COMPOSITIO MATHEMATICA

NOAM D. ELKIES

# The automorphism group of the modular curve $X_0(63)$

*Compositio Mathematica*, tome 74, n° 2 (1990), p. 203-208
<http://www.numdam.org/item?id=CM_1990__74_2_203_0>

*Compositio Mathematica* **74**: 203–208, 1990.


# The automorphism group of the modular curve $X_0(63)$

NOAM D. ELKIES*
*Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02138, USA*

Received 22 August 1989; accepted 28 August 1989

## 0. Introduction

For each positive integer $N$, the modular curve $X_0(N)$ parametrizes elliptic curves with an $N$-isogeny; recall that over $\mathbf{C}$ this curve can be realized as the quotient of the extended upper half-plane $\{\tau_1 \in \mathbf{C}: \operatorname{Im} \tau_1 > 0\} \cup \mathbf{P}^1(\mathbf{Q})$ by the group $\Gamma_0(N)$ of fractional linear transformations $\tau_1 \mapsto (a\tau_1 + b)/(c\tau_1 + d)$ where $a, b, c, d$ are integers such that $ad - bc = 1$ and $c$ is divisible by $N$, with $\tau_1$ corresponding to the isogeny $\mathbf{C}/(\mathbf{Z} + \tau_1\mathbf{Z}) \to \mathbf{C}/((1/N)\mathbf{Z} + \tau_1\mathbf{Z})$. The normalizer of $\Gamma_0(N)$ in $\mathrm{PSL}_2(\mathbf{R})$ is an extension of $\Gamma_0(N)$ by a finite group $B(N)$ of automorphisms of $X_0(N)$, and it is natural to ask whether this is the entire automorphism group of this curve, assuming that it has genus at least 2 (this excludes only a known finite list of $N$ of which the largest is 49;[1] of course a curve of genus 0 or 1 has infinitely many automorphisms over $\mathbf{C}$). In [3, Thm. 2.17] it is shown that, in this genus $\geqslant 2$ case, $X_0(N)$ has no automorphisms outside $B(N)$, with the exception of $N = 37$ and possibly $N = 63$. For $N = 37$, $B(N)$ contains only the identity and the class of the Fricke involution $w_{37}: \tau_1 \to -37/\tau_1$, and $X_0(37)$ is a curve of genus two whose hyperelliptic involution is different from $w_{37}$; this situation was described thoroughly in [4]. For $N = 63$, $B(N)$ is a 24-element group isomorphic to $A_4 \times \mathbf{Z}/2$, and $[\mathrm{Aut}\, X_0(63): B(63)]$ is either 1 or 2, and in the latter case $\mathrm{Aut}\, X_0(63)$ is isomorphic to $S_4 \times \mathbf{Z}/2$ and contains an automorphism $u$ not permuting the cusps ([3, Prop. 2.18]), but the existence of such $u$ was not settled, and [3] suggested that the determination of $\mathrm{Aut}\, X_0(63)$ would require the computation of explicit modular functions on $X_0(63)$.

In this note we complete the determination of $\mathrm{Aut}\, X_0(N)$ for all $N$ by showing that the automorphism group of $\mathrm{Aut}\, X_0(63)$ is indeed the group $S_4 \times \mathbf{Z}/2$ described in [3, Prop. 2.18]. The extra automorphism $u$ was initially constructed using explicit modular equations (for the elliptic curve $X_0(21)$, not the genus-5 curve $X_0(63)$), but it turns out that its existence can be confirmed "synthetically",

*NSF Grant DMS-87-18965.

[1] See for instance the "Remarks on isogenies" and Table 5 of [1]. More specifically we find there that there are precisely twenty-seven $N$ such that $X_0(N)$ has genus $<2$: all $N \leqslant 21$, and $N = 24, 25, 27, 32, 36, 49$.

using only the modular structure and enumerative geometry. We present this conceptual proof first, and then exhibit the modular equations.

We shall work over the ground field $\mathbf{C}$ throughout; whenever a square root appears it indicates the principal value with argument in $[0, \pi)$.

