The Eightfold Way
MSRI Publications
Volume **35**, 1998

The Klein Quartic in Number Theory

NOAM D. ELKIES

Abstract. We describe the Klein quartic $\mathcal{X}$ and highlight some of its remarkable properties that are of particular interest in number theory. These include extremal properties in characteristics 2, 3, and 7, the primes dividing the order of the automorphism group of $\mathcal{X}$; an explicit identification of $\mathcal{X}$ with the modular curve $X(7)$; and applications to the class number 1 problem and the case $n = 7$ of Fermat.

Introduction

Overview. In this expository paper we describe some of the remarkable properties of the *Klein quartic* that are of particular interest in number theory. The Klein quartic $\mathcal{X}$ is the unique curve of genus 3 over $\mathbb{C}$ with an automorphism group G of size 168, the maximum for its genus. Since G is central to the story, we begin with a detailed description of G and its representation on the three-dimensional space V in whose projectivization $\mathbb{P}(V) = \mathbb{P}^2$ the Klein quartic lives. The first section is devoted to this representation and its invariants, starting over $\mathbb{C}$ and then considering arithmetical questions of fields of definition and integral structures. There we also encounter a G-lattice that later occurs as both the period lattice and a Mordell–Weil lattice for $\mathcal{X}$. In the second section we introduce $\mathcal{X}$ and investigate it as a Riemann surface with automorphisms by G. In the third section we consider the arithmetic of $\mathcal{X}$: rational points, relations with the Fermat curve and Fermat's "Last Theorem" for exponent 7, and some extremal properties of the reduction of $\mathcal{X}$ modulo the primes $2, 3, 7$ dividing $\#G$. In the fourth and last section, we identify $\mathcal{X}$ explicitly with the modular curve $X(7)$, describe some quotients of $\mathcal{X}$ as classical modular curves, and report on Kenku's use of one of these quotients in a novel proof of the Stark–Heegner theorem on imaginary quadratic number fields of class number 1. We close that section with Klein's identification of $\pi_1(\mathcal{X})$ with an arithmetic congruence subgroup of $\mathrm{PSL}_2(\mathbb{R})$, and thus of $\mathcal{X}$ with what we now recognize as a Shimura curve.

Notations. We reserve the much-abused word "trivial" for the identity element of a group, the 1-element subgroup consisting solely of that element, or a group representation mapping each element to the identity.

Matrices will act from the left on column vectors.

We fix the seventh root of unity

$$\zeta := e^{2\pi i/7}, \tag{0.1}$$

and set

$$\alpha := \zeta + \zeta^2 + \zeta^4 = \frac{-1+\sqrt{-7}}{2}. \tag{0.2}$$

The seventh cyclotomic field and its real and quadratic imaginary subfields will be called

$$K := \mathbb{Q}(\zeta), \quad K_+ := \mathbb{Q}(\zeta+\zeta^{-1}), \quad k := \mathbb{Q}\big(\sqrt{-7}\big) = \mathbb{Q}(\alpha). \tag{0.3}$$

These are all cyclic Galois extensions of $\mathbb{Q}$. The nontrivial elements of $\mathrm{Gal}(K/\mathbb{Q})$ fixing k are the Galois automorphisms of order 3 mapping ζ to ζ^2, ζ^4; the nontrivial Galois automorphism preserving K_+ is complex conjugation $x \leftrightarrow \bar{x}$. As usual we write O_F for the ring of integers of a number field F; recall that O_K, O_{K_+}, O_k are respectively the polynomial rings $\mathbb{Z}[\zeta]$, $\mathbb{Z}[\zeta+\zeta^{-1}]$, $\mathbb{Z}[\alpha]$.

We use G throughout for the second-smallest noncyclic simple group

$$\mathrm{PSL}_2(\mathbb{F}_7) \cong \mathrm{SL}_3(\mathbb{F}_2)\ [\, = \mathrm{GL}_3(\mathbb{F}_2)\,] \tag{0.4}$$

of 168 elements.

Acknowledgements. Many thanks to Silvio Levy for soliciting this paper for the present MSRI volume and for his patience during repeated delays in the paper's completion.

I am grateful to Allan Adler, Benedict Gross, Barry Mazur, and J.-P. Serre for introducing me to many of the remarkable properties of the Klein quartic and for numerous enlightening conversations on various aspects of the geometry and arithmetic of $\mathcal{X}$ and of its automorphism group G. I also thank them, as well as Michael Bennett, Enrico Bombieri, Armand Brumer, Joe Harris, and Curt McMullen, for references to their and others' work and/or for clarifications of specific concepts and questions that arose in the process of putting this exposition together.

Hardly any of the results contained in this paper are original with me; some go back to Klein's work over a century ago, such as the explicit formulas for the representation of G and the determinantal expressions for its invariants [Klein 1879b], and the equations Kenku [1985] uses, referring to [Klein 1879a, § 7]. Much of the mathematical work of writing this paper lay in finding explicit equations that not only work locally to exhibit particular aspects of $(\mathcal{X}, G)$ but are also consistent between different parts of the exposition. The extensive symbolic computations needed to do this were greatly facilitated by the computer packages PARI and MACSYMA.

This work was made possible in part by funding from the National Science Foundation and the Packard Foundation.

1. The Group G and its Representation (V, ρ)

1.1. ***G* and its characters.** We reproduce from the ATLAS [Conway et al. 1985, p. 3] some information about G and its representations over $\mathbb{C}$. (That ATLAS page is also the source of facts concerning G cited without proof in the sequel.) The conjugacy classes c and character table of G are as follows:

c	$1A$	$2A$	$3A$	$4A$	$7A$	$7B$
$\#c$	1	21	56	42	24	24
χ_1	1	1	1	1	1	1
χ_3	3	-1	0	1	α	$\bar{\alpha}$
$\overline{\chi}_3$	3	-1	0	1	$\bar{\alpha}$	α
χ_6	6	2	0	0	-1	-1
χ_7	7	-1	1	-1	0	0
χ_8	8	0	-1	0	1	1

(1.1)

The outer automorphism group $\mathrm{Aut}(G)/G$ of G has order 2; an outer automorphism switches the conjugacy classes 7A,7B and the characters $\chi_3, \overline{\chi}_3$, and (necessarily) preserves the other conjugacy classes and characters. Having specified α in (0.2), we can distinguish χ_3 from $\overline{\chi}_3$ by labeling one of the conjugacy classes of 7-cycles as 7A; we do this by regarding G as $\mathrm{PSL}_2(\mathbb{F}_7)$ and selecting for 7A the conjugacy class of $\pm\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$. When we regard G as $\mathrm{PSL}_2(\mathbb{F}_7)$, the group $\mathrm{Aut}(G)$ is $\mathrm{PGL}_2(\mathbb{F}_7)$; if we use the $\mathrm{SL}_3(\mathbb{F}_2)$ description of G, we obtain an outer involution of G by mapping each 3×3 matrix to its inverse transpose.

Modulo the action of $\mathrm{Aut}(G)$ there are only two maximal subgroups in G (every other noncyclic simple group has at least three), of orders 21 and 24. These are the point stabilizers in the doubly transitive permutation representations of G on 8 and 7 letters respectively. These come respectively from the action of $G \cong \mathrm{PSL}_2(\mathbb{F}_7)$ on the projective line mod 7 and of $G \cong \mathrm{SL}_3(\mathbb{F}_2)$ on the projective plane mod 2. The 21-element subgroup is the normalizer of a 7-Sylow subgroup of G, and is the semidirect product of that subgroup (which is of course cyclic of order 7) with a group of order 3. Since all the 7-Sylows are conjugate under G, so are the 21-element subgroups, which extend to 42-element maximal subgroups of $\mathrm{Aut}(G)$ isomorphic to the group of permutations $x \mapsto ax + b$ of $\mathbb{F}_7$. The 24-element subgroup is the normalizer of a noncyclic subgroup of order 4 in G, and is the semidirect product of that subgroup with its automorphism group, isomorphic with the symmetric group S_3; thus the 24-element maximal subgroup is isomorphic with S_4. There are 14 such subgroups, in two orbits of size 7 under conjugation by G that are switched by an outer automorphism; thus these groups do not extend to 48-element subgroups of $\mathrm{Aut}(G)$.[1]

From these groups we readily obtain the irreducible representations of G with characters χ_6, χ_7, χ_8: the first two are the nontrivial parts of the 7- and 8-letter permutation representations of G, and the last is induced from a nontrivial one-dimensional character of the 21-element subgroup.

We now turn to χ_3 and $\overline{\chi}_3$. Let (V, ρ) and (V^*, ρ^*) be the representation with character χ_3 and its contragredient representation with character $\overline{\chi}_3$. Both V and V^* remain irreducible as representations of the 21- and 24-element subgroups; we use this to exhibit generators for $\rho(G)$ explicitly.

Fix an element g in the conjugacy class 7A. Then V decomposes as a direct sum of one-dimensional eigenspaces for $\rho(g)$ with eigenvalues ζ, ζ^2, ζ^4. The normalizer of $\langle g \rangle$ in G is generated by g and a 3-cycle h such that $h^{-1}gh = g^2$. Thus h cyclically permutes the three eigenspaces. The images of any eigenvector under $1, h, h^2$ therefore constitute a basis for V; relative to this basis, the matrices for $\rho(g), \rho(h)$ are simply

$$\rho(g) = \begin{pmatrix} \zeta^4 & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta \end{pmatrix}, \qquad \rho(h) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}. \tag{1.2}$$

In other words, the representation (V, ρ) restricted to the 21-element subgroup $\langle g, h \rangle$ of G is induced from a one-dimensional character of $\langle g \rangle$ sending g to ζ. Since this subgroup is maximal in G, we need only exhibit the image under ρ of some group element not generated by g, h. In his historic paper introducing (V, ρ) and his eponymous quartic curve, Klein [1879b, § 5] found that the involution

$$-\frac{1}{\sqrt{-7}} \begin{pmatrix} \zeta - \zeta^6 & \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 \\ \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 & \zeta - \zeta^6 \\ \zeta^4 - \zeta^3 & \zeta - \zeta^6 & \zeta^2 - \zeta^5 \end{pmatrix} \tag{1.3}$$

fills this bill. We thus refer to the image of G in $\mathrm{SL}_3(\mathbb{C})$ generated by the matrices (1.2,1.3) as the *Klein model* of (V, ρ).

The transformation (1.3) may seem outlandish, especially compared with (1.2), but we can explain it as follows. Except for the scaling factor $-1/\sqrt{-7}$, it is just the discrete Fourier transform on the space of odd functions $\mathbb{F}_7 \to \mathbb{C}$: identify such a function f with the vector $(f(1), f(2), f(4)) \in V$. It follows that this involution (1.3), as well as the transformations $\rho(g), \rho(h)$, are contained in Weil's group of unitary operators of the space of complex-valued functions on $\mathbb{F}_7$ [Weil

[1]Let H, H' be two subgroups of G isomorphic to S_4 in different orbits. Then H, H' are not conjugate in G, but are *almost conjugate* (a.k.a. "Gassmann equivalent" [Perlis 1977]): H, H' intersect each G-conjugacy class in subsets of equal size. Equivalently, the permutation representations of the action of G on the coset sets G/H, G/H' are isomorphic (in our case with character $\chi_6 \oplus \chi_1$). This has been used by Perlis to construct non-isomorphic number fields of degree 7 (the minimum) with the same zeta function [Perlis 1977] and, following [Sunada 1985], to exhibit isospectral planar domains [Gordon et al. 1992; Buser et al. 1994].

1964, § I]; they all commute with the parity involution $\iota : f(x) \leftrightarrow f(-x)$, and together generate the restriction to V of the commutator of ι in Weil's group. Starting with any odd prime p instead of 7, this would produce the $((p-1)/2)$-dimensional representation of $\mathrm{PSL}_2(\mathbb{F}_p)$ or of its double cover according as p is congruent to 3 or 1 mod 4; see also [Adler 1981, p. 116] for a concrete approach to the first case, of which G is the instance $p = 7$. If we take $g = \pm\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, $h = \pm\left(\begin{smallmatrix}2&0\\0&4\end{smallmatrix}\right)$ in $\mathrm{PSL}_2(\mathbb{F}_7)$ then (1.3) is the image under ρ of the involution $s = \pm\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$.

The restriction of ρ to $S_4 \subset G$ is the group of orientation-preserving symmetries of the cube, that is, the group of signed 3×3 matrices of determinant 1. (The action on the four diagonals of the cube identifies this group with S_4; the 3-dimensional representation is the nontrivial part of the permutation representation of S_4 twisted by its sign character.) Unlike (V, ρ) and its restriction to the 21-element subgroup, this representation leaves a quadratic form invariant. We choose the subgroup isomorphic with S_4 generated by s, h, and $g^2sg^{-2} = \pm\left(\begin{smallmatrix}2&2\\1&-2\end{smallmatrix}\right)$. Then the invariant quadric (which we shall need later) is a multiple of

$$X^2 + Y^2 + Z^2 + \bar{\alpha}(XY + XZ + YZ); \tag{1.4}$$

under the change of basis with matrix

$$\begin{pmatrix} 1 & 1+\zeta\alpha & \zeta^2+\zeta^6 \\ 1+\zeta\alpha & \zeta^2+\zeta^6 & 1 \\ \zeta^2+\zeta^6 & 1 & 1+\zeta\alpha \end{pmatrix} \tag{1.5}$$

we find that s, h, g^2sg^{-2} map to the signed permutation matrices

$$-\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \tag{1.6}$$

while g maps to

$$\frac{1}{2}\begin{pmatrix} -1 & 1 & \bar{\alpha} \\ \alpha & \alpha & 0 \\ -1 & 1 & -\bar{\alpha} \end{pmatrix}. \tag{1.7}$$

The matrices (1.6) and (1.7) generate an image of G in $\mathrm{SL}_3(\mathbb{C})$, which we shall call the S_4 *model* of (V, ρ).

We can also recover from (V, ρ) and (V^*, ρ^*) the irreducible representations of G of dimensions 6,7,8: the first is the symmetric square $\mathrm{Sym}^2(V)$; the second is $\mathrm{Sym}^3(V) \ominus V^*$; and the last is $(V \otimes V^*) \ominus \mathbf{1}$.

1.2. G-invariant polynomials in V. The action of G on V^* extends to an action on the ring

$$\mathbb{C}[V^*] = \bigoplus_{m=0}^{\infty} \mathrm{Sym}^m(V^*) \tag{1.8}$$

of polynomials on V. Klein determined over a century ago [1879b, § 6] the subring $\mathbb{C}[V^*]^G$ of polynomials invariant under this action: it is generated by three algebraically independent homogeneous polynomials of degrees 4, 6, 14, and a fourth polynomial of degree 21 whose square is a polynomial in the first three. It follows that the subring of polynomials invariant under the 336-element group $\pm G = \{\pm 1\} \times G$ is a polynomial ring generated by invariants of degrees 4, 6, 14. It is known [Shephard and Todd 1954] that a finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ has a polynomial invariant ring if and only if it is a *complex reflection group*, that is, a group generated by its elements g such that $\mathbf{1}_n - g$ has rank 1. In our case the complex reflections in $\{\pm 1\} \times G$ are $-\rho(s)$ and its conjugates, of which there are 21 (the size of the conjugacy class $2A$). We next find explicit polynomials $\Phi_4, \Phi_6, \Phi_{14}, \Phi_{21}$ such that the invariant rings $\mathbb{C}[V^*]^{\pm G}$ and $\mathbb{C}[V^*]^G$ are generated by $\{\Phi_4, \Phi_6, \Phi_{14}\}$ and $\{\Phi_4, \Phi_6, \Phi_{14}, \Phi_{21}\}$ respectively, and determine Φ_{21}^2 as a polynomial in $\Phi_4, \Phi_6, \Phi_{14}$.

Letting $X, Y, Z \in V^*$ be the coordinate functions in the Klein model of (V, ρ), we can write the quartic invariant as

$$\Phi_4 := X^3Y + Y^3Z + Z^3X, \tag{1.9}$$

because even the action on $\mathrm{Sym}^4(V^*)$ of the 21-element subgroup of G generated by $(X, Y, Z) \mapsto (\zeta X, \zeta^4 Y, \zeta^2 Z)$ and cyclic permutations of X, Y, Z (see (1.2)) has only a one-dimensional invariant subspace, generated by Φ_4. The *Klein quartic* is the zero locus

$$\mathcal{X} := \{(X : Y : Z) \in \mathbb{P}(V) : \Phi_4(X, Y, Z) = 0\} \tag{1.10}$$

of Φ_4 in the projective plane $\mathbb{P}(V) = (V - \{\mathbf{0}\})/\mathbb{C}^*$. In the S_4 model the monomial matrices do not suffice to determine Φ_4 up to scaling, but starting from (1.9) we may use the change of basis (1.5) to find that Φ_4 is proportional to

$$X'^4 + Y'^4 + Z'^4 + 3\alpha(X'^2Y'^2 + X'^2Z'^2 + Y'^2Z'^2). \tag{1.11}$$

[We could also have determined the coefficient 3α by requiring invariance under the 7-cycle (1.7).] The formulas we exhibit[2] in the next three paragraphs for $\Phi_6, \Phi_{14}, \Phi_{21}$ in terms of Φ_4 can then be used to obtain those invariants as polynomials in the coordinates X', Y', Z' of the S_4 model, starting from (1.11).

