]$ | $2^{3}3^{5}19^{2}$ |
| -1/3| -70043919611288518656 | $[0, 0, 1, -1127379978, -14569799990728]$ | $3^{5}97^{2}101^{2}$ |

The smallest conductor here is 1944 = $2^{3}3^{5}$, still too large to appear in Cremona’s published tables [2] of curves of conductor ≤ 1000. But Cremona has pursued his computations up to $10^5$ and beyond (see [3] for the status as of mid-2006), enough to find our first curve as well as those of conductors 6075 = $3^{5}5^{2}$, 7776 = $2^{3}3^{5}$, and 62208 = $2^{3}3^{5}$. Curves with $j = 4374$, $j = 419904$, and $j = 15786448344$ already appeared in the tables of elliptic curves with good reduction away from 2 and 3, compiled in 1966 by F.B. Coghlan and published as “Table 4” in [1] p.123]: see rows 52, 84, and 86 of “Table 4a” [1] p.125, and [1] p.75 for the attribution to Coghlan.

A search up to height 256 found no more integral values of $f(x)$. Since $f$ has three distinct poles, there can be only finitely many $x$ for which $f(x) \in \mathbb{Z}$. We claim that in fact we have found them all. Suppose $x = m/n$ in lowest terms. The resultant of the numerator and denominator of $f(x)$ is $3^{486}$, so when we write $f(m/n)$ as the quotient of homogeneous polynomials in $m,n$ the denominator $(m^3 - 3mn^2 - n^3)^{3A}$ must be $\pm 3^{A}$ for some $A$. Thus $m^3 - 3mn^2 - n^3 = \pm 1$ or $\pm 3$, because the only $(m,n) \in \mathbb{Z}^2$ for which $9 \mid m^3 - 3mn^2 - n^3$ are those for which $3|m$ and $3|n$. The only cases of $m^3 - 3mn^2 - n^3 = \pm 3$ are $x = 1, -2, -1/2$, because these are the only rational points on the elliptic curve $x^3 - 3x - 1 = 3z^3$ (isogenous with the cubic Fermat curve). For $m^3 - 3mn^2 - n^3 = \pm 1$ one must work harder because the elliptic curve $x^3 - 3x - 1 = z^3$ has rank 1. Fortunately this work was already done by Ljunggren, who proved in 1942 that the Thue equation $m^3 - 3mn^2 - n^3 = 1$ has only the six solutions $(1, 0), (0, -1), (-1, 1), (2, 1), (1, -3), (-3, 2)$, corresponding to values of $x$ already listed above. (See [5] §2, cited by Nagell [6] who also notes the connection between $X^3 + Y^3 = Z^3$.
and \( m^3 - 3mn^2 - n^3 = 3 \). The solutions of \( m^3 - 3mn^2 - n^3 = -1 \) are obtained from these six by changing each \((m, n)\) to \((-m, -n)\), which yields the same values of \( x = m/n \). Thus our list contains all the nonzero integral \( j \)-invariants of elliptic curves parametrized by \( X_9 \).

References

[1] Birch, B.J., Kuyk, W., ed.: Modular Functions of One Variable IV. Lect. Notes in Math. \textbf{476}, 1975.

[2] Cremona, J.E.: Algorithms for modular elliptic curves. Cambridge University Press, 1992.

[3] Cremona, J.E.: The elliptic curve database for conductors to 130000, Lecture Notes in Computer Science 4076 (Proceedings of ANTS-7, 2006; F.Hess, S.Pauli, and M.Pohst, ed.), 11–29.

[4] Kubert, D.S., Lang, S.: Modular Units. New York: Springer 1991.

[5] Ljunggren, W.: Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante, \textit{Acta math.} \textbf{75} (1942), 1–21.

[6] Nagell, T.: Sur un type particulier d’unités algébriques, \textit{Arkiv för Math.} \textbf{8} (1969), 163–184.

[7] Serre, J.-P.: \textit{Abelian l-adic Representations and Elliptic Curves}. Wellesley, Mass.: A.K. Peters, 1997.