## 1. First construction

As in [3, Remark 2.19] we consider $X_0(63)$ as the quotient of the extended upper half-plane by $\Gamma_0(7) \cap \Gamma(3)$, where $\Gamma(3)$ is the group of fractional linear transformations $\tau \mapsto (a\tau + b)/(c\tau + d)$ with $a, b, c, d$ integers such that $ad - bc = 1$ and $a, c$ are both divisible by 3 (i.e. such that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbf{Z})$ is congruent to the identity matrix mod 3); this works because the transformation $\tau = 3\tau_1$ identifies that group $\Gamma_0(7) \cap \Gamma(3)$ with a conjugate of $\Gamma_0(63)$ in $\mathrm{PSL}_2(\mathbf{Q})$. That group is the intersection of the four conjugates of $\Gamma_0(7) \cap \Gamma_0(3) = \Gamma_0(21)$ in $\Gamma_0(7)$, and thus $X_0(63)$ is the normal cover of the degree-4 map $\phi: X_0(21) \to X_0(7)$, with covering group $A_4$ (this is the $A_4$ factor of $B(63) \cong A_4 \times \mathbf{Z}/2$). Here $X_0(21)$ and $X_0(7)$ have genus one and zero respectively; $\phi$ has ramification of type (3, 1) above four points of $X_0(7)$, namely the two cusps 0 and $\infty$ and the two complex multiplication points $P_\pm$ of discriminant $-3$, for which we take representatives $\tau = (\sqrt{-3} \pm 5)/14$ in the upper half-plane. The covering group $A_4$ and the map $\phi$ commute with the involution $w_7$ (the $\mathbf{Z}/2$ factor of $B(63)$); $w_7$ acts on the four ramification points of $\phi$ by the double transposition $(0\infty)(P_+ P_-)$. To construct the extra automorphism of $X_0(63)$ it is then necessary and sufficient to lift to $X_0(21)$ the other two automorphisms, say $u_1$ and $w_7 u_1$, of $X_0(7) \cong \mathbf{P}^1(\mathbf{C})$ that act by double transpositions on these four ramification points.

Now $w_7$ has two fixed points on $X_0(7)$: the two complex multiplication points $Q, Q'$ of discriminants $-7$ and $-28$ respectively, represented by $\tau = (7 + \sqrt{-7})/14$ and $\tau = \sqrt{-7}/7$. But $w_7$ has no fixed points on $X_0(21)$: a putative fixed point would necessarily lie above $Q$ or $Q'$ and so correspond to an endomorphism of degree 21 of an elliptic curve with complex multiplication by an order in $\mathbf{Q}(\sqrt{-7})$, but that is impossible because 3 is inert in this field. Thus $w_7$ must act on the elliptic curve $X_0(21)$ by translation by some 2-torsion point, and the preimage of each of $Q$ and $Q'$ consists of two pairs of points interchanged by that involution. Let $X_0(21)^+$ and $X_0(7)^+$ be the quotients of $X_0(21)$ and $X_0(7)$ by $w_7$; these are again curves of genus one and zero respectively, and since $\phi$ commutes with $w_7$ it descends to a degree-4 map $\phi^+: X_0(21)^+ \to X_0(7)^+$. This map again ramifies over four points of $X_0(7)$: the image $\infty^+$ of the cusps 0 and $\infty$, and the image $P$ of the points $P_\pm$, both of type (3,1); and the images of $Q$ and of $Q'$, which we again call $Q$ and $Q'$, both of type (2,2). Also $u_1$ and $w_7 u_1$ both commute with $w_7$ and so descend to an involution $u_1^+$ of $X_0(7)^+$ that takes $\infty^+$ to $P$ and $Q$ to $Q'$.

We now claim:

PROPOSITION. *If $\psi: C \to \mathbf{P}^1(\mathbf{C})$ is any rational function of degree 4 on a curve $C$ of genus 1 such that $\psi$ ramifies above 4 points of $\mathbf{P}^1(\mathbf{C})$, two of type (3,1) and two of type (2,2), then the involution $v_1$ of $\mathbf{P}^1(\mathbf{C})$ that takes each of these points to the other ramification point of the same type lifts to a unique involution $v$ of $C$ with four fixed points (equivalently, an involution that multiplies the holomorphic differentials of $C$ by $-1$), with two fixed points lying above each fixed point of $v_1$.*

In our case we obtain an involution $u_1$ of $X_0(21)^+$, and because $u_1$ is not a translation by a 2-torsion point on that curve it clearly lifts to a pair of involutions $u$, $w_7u$ on $X_0(21)$ which are the desired lifts of $u_1, w_7u_1$. So we need only demonstrate this Proposition to complete the determination of Aut $X_0(63)$.