Since Φ_4 is invariant under G, so is its Hessian determinant

$$H(\Phi_4) = \begin{vmatrix} \partial^2\Phi_4/\partial X^2 & \partial^2\Phi_4/\partial X\,\partial Y & \partial^2\Phi_4/\partial X\,\partial Z \\ \partial^2\Phi_4/\partial Y\,\partial X & \partial^2\Phi_4/\partial Y^2 & \partial^2\Phi_4/\partial Y\,\partial Z \\ \partial^2\Phi_4/\partial Z\partial X & \partial^2\Phi_4/\partial Z\,\partial Y & \partial^2\Phi_4/\partial Z^2 \end{vmatrix}, \tag{1.12}$$

[2]These determinantal formulas (1.13), (1.14), and (1.17) come straight from [Klein 1879b, §6]. Except for the coefficients 1/54, 1/9, 1/14, they can also be found in [Benson 1993, p. 101]; note that Benson's coordinates are related with ours by an odd permutation of the Klein coordinates X, Y, Z, and the 3×3 matrix for $\rho(s)$ in [Benson 1993] is missing the factor $1/\sqrt{-7}$ and has an incorrect $(3, 3)$ entry.

and we may take

$$\Phi_6 := -\frac{1}{54} H(\Phi_4) = XY^5 + YZ^5 + ZX^5 - 5X^2Y^2Z^2 \tag{1.13}$$

as the sextic invariant. These polynomials Φ_4, Φ_6 are f and $(-\nabla)$ in Klein's notation [1879b]. They are irreducible: each of Φ_4, Φ_6 can have at most 6 irreducible factors, permuted by G up to scaling, and since G has no proper subgroup of index ≤ 6 the factors must be themselves invariant; but the only invariant polynomials of degree < 4 are constant, so neither Φ_4 nor Φ_6 can admit a proper factorization.

The degree-14 invariant is not uniquely determined even up to scaling: one can also add any multiple of $\Phi_4^2\Phi_6$. But we will usually work mod Φ_4, so this additional ambiguity will disappear. A G-invariant polynomial of degree 14 not proportional to $\Phi_4^2\Phi_6$ can be obtained from either of the two conjugacy classes of subgroups $S_4 \subset G$: each of these contains seven subgroups, each of which has a unique invariant quadric (that is, an invariant line in $\operatorname{Sym}^2(V^*)$), and the product of these seven quadrics is a G-invariant polynomial of degree $7 \cdot 2 = 14$. We may choose for Φ_{14} any linear combination of this product and $\Phi_4^2\Phi_6$. Alternatively Φ_4 may be obtained as a differential determinant from Φ_4, Φ_6 by extending the Hessian determinant we used to obtain Φ_6 from Φ_4:

$$\Phi_{14} = \frac{1}{9} \begin{vmatrix} \partial^2\Phi_4/\partial X^2 & \partial^2\Phi_4/\partial X\,\partial Y & \partial^2\Phi_4/\partial X\,\partial Z & \partial\Phi_6/\partial X \\ \partial^2\Phi_4/\partial Y\,\partial X & \partial^2\Phi_4/\partial Y^2 & \partial^2\Phi_4/\partial Y\,\partial Z & \partial\Phi_6/\partial Y \\ \partial^2\Phi_4/\partial Z\,\partial X & \partial^2\Phi_4/\partial Z\,\partial Y & \partial^2\Phi_4/\partial Z^2 & \partial\Phi_6/\partial Z \\ \partial\Phi_6/\partial X & \partial\Phi_6/\partial Y & \partial\Phi_6/\partial Z & 0 \end{vmatrix}, \tag{1.14}$$

which in terms of the Klein coordinates for V is

$$\sum_{\text{cyc}} (X^{14} - 34X^{11}Y^2Z - 250X^9YZ^4 + 375X^8Y^4Z^2 + 18X^7Y^7 - 126X^6Y^3Z^5) \tag{1.15}$$

(in which $\sum_{\text{cyc}}$ means sum over the three cyclic permutations of X, Y, Z, so for instance $\Phi_4 = \sum_{\text{cyc}} X^3Y$). All the invariant polynomials of degree 14 are irreducible except for $\Phi_4^2\Phi_6$ and the products of the two orbits of S_4-invariant quadrics. Multiplying the images of the quadric (1.4) under powers of $\rho(g)$ yields

$$\Phi_{14} + (69 + 7\alpha)\Phi_4^2\Phi_6, \tag{1.16}$$

so the reducible combinations of $\Phi_4^2\Phi_6$ and Φ_{14} are $\Phi_4^2\Phi_6$ itself, (1.16), and its conjugate $\Phi_{14} + (62 - 7\alpha)\Phi_4^2\Phi_6$.

Finally the invariant Φ_{21} may be described as the product of 21 linear forms: from the character table, each of the 21 involutions in G fixes a one-dimensional subspace of V^*, and we obtain Φ_{21} by multiplying generators of these subspaces. Alternatively Φ_{21} may be described as a multiple of the Jacobian determinant of $(\Phi_4, \Phi_6, \Phi_{14})$ with respect to (X, Y, Z). We choose the multiple

$$\Phi_{21} = \frac{\partial(\Phi_4, \Phi_6, \Phi_{14})}{14\,\partial(X, Y, Z)} = \frac{1}{14}\begin{vmatrix} \partial\Phi_4/\partial X & \partial\Phi_4/\partial Y & \partial\Phi_4/\partial Z \\ \partial\Phi_6/\partial X & \partial\Phi_6/\partial Y & \partial\Phi_6/\partial Z \\ \partial\Phi_{14}/\partial X & \partial\Phi_{14}/\partial Y & \partial\Phi_{14}/\partial Z \end{vmatrix}; \qquad (1.17)$$

the factor $1/14$ makes this an integral polynomial $X^{21} + Y^{21} + Z^{21} + \cdots$ in the Klein coordinates. Then Φ_{21}^2 is invariant under $\pm G$, and is thus a polynomial in $\Phi_4, \Phi_6, \Phi_{14}$. By comparing coefficients we find

$$\begin{aligned}\Phi_{21}^2 = \Phi_{14}^3 - 1728\Phi_6^7 + 1008\Phi_4\Phi_6^4\Phi_{14} - 32\Phi_4^2\Phi_6\Phi_{14}^2 + 19712\Phi_4^3\Phi_6^5 \\ - 1152\Phi_4^4\Phi_6^2\Phi_{14} + 11264\Phi_4^6\Phi_6^3 - 256\Phi_4^7\Phi_{14} + 12288\Phi_4^9\Phi_6. \quad (1.18)\end{aligned}$$

Thus

$$\boxed{\Phi_{14}^3 - \Phi_{21}^2 \equiv 1728\Phi_6^7 \bmod \Phi_4.} \qquad (1.19)$$

The existence of a linear dependence mod Φ_4 between Φ_6^7, Φ_{14}^3, and Φ_{21}^2 could have been surmised from the degrees of these invariants; we shall see that it is closely related to the description of $\mathcal{X}$ as a G-cover of $\mathbb{CP}^1$ branched at only three points, with ramification indices $2, 3, 7$. (It is also the reason that this curve figures in the analysis of the Diophantine equation $Ax^2 + By^3 = Cz^7$ in [Darmon and Granville 1995].) The occurrence of the coefficient $1728 = 12^3$ in (1.19), reminiscent of the identity $E_2^3 - E_3^2 = 1728\Delta$ for modular forms on $\mathrm{PSL}_2(\mathbb{Z})$, suggests that $\mathcal{X}$ may be closely related with elliptic and modular curves; we shall see that this is in fact the case in the final section.

1.3. Arithmetic of (V, ρ): fields of definition. So far we have worked over $\mathbb{C}$. In fact all the representations of G except those of dimension 3 can be realized by homomorphisms of G to $\mathrm{GL}_d(\mathbb{Q})$; we say that these representations are *defined over* $\mathbb{Q}$. This is obvious for the trivial representation, and clear for the 6- and 7-dimensional ones from their relation with the 7- and 8-letter permutation representations of G. By comparing characters we see that the direct sum of the 7- and 8-dimensional representations is isomorphic with the exterior square of the 6-dimensional one, whence the 8-dimensional representation is also defined over $\mathbb{Q}$. We cannot hope for the 3-dimensional representations to be defined over $\mathbb{Q}$, because χ_3 takes irrational values $\alpha, \bar{\alpha}$ on the 7-cycles in G. We next investigate how close we can come to overcoming this difficulty.

The S_4 model shows that (V, ρ) can be defined over the quadratic extension k of $\mathbb{Q}$ generated by the values of χ_3. On the other hand, the Klein model of (V, ρ) uses matrices over the larger field K, but is defined over $\mathbb{Q}$ in the weaker sense that $\rho(G) \subset \mathrm{SL}_3(K)$ is stable under $\mathrm{Gal}(K/\mathbb{Q})$. Indeed the Galois conjugates of $\rho(g)$ are its powers, $\rho(h) \in \mathrm{SL}_3(\mathbb{Q})$ is fixed by $\mathrm{Gal}(K/\mathbb{Q})$, and the involution (1.3) is contained in $\mathrm{SL}_3(K_+)$ and taken by $\mathrm{Gal}(K_+/\mathbb{Q})$ to its conjugates by powers of h, so the group $\rho(G)$ generated by these three linear transformations is permuted by $\mathrm{Gal}(K/\mathbb{Q})$. The S_4 model cannot be defined over $\mathbb{Q}$ even in this weaker sense: if it were, complex conjugation would induce a nontrivial automorphism of G fixing $S_4 \subset G$ pointwise, but no such automorphism exists. This is why the invariants $\Phi_4, \Phi_6, \Phi_{14}, \Phi_{21}$ are polynomials over $\mathbb{Q}$ in the Klein model but not in the S_4 model. This still leaves open the possibility of finding a model in which $\rho(G)$ is both contained in $\mathrm{SL}_3(k)$ and stable under $\mathrm{Gal}(k/\mathbb{Q})$ by applying a suitable $\mathrm{GL}_3(K)$ or $\mathrm{GL}_3(k)$ change of basis to the Klein or S_4 model.

Indeed it turns out that such a model, giving in effect a faithful representation of $\mathrm{Aut}(G)$ into $\Gamma\mathrm{L}_3(k)$,[3] does exist, and is in fact unique up to isomorphism. This is because constructing such a model amounts to choosing an outer involution of G to map to the Galois involution of $k/\mathbb{Q}$, and there is just one conjugacy class of involutions in $\mathrm{Aut}(G) - G$. Under the identification of $\mathrm{Aut}(G)$ with $\mathrm{PGL}_2(\mathbb{F}_7)$, one such involution is $r = \pm\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$. The subgroup of G fixed by this involution is the copy of S_3 generated by h, s; thus only this subgroup will map to matrices in $\mathrm{GL}_3(\mathbb{Q})$. Allan Adler points out (in e-mail) a beautiful way to see the image of the 42-element subgroup $\langle g, h, r\rangle$ of $\mathrm{Aut}(G)$: regard K as a three-dimensional vector space over k; let g be multiplication by ζ; let h be generator of $\mathrm{Gal}(K/k)$ taking ζ to ζ^2; and let r be complex conjugation, acting k-antilinearly as it should. Since, as noted already, $\langle g, h\rangle$ acts irreducibly on V, this suffices to determine the representation. We choose the basis $(\zeta - \zeta^6, \zeta^2 - \zeta^5, \zeta^4 - \zeta^3)$ for K/k — note that this basis is orthogonal under the G-invariant Hermitian norm $\|\beta\| = \mathrm{Tr}_{K/k}(\beta\bar{\beta})$ on K. We find that this basis is related with the basis for the S_4 model by the change of basis with matrix

$$\begin{pmatrix} -\alpha & 1 & 2\alpha+3 \\ 2\alpha+3 & -\alpha & 1 \\ 1 & 2\alpha+3 & -\alpha \end{pmatrix}, \tag{1.20}$$

and that in this basis the matrices for $\rho(g), \rho(h), \rho(s)$ are

$$\frac{1}{\sqrt{-7}}\begin{pmatrix} -2 & \alpha & -1 \\ \alpha & -1 & 1-\alpha \\ -1 & 1-\alpha & -1-\alpha \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \frac{1}{7}\begin{pmatrix} -3 & -6 & 2 \\ -6 & 2 & -3 \\ 2 & -3 & -6 \end{pmatrix}. \tag{1.21}$$

We call this the *rational S_3 model* of (V, ρ). Since it is weakly defined over $\mathbb{Q}$, its polynomial invariants have rational coefficients. For most purposes it is still more convenient to use the simpler invariants of the Klein model; for instance the quartic invariant Φ_4, which is the pretty trinomial (1.9) in the Klein model, becomes a multiple of

$$A^4+B^4+C^4+6(AB^3+BC^3+CA^3)-3(A^2B^2+B^2C^2+C^2A^2)+3ABC(A+B+C) \tag{1.22}$$

in our basis, and looks even worse with other coordinate choices. But it does have the advantage not only of minimal fields of definition but also of identifying

[3] By this is meant the semidirect product of $\mathrm{GL}_3(k)$ with $\mathrm{Gal}(k/\mathbb{Q})$, in analogy with the semilinear groups $\Gamma\mathrm{L}_n(\mathbb{F}_q)$ over finite fields properly containing $\mathbb{F}_p$.

G with linear groups over both $\mathbb{F}_2$ and $\mathbb{F}_7$ by reducing (V, ρ) modulo primes of O_K with those residue fields.

1.4. Arithmetic of (V, ρ): reduction mod p and the lattice L. Remarkably the representation (V, ρ) remains irreducible at every prime, and its reductions mod 2 and 7 reveal the identification of G with $\mathrm{SL}_3(\mathbb{F}_2)$ and $\mathrm{PSL}_2(\mathbb{F}_7)$ respectively. Before showing this we put it in context by briefly recalling what it means to reduce a representation mod p.

For this paragraph only, let G be any finite group, and (V, ρ) an irreducible representation of G defined over a number field F. Let $L \subset V$ be an O_F-lattice stable under G. (Such a lattice always exists; for instance we may choose any nonzero $v \in V$ and take for L the O_F-linear combinations $\sum_{g\in G} a_g \rho(g)(v)$.) For each prime ideal p of O_F, we then obtain a representation of G on the (O_F/p)-vector space L/pL. If this representation is irreducible then it does not depend on the choice of L, and we may unambiguously say that (V, ρ) is irreducible mod p and call L/pL its reduction mod p. This is the case for all but finitely many p, including all primes whose residual characteristic does not divide the order of G. But it may, and usually does, happen that there are some primes p, necessarily with $\#G \equiv 0 \bmod p$, such that L/pL is reducible, in which case that representation may depend on the G-stable lattice L (though the composition factors of L/pL depend only on (V, ρ) and p). For instance, if $F = \mathbb{Q}$ and G is the symmetric group S_n $(n > 3)$, and we take for (V, ρ) its usual $(n-1)$-dimensional representation, then it is reducible mod p if and only if p divides n. When p divides n, the representation L/pL depends on the choice of L. If we choose for L the root lattice

$$A_{n-1} = \Big\{(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n : \sum\nolimits_1^n a_i = 0\Big\},$$

the representation L/pL contains the 1-dimensional trivial representation generated by $(1, 1, \ldots, 1)$; if we choose instead the dual lattice A_{n-1}^* then L/pL has a G-invariant functional but no invariant proper subspace of positive dimension.

We return now to the case that G is the simple group of 168 elements and V is its 3-dimensional representation with character χ_3. We may choose either $F = K$ or $F = k$. In either case we may see without any computation that V is reducible mod p for each prime p of F. Indeed if V was reducible then G would have a nontrivial representation mod p of dimension 1 or 2; since G is simple and non-abelian, it would thus be a subgroup of $\mathrm{GL}_2(O_F/p)$. But the only non-abelian simple groups with an irreducible 2-dimensional representation over some field are the groups $\mathrm{SL}_2(\mathbb{F}_{2^r})$ for $r > 1$ (this follows from the classification of finite subgroups of SL_2 over an arbitrary field, see for instance [Suzuki 1982, Theorem 6.17]). But G is not such a group — it does not even have order $2^{3r} - 2^r$. This completes the proof that V is irreducible at each prime of F.

Thus (V, ρ) is one of the few known representations of finite groups in dimension greater than 1 that are "absolutely irreducible" in the sense of [Gross

1990], that is, are irreducible and remain so in every characteristic.[4] Since k has unique factorization, the main result (Prop. 5.4) of [Gross 1990] then shows that the lattice L is unique up to scaling. In the coordinates of the rational S_3 model L is proportional to the self-dual lattice

$$\left\{\frac{1}{\sqrt{-7}}(x,y,z) : x,y,z \in O_k;\ y-2x, z-4x \in \sqrt{-7}\,O_K;\ x+2y+4z \in 7O_K\right\}. \tag{1.23}$$

In the coordinates of the S_4 model we may take L to be the O_k-lattice generated by the column vectors

$$(2,0,0), \quad (\alpha,\alpha,0) \quad (\bar{\alpha},1,1). \tag{1.24}$$

The group G can in turn be defined as the group of determinant-1 automorphisms of this lattice [Conway et al. 1985]. Likewise the only G-invariant lattices in V^* are of the form cL^* for nonzero c, where L^* is generated by

$$(2,0,0), \quad (\bar{\alpha},\bar{\alpha},0) \quad (\alpha,1,1); \tag{1.25}$$

this L^* may be identified with the dual lattice of L. (Of course L, L^* are isomorphic *qua* lattices because the representations V, V^* are identified by an automorphism of G.) We note two facts for future reference. First, that in our case it is enough to assume that L or L^* is a $\mathbb{Z}$-lattice stable under the action of G: we obtain the action of O_k automatically because $\rho(g)+\rho(g^2)+\rho(g^4)$ is multiplication by α on V and by $\bar{\alpha}$ on V^*. Second, that L is known to be the unique indecomposable positive-definite unimodular Hermitian O_k-lattice of rank 3 [Hoffmann 1991, Theorem 6.1].

We next consider the reductions of (V,ρ) in characteristics 2, 7. We deal with characteristic 2 first. There are two primes $\wp_2, \bar{\wp}_2$ above 2 in O_k, interchanged by complex conjugation. We may take $\wp_2 = (\alpha)$, $\bar{\wp}_2 = (\bar{\alpha})$. Thus the reductions of the rational S_3 model for (V,ρ) modulo those primes are related by an outer automorphism of G. Using either prime, we obtain a nontrivial representation $G \to \mathrm{GL}_3(\mathbb{F}_2)$. Since G is simple, this map must be an isomorphism. That is, each invertible linear transformation of V mod $\wp_2$ or $\bar{\wp}_2$ comes from a unique element of G; equivalently, each automorphism of $L/\wp_2 L$ or $L/\bar{\wp}_2 L$ lifts to a unique determinant-1 isometry of L! Now Dickson proved that for each prime power q and every positive integer n the ring of invariants for the action of $\mathrm{GL}_n(\mathbb{F}_q)$ on its defining representation is polynomial, with generators of degrees $q^n - q^m$ for $m = 0, 1, \ldots, n-1$. (See the original paper [Dickson 1934], and [Bourbaki 1968, Chapter V, § 5, Ex. 6 on pp. 137–8] for a beautiful proof; the

[4]The best known examples of absolutely irreducible representations are the defining representations of the Weyl group of E_8 and the isometry group of the Leech lattice. Both of those representations are defined over $\mathbb{Q}$; thus the uniqueness up to scaling of the stable lattices for those groups is already contained in the work of Thompson [1976], who gave those examples as well as the 248-dimensional representation of his sporadic simple group. Gross's paper [Gross 1990] extends Thompson's work to several classes of representations not defined over $\mathbb{Q}$, and gives many examples.

Dickson invariants and the invariants of subgroups of $\mathrm{GL}_n(\mathbb{F}_q)$ are treated in greater detail in the last chapter of [Benson 1993].) In our case, $(q,n) = (2,3)$, so the degrees are $4,6,7$. Indeed (1.18) reduces mod 2 to[5] $\Phi_{21}^2 = \Phi_{14}^3$, so that mod 2 there is a new invariant Φ_7 such that $\Phi_7^2 = \Phi_{14}$, $\Phi_7^3 = \Phi_{21}$; the Dickson invariants for $\mathrm{GL}_3(\mathbb{F}_2)$ are this Φ_7 together with Φ_4, Φ_6 — note that indeed the degrees $4,6,7$ are 2^3-2^2, 2^3-2^1, 2^3-2^0.

There is a unique prime $\wp_7 = (\sqrt{-7}\,)$ of O_k above 7. The action of G on the 3-dimensional $\mathbb{F}_7$-vector space $L/\wp_7 L$ is then the unique reduction of (V,ρ) in characteristic 7. Since $\beta \equiv \bar\beta \bmod \wp_7$ for all $\beta \in O_k$, the G-invariant Hermitian form on L reduces to a non-degenerate quadratic form on $L/\wp_7 L$, which G must respect. Thus the image of our representation $G \to \mathrm{GL}_3(\mathbb{F}_7)$ is contained in the orthogonal group $\mathrm{SO}_3(\mathbb{F}_7)$ (not merely $\mathrm{O}_3(\mathbb{F}_7)$ because $\rho(G) \subset \mathrm{SL}(V)$ already in characteristic zero). But we already know a 3-dimensional representation of $G \cong \mathrm{PSL}_2(\mathbb{F}_7)$ in characteristic 7, namely the symmetric square $\mathrm{Sym}^2(V_2)$ of its defining representation. [Note that the matrix -1 in the center of $\mathrm{SL}_2(\mathbb{F}_7)$ acts on $\mathrm{Sym}^2(V_2)$ by multiplication by $(-1)^2 = +1$, which is to say trivially, so we actually do obtain a 3-dimensional representation of the quotient group $\mathrm{PSL}_2(\mathbb{F}_7)$.] Moreover, this representation has an invariant quadratic form, namely the discriminant of a binary quadric, and G acts on $\mathrm{Sym}^2(V_2)$ by linear transformations of determinant 1. Thus we obtain a map $\mathrm{PSL}_2(\mathbb{F}_7) \to \mathrm{SO}_3(\mathbb{F}_7)$. The image is not quite all of $\mathrm{SO}_3(\mathbb{F}_7)$; indeed

$$\mathrm{SO}_3(\mathbb{F}_7) \cong \mathrm{Aut}(G). \tag{1.26}$$

Both groups have order $336 = 2 \cdot 168$, so to obtain the isomorphism (1.26) we need only extend the action of G on $\mathrm{Sym}^2(V_2)$ to $\mathrm{Aut}(G) \cong \mathrm{PGL}_2(\mathbb{F}_7)$. To do this, begin by choosing for each element of $\mathrm{Aut}(G) - G$ a representative $\gamma \in \mathrm{GL}_2(\mathbb{F}_7)$ of determinant -1; such a γ exists since -1 is not a square in $\mathbb{F}_7$, and is well-defined up to $\gamma \leftrightarrow -\gamma$. Then γ induces a linear transformation $\mathrm{Sym}^2 \gamma$ $[\ = \mathrm{Sym}^2(-\gamma)\,]$ of determinant -1 on $\mathrm{Sym}^2(V_2)$ that preserves the quadratic form. We thus obtain a well-defined $-\mathrm{Sym}^2 \gamma \in \mathrm{SO}_3(\mathbb{F}_7)$ not contained in the image of G. These elements, together with $\mathrm{Sym}^2 \gamma$ for $\gamma \in G$, fill out all of $\mathrm{SO}_3(\mathbb{F}_7)$. (Geometrically, the actions of PGL_2 and SO_3 induce automorphisms of $\mathbb{P}^1$ and of a conic in $\mathbb{P}^2$ respectively, and the isomorphism (1.26) reflects the identification of the conic with $\mathbb{P}^1$ [Fulton and Harris 1991, p. 273].) We've seen that the G part of $\mathrm{SO}_3(\mathbb{F}_7)$ is obtained from the action of G on $L/\wp_7 L$. But $\mathrm{Aut}(G)$ acts on L too, and since $\wp_7$ is Galois-invariant, the conjugate-linear automorphisms of L also act on $L/\wp_7 L$.

We thus see that, as in the mod-2 case, each automorphism of $L/\wp_7 L$ preserving the quadratic form lifts uniquely to an automorphism (possibly conjugate-

[5] It might be objected that we should not be using (1.18) because that equation relates the invariants of the Klein model. But that model still reduces well in characteristic 2; its only flaw there is that the field of definition is too large: $\mathbb{F}_8$ instead of $\mathbb{F}_2$. But this does not affect the structure of the $\overline{\mathbb{F}}_2$-ring of invariants.

linear and/or of determinant -1) of L. Moreover, L "explains" the sporadic isomorphism between $\mathrm{SL}_3(\mathbb{F}_2)$ and $\mathrm{PSL}_2(\mathbb{F}_7)$: these two linear groups are just the mod-2 and mod-7 manifestations of the isometries of L.[6]

The invariant quadratic form on $L/\wp_7 L$ can also be seen by reducing the ring of G-invariants mod $\wp_7$. As in the characteristic-2 case, there is a new invariant Φ_2, and here each of Φ_4, Φ_6, Φ_{14} is proportional to the appropriate power Φ_2^2, Φ_2^3, Φ_2^7 of this invariant quadric! Note that our formulas (1.11,1.22) for the quartic invariant in the S_4 and rational S_3 models both reduce mod $\wp_7$ to perfect squares, namely $(X^2+Y^2+Z^2)^2$ and $\bigl(X^2+Y^2+Z^2+3(XY+YZ+ZX)\bigr)^2$. Curiously, though, it is the S_4 form that is pertinent for $\Phi_4 = \Phi_2^2$; that Φ_4 is also a square mod 7 in the rational S_3 model is not directly relevant. This is because the matrices (1.6,1.7) for $\rho(G)$ in the S_4 model are $\wp_7$-integral, while the matrices (1.21) in the rational S_3 model have denominators $\sqrt{-7}$ and even 7, and thus do not reduce well mod $\wp_7$. [For each odd prime power q, the full ring of invariants of the three-dimensional representations of $\mathrm{O}_3(\mathbb{F}_q)$, $\mathrm{PSL}_2(\mathbb{F}_q)$, and the three intermediate groups have been determined by Kemper [1996, Theorem 2.4(c)]. Of these five groups, only two have polynomial invariants, including $\mathrm{O}_3(\mathbb{F}_q)$ but not $\mathrm{PSL}_2(\mathbb{F}_q)$ of $\{\pm 1\} \times \mathrm{PSL}_2(\mathbb{F}_q)$. In our case of $q = 7$, the invariants of $\mathrm{O}_3(\mathbb{F}_7)$ are generated by Φ_2, Φ_{21}^2, and a new invariant Φ_8 given by $X^8+Y^8+Z^8$ in the coordinates of the reduced S_4 model; G and $\pm G$ do not have polynomial invariant rings, though another index-2 subgroup of $\mathrm{O}_3(\mathbb{F}_7)$ has invariant ring $\mathbb{F}_7[\Phi_2, \Phi_8, \Phi_{21}]$. See [Kemper 1996] for further details.]

2. The Klein Quartic $\mathcal{X}$ as a Riemann Surface

2.1. The action of G on $\mathcal{X}$. The action of G on V induces an action on the projective plane $(V - \{\mathbf{0}\})/\mathbb{C}^* \cong \mathbb{CP}^2$, and on the Klein quartic $\mathcal{X} \subset \mathbb{CP}^2$, which is the zero-locus of the invariant quartic polynomial Φ_4. We use this to describe the geometry of $\mathcal{X}$.

We have seen already that Φ_4 is an irreducible polynomial. Thus its zero locus $\mathcal{X}$ is an irreducible curve. An irreducible plane quartic curve can have at most $\binom{4-1}{2} = 3$ singularities. Any singular points of $\mathcal{X}$ would be permuted by G; since the largest proper subgroups of G have index 7, each singular point would have to be fixed by G. But G fixes no point on $\mathbb{CP}^2$ because the representation (V, ρ) is irreducible. Thus $\mathcal{X}$ has no singularities, so is a curve of genus 3 canonically embedded in $\mathbb{CP}^2$.

Since each element of G other than the identity can have only finitely many fixed points on $\mathcal{X}$, there are only a finite number of orbits of G of size less than $\#G = 168$. We next describe these orbits and their point stabilizers:

[6]Several of the other sporadic isomorphisms between linear groups in different characteristics are likewise explained by highly symmetrical lattices in small dimension. For instance the Weyl group of E_6 occurs as both an orthogonal group acting on $\mathbb{F}_3^5$ and a symplectic group acting on $\mathbb{F}_2^6$, these vector spaces arising as $E_6/3E_6^*$ and $E_6/2E_6$. See [Kneser 1967].

Proposition. (i) *Each of the eight* 7*-Sylow subgroups* $H_7 \subset G$ *has three fixed points in* $\mathbb{CP}^2$ *and is the stabilizer in* G *of each of these three points, all of which are on* $\mathcal{X}$. *The* $8 \cdot 3 = 24$ *points thus obtained are all distinct and constitute a single orbit of* G. *They are Weierstrass points of* $\mathcal{X}$ *of weight* 1, *and* $\mathcal{X}$ *has no other Weierstrass points.*

(ii) *Each of the twenty-eight* 3*-Sylow subgroups* $H_3 \subset G$ *has three fixed points in* $\mathbb{CP}^2$. *The normalizer* $N(H_3)$ *of* H_3 *in* G, *isomorphic with the symmetric group* S_3, *is the stabilizer in* G *of one of these points*; *this point is not on* $\mathcal{X}$. *The remaining fixed points of* H_3 *are on* $\mathcal{X}$ *and each has stabilizer* H_3. *The line joining these two points is the unique line of* $\mathbb{CP}^2$ *stable under* $N(H_3)$, *and is tangent to* $\mathcal{X}$ *at both points. The* $28 \cdot 2 = 56$ *points thus obtained are all distinct and constitute a single orbit of* G. *The lines joining pairs of these points with the same stabilizer are the* 28 *bitangents of* $\mathcal{X}$.

(iii) *Each of the twenty-one* 2*-element subgroups* $H_2 \subset G$ *fixes a point and a line in* $\mathbb{CP}^2$. *The normalizer* $N(H_2)$ *of* H_2 *in* G, *isomorphic with the* 8*-element dihedral group*, *is the stabilizer in* G *of the fixed point*, *which is not on* $\mathcal{X}$. *The fixed line meets* $\mathcal{X}$ *in four distinct points*, *each of which has stabilizer* H_2 *in* G; *these four points are permuted transitively by* $N(H_2)$. *The* $21 \cdot 4 = 84$ *points thus obtained are all distinct and constitute a single orbit of* G.

(iv) *Every* G*-orbit in* $\mathcal{X}$, *other than the orbits of size* 24, 56, 84 *described in* (i), (ii), (iii) *above*, *has size* 168 *and trivial stabilizer*.

Proof. Since there are no points of $\mathbb{CP}^2$ fixed by all of G, the stabilizer of every point $P \in \mathbb{CP}^2$ must be contained in a maximal subgroup. For both kinds of maximal subgroup we have representations by monomial matrices relative to a suitable choice of coordinates, which let us readily describe the point stabilizers.

If the stabilizer $S(P)$ has even order it must be contained in one of the 24-element subgroups. In the coordinates of the S_4 model, we find that such a point P must be one of:

- a unit vector, with $S(P)$ an 8-element dihedral group;
- a vector $(1 : \pm 1 : \pm 1)$, with $S(P) \cong S_3$;
- a permutation of $(1 : \pm 1 : 0)$, with $S(P)$ a noncyclic group of order 4 (these last three cases coming from an opposite pair of faces, edges, or sides of the cube respectively);
- a permutation of $(1 : i : 0)$, with $S(P)$ a cyclic group of order 4, or
- a permutation of $(1 : x : \pm x)$ for some $x \notin \{0, \pm 1\}$, with $S(P)$ a two-element group.[7]

Moreover, the only nontrivial groups of odd order in S_4 are its 3-Sylows, which are conjugate to the group of cyclic permutations of the coordinates; this group

[7]There are several $x \notin \{0, \pm 1\}$ for which the stabilizer of this point in G is larger, but then that stabilizer is contained in a different maximal $S_4 \subset G$, and the point's coordinates in *that* subgroup's S_4 model appear earlier in this list.

fixes $(1:1:1)$, which we already saw has stabilizer S_3, and the two points $(1 : e^{\pm 2\pi i/3} : e^{\mp 2\pi i/3})$. The stabilizer of each of these last points must be the 3-Sylow: it cannot be a larger subgroup of S_4, because we have already accounted for all of these; and the only other possibility would be a 21-element subgroup, which has no fixed points at all because it acts irreducibly on $\mathbb{CP}^2$. Turning to subgroups of the 21-element subgroup, we use the coordinates of the Klein model: the 7-element normal subgroup $\langle g \rangle$ fixes only the three unit vectors, and all 3-element subgroups are conjugate to $\langle h \rangle$ which fixes only $(1:1:1)$ and the two points

$$(1 : e^{\pm 2\pi i/3} : e^{\mp 2\pi i/3}).$$

Clearly the first of these is also fixed by the involution (1.3). From our analysis of the S_4 model it follows that its stabilizer is the S_3 generated by h and that involution, while the other two fixed points of h have stabilizer $\langle h \rangle$.