*Proof of Proposition.* Uniqueness is clear: if there were two lifts $v$, their composition would be an automorphism of $C$ nontrivially permuting the fibers of $\psi$, but there is no such permutation consistent with both the (3,1) and the (2,2) ramification. To obtain existence, we use the techniques of [5] to show that, given the four ramification points of $\psi$, there are three possible fourfold covers $(C, \psi)$ of $\mathbf{P}^1(\mathbf{C})$ with the specified ramification, and three fourfold covers of $\mathbf{P}^1(\mathbf{C})/v_1$ which lift to such a cover of $\mathbf{P}^1(\mathbf{C})$ with an involution $v$ such that $\psi \circ v = v_1 \circ \psi$, and thus that each of the three possible $(C, \psi)$ admits a lift $v$ of $v_1$. Indeed, a small loop counterclockwise around each of the four ramification points of $\psi$ induces a permutation of that map's four sheets, and some conjugates $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ of these permutations in the Galois group $A_4$ of the normal cover of $\psi$ satisfy $\sigma_1\sigma_2\sigma_3\sigma_4 = 1$; since $\sigma_1, \sigma_2$ are 3-cycles and $\sigma_3, \sigma_4$ are double transpositions it follows that $\sigma_1$ and $\sigma_2$ must lie in different conjugacy classes of $A_4$. By renumbering the sheets if necessary (i.e. applying an outer automorphism of $A_4$) we may assign $\sigma_1$ to one of the two conjugacy classes of 3-cycles in $A_4$ and $\sigma_2$ to the other. Then, since $A_4$ has trivial center, it follows from [5, p. 63] that the number of covers $(C, \psi)$ given this ramification is $(1/|A_4|)$ of the number of solutions in $A_4$ of $\sigma_1\sigma_2\sigma_3\sigma_4 = 1$ with $\sigma_1, \sigma_2$ in their assigned conjugacy classes and $\sigma_3, \sigma_4$ in the conjugacy class of double transpositions, such that the four $\sigma_i$ generate $A_4$; in our case this last condition is satisfied automatically. Now there are four choices of $\sigma_1, \sigma_2$ with $\sigma_1\sigma_2 = 1$, each of which gives three choices for $(\sigma_3, \sigma_4)$, and the twelve other choices of $\sigma_1$ and $\sigma_2$ make $\sigma_1\sigma_2$ a double transposition and force $\sigma_3, \sigma_4$ to be the other two double transpositions in one of two orders; hence the total number of solutions is $3 \cdot 4 + 2 \cdot 12 = 36$, giving $36/|A_4| = 3$ covers $(C, \psi)$. Now if $C$ has an involution $v$ as described in the Proposition, then $C/v$ is a curve of genus zero with a map to $\mathbf{P}^1(\mathbf{C})/v_1$ ramified above four points: the two images of the ramification locus of $\psi$, one of type (3, 1) and one of type (2, 2), and the images of the two fixed points of $v$, each of type (2, 1, 1). Here the Galois group is $S_4$, and so the number of such coverings of $\mathbf{P}^1(\mathbf{C})/v_1$

given the location of the ramification points is (1/4!) the number of solutions to $g_1g_2g_3g_4 = 1$ in $S_4$ with $g_1$ a 3-cycle, $g_2$ a double transposition and $g_3, g_4$ single transpositions (again such $g_i$ necessarily generate $S_4$). For each of the $8 \cdot 3 = 24$ choices of $g_1$ and $g_2$, their product $g_1g_2$ is a 3-cycle, so its inverse can be written as the product of two single transpositions in three ways, for a total of 72 solutions and 3 coverings of $\mathbf{P}^1(\mathbf{C})/v_1$. Each of these is easily seen to lift to a cover $(C, \psi)$ of $\mathbf{P}^1(\mathbf{C})$ with an involution $v$ as described in the Proposition; since these $(C, \psi)$ are distinct (by the uniqueness part of the Proposition, proved above), it follows that each of the three $(C, \psi)$ arises this way. Q.E.D.

## 2. Second construction

We give explicit formulas for $\phi$ and the involutions of the modular curves $X_0(7)$ and $X_0(21)$ described above in terms of modular functions on these curves. [Naturally our equations for $X_0(7)$ and $X_0(21)$ are versions of classical formulas such as those of [2], but it was easier to derive them from scratch than to look for them in that tome and then adapt them to our needs.]

We uniformize $X_0(7) \cong \mathbf{P}^1(\mathbf{C})$ by the Hauptmodul

$$H = \left[\frac{\eta(\tau)}{\eta(7\tau)}\right]^4 = q^{-1} - 4 + 2q + 8q^2 - 5q^3 - 4q^4 - 10q^5 + 12q^6 \cdots$$

(where $q = e^{2\pi i\tau}$ as usual); this has a simple pole at the cusp $\infty$ and a simple zero at the cusp 0, and $w_7$ takes the form $H \leftrightarrow 49/H$. By applying the identities $\eta(z + k) = e^{\pi ik/12}\eta(z)\,(k \in \mathbf{Z})$ and $\eta(-1/z) = (-iz)^{1/2}\eta(z)$ we can then find the coordinates of $P_\pm, Q$ and $Q'$: since the value $\tau = (\sqrt{-3} + 5)/14$ representing $P_+$ satisfies $7\tau = 5 - 1/\tau$, we obtain

$$\eta^4(7\tau) = \eta^4(5 - 1/\tau) = e^{5\pi i/3}\eta^4(-1/\tau) = -e^{5\pi i/3}\tau^2\eta^4(\tau),$$

whence $H(P_+) = -e^{\pi i/3}\tau^{-2} = -(13 + 3\sqrt{-3})/2$; likewise (or by applying $w_7$) we find $H(P_-) = -(13 - 3\sqrt{-3})/2$, and also $H(Q) = -7, H(Q') = 7$. [For a check on these computations, note that the $X_0(1)$-Hauptmodul $j = j(\tau)$ is a degree-8 function on $X_0(7)$ with a simple pole at $\infty$ and an order-7 pole at 0, so $j = F(H)/H^7$ for some degree-8 polynomial $F$; comparing coefficients of the $q$-expansions at infinity we find $F(H) = (H^2 + 13H + 49)(H^2 + 245H + 2401)^3$, and substituting $H = -(13 \pm 3\sqrt{-3})/2, -7, 7$ we find $j(P_\pm) = 0, j(Q) = -15^3$, and $j(Q') = 255^3$, which are the correct CM-values of the $j$-invariant for discriminant $-3, -7, -28$.]

On $X_0(21)$ we have a function of degree two

$$f = \left[\frac{\eta(3\tau)\eta(7\tau)}{\eta(\tau)\eta(21\tau)}\right]^2 = q^{-1} + 2 + 5q + 8q^2 + 16q^3 + 26q^4 + 44q^5 + 66q^6 + \cdots$$

invariant under $w_{21}$, with simple poles at the cusps 0 and $\infty$ and simple zeros at the cusps 1/3, 1/7. Another function of degree two is

$$g_1 = \frac{\eta(\tau)\eta(3\tau)}{\eta(7\tau)\eta(21\tau)} = q^{-1} - 1 - q - q^2 + q^3 + 2q^4 - q^5 + 3q^6 \cdots$$

with simple poles at $\infty$ and 1/7 and simple zeros at 0 and 1/3; we have $w_{21}g_1 = 7/g_1$ and so $(g_1 + 7/g_1)f$ is necessarily a quadratic polynomial in $f$, which a comparison of $q$-expansions determines to be $f^2 - 3f + 1$. Thus the degree-4 function

$$g = (g_1 - 7/g_1)f = q^{-2} + q^{-1} - 5 - 21q - 61q^2 - \\ - 146q^3 - 334q^4 - 694q^5 - 1386q^6 - \cdots$$

has double poles at 0 and $\infty$ and satisfies $w_{21}g = -g$ and

$$g^2 = (f^2 - 3f + 1)^2 - 28f^2 = f^4 - 6f^3 - 17f^2 - 6f + 1,$$

which we take to be the defining equation for $X_0(21)$. [Check: the minimal Néron model of that equation is

$$Y^2 + XY = X^3 - 4X - 1,$$

the same as the equation for the elliptic curve $\#21B \cong X_0(21)$ given in [1]; here

$$(X, Y) = (\tfrac{1}{2}(f^2 - 3f - 3 - g), \tfrac{1}{2}(f^3 - 5f^2 - 7f + (2 - f)g)).]$$