Moreover, using the explicit formula for Φ_4 in the S_4 and Klein models we see that the stabilizers of any points of $\mathcal{X}$ must be cyclic of order 1,2,3, or 7. Thus part (iv) of the Proposition will follow from the first three parts.

Now a Weierstrass point of any Riemann surface of genus $w > 1$ is a point at which some holomorphic differential vanishes to order at least w. (See [Arbarello et al. 1985, 41–43] for the facts we'll need on Weierstrass points.) For a smooth plane quartic, the holomorphic differentials are linear combinations of the coordinates, so since $w = 3$ the Weierstrass points are those at which some line meets the curve at least triply, which is to say the inflection points of the curve. In our case the tangent to

$$\mathcal{X} : X^3Y + Y^3Z + Z^3X = 0$$

at $(1:0:0)$ is the line $Y = 0$, which indeed meets $\mathcal{X}$ triply at that point. Thus $(1:0:0)$ is a Weierstrass point, and by G-symmetry so are all 24 points in its orbit. But each Weierstrass point of a Riemann surface has a positive integral weight, and the sum of these weights is $w^3 - w$. Since this is 24 in our case, each point has weight 1 and there are no other Weierstrass points, as claimed. (Knowing the $w^3 - w$ formula we could have also concluded this directly from the existence of a unique orbit of size as small as 24, even without computing that it consists of inflection points.) We have thus proved Part (i) of the proposition.

(ii) First we check that $N(H_3)$ is indeed S_3. Since all 3-Sylows are conjugate in G, it is enough to do this when H_3 is contained in a maximal S_4. But the normalizer of every 3-element subgroup of S_4 is an S_3, so its normalizer in G is a subgroup of even order that is thus contained in a (perhaps different) maximal S_4, so is indeed S_3 as claimed.

To get at the fixed points of H_3 and its normalizer we again use the Klein model. We find that the fixed point $(1:1:1)$ of h is not on $\mathcal{X}$, while the other two fixed points are. Moreover the line connecting those two points is $X+Y+Z = 0$; solving for Z and substituting into Φ_4 we obtain $-(X^2 + XY + Y^2)^2$, so this line is indeed a bitangent of $\mathcal{X}$. That any smooth plane quartic curve has 28 bitangents is well known; see for instance [Hartshorne 1977, p. 305, Ex. 2.3h]. The remaining claims of (ii) either follow, as in (i), from the conjugacy in G of all 3-Sylow subgroups, or were already established during the above analysis of the stabilizers of points in $\mathbb{CP}^2$.

(iii) Again we first check that $N(H_2)$ is as claimed, using the fact that the involutions in G constitute a single conjugacy class. The normalizer of a double transposition in $S_4 \subset G$ is an 8-element dihedral group. Thus its normalizer in G is either that group, a maximal S_4, or all of G, but the last two are not possible because these groups have trivial centers. So $N(H_2)$ is indeed an 8-element dihedral group.

The noncyclic 4-group $N(H_2)/H_2$ acts on the fixed line of H_2 and on its intersection with $\mathcal{X}$. Since no point of $\mathcal{X}$ may have stabilizer properly containing H_2, the number of points of $\mathcal{X}$ on the fixed line must be a multiple of 4. But the intersection of a line with a smooth quartic curve consists of at least 1 and at most 4 points. Thus there are four fixed points of H_2 on $\mathcal{X}$, transitively permuted by $N(H_2)$. The remaining claims of (iii) follow as before. □

Corollary [Klein 1879b, § 6]. *The* 24-, 56- *and* 84-*point orbits are the zero loci of* Φ_6, Φ_{14}, *and* Φ_{21} *on* $\mathcal{X}$, *each with multiplicity* 1.

Proof. Since none of Φ_6, Φ_{14}, and Φ_{21} is a multiple of Φ_4, these polynomials do not vanish identically on $\mathcal{X}$, so their zero loci contain respectively 24, 56, and 84 points with multiplicity. Since the polynomials are G-invariant, their zero loci must be positive linear combinations of G-orbits. But by the Proposition there are only three orbits of size < 168. Moreover none of the integers 24, 56, 84 can be written as a nonnegative integer combination of the others: this is clear for 24, which is the smallest of the three; and almost as clear for 56, which is not a multiple of 24, and for 84, which is congruent to neither 0 nor 56 mod 24. Thus the vanishing loci can only be as claimed in the Corollary. □

(The Φ_6 case could also have been obtained from (1.13), since the inflection points of any smooth plane curve $P(X, Y, Z) = 0$ are the zeros of the Hessian $H(P)$ [Coolidge 1931, p. 95, Theorem 18]. The case of Φ_{21} could also be deduced from our description of Φ_{21} as the product of linear forms fixed by the 21 involutions in G. Klein also identifies the zeros of Φ_{21} on $\mathcal{X}$ with the curve's 84 "sextactic points", that is, the points at which the osculating conic meets $\mathcal{X}$ with multiplicity 6 rather than the generic 5.)

Hirzebruch [1983, pp. 120, 140] draws attention to the configuration in $\mathbb{CP}^2$ of the 21 lines fixed by involutions in G. Three of these meet at each of the 28 points fixed by subgroups $S_3 \subset G$, and four lines meet at each of the 21 points fixed by 2-Sylows in G. These are all the points of $\mathbb{CP}^2$ that lie on more than one of the 21 lines. In the notation of [Hirzebruch 1983], we thus have a configuration of $k = 21$ lines with $t_3 = 28$, $t_4 = 21$, and $t_n = 0$ for $n \neq 3, 4$. Thus this is one of the few nondegenerate line configuration known to achieve equality in the inequality

$$t_2 + \tfrac{3}{4}t_3 \geq k + \sum_{n>4}(n-4)t_n$$

of [Hirzebruch 1983, p. 140].

We can also use this Proposition to obtain, via the Riemann–Hurwitz formula, the genus of the quotient of $\mathcal{X}$ by each subgroup $H \subset G$: the quotient by the trivial group is of course $\mathcal{X}$ itself, with genus 3; the quotient by a cyclic subgroup of order 2, 3, or 4 is a curve of genus 1; and the quotient by any other subgroup has genus zero. Another way to obtain these is to identify the space $H_1(\mathcal{X}/H)$ of holomorphic differentials on $\mathcal{X}/H$ with the subspace $(H_1(\mathcal{X}))^H$ of such differentials on $\mathcal{X}$ fixed by H. But since $\mathcal{X}$ is a smooth plane quartic, we can identify $H_1(\mathcal{X})$ with the space of linear forms in the coordinates. Thus in our case the representation of G on $H_1(\mathcal{X})$ is isomorphic with (V^*, ρ^*), and we may recover the dimension of the subspace fixed by each subgroup H from the character table.

Since the quotient of $\mathcal{X}$ by the 7-Sylow $\langle g \rangle \subset G$ has genus 0, we can regard $\mathcal{X}$ as a cyclic cover of $\mathbb{CP}^1$ of degree 7. We can see this explicitly: the covering map sends $(X : Y : Z) \in \mathcal{X}$ to $(X^3Y : Y^3Z : Z^3X)$ on the line

$$\{(a : b : c) \in \mathbb{CP}^2 : a + b + c = 0\}. \tag{2.1}$$

Then $(Y/Z)^7 = ab^2/c^3$, and $(X : Y : Z)$ is determined by $(a : b : c)$ together with the seventh root Y/Z of ab^2/c^3. Thus if we take $y = -Y/Z$ and $x = b/c$ we find that $\mathcal{X}$ is birational with the curve

$$y^7 = x^2(x+1). \tag{2.2}$$

This model of $\mathcal{X}$ exhibits the action of the 21-element subgroup $\langle g, h \rangle$ of G: g multiplies y by ζ^{-1}, while g cyclically permutes a, b, c (or equivalently the points $-1, 0, \infty$ on the x-line). It also lets us write periods of differentials on $\mathcal{X}$ as linear combinations of Beta integrals. For instance, for the form dx/y^3 we find

$$\int_{-\infty}^{-1} \frac{dx}{y^3} = B\left(\tfrac{2}{7}, \tfrac{4}{7}\right), \quad \int_{-1}^{0} \frac{dx}{y^3} = B\left(\tfrac{1}{7}, \tfrac{4}{7}\right), \quad \int_{0}^{\infty} \frac{dx}{y^3} = B\left(\tfrac{1}{7}, \tfrac{2}{7}\right); \tag{2.3}$$

the identity $\Gamma(u)\Gamma(1-u) = \pi/\sin \pi u$ shows that each of these integrals is a K_+ multiple of

$$\Pi_7 := \frac{1}{\pi\sqrt{7}} \Gamma\left(\tfrac{1}{7}\right)\Gamma\left(\tfrac{2}{7}\right)\Gamma\left(\tfrac{4}{7}\right), \tag{2.4}$$

and thus that all the periods of dx/y^3 on $\mathcal{X}$ are in $K\Pi_7$. We later (2.12) use this to evaluate a complete elliptic integral as a multiple of Π_7.

We also compute for later use the quotient curve $\mathcal{X}/\langle h \rangle$ of genus 1. Since Φ_4 is not fixed by odd coordinate permutations, we can do this by multiplying Φ_4

by its image under such a permutation, and expressing the resulting symmetric function

$$(X^3Y + Y^3Z + Z^3X)(X^3Z + Z^3Y + Y^3X) \tag{2.5}$$

in terms of the elementary symmetric functions

$$s_1 = X + Y + Z, \quad s_2 = XY + YZ + ZX, \quad s_3 = XYZ. \tag{2.6}$$

We find that (2.5) is

$$s_2^4 + s_3(s_1^5 - 5s_1^3 s_2 + s_1 s_2^2 + 7s_1^2 s_3). \tag{2.7}$$

We thus get an affine model for $\mathcal{X}/\langle h\rangle$ by setting this polynomial equal to zero and substituting 1 for s_1:

$$7s_3^2 + (s_2^2 - 5s_2 + 1)s_3 + s_2^4 = 0. \tag{2.8}$$

To put this in Weierstrass form, divide (2.8) by s_2^4 and rewrite it as

$$7\Big(\frac{s_3}{s_2^2}\Big)^2 + (s_2^{-2} - 5s_2^{-1} + 1)\frac{s_3}{s_2^2} + 1 = 0. \tag{2.9}$$

Let $u = s_3/s_2^2$. Then (2.9) is a quadratic polynomial in s_2^{-1} over $\mathbb{Q}(u)$, so it has a root if and only if its discriminant $-28u^3 + 21u^2 - 4u$ is a square. The further substitution $u = -1/x$ then yields the desired form

$$E_k : y^2 = 4x^3 + 21x^2 + 28x \tag{2.10}$$

of the quotient curve. We can then compute that the curve has j-invariant $-3375 = -15^3$, and thus has complex multiplication (CM) by O_k. We note for future reference that the unit vectors, which have $s_2 = s_3 = 0$, map to the point at infinity of E_k, while the branch points of the cover $\mathcal{X} \to E_k$ are the fixed points $(1 : e^{\pm 2\pi i/3} : e^{\mp 2\pi i/3})$ of h, which have $s_1 = s_2 = 0$ and turn out to map to two points on E_k whose x-coordinates are roots $-\alpha$, $-\bar{\alpha}$ of

$$x^2 - x + 7 = 0. \tag{2.11}$$

The 2-element group $N(\langle h\rangle)/\langle h\rangle = \langle h, s\rangle/\langle h\rangle$ acts on E_k. Since $\mathcal{X}/\langle h, s\rangle$ has genus 0, the involution in $\langle h, s\rangle/\langle h\rangle$ must multiply the invariant differential on E_k by -1. Thus it is of the form $P \leftrightarrow P_0 - P$ for some $P_0 \in E_k$ (using the group law on E_k), and is determined by the image of a single point. We compute that s takes the unit vectors to points on $\mathcal{X}$ whose coordinates are proportional to the three roots of $u^3 - 7u^2 + 49$, and that these points map to the 2-torsion point $(0, 0)$ on E_k. Thus this point is P_0; in other words, the nontrivial element of $\langle h, s\rangle/\langle h\rangle$ acts on E_k by the involution that switches the point at infinity with $(0, 0)$ but is *not* translation by that 2-torsion point of E_k.

We further find that the curve E_k has conductor 49. (To see that the conductor is odd, note that the linear change of variable $y = 2y_1 + x$ puts E_k in the form $y_1^2 + xy_1 = x^3 + 5x^2 + 7x$ with good reduction at 2.) This conductor is small enough that we may locate the curve in the tables of elliptic curves dominated by modular curves compiled by Tingley et al. (the "Antwerp Tables" in [Birch and Kuyk 1975]) and Cremona [1992]: the curve is listed as 49A and 49-A1 respectively. We find there that E_k is literally a modular elliptic curve: it is not only dominated by, but in fact isomorphic with, $X_0(49)$. We shall later obtain this isomorphism from the identification of $\mathcal{X}$ with the modular curve $X(7)$. Likewise the fact that E_k has CM by O_k is no accident: we shall see that if there is a nonconstant map from $\mathcal{X}$ to an elliptic curve then the elliptic curve has CM by some order (subring of finite index) in O_k; equivalently, such a curve must be isogenous with E_k. (It is clear that conversely a curve isogenous with E_k admits such a map, since we have just constructed a nonconstant map from $\mathcal{X}$ to E_k itself.) For instance this must be true of the quotient of $\mathcal{X}$ by one of the 21 two-element subgroups of G. Since these subgroups are all conjugate in G, the resulting curves are isomorphic; in fact the reader may check (starting from the S_4 model of $\mathcal{X}$, in which several of these involutions are visible) that these elliptic curves are all $\bar{\mathbb{Q}}$-isomorphic with E_k.

An algebraic map from $\mathcal{X}$ to E_k can be used to pull back an invariant differential on E_k to $H_1(\mathcal{X})$. Thus the periods of E_k can be evaluated in terms of the Beta integrals that arise in the periods of $\mathcal{X}$. This yields the formula

$$\int_0^\infty \frac{dx}{\sqrt{4x^3+21x^2+28x}} = \tfrac{1}{4}\Pi_7 = \frac{1}{4\pi\sqrt{7}}\,\Gamma\bigl(\tfrac{1}{7}\bigr)\Gamma\bigl(\tfrac{2}{7}\bigr)\Gamma\bigl(\tfrac{4}{7}\bigr), \tag{2.12}$$

equivalent to Selberg and Chowla's result [1967, pp. 102–3]; its explanation via $\mathcal{X}$ is essentially the argument of Gross and Rohrlich [1978], though they pulled the differential all the way back to the Fermat curve $\mathcal{F}_7$, for which see Section 3.2 below.

2.2. $\mathcal{X}$ as the simplest Hurwitz curve. A classical theorem of Hurwitz ([1893]; see also [Arbarello et al. 1985, Chapter I, Ex. F-3 ff., pp. 45–47]) asserts that a Riemann surface S of genus $g > 1$ can have at most $84(g-1)$ automorphisms, and a group of order $84(g-1)$ is the automorphism group of some Riemann surface of genus g if and only if it is generated by an element of orders 2 and one of order 3 such that their product has order 7. In that case the quotient of S by the group is the Riemann sphere, and the quotient map $S \to \mathbb{CP}^1$ is ramified above only three points of $\mathbb{CP}^1$, with the automorphisms of orders $2, 3, 7$ of S appearing as the deck transformations lifted from cycles around the three branch points. Thus the group elements of orders $2, 3, 7$ specify S by Riemann's existence theorem for Riemann surfaces. Note that the construction does not depend on the location of the three branch points on $\mathbb{CP}^1$, because $\mathrm{Aut}(\mathbb{CP}^1) = \mathrm{PGL}_2(\mathbb{C})$ acts on $\mathbb{CP}^1$ triply transitively.

A Riemann surface with the maximal number $84(g-1)$ of automorphisms, regarded as an algebraic curve over $\mathbb{C}$, is called a *Hurwitz curve* of genus g. Necessarily $g \geq 3$, because a curve C genus 2 over $\mathbb{C}$ has a hyperelliptic involution ι, and $\mathrm{Aut}(C)/\{1,\iota\}$ is the subgroup of $\mathrm{PGL}_2(\mathbb{C}) = \mathrm{Aut}(\mathbb{CP}^1)$ permuting the six ramified points, but the stabilizer in $\mathrm{Aut}(\mathbb{CP}^1)$ of a six-point set has size at most 24. So a Hurwitz curve must have genus at least 3. We know already that $\mathcal{X}$ is such a curve. In fact one may check that G is the only group of order 168 satisfying the Hurwitz condition, and that up to $\mathrm{Aut}(G)$ there is a unique choice of elements of orders $2, 3$ in G whose product has order 7. (For instance we may take the involution s and the 3-cycle sg.) Thus $\mathcal{X}$ is the unique Hurwitz curve of genus 3. We readily write the quotient map $\mathcal{X} \to \mathcal{X}/G \cong \mathbb{CP}^1$ explicitly, using our invariant polynomials $\Phi_6, \Phi_{14}, \Phi_{21}$: a point $(X : Y : Z)$ on $\mathcal{X}$ maps to

$$j := \frac{\Phi_{14}^3}{\Phi_6^7} = \frac{\Phi_{21}^2}{\Phi_6^7} + 1728 \tag{2.13}$$

on $\mathbb{CP}^1$. Note that this is a rational function of degree $4 \cdot 42 = 168 = \#G$ on $\mathcal{X}$, and thus of degree 1 on $\mathcal{X}/G$. That the two expressions in (2.13) are indeed equal on $\mathcal{X}$ follows from (1.19). We then see from (2.13) that the branch points of orders $2, 3, 7$ on $\mathbb{CP}^1$ have j coordinates $1728, 0, \infty$ respectively. Of course we have chosen this coordinate j on $\mathcal{X}/G \cong \mathbb{CP}^1$ to facilitate the identification of $\mathcal{X}$ and $\mathcal{X}/G$ with the modular curves $X(7)$ and $X(1)$ later in this paper.

Hurwitz curves can also be characterized in terms of their uniformization by the hyperbolic plane $\mathcal{H}$. Any Riemann surface S of genus > 1 can be identified with $\mathcal{H}/\pi_1(S)$; conversely, any discrete co-compact subgroup $\Gamma \subset \mathrm{Aut}(\mathcal{H}) \cong \mathrm{PSL}_2(\mathbb{R})$ that acts freely on $\mathcal{H}$ (that is, every point has trivial stabilizer) yields a Riemann surface $\mathcal{H}/\Gamma$ of genus > 1 whose fundamental group is Γ. The automorphism group of $\mathcal{H}/\Gamma$ is $N(\Gamma)/\Gamma$, where $N(\Gamma)$ is the normalizer of Γ in $\mathrm{Aut}(\mathcal{H})$. It follows that $\mathcal{H}/\Gamma$ is a Hurwitz curve if and only if $N(\Gamma)$ is the *triangle group* $G_{2,3,7}$ of orientation-preserving transformations generated by reflections in the sides of a given hyperbolic triangle with angles $\pi/2, \pi/3, \pi/7$ in $\mathcal{H}$. Equivalently, Γ is to be a normal subgroup of $G_{2,3,7}$. Since $G_{2,3,7}$ has the presentation

$$G_{2,3,7} = \left\langle \sigma_2, \sigma_3, \sigma_7 \mid \sigma_2^2 = \sigma_3^3 = \sigma_7^7 = \sigma_2\sigma_3\sigma_7 = 1 \right\rangle \tag{2.14}$$

(with σ_j being a $2\pi/j$ rotation about the π/j vertex of the triangle), this yields our previous characterization of the groups that can occur as $\mathrm{Aut}(S) = G_{2,3,7}/\Gamma$. In Section 4.4 we identify $\mathcal{X}$ with a Shimura modular curve by recognizing $G_{2,3,7}$ as an arithmetic group in $\mathrm{PSL}_2(\mathbb{R})$, and $\pi_1(\mathcal{X})$ with a congruence subgroup of $G_{2,3,7}$.

2.3. The Jacobian of $\mathcal{X}$. We have noted already that the representation of G on $H_1(\mathcal{X})$ isomorphic with (V^*, ρ^*). In particular, the representation is irreducible and defined over k, and its character takes values $\notin \mathbb{Q}$. It follows as in [Ekedahl and Serre 1993] that the Jacobian $J = J(\mathcal{X})$ is isogenous to the cube of an elliptic curve with CM by O_k. This does not determine J completely, but the fact that G acts on the period lattice of J means that this period lattice is proportional to L, and this does specify J. (See [Mazur 1986, pp. 235–6], where this is attributed to Serre; also compare [Buser and Sarnak 1994, Appendix 1], where the packing of congruent spheres in $\mathbb{R}^6$ obtained from L is conjectured to maximize the density of a packing coming from the period lattice of the Jacobian of a curve of genus 3.) In the notation of [Serre 1967] we have[8] $J \cong E_k \otimes L$.

We next describe a Mordell–Weil lattice associated with $\mathcal{X}$; see for instance [Elkies 1994] for more background on Mordell–Weil lattices.

Let E be an elliptic curve, and consider algebraic maps from $\mathcal{X}$ to E. These constitute an abelian group using the group law on E. This group may also be regarded as the group of rational points of E defined over the function field of $\mathcal{X}$; we thus call it the *Mordell–Weil group* M of maps from $\mathcal{X}$ to E, in analogy with the Mordell–Weil group of an elliptic curve over a number field. This group contains a subgroup isomorphic with E, namely the group of constant maps; the quotient group M/E may in turn be identified (via the embedding of X into J) with the group of morphisms from J to E. It follows that this group is trivial unless E has CM by an order in O_k, in which case it is a free abelian group of rank 6. This proves our earlier claim that the elliptic curves E admitting a nonconstant map from $\mathcal{X}$ are exactly the curves isogenous with E_k.

The function $\hat{h} : M \to \mathbb{Z}$ taking each $f : \mathcal{X} \to E$ to twice its degree as a rational map turns out to be a quadratic form. (For Riemann surfaces this is easy to see: let ω be a nonzero invariant differential on E; then $f \mapsto f^*\omega$ is a group homomorphism from M to $H_1(\mathcal{X})$, and $\hat{h}(f) = 2\deg(f)$ is the image of $f^*\omega$ under the quadratic form $\theta \mapsto 2\int_{\mathcal{X}} \theta \wedge \bar{\theta} \big/ \int_C \omega \wedge \bar{\omega}$. Several proofs that $\hat{h}$ is a quadratic form valid in arbitrary characteristic are given in [Elkies 1994]. We use the notation $\hat{h}$ because this is a special case of the Néron–Tate canonical height; note that thanks to the factor of 2 the associated bilinear pairing

$$\langle f_1, f_2 \rangle = \tfrac{1}{2}\big(\hat{h}(f_1 + f_2) - \hat{h}(f_2) - \hat{h}(f_1)\big)$$

is integral.) This quadratic form is positive-definite on the free abelian group M/E, and gives this group the structure of a Euclidean lattice, which we thus call the *Mordell–Weil lattice* of maps from $\mathcal{X}$ to E.

Assume now that E is an elliptic curve with CM by O_k, i.e. that E is isomorphic with E_k. Then the Mordell–Weil lattice inherits the action of O_k on E as well as the action of G on $\mathcal{X}$. Therefore it is isomorphic with our lattice L^* of (1.25) up to scaling. Moreover, the quadratic form $\hat{h}$ satisfies the identity $\hat{h}(\beta f) = |\beta|^2 \hat{h}(f)$ for each $\beta \in O_k$, because $|\beta|^2$ is the degree of the isogeny $\beta : E \to E$. Thus $\hat{h}$ is a Hermitian pairing on L. This pairing is again unique up to scaling, this time because V^* is unitary and Hermitian (see again [Gross 1990]). If we identify L^* with the lattice generated by the three vectors (1.25) then we have

$$\hat{h}(v) = |v_1|^2 + |v_2|^2 + |v_3|^2. \tag{2.15}$$

[8] Serre actually defines $E \otimes L$ (or rather $L^* * E$) only when L is a lattice of rank 1 over $\mathrm{End}(E)$, but for each $g \geq 1$ the same construction for a lattice of rank g yields a polarized abelian variety isogenous with E^g.

This lattice has 21 pairs of vectors such as $(2,0,0)$ of minimal nonzero norm 4. These correspond to maps of degree 2 from C to E, which in turn are indexed by the 21 involutions $g \in G$. Each g is counted twice, because there are up to translation in E two ways to identify the quotient curve $\mathcal{X}/\{1,g\}$ with E, each yielding a map: $\mathcal{X} \to E$ of degree 2. Likewise the 28 pairs of vectors such as (α,α,α) of the next-lowest norm 6 correspond to maps of degree 3, all of which turn out to be quotient maps by the twenty-eight 3-Sylow subgroups of G. For each n the number N_n of maps of degree n up to translation on E is the number of vectors of norm $2n$ in L, which is the q^n coefficient of the theta series

$$\theta_L := \sum_{n=0}^{\infty} N_n q^n = \sum_{v \in L} q^{\frac{1}{2}\hat{h}(v)} \tag{2.16}$$

of L. But θ_L is a modular form of weight 3 with quadratic character on $\Gamma_0(7)$ fixed by the Fricke involution w_7 ([Gross 1990, § 9]; we shall encounter $\Gamma_0(7)$ and w_7 again in Section 4.2), and the space of such modular forms is 2-dimensional. The constraints $N_0 = 1$, $N_1 = 0$ determine θ_L uniquely, and we find

$$\begin{aligned} \theta_L &= \Biggl(\sum_{\beta \in O_k} q^{\beta\bar{\beta}}\Biggr)^3 - 6q \prod_{n=1}^{\infty} (1-q^n)^3 (1-q^{7n})^3 \\ &= 1 + 42q^2 + 56q^3 + 84q^4 + 168q^5 + 280q^6 + 336q^7 + 462q^8 + \cdots. \end{aligned} \tag{2.17}$$

This confirms our values $N_2 = 42$ and $N_3 = 56$ and lets us easily calculate as many N_n as we might reasonably desire.

3. Arithmetic Geometry of $\mathcal{X}$

3.1. Rational points on $\mathcal{X}$. Faltings' theorem (né Mordell's conjecture) asserts that a curve of genus at least 2 over a number field has finitely many rational points. Unfortunately both of Faltings' proofs of this [1983; 1991] are ineffective, in that neither yields an algorithm for provably listing all the points; even for a specific curve of low genus over $\mathbb{Q}$ this problem can be very difficult. (See for instance [Poonen 1996].) Fortunately the special case of $\mathcal{X}$ is much easier. One shows that the elliptic curve E_k has rank zero, and its only rational points are the point at infinity and $(0,0)$. Since $\mathcal{X}$ admits a nonconstant map to E_k defined over $\mathbb{Q}$, namely the quotient map $\mathcal{X} \to \mathcal{X}/\langle h \rangle \cong E_k$, the $\mathbb{Q}$-rational points of $\mathcal{X}$ are just the rational preimages of the two points of $E_k(\mathbb{Q})$. We find that the only points of $\mathcal{X}(\mathbb{Q})$ are the obvious ones at $(1:0:0)$, $(0:1:0)$, $(0:0:1)$. Equivalently, the only integer solutions of $X^3Y + Y^3Z + Z^3X = 0$ are those in which at least two of the three variables vanish. This is all for the Klein model; one may likewise analyze the rational S_3 model for $\mathcal{X}$, computing[9] that its quotient by $\langle h \rangle$ is isomorphic with E_k, and that neither of the rational points

[9]This computation begins in the same way as our derivation of (2.10), but yields an equation $y^2 = x^4 - 10x^3 + 27x^2 - 10x - 27$ for the quotient curve; to bring this to Weierstrass form,

of E_k lies under a rational point of $\mathcal{X}$. However, the fact that $\mathcal{X}$ has no rational points in the rational S_3 model can be obtained much more simply, without any computation of quotient curves and analysis of elliptic curves over $\mathbb{Q}$: one need only observe that the polynomial (1.22) does not vanish mod 2 unless X, Y, Z are all even.

The proof that $E_k(\mathbb{Q})$ consists only of the point at infinity and $(0,0)$ is an application of Fermat's method of descent. Suppose that $x \neq 0$ is a rational number such that $x(4x^2 + 21x + 28) = y^2$ for some $y \in \mathbb{Q}$. Necessarily $x > 0$, because $4x^2 + 21x + 28 > 0$ for all $x \in \mathbb{R}$. Write x as a fraction m/n in lowest terms. If x works then so does $7/x$ (note that $(7/x, -7y/x^2)$ is the translate of (x, y) by the 2-torsion point $(0,0)$ in the group law of E_k). Replacing x by $7/x$ if necessary, we may assume that the exponents of 7 in the factorizations of m, n are both even. Then the integer $(n^2y)^2 = mn(4m^2 + 21mn + 28n^2)$ is a perfect square, and its factors m, n, $4m^2 + 21mn + 28n^2$ are relatively prime in pairs except possibly for common factors of $2 \cdot 49^r$ or $4 \cdot 49^r$. Thus either all three are squares, or one is a square and the each of the other two is twice a square. We claim that the latter is impossible. Indeed, since m, n cannot both be even, we would have either $(m, n) = (M^2, 2N^2)$ or $(m, n) = (2M^2, N^2)$. In the first case,

$$4m^2 + 21mn + 28n^2 = 2(2M^4 + 21M^2N^2 + 56N^4). \tag{3.1}$$

But M is odd (else m, n are both even), so $2M^4 + 21M^2N^2 + 56N^4$ is either 2 or 3 mod 4 according as N is even or odd; in neither case can it be a perfect square. In the second case, N is odd and

$$4m^2 + 21mn + 28n^2 = 2(8M^4 + 21M^2N^2 + 14N^4). \tag{3.2}$$

Again the parenthesized factor is either 2 or 3 mod 4, this time depending on the parity of M, so it cannot be a square.

So we conclude that m, n are both squares. Thus $x = x_1^2$ for some $x_1 \in \mathbb{Q}^*$, and $4x_1^4 + 21x_1^2 + 28 \in \mathbb{Q}^{*2}$. We "complete the square" by writing $\sqrt{4x_1^4 + 21x_1^2 + 28}$ as $2x^2 + (21 - \xi)/4$, finding

$$16\xi x^2 = \xi^2 - 42\xi - 7. \tag{3.3}$$

Necessarily $\xi \neq 0$ because the right-hand side has irrational roots. Thus we obtain a point on the elliptic curve

$$E_k' : \eta^2 = \xi(\xi^2 - 42\xi - 7) \tag{3.4}$$

other than the origin and $(0,0)$. We then mimic the argument in the previous paragraph to show that either ξ or $-7/\xi$ must be a square. This time the possibility that must be excluded is that that one of them is $-\xi_1^2$ for some $\xi_1 \in \mathbb{Q}$. Taking $\xi_1 = M/N$, we would then have a square of the form $7N^4 - 42M^2N^2 - M^4$. But this is congruent to 3 mod 4 if either M or N is even, and to -4 mod 16

complete the square as we do several times in the sequel, for instance when obtaining (3.4) or in the calculation starting with (3.9).

if they are both odd, so again we reach a contradiction. Thus $\xi = \xi_1^2$ and we find that $\xi_1^4 - 42\xi_1^2 - 7$ is a square, say $\bigl(\xi^2 - (8x_2 + 21)\bigr)^2$. This yields $x_2\xi^2 = 4x_2^2 + 21x_2 + 28$; again the right-hand side has irrational roots, so we find $x_2 \in \mathbb{Q}^*$ such that $x_2(4x_2^2 + 21x_2 + 28) \in \mathbb{Q}^2$ — which is to say, a new point on E_k! Moreover, we can compute our original x or $7/x$ as a rational function in x_2 of degree 4, which means that if the numerator and denominator of x are at all large ($|M|, |N| > 100$ is more than enough) then those of x_2 are smaller. Iterating this descent process enough times, we eventually find a rational solution of $y^2 = 4x^3 + 21x^2 + 28x$ with nonzero $x = M/N$ such that $|M|, |N| \le 100$. But a direct search shows that there is no such x. This completes the proof that the only rational points on E_k are the two torsion points already known.

[In modern terminology, Fermat's method is "descent via a 2-isogeny" $E'_k \to E_k$ [Silverman 1986, pp. 301 ff.]. The method can be used on any elliptic curve with a rational 2-torsion point, and will often prove that the curve has only finitely many rational points. The reappearance of E_k at the second step, which makes it possible to iterate the process until reaching a small point, is due to the existence of a dual isogeny $E_k \to E'_k$ also of degree 2. Composing these two isogenies yields the multiplication-by-2 map on E_k; thus we proved in effect that any rational point on E_k is in either divisible by 2 or of the form $2P+(0,0)$ in $E_k(\mathbb{Q})$, and then used the fact that multiplication by 2 in $E_k(\mathbb{Q})$ quadruples the height to reduce the determination of $E_k(\mathbb{Q})$ to a finite search. In our case the 2-isogenous curve E'_k has j-invariant 255^3 and CM by $\mathbb{Z}[\sqrt{-7}]$; it is the elliptic curve numbered 49B in [Birch and Kuyk 1975] and 49-A2 in [Cremona 1992].]

It remains to find the preimages on $\mathcal{X}$ of the two rational points of E_k. We saw already that the point at infinity comes from the unit vectors on $\mathcal{X}$, and that the 2-torsion point $(x, y) = (0, 0)$ is the image of an $\langle h \rangle$-orbit of points on $\mathcal{X}$ whose coordinates are proportional to the three roots of $u^3 - 7u^2 + 49$. These roots (and their ratios) are contained in K_+ but not in $\mathbb{Q}$. Thus the unit vectors are the only rational points on $\mathcal{X}$, as claimed.