Next we compute the map $\phi: X_0(21) \to X_0(7)$, that is, write $H$ as a rational function of $f$ and $g$: the $\eta$-products give $H = g_1^2/f$, and

$$g_1 = \tfrac{1}{2}((g_1 + 7/g_1) + (g_1 - 7/g_1)) = \frac{1}{2f}(f^2 - 3f + 1 + g).$$

This function $H(f, g) = (f^2 - 3f + 1 + g)^2/(4f^3)$ indeed has a triple pole at $(f, g) = (0, 1)$ and a simple pole at $(f, g) = (\infty, +\infty^2)$, a triple zero at $(f, g) = (\infty, -\infty^2)$ and a simple zero at $(f, g) = (0, -1)$ (this was confirmed by expanding

$\pm(f^4 - 6f^3 - 17f^2 - 6f + 1)^{1/2}$ in power series about $f = 0, \infty$); also $H - H(P_\pm)$ has a triple zero at $(f, g) = ((-1 \mp \sqrt{-3})/2, -3 \pm \sqrt{-3})$ and a simple zero at $(f, g) = (1, \pm 3\sqrt{-3})$ – all in accordance with the ramification behavior of $\phi$. (It so happens that these 8 preimages of $0, \infty$, and $P_\pm$ all lie in the $\mathbf{Q}(\sqrt{-3})$-rational torsion subgroup $(\mathbf{Z}/8) \times (\mathbf{Z}/2)$ of the elliptic curve $X_0(21)$, but the significance here of this is not clear.)

Finally, we use the involution $u_1 : H \mapsto (H(P_+) \cdot H - 49)/(H - H(P_+))$ which commutes with $w_7$ and takes 0 to $P_-$ and $\infty$ to $P_+$. A lift of $u_1$ to an involution $u$ of $X_0(21)$ must interchange the triple zeros $(\infty, -\infty^2)$ and $((-1 + \sqrt{-3})/2, -3 - \sqrt{-3})$ of $H$ and $u_1 H$; and this specifies $u$ uniquely: the image under $u$ of any point $(f, g) = (x, y)$ is the unique point $u(x, y)$ such that $(x, y) + u(x, y) - (\infty, -\infty^2) - ((-1 + \sqrt{-3})/2, -3 - \sqrt{-3})$ is the divisor of a rational function on $X_0(21)$. Such a function must be either constant or proportional to $2(g - 3 - \sqrt{-3})/(2f + 1 - \sqrt{-3}) - f - A$ for some constant $A$; thus two points on $X_0(21)$ are interchanged by $u$ if and only if the degree-2 rational function $2(g - 3 - \sqrt{-3})/(2f + 1 - \sqrt{-3}) - f$ assumes the same (possibly infinite) value $A$ at these points. This is true for the triple zeros of $H$ and $u_1 H$ by construction; it is also true for the simple zeros $(0, -1)$, $(1, -3\sqrt{-3})$ with $A = -(1 + 5\sqrt{-3})/2$, for the simple poles $(\infty, +\infty^2)$, $(1, 3\sqrt{-3})$ with $A = (\sqrt{-3} - 7)/2$, and for the triple poles $(0, 1)$, $((-1 - \sqrt{-3})/2, -3 + \sqrt{-3})$ with $A = (1 - 3\sqrt{-3})/2$. It follows that the rational functions $H \circ u$ and $u_1 \circ H$ on $X_0(21)$ have the same zeros and poles and agree on one (indeed several) nonzero values, and therefore they are equal and so $u$ gives the desired lift of $u_1$.

Q.E.F.

**Acknowledgements**

The symbolic computations of the second construction were considerably facilitated by the computer program MACSYMA. I gratefully acknowledge the support of the Harvard Society of Fellows.

**References**

[1] Birch, B.J., Kuyk, W., ed: Modular Functions of One Variable IV, *Lect. Notes Math.* 476, 1975.
[2] Fricke, R.: Die elliptischen Functionen und ihre Anwendungen. Leipzig-Berlin: Teubner 1922.
[3] Kenku, M.A., Momose, F., Automorphism groups of the modular curves $X_0(N)$. Comp. Math. 65 (1988) 51–80.
[4] Mazur, B., Swinnerton-Dyer, P., Arithmetic of Weil Curves. *Inv. Math.* 25 (1974) 1 – 61.
[5] Matzat, B.H., Konstruktive Galoistheorie. *Lect. Notes Math.* 1284, 1987.