3.2. Fermat's Last Theorem for exponent 7. The Fermat curve

$$\mathcal{F}_7 : A^7 + B^7 + C^7 = 0$$

admits a nonconstant map to $\mathcal{X}$ defined over $\mathbb{Q}$, namely

$$(A : B : C) \mapsto (A^3C : B^3A : C^3B).$$

(The map is a cyclic unramified cover of degree 7, but we do not need this for now.) Thus any rational point on $\mathcal{F}_7$ maps to a rational point on $\mathcal{X}$. Having just listed the rational points on $\mathcal{X}$ we can thus determine the rational points on $\mathcal{F}$. It turns out that each point of $\mathcal{X}(\mathbb{Q})$ lies under a unique point of $\mathcal{F}(\mathbb{Q})$. This yields a proof of the case $n = 7$ of "Fermat's Last Theorem", a proof that is elementary in that it uses only tools available to Fermat (algebraic manipulation and 2-descent on an elliptic curve with a rational 2-torsion point); in particular it does not require arithmetic in cyclotomic number fields such as K. Indeed the proof is analogous to Fermat's own proof of the case $n = 4$, in the sense that in both cases one maps $\mathcal{F}_n$ to an elliptic curve and proves that the elliptic curve has rank 0; it is arguably easier than Euler's proof of the case $n = 3$, for which $\mathcal{F}_3$ is already an elliptic curve but the determination of $\mathcal{F}_3(\mathbb{Q})$ requires what we now recognize as a 3-descent. As is the case for $n = 4$, the map from $\mathcal{F}_7$ to E_k is a quotient map, here by a 21-element subgroup of $\mathrm{Aut}(\mathcal{F}_7)$ isomorphic with $\langle g, h\rangle \subset G$.

Stripped of all algebro-geometric machinery, this elementary proof runs as follows: Suppose there existed nonzero integers a, b, c such that $a^7 + b^7 + c^7 = 0$. Then

$$x := a^3c, \quad y := b^3a, \quad z := c^3b \tag{3.5}$$

would be nonzero integers with

$$x^3y + y^3z + z^3x = a^3b^3c^3(a^7 + b^7 + c^7) = 0, \tag{3.6}$$

which we showed impossible in the previous section.

Curiously there is yet another proof of the $n = 7$ case of Fermat along the same lines, which was discovered in the mid-19th century [Genocchi 1864][10] but is practically unknown today. Here we use the quotient of $\mathcal{F}_7$ by the group S_3 of coordinate permutations. This yields the following nice generalization of Fermat for $n = 7$:

THEOREM [Genocchi 1864][11]. *Let a, b, c be the solutions of a cubic $x^3 - px^2 + qx - r = 0$ with rational coefficients p, q, r. If $a^7 + b^7 + c^7 = 0$ then either $abc = 0$ or $a^3 = b^3 = c^3$.*

That is, the only rational points on $\mathcal{F}_7/S_3$ are the orbits of $(1 : -1 : 0)$ and $(1 : e^{2\pi i/3} : e^{-2\pi i/3})$. We compute equations for $\mathcal{F}_7/S_3$ by writing $a^7 + b^7 + c^7$ as a polynomial in the elementary symmetric functions

$$p = a + b + c, \qquad q = ab + ac + bc, \qquad r = abc \tag{3.7}$$

of a, b, c.

PROOF. We easily calculate

$$0 = a^7 + b^7 + c^7 = p^7 - 7p^5q + 7p^4r + 14p^3q^2 - 21p^2qr - 7pq^3 + 7pr^2 + 7q^2r \tag{3.8}$$

(for instance by using the fact that the power moments $\pi_n = a^n + b^n + c^n$ satisfy the recursion $\pi_{n+3} - p\pi_{n+2} + q\pi_{n+1} - r\pi_n = 0$ and starting from $\pi_0 = 3$, $\pi_1 = p$,

[10] From Dickson [1934, p. 746], footnote 85. Dickson further notes that Genocchi's method may be viewed as a simplification of Lamé's, and that Genocchi does not carry out the descent for proving that (3.9) has no finite rational points. We likewise leave the 2-descent on the equivalent curve (3.12) to the reader, who may either do it by hand using the method described in [Silverman 1986, pp. 301 ff.] or automatically with Cremona's mwrank program.

[11] In fact Genocchi states at the end of his paper that he had announced the results several years earlier in "*Cimento* di Torino, vol. VI, fasc. VIII, 1855."

$\pi_2 = p^2 - 2q$ to reach the formula (3.8) for π_7). Now if $p = 0$ then (3.8) reduces to $\pi_7 = 7q^2 r$, so if $\pi_7 = 0$ then either $r = 0$ or $q = 0$, which yields $abc = 0$ or $a^3 = b^3 = c^3$ respectively. If on the other hand $p \neq 0$ then we may assume $p = 1$ by replacing a, b, c by $a/p, b/p, c/p$. We then find that (3.8) is a quadratic polynomial in r of discriminant $49q^4 - 98q^3 + 147q^2 - 98q + 21$. We note that the resulting elliptic curve

$$u^2 = 49q^4 - 98q^3 + 147q^2 - 98q + 21 \tag{3.9}$$

has rational points at infinity, and use them to obtain a Weierstrass form for the curve by the usual device of completing the square: let

$$u = 7(q^2 - q + 1 - 2t) \tag{3.10}$$

in (3.9) to find

$$7t(q^2 - q) = 7t^2 - 7t + 1, \tag{3.11}$$

a quadratic in q with discriminant $196t^3 - 147t^2 + 28t$. Thus $196t^3 - 147t^2 + 28t$ must be a square. Taking $t = -x/7$, then, we obtain the elliptic curve

$$-7y^2 = 4x^3 + 21x^2 + 28x, \tag{3.12}$$

which we recognize as the $\sqrt{-7}$-twist of E_k. Since that curve has CM by $\mathbb{Z}[\alpha]$, this new curve (3.12) is also 7-isogenous with E_k, and thus has rank zero. (This curve appears as 49C in [Birch and Kuyk 1975] and 49-A3 in [Cremona 1992].) In fact we can apply a 2-descent directly to (3.12) using the 2-torsion point $(0, 0)$, and then find that this point is the only rational point of (3.12) other than the point at infinity. But if $x = 0$ then $t = 7x = 0$ and (3.11) becomes $0 = 1$, which is impossible (indeed the points $x = 0, \infty$ on (3.12) come from the solutions $p = r = 0$ and $p = q = 0$ of (3.8) — which solution is which depends on the choice of square root u implicit in (3.9)). Thus indeed $p = 0$ in any rational solution of (3.8), which completes the proof of Genocchi's theorem. $\square$

[Along these lines we note that Gross and Rohrlich [1978] have shown that the orbits of $(1 : -1 : 0)$ and $(1 : e^{2\pi i/3} : e^{-2\pi i/3})$ also contain the only points of $\mathcal{F}_7$ rational over any number field of degree at most 3.]

3.3. Reduction of $\mathcal{X}$ modulo 2,3,7. For each of the primes $p = 2, 3, 7$ dividing $\#G$, the reduction of $\mathcal{X}$ mod p enjoys some remarkable extremal properties: maximal or minimal numbers of points over finite fields in each case, and maximal group of automorphisms for $p = 3$. We consider these three primes in turn.

Characteristic 2. Since we want all the automorphisms of G to be defined over $\mathbb{F}_2$, we use the S_4 or rational S_3 model for $\mathcal{X}$. Then the Jacobian of $\mathcal{X}$ is $\mathbb{F}_2$-isogenous to the cube of an elliptic curve with CM by $\mathbb{Z}[\alpha]$ and trace 1. It follows that the characteristic polynomial of Frobenius for $\mathcal{X}/\mathbb{F}_2$ is $(T^2-T+2)^3$, with triple roots $-\alpha, -\bar{\alpha}$. Thus for each $m \geq 1$ our curve has

$$2^m + 1 - 3\big((-\alpha)^m + (-\bar{\alpha})^m\big) \tag{3.13}$$

rational points over $\mathbb{F}_{2^m}$. We tabulate this for the first few m:

m	1	2	3	4	5	6	7	8	...
$\#(\mathcal{X}(\mathbb{F}_{2^m}))$	0	14	24	14	0	38	168	350	...

(3.14)

We noted already that the reduction mod 2 of the rational S_3 model for $\mathcal{X}$ has no $\mathbb{F}_2$-rational points. That it has no $\mathbb{F}_{32}$-rational points is rather more remarkable. By the Weil estimates, a curve of genus w over $\mathbb{F}_q$ has at least $q - 2wq^{1/2} + 1$ rational points; if $w > 1$, this lower bound may be negative, but only for $q \leq 4w^2 - 3$. In our case $w = 3$, this bound on q is 33, which is not a prime power, so $\mathbb{F}_{32}$ is the largest finite field over which a curve of genus 3 may fail to have any rational point. [For $w = 2$, the bound $4w^2 - 3$ is the prime 13, but Stark showed ([1973]; see in particular pages 287–288) that there is no pointless curve of genus 2 over $\mathbb{F}_{13}$; an explicit such curve over $\mathbb{F}_{11}$ is $y^2 = -(x^2+1)(x^4+5x^2+1)$.]

The 14 points of our curve over $\mathbb{F}_4$ are all the points of $\mathbb{P}^2(\mathbb{F}_4) - \mathbb{P}^2(\mathbb{F}_2)$. It is known that this is the maximal number of points of a genus-3 curve over $\mathbb{F}_4$ [Serre 1983a; 1983b; 1984]. Note that the only $\mathbb{F}_{16}$-points are those already defined over $\mathbb{F}_4$; indeed one can use the "Riemann hypothesis" (which is a theorem of Weil for curves over finite fields) to show as in [Serre 1983b] that a genus-3 curve over $\mathbb{F}_4$ with more than 14 points would have *fewer* $\mathbb{F}_{16}$ points than $\mathbb{F}_4$ points, and thus prove that 14 is the maximum. The 24 points over $\mathbb{F}_8$ likewise attain the maximum for a genus-3 curve over that field [Serre 1983a; 1984]. Note that the only $\mathbb{F}_{64}$-points are those already rational over a subfield $\mathbb{F}_4$ or $\mathbb{F}_8$.

Upon reading a draft of this paper, Serre noted that in fact for $m = 2, 3, 5$ the curve $\mathcal{X}$ is the unique curve of genus 3 over $\mathbb{F}_{2^m}$ with the maximal ($m = 2, 3$) or minimal ($m = 5$) number of rational points. He shows this as follows. Let $C/\mathbb{F}_{2^m}$ be any curve with the same number of points as $\mathcal{X}$. First Serre proves that C has the same eigenvalues of Frobenius as $\mathcal{X}$. For $m = 3, 5$ this follows from the fact that C attains equality in the refined Weil bound

$$\big|\#C(\mathbb{F}_q) - (q+1)\big| \leq g\lfloor 2q^{1/2} \rfloor \tag{3.15}$$

(see [Serre 1983b, Theorem 1]). For $m = 2$ we instead use the fact that $\#C(\mathbb{F}_{16}) \geq \#C(\mathbb{F}_4) = 14$. Serre then notes that in each of the three cases $m = 2, 3, 5$ we have $\alpha^m = (x \pm \sqrt{-7}\,)/2$ for some $x \in \mathbb{Z}$, from which it follows that $\mathbb{Z}[(-\alpha)^m]$ is the full ring of integers in k. Thus the Jacobian of C is isomorphic as a principally polarized abelian threefold $E_k \otimes M$, where M is some indecomposable positive-definite unimodular Hermitian O_k-lattice of rank 3. But by Hoffmann's result [1991, Theorem 6.1] cited above, L is the unique such lattice. Thus C has the same Jacobian as $\mathcal{X}$, from which $C \cong \mathcal{X}$ follows by Torelli.

Since k has unique factorization, the condition $\alpha^m = \bigl(x \pm \sqrt{-7}\,\bigr)/2$ is equivalent to the Diophantine equation

$$x^2 + 7 = 2^n \tag{3.16}$$

with $n = m + 2$. (This equation also arises in [Serre 1983a], in connection with curves of genus 2 over $\mathbb{F}_{2^m}$ with many points, and even in coding theory [MacWilliams and Sloane 1977, p. 184], because it is equivalent to the condition that the volume of the Hamming sphere of radius 2 in $(\mathbb{Z}/2)^{(x-1)/2}$ be a power of 2.) Ramanujan observed[12] that, in addition to the cases $n = 3, 4, 5, 7$ already encountered, this equation has a pair of solutions $(n, x) = (15, \pm 181)$. We find that $(-\alpha)^{13}$ has negative real part, and conclude from Serre's argument that $\mathcal{X}$ is the unique curve of genus 3 over $\mathbb{F}_{2^{13}}$ with the maximal number of rational points, namely $8736 = 2^5 3 \cdot 7 \cdot 13$. Nagell [1960] was apparently the first to show that the Diophantine equation (3.16) has no further integer solutions.

The 24 points over $\mathbb{F}_8$ are, as could be expected, the reduction mod 2 of the 24-point orbit of Weierstrass points of $\mathcal{X}$ in characteristic zero. The $\mathbb{F}_4$ points require some more comment: since G acts on $\mathcal{X}$ by automorphisms defined over the prime field, it permutes these 14 points, whereas in characteristic zero there was no orbit as small as 14 in the action of G on $\mathcal{X}$, or even on $\mathbb{P}^2$. But in characteristic 2 the 24-element subgroups of $G \cong \mathrm{SL}_3(\mathbb{F}_2)$ arise naturally as stabilizers of points and lines in $\mathbb{P}^2(\mathbb{F}_2)$. The stabilizer of a line $\mathbb{P}^1(\mathbb{F}_2) \subset \mathbb{P}^2(\mathbb{F}_2)$ permutes the two points of the line rational over $\mathbb{F}_4$ but not $\mathbb{F}_2$; the subgroup fixing each of those points thus has index 2 in the line stabilizer. Moreover each point of $\mathbb{P}^2(\mathbb{F}_4) - \mathbb{P}^2(\mathbb{F}_2)$ lies on a unique $\mathbb{F}_2$-rational line. Thus the stabilizer of each of these points is a subgroup $A_4 \subset G$. Such a subgroup contains three involutions, each now having two instead of four fixed points on $\mathcal{X}$, and four 3-Sylows. Thus the 14 points of $\mathcal{X}(\mathbb{F}_4)$ are the reductions mod 2 of both the 56-point and the 84-point G-orbits. All points of $\mathcal{X}$ not defined over $\mathbb{F}_4$ or $\mathbb{F}_8$ have trivial stabilizer in G; such points first occur over $\mathbb{F}_{2^7}$, where the 168 points of $\mathcal{X}(\mathbb{F}_{2^7})$ constitute a single G-orbit. The image of this orbit, together with those of $\mathcal{X}(\mathbb{F}_4)$ and $\mathcal{X}(\mathbb{F}_8)$, account for the three $\mathbb{F}_2$-points of $\mathcal{X}/G \cong \mathbb{P}^1$. The $350 - 14 = 336$ points in $\mathcal{X}(\mathbb{F}_{2^8}) - \mathcal{X}(\mathbb{F}_{2^2})$ are likewise the preimages of the two points of $\mathcal{X}/G$ defined over $\mathbb{F}_4$ but not $\mathbb{F}_2$.

We conclude the description of $\mathcal{X}$ in characteristic 2 with an amusing observation of Seidel concerning the $\mathbb{F}_8$-rational points of $\mathcal{X}$, reported by R. Pellikaan at a 1997 conference talk. Since $\mathbb{F}_8$ is the residue field of the primes above 2 of K, the reductions mod 2 of the Klein and S_4 models of $\mathcal{X}$ become isomorphic over

[12] On page 120 of the *Journal of the Indian Mathematical Society*, Volume 5 #3 (6/1913), we find under "Questions for Solution":

> 464. (S. Ramanujan):— $(2^n - 7)$ is a perfect square for the values 3, 4, 5, 7, 15 of n. Find other values.

No other values were found, but it does not seem that a proof that none exist ever appeared in the *Journal*.

that field; we use the Klein model. Consider the $24 - 3 = 21$ points of $\mathcal{X}(\mathbb{F}_8)$ other than the three unit vectors. These may be identified with the solutions in $\mathbb{F}_8^*$ of the affine equation $x^3y + y^3 + x = 0$ (with $x = X/Z$, $y = Y/Z$) for the Klein model of $\mathcal{X}$. We choose (α) for our prime above 2, so ζ reduces to a root of $\zeta^3 + \zeta + 1$ in $\mathbb{F}_8$. The 21 solutions (x, y) are then entered in the following table:

$y \backslash x$	1	ζ^3	ζ^6	ζ^2	ζ^5	ζ^1	ζ^4
1				•		•	•
ζ	•				•		•
ζ^2	•	•				•	
ζ^3		•	•				•
ζ^4	•		•	•			
ζ^5		•		•	•		
ζ^6			•		•	•	

(3.17)

(note that we have listed the x- and y-coordinates in different orders so as to make the $\langle g \rangle$ symmetry visible). Seidel's observation is that (3.17) is the adjacency matrix for the finite projective plane of order 2! The explanation is that for $x, y \in \mathbb{F}_8^*$,

$$x^3y + y^3 + x = 0 \iff x^4y^2 + xy^4 + x^2y = 0 \iff \mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}\, x^2y = 0. \quad (3.18)$$

Now $(x, y) \mapsto \mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}\, x^2y$ is a nondegenerate pairing from $\mathbb{F}_8 \times \mathbb{F}_8$ to $\mathbb{F}_2$, so if we regard $x \in \mathbb{F}_8$ an element of 3-dimensional vector space over $\mathbb{F}_2$ then y is a functional on that vector space and (3.18) is the condition that a nonzero functional annihilate a nonzero vector. Thus if we regard $x, y \in \mathbb{F}_8^*$ as 1- and 2-dimensional subspaces of $\mathbb{F}_2^3$ then $x^3y + y^3 + x = 0$ if and only if the x-line is contained in the y-plane, which is precisely the incidence relation on the points and lines of the finite projective plane $\mathbb{P}^2(\mathbb{F}_2)$.

Characteristic 3. Since 3 is inert in k, the smallest field over which all the automorphisms in G might be defined is $\mathbb{F}_9$. Again we make sure that they are in fact defined over that field by using the S_4 or rational S_3 model for $\mathcal{X}$. That 3 does not split in k also makes the elliptic curve E_k, with CM by O_k, supersingular in characteristic 3; we find that its characteristic polynomial of Frobenius over $\mathbb{F}_9$ is $(T + 3)^2$, and hence that $\mathcal{X}$ has $9^m - 6(-3)^m + 1$ rational points over $\mathbb{F}_{9^m}$. Thus, depending on whether m is odd or even, $\mathcal{X}$ has the maximal or minimal number of rational points for a curve of genus 3 over $\mathbb{F}_{9^m}$. Moreover, the curve has 28 points over both $\mathbb{F}_9$ and $\mathbb{F}_{81}$, and thus maximizes the genus w of a curve $C/\mathbb{F}_9$ that can attain the Weil upper bound $9 + 6w + 1$ on $\#C(\mathbb{F}_9)$.

In fact this turns out to be a special case of a known construction of curves attaining the Weil bound over $\mathbb{F}_{q^2}$. Note that Φ_4, as given by either (1.11) or (1.22), reduces mod 3 to $X'^4+Y'^4+Z'^4$ or $A^4+B^4+C^4$. That is, *the Klein and Fermat quartics are isomorphic in characteristic 3.* Now for each prime power q, the equation $x^{q+1}+y^{q+1}+z^{q+1}=0$ defining the Fermat curve $\mathcal{F}_{q+1}$ can be written as

$$x^q x + y^q y + z^q z = 0. \tag{3.19}$$

For $a \in \mathbb{F}_{q^2}$ we note that $a^q a$ is just the norm of a from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$. This lets us easily count the solutions of (3.19) in $\mathbb{F}_{q^2}$, and we calculate that $\mathcal{F}_{q+1}$ has q^3+1 rational points over $\mathbb{F}_{q^2}$. Since this curve has genus $(q^2-q)/2$, it thus attains the Weil bound. Therefore its characteristic polynomial of Frobenius over $\mathbb{F}_{q^2}$ is $(T+q)^{q^2-q}$, so the number of $\mathbb{F}_{q^4}$-rational points of $\mathcal{F}_{q+1}$ is

$$q^4-(q^2-q)q^2+1=q^3+1 \tag{3.20}$$

again. If there were a curve $C/\mathbb{F}_{q^2}$ of genus $w>(q^2-q)/2$ attaining the Weil bound, its number $q^2+2qw+1$ of $\mathbb{F}_{q^2}$-rational points would exceed the number q^4-2q^2w+1 of points rational over $\mathbb{F}_{q^4}$; thus again $\mathcal{F}_{q+1}$ is the curve of largest genus attaining the Weil bound over $\mathbb{F}_{q^2}$. These properties of $\mathcal{F}_{q+1}$ over $\mathbb{F}_{q^2}$ are well-known, see for instance [Serre 1983a; 1984].

Since $\mathcal{X} \cong \mathcal{F}_4$ in characteristic 3, its group of automorphisms over $\mathbb{F}_9$ must accommodate both G and the 96-element group of automorphisms of $\mathcal{F}_4$ in characteristic zero. In fact $\mathrm{Aut}_{\mathbb{F}_9}(\mathcal{X})$ is the considerably larger group $\mathrm{U}_3(3)$ of order 6048, consisting of the unitary 3×3 matrices over $\mathbb{F}_9$; it is the largest automorphism group of any genus-3 cuver over an arbitrary field. Again this is a special case of the remarkable behavior of the "Hermitian curve" $\mathcal{F}_{q+1}/\mathbb{F}_{q^2}$: by regarding $x^qx+y^qy+z^qz$ as a ternary Hermitian form over $\mathbb{F}_{q^2}$ we see that any linear transformation of x,y,z which preserves this form up to scalar multiples also preserves the zero-locus (3.19); since of those transformations only multiples of the identity act trivially on $\mathcal{F}_{q+1}$, we conclude that the group $\mathrm{PGU}_3(q)$ acts on $\mathcal{F}_{q+1}$ over $\mathbb{F}_{q^2}$. Once $q>2$, this is the full $\overline{\mathbb{F}}_q$-automorphism group of $\mathcal{F}_{q+1}$, and is the only example of a group of order $>16w^4$ acting on a curve of genus $w>1$ (here $w=(q^2-q)/2$ and the group has order $q^3(q^2-1)(q^3+1)$) over an arbitrary field [Stichtenoth 1973].

Returning to the special case of $\mathcal{X}$, we note that the stabilizer in G of each of its 28 $\mathbb{F}_9$-rational points is a subgroup $N(H_3)\cong S_3$. Thus the two fixed points on $\mathcal{X}$ of H_3 collapse mod 3 to a single point; for each of the three involutions in S_3, this point is also the reduction of one of its four fixed points. Thus the 56- and 84-point G-orbits reduce mod 3 to the same 28-point orbit. The 24-point orbit is undisturbed, and is first seen in $\mathcal{X}(\mathbb{F}_{9^3})$; all other points of $\mathcal{X}$ in characteristic 3 have trivial stabilizer.

Since E_k is supersingular in characteristic 3, its ring of $\bar{\mathbb{F}}_3$-endomorphisms has rank 4 instead of 2; thus the Mordell–Weil lattice of $\bar{\mathbb{F}}_3$-maps from $\mathcal{X}$ to E_k

now has rank 12 instead of 6. Gross [1990, p. 957] used the action of $\mathrm{U}_3(3)$ on this lattice to identify it with the Coxeter–Todd lattice. This lattice has $756 = 63 \cdot 12$ minimal vectors of norm 4, which as before come from involutions of the curve; the count is higher than in characteristic zero because there are 63 involutions in $\mathrm{U}_3(3) = \mathrm{Aut}_{\bar{\mathbb{F}}_3} \mathcal{X}$ and 12 automorphisms of E_k, rather than 21 and 2 respectively. To see the new automorphisms, reduce (2.10) mod 3 to obtain $y^2 = x^3 + x$, with automorphisms generated by $(x, y) \mapsto (x + 1, y)$ and $(x, y) \mapsto (-x, iy)$ with $i^2 = -1$.

Adler [1997] found that the modular curve $X(11)$, with automorphism group $\mathrm{PSL}_2(\mathbb{F}_{11})$ in characteristic zero, has the larger automorphism group M_{11} when reduced mod 3. Once we identify $\mathcal{X}$ with the modular curve $X(7)$ in the next section we'll be able to regard its extra automorphisms mod 3 as a similar phenomenon. This quartic in characteristic 3 has another notable feature: each of its points is an inflection point! See [Hartshorne 1977, p. 305, Ex. 2.4], where the curve[13] is described as "funny" for this reason. (The 28 points of $\mathcal{X}(\mathbb{F}_9)$ are distinguished in that their tangents meet $\mathcal{X}$ with multiplicity 4 instead of 3; these fourfold tangents are the reductions mod 3 of the bitangents of $\mathcal{X}$ in characteristic zero.) Again Adler found in [1997] that $X(11)$, naturally embedded in the 5-dimensional representation of $\mathrm{PSL}_2(11)$, is also "funny" in this sense when reduced mod 3. While it is not reasonable to expect the extra automorphisms of $X(7)$ and $X(11)$ in characteristic 3 to generalize to higher modular curves $X(N)$ (the Mathieu group M_{11}, being sporadic, can hardly generalize), one might ask whether further modular curves are "funny" mod 3 or in other small characteristics.

Characteristic 7. The curve $\mathcal{X}$ even has good reduction in characteristic 7 over a large enough extension of $\mathbb{Q}$; that is, $\mathcal{X}$ has "potentially good reduction" mod 7. We can see this from our realization of $\mathcal{X}$ as a cyclic triple cover of E_k. The elliptic curve E_k has potentially good reduction mod 7, because the change of variable $x = \sqrt{-7}\, x_1$ puts its Weierstrass equation (2.10) in the form

$$(\sqrt{-7}\,)^{-3} y^2 = 4x_1^3 - 3\sqrt{-7}\, x_1^2 - 4x_1, \tag{3.21}$$

and over a number field containing $(-7)^{1/4}$ the further change of variable $y = 2(-7)^{3/4} y_1$ makes (3.21) reduce to $y_1^2 = x_1^3 - x_1$ at a prime above 7. [In general any CM elliptic curve has potentially good reduction at all primes; equivalently, the j-invariant of any CM curve is an algebraic integer.] Since the x-coordinates of the two branch points of the cover $\mathcal{X} \to E_k$ are the roots of (2.11), their x_1 coordinates are the roots of $\sqrt{-7} x_1^2 + x_1 = \sqrt{-7}$, one of which has negative 7-valuation while the other's 7-valuation is positive. Thus these points reduce to distinct points on $y_1^2 = x_1^3 - x_1$, namely the point at ∞ and the 2-torsion point $(0, 0)$, and the cover $\mathcal{X} \to E_k$ branched at those points has good reduction mod 7 as well.

[13] In its Klein model, but for once the distinction is irrelevant.

On the other hand, the homogeneous quartic defining $\mathcal{X}$ cannot have good reduction mod 7, even potentially: we have seen that even in the rational S_3 model the quartic invariant Φ_4 factors mod 7 as Φ_2^2. How can a plane quartic curve have good reduction if its defining equation becomes so degenerate?

This apparent paradox is resolved only by realizing that the moduli space of curves of genus 3 contains not only plane quartics but also hyperelliptic curves. While a non-hyperelliptic curve of genus 3 is embedded as a quartic in $\mathbb{P}^2$ canonically[14], the canonical map to $\mathbb{P}^2$ from a hyperelliptic curve of genus 3 is a double cover of a conic $C : Q_2 = 0$. Moreover, the moduli space of curves of genus 3 is connected, so a hyperelliptic curve S of genus 3 may be contained in a one-parameter family of curves of the same genus most of which are not hyperelliptic. In that case, the neighbors of S in the family are plane quartics $Q_4 = 0$ that approach the double conic $Q_2^2 = 0$ coming from S; if we write Q_4 as $Q_2^2 + \varepsilon Q_4' + O(\varepsilon^2)$ in a neighborhood of S then the branch points of the double cover $S \to C$ are the $2 \cdot 4 = 8$ zeros of Q_4' on C.[15] This means that a smooth plane quartic curve $Q_4 = 0$ may reduce to a hyperelliptic curve of genus 3 modulo a prime at which $Q_4 \equiv Q_2^2$. This is in fact the case for our curve $\mathcal{X}$, with $Q_4 = \Phi_4$ and $Q_2 = \Phi_2$: Serre found [Mazur 1986, p. 238, footnote] that, over an extension of k sufficiently ramified above $\wp_7$, the Klein quartic reduces to

$$v^2 = u^7 - u \tag{3.22}$$

at that prime, where u is a degree-1 function on the conic $\Phi_2 = 0$ in $\mathbb{P}^2$ that identifies this conic with $\mathbb{P}^1$. This reduced curve (3.22) inherits the action of G: a group element $\pm\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{F}_7)$ acts on (3.22) by

$$\pm\begin{pmatrix} a & b \\ c & d \end{pmatrix} : (u, v) \mapsto \left(\frac{au+b}{cu+d}, \frac{v}{(cu+d)^4}\right). \tag{3.23}$$

As in the case of characteristic 3, the group of automorphisms of the reduced curve properly contains G; here it is the direct product of G with the two-element group $(u, v) \mapsto (u, \pm v)$ generated by the hyperelliptic involution. Also as in characteristic 3, this reduced curve attains the upper or lower Weil bound on the number of points of a genus-3 curve over finite fields of even degree over the prime field. This is because the prime 7 is not split in k, so the reduction of E_k to an elliptic curve in characteristic 7 is supersingular. The supersingularity could also be seen directly from its Weierstrass model $y_2^2 = x_1^3 - x_1$; that the eigenvalues of Frobenius for $v^2 = u^7 - u$ over $\mathbb{F}_{49}$ all equal -7 could also be seen by counting points: since $(u^7 - u)/\sqrt{-1} \in \mathbb{F}_7$ for all $\mathbb{F}_{49}$, and $\sqrt{-1}$ is a square in $\mathbb{F}_{49}$, the preimages of each $u \in \mathbb{P}^1(\mathbb{F}_{49}) - \mathbb{P}^1(\mathbb{F}_7)$ are $\mathbb{F}_{49}$-rational, and these

[14]Here "canonically" means via curve's holomorphic differentials, which are sections of the canonical divisor; see for instance [Hartshorne 1977, p. 341].

[15]Thanks to Joe Harris for explaining this point; it should be well-known, but is not easy to find in the literature. Armand Brumer points out that this picture is explained in [Clemens 1980, pp. 155–157].

$2 \cdot 42 = 84$ points together with the 8 Weierstrass points $u \in \mathbb{P}^1(\mathbb{F}_7)$ add up to 92, which attains the Weil bound $49 + 6 \cdot 7 + 1$.

4. $\mathcal{X}$ as a Modular Curve

4.1. $\mathcal{X}$ as the modular curve $X(7)$. Since $G \cong \mathrm{PSL}_2(\mathbb{F}_7)$ we can realize G as the quotient group $\Gamma(1)/\Gamma(7)$, where $\Gamma(1)$ is the modular group $\mathrm{PSL}_2(\mathbb{Z})$ and $\Gamma(7)$ is the subgroup of matrices congruent to the identity mod 7. The following facts are well known: $\Gamma(1)$ acts on the upper half-plane $\mathcal{H} = \{\tau \in \mathbb{C} : \operatorname{Im} \tau > 0\}$ by fractional linear transformations $\pm\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : \tau \mapsto (a\tau + b)/(c\tau + d)$; the quotient curve $\mathcal{H}/\Gamma(1)$ parametrizes elliptic curves up to $\mathbb{C}$-automorphism; if we extend $\mathcal{H}$ by to $\mathcal{H}^*$ by including the "cusps" $\mathbb{Q} \cup \{\infty\} = \mathbb{P}^1(\mathbb{Q})$, the resulting quotient curve $X(1)$ may be regarded as a compact Riemann surface of genus 0; and for each $N \geq 1$, the quotient of $\mathcal{H}^*$ by the normal subgroup $\Gamma(N)$ of $\Gamma(1)$ is the modular curve $X(N)$ whose non-cusp points parametrize elliptic curves E with a full level-N structure. A "full level-N structure" means an identification of the group $E[N]$ of N-torsion points with some fixed group T_N. Why T_N and not simply $(\mathbb{Z}/N)^2$ as expected? We can certainly use $T_N = (\mathbb{Z}/N)^2$ if we regard $X(N)$ as a curve over an algebraically closed field such as $\mathbb{C}$. But that will not do over $\mathbb{Q}$ once $N > 2$: the *Weil pairing* (see for instance [Silverman 1986, III.8, pp. 95 ff.]) identifies $\wedge^2 E[N]$ with the N-th roots of unity $\boldsymbol{\mu}_N$, which are not contained in $\mathbb{Q}$. So T_N must be some group $\cong (\mathbb{Z}/N)^2$ equipped with an action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ such that $\wedge^2 T_N \cong \boldsymbol{\mu}_N$ as Galois modules. There are many choices for T_N — for instance, $E[N]$ for any elliptic curve $E/\mathbb{Q}$! — which in general yield different modular curves over $\mathbb{Q}$ (though they all become isomorphic over $\overline{\mathbb{Q}}$): T_N and T'_N yield the same curve only if $T'_N \cong T_N \otimes \psi$ for some quadratic character ψ. The simplest choice is

$$T_N = (\mathbb{Z}/N) \times \boldsymbol{\mu}_N, \tag{4.1}$$

and that is the choice that we shall use to define X_N as a curve over $\mathbb{Q}$. Note, however, that the action of $\Gamma(1)/\Gamma(N)$ is still defined only over the cyclotomic field $\mathbb{Q}(\boldsymbol{\mu}_N)$. The canonical map $X(N) \to X(1)$ that forgets the level-N structure is a Galois cover with group $\Gamma(1)/\Gamma(N) = \mathrm{PSL}_2(\mathbb{Z}/N)$; it is ramified only above three points of $X(1)$, namely the cusp and the elliptic points that parametrize elliptic curves with complex multiplication by $\mathbb{Z}[i]$ and $\mathbb{Z}[e^{2\pi i/3}]$, and the ramification indices at these points are N, 2, and 3 respectively.

Now consider $N = 7$. Then $X(7)$ is a G-cover of the genus-0 curve $X(1)$ with three branch points of indices $2, 3, 7$; therefore it is a Hurwitz curve, and thus isomorphic with $\mathcal{X}$ at least over $\mathbb{C}$. The 24-point orbit is the preimage of the cusp, and the 56- and 84-point orbits are the preimages of the elliptic points $\tau = e^{2\pi i/3}$ and $\tau = i$ on $X(1)$ parametrizing CM elliptic curves with j-invariants 0 and 1728. We shall show that the choice (4.1) of T_7 yields $X(7)$ as a curve over $\mathbb{Q}$ isomorphic with the Klein model of $\mathcal{X}$, and give explicitly an elliptic curve and 7-torsion points parametrized by a generic point $(x : y : z) \in \mathbb{P}^2$ with $x^3y + y^3z + z^3x = 0$.

The projective coordinates for $\mathcal{X}$ can be considered as a basis for $H_1(\mathcal{X})$. Holomorphic differentials on a modular curve $\mathcal{H}^*/\Gamma$ are differentials $f(\tau)\,d\tau$ on $\mathcal{H}^*$ that are regular and invariant under Γ, i.e. such that $f(\tau)$ is a *modular cusp form of weight* 2 for Γ: a holomorphic function satisfying the identity

$$f\Bigl(\frac{a\tau+b}{c\tau+d}\Bigr) = (c\tau+d)^2 f(\tau) \tag{4.2}$$

for all $\pm\bigl(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\bigr) \in \Gamma$ and vanishing at the cusps. We next choose a convenient basis for the modular cusp forms of weight 2 for $\Gamma(7)$.

Taking $\pm\bigl(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\bigr) = \pm\bigl(\begin{smallmatrix} 1 & 7 \\ 0 & 1 \end{smallmatrix}\bigr)$ in (4.2) we see that f must be invariant under $\tau \mapsto \tau + 7$; thus it has a Fourier expansion in powers of $q^{1/7}$, where as usual

$$q := e^{2\pi i\tau} \qquad \Bigl(\text{so}\quad d\tau = \frac{1}{2\pi i}\frac{dq}{q}\Bigr). \tag{4.3}$$

Since we require vanishing at the cusp $\tau = i\infty$, the expansion must involve only positive powers of $q^{1/7}$. The action of $g = \pm\bigl(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\bigr)$ on modular forms multiplies q by ζ; thus g decomposes our space of modular forms into eigen-subspaces with eigenvalues ζ^a, such that for each a mod 7 the ζ^a eigenspace consists of forms $\sum_{m>0} c_m q^{m/7}$ whose coefficients c_m vanish at all $m \not\equiv a$ mod 7. We find three such forms:

$$\begin{aligned}
\mathsf{x} &= q^{4/7}(-1 + 4q - 3q^2 - 5q^3 + 5q^4 + 8q^6 - 10q^7 + 4q^9 - 6q^{10} \cdots),\\
\mathsf{y} &= q^{2/7}(1 - 3q - q^2 + 8q^3 - 6q^5 - 4q^6 + 2q^8 + 9q^{10} \cdots),\\
\mathsf{z} &= q^{1/7}(1 - 3q + 4q^3 + 2q^4 + 3q^5 - 12q^6 - 5q^7 + 7q^9 + 16q^{10} \cdots).
\end{aligned} \tag{4.4}$$

These can be expressed as the modified theta series

$$\mathsf{x}, \mathsf{y}, \mathsf{z} = \sum_{\beta} \operatorname{Re}(\beta)\, q^{\beta\bar\beta/7}, \tag{4.5}$$

the sum extending over $\beta \in \mathbb{Z}[\alpha]$ congruent mod $(\sqrt{-7}\,)$ to $2, 4, 1$ respectively. They also have the product expansions

$$\mathsf{x}, \mathsf{y}, \mathsf{z} = \varepsilon q^{a/7} \prod_{n=1}^{\infty} (1-q^n)^3 (1-q^{7n}) \prod_{\substack{n>0 \\ n \equiv \pm n_0 \bmod 7}} (1-q^n), \tag{4.6}$$

where the parameters ε, a, n_0 are: for x, $-1, 4, 1$; for y, $+1, 2, 2$; and for z, $+1, 1, 4$. That these in fact yield modular forms can be seen by factoring the resulting products (4.6) into Klein forms (for which see for instance [Kubert and Lang 1981, pp. 25 ff. and 68 ff.]); it follows that $\mathsf{x}, \mathsf{y}, \mathsf{z}$ do not vanish except at the cusps of $X(7)$.

Since $\mathsf{x}, \mathsf{y}, \mathsf{z}$ are ζ^4-, ζ^2-, and ζ-eigenforms for g, the three-dimensional representation of G that they generate must be isomorphic with (V, ρ), and so the action of G on $X(7)$ will make it a quartic in the projectivization not of (V, ρ) but of (V^*, ρ^*).[16] Using either the sum or the product formulas for $\mathsf{x}, \mathsf{y}, \mathsf{z}$, together with the action of $\Gamma(1)$ on theta series or on Klein forms, we can compute that h cyclically permutes $\mathsf{x}, \mathsf{y}, \mathsf{z}$. This is enough to identify $(\mathsf{x}, \mathsf{y}, \mathsf{z})$ up to scaling with our standard basis for V (again thanks to the fact that the 21-element subgroup $\langle g, h\rangle$ of G acts irreducibly on V). This leads us to expect that

$$\Phi_4(\mathsf{x}, \mathsf{y}, \mathsf{z}) = \mathsf{x}^3\mathsf{y} + \mathsf{y}^3\mathsf{z} + \mathsf{z}^3\mathsf{x} = 0, \tag{4.7}$$

and the q-expansions corroborate this. To prove it we note that $\Phi_4(\mathsf{x}, \mathsf{y}, \mathsf{z})$, being a G-invariant polynomial in the cusp forms $\mathsf{x}, \mathsf{y}, \mathsf{z}$, must be a cusp form of weight $4 \cdot 2 = 8$ for the full modular group $\Gamma(1)$; but the only such form is zero. (See for instance [Serre 1973, Ch.VII] for the complete description of cusp forms on $\Gamma(1)$.) Thus the coordinates $(\mathsf{x} : \mathsf{y} : \mathsf{z})$ for the canonical image of $X(7)$ in $\mathbb{CP}^2$ identify it with the Klein model of $\mathcal{X}$.

We next identify the other G-invariant polynomials in $\mathsf{x}, \mathsf{y}, \mathsf{z}$ with known modular cusp forms for $\Gamma(1)$. We find that

$$\Phi_6(\mathsf{x}, \mathsf{y}, \mathsf{z}) = \Delta\ [= q\prod_{n=1}^{\infty}(1-q^n)^{24} = q - 24q^2 + 252q^3 \cdots], \tag{4.8}$$

which requires only checking the q^1 coefficient because every $\Gamma(1)$ cusp form of weight 12 is a multiple of Δ. Likewise the leading terms of $\Phi_{14}(\mathsf{x}, \mathsf{y}, \mathsf{z})$ and $\Phi_{21}(\mathsf{x}, \mathsf{y}, \mathsf{z})$, together with their weights 28, 42, suffice to identify these modular forms with

$$\Phi_{14}(\mathsf{x}, \mathsf{y}, \mathsf{z}) = \Delta^2 E_2\ [= \Delta^2\Big(1 + 240\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n}\Big) = q^2 + 192q^3 - 8280q^4 \cdots], \tag{4.9}$$

$$\Phi_{21}(\mathsf{x}, \mathsf{y}, \mathsf{z}) = \Delta^3 E_3\ [= \Delta^3\Big(1 - 504\sum_{n=1}^{\infty}\frac{n^5q^n}{1-q^n}\Big) = q^3 - 576q^4 + 22140q^5 \cdots]. \tag{4.10}$$

Thus the elliptic curve parametrized by a non-cusp point $(x : y : z)$ on $\mathcal{X}$ is

$$E_{(x:y:z)} :\ v^2 = u^3 - \tfrac{1}{48}\lambda^2\Phi_{14}(x, y, z) + \tfrac{1}{864}\lambda^3\Phi_{21}(x, y, z), \tag{4.11}$$

for some yet unknown λ of weight -14 (that is, homogeneous of degree -7 in x, y, z) that only changes $E_{(x:y:z)}$ by a quadratic twist.

To determine the values of u at 7-torsion points of $E_{(x:y:z)}$ we identify that curve with $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau) \cong \mathbb{C}^*/q^{\mathbb{Z}}$ and expand the Weierstrass $\wp$-function of that curve at some point $q_1 \in \mathbb{C}^*/q^{\mathbb{Z}}$ in a q-series depending on q_1. We find

$$u = \lambda\Delta\bigg(\frac{1}{12} - 2\sum_{n=1}^{\infty}\frac{q^n}{(1-q^n)^2} + \sum_{n=-\infty}^{\infty}\frac{q^nq_1}{(1-q^nq_1)^2}\bigg). \tag{4.12}$$

[16] This mildly unfortunate circumstance could only have been avoided by more awkward artifices such as declaring ζ to be $e^{-2\pi i/7}$ instead of $e^{+2\pi i/7}$ in (0.1). Of course the distinction between the V and V^* models of $\mathcal{X}$ is harmless because the two representations are related by an outer automorphism of G.

The 7-torsion points of $\mathbb{C}^*/q^{\mathbb{Z}}$ are generated by ζ and $q^{1/7}$. Substituting these for q_1 in (4.12) we obtain $\lambda P(\mathsf{x},\mathsf{y},\mathsf{z})$ for certain polynomials P of degree 7 determined up to multiples of Φ_4. We find P by comparing q-expansions. For $q_1=\zeta$ we obtain the symmetrical form

$$P = \tfrac{1}{7}\big((c_1-2c_2-\tfrac{53}{12})\mathsf{x}^7+(c_2-2c_4-\tfrac{53}{12})\mathsf{y}^7+(c_4-2c_1-\tfrac{53}{12})\mathsf{z}^7\big)$$
$$+\tfrac{2}{3}\big((c_2-c_4)\mathsf{x}^4\mathsf{y}^2\mathsf{z}+(c_4-c_1)\mathsf{y}^4\mathsf{z}^2\mathsf{x}+(c_1-c_2)\mathsf{z}^4\mathsf{x}^2\mathsf{y}\big), \quad (4.13)$$

using the abbreviation $c_j := \zeta^j+\zeta^{-j}\in K_+$. the polynomials for ζ^2,ζ^4 are obtained from these by cyclically permuting c_1,c_2,c_4 and $\mathsf{x},\mathsf{y},\mathsf{z}$. That only these six monomials can occur is forced by the invariance of the polynomial under $\langle g\rangle$. The polynomial for $q_1=q^{1/7}$ looks more complicated, because invariance under sgs is not so readily detectable; we refrain from exhibiting that polynomial in full, but note that it can be obtained from (4.13) by the linear substitution $\rho(s)$, and that its coefficients, unlike those of (4.13), are *rational*.[17]

It remains to choose λ. We would have liked to make it G-invariant, since the action of G would then preserve our model (4.11) for $E_{(x:y:z)}$ and only permute its 7-torsion points. But we cannot make λ an arbitrary homogeneous function of degree -7 in $\mathsf{x},\mathsf{y},\mathsf{z}$ because we are constrained by the condition that $E_{(x:y:z)}[7]\cong T_7$ for all non-cusp $(x:y:z)\in X(7)$. This means, first, that $E_{(x:y:z)}$ must be a nondegenerate elliptic curve, and second, that its 7-torsion group be generated by a rational point (for the $\mathbb{Z}/7$ part of T_7) and a point that every $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ element taking ζ to ζ^a multiplies by a (for the $\boldsymbol{\mu}_7$ part). The first condition amounts to the requirement that the divisor of λ be supported on the cusps of $X(7)$; this determines λ up to multiplication by a "modular unit" in $\mathbb{C}(X(7))$. The second condition then determines λ up to multiplication by the square of a modular unit. It turns out that already the first condition prevents us from choosing a G-invariant λ: such a λ would be Φ_{14}/Φ_{21} times a rational function of j, and thus would have zeros or poles on the elliptic points of order 2 and 3 (the 56- and 84-point orbits of $\mathcal{X}$).

We next find a λ, necessarily not G-invariant, that does the job. From our computation of u-coordinates at 7-torsion points we know that $u/\lambda\Delta$ is a polynomial $P(\mathsf{x},\mathsf{y},\mathsf{z})\in\mathbb{Q}[\mathsf{x},\mathsf{y},\mathsf{z}]$. Moreover

$$Q := P^3-\tfrac{1}{48}\Phi_{14}P+\tfrac{1}{864}\Phi_{21} \quad (4.14)$$

cannot vanish except at a cusp, lest a 7- and a 2-torsion point on $\mathbb{C}^*/q^{\mathbb{Z}}$ coincide. [In fact Q has the product expansion

$$q^{23/7}\prod_{n=1}^{\infty}\big((1-q^{n-\frac{6}{7}})(1-q^{n-\frac{1}{7}})\big)^{-8}\big((1-q^{n-\frac{5}{7}})^2(1-q^{n-\frac{2}{7}})\big)^2(1-q^n)^{84}, \quad (4.15)$$

[17] This is ultimately due to the fact that the coefficients of (4.12) are rational. In fact it is no accident the least common denominator of the coefficients of P for $q_1=q^{1/7}$ is 12, same as for (4.12); but we need not pursue this here.

which manifestly has neither zero nor pole in $X(7) - \{\text{cusps}\}$.] Thus for any λ_0 homogeneous of degree 14 in $\mathsf{x}, \mathsf{y}, \mathsf{z}$ whose divisor is supported on the cusps (for instance $\lambda_0 = \mathsf{x}^{14}$) we may take

$$\lambda = Q/\lambda_0^2, \tag{4.16}$$

which satisfies the first condition and yields a 7-torsion point on the curve (4.11) rational over $\mathbb{Q}(x, y, z)$.

We claim that this, together with our computations thus far, lets us deduce that λ also satisfies the second condition, and thus completes our proof that $X(7)$ is $\mathbb{Q}$-isomorphic with $\mathcal{X}$, as well as the determination of the 7-torsion points on the generic elliptic curve (4.11) parametrized by $\mathcal{X}$. We must show that $E[7]$ is isomorphic as a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ module with $T_7 = (\mathbb{Z}/7) \times \boldsymbol{\mu}_7$. Indeed, consider the action on $E[7]$ of an element γ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ that takes ζ to ζ^a. By our choice of λ, this γ fixes the point with $q_1 = q^{1/7}$; thus this point generates a subgroup $\cong \mathbb{Z}/7$ of $E[7]$. From our computation of (4.13) we see that γ multiplies the $q_1 = \zeta$ point by either a or $-a$. But the Weil pairing of the ζ and $q^{1/7}$ points is ζ, which γ takes to ζ^a. Thus γ must also take the $q_1 = \zeta$ point to ζ^a. In other words, the $q_1 \in \boldsymbol{\mu}_7$ points comprise a subgroup of $E[7]$ isomorphic as a Galois module with $\boldsymbol{\mu}_7$. Having found subgroups of $E[7]$ isomorphic with $\mathbb{Z}/7$ and $\boldsymbol{\mu}_7$, we are done.

4.2. The modular interpretation of quotients of $\mathcal{X}$. Now let H be a subgroup of G, and consider the quotient curve $\mathcal{X}/H$. When H is trivial, this quotient is $\mathcal{X}$ itself, which we have just identified with the moduli space $X(7)$ of elliptic curves with full level-7 structure. When $H = G$, the quotient is the moduli space $X(1)$ of elliptic curves with no further structure, and the quotient map $X(7) \to X(1)$ in effect forgets the level-7 structure. For intermediate groups H, the quotient curve, which can still be regarded also as the quotient of $\mathcal{H}^*$ by a congruence subgroup of $\Gamma(1)$, parametrizes elliptic curves with partial level-7 structure such as a choice of a 7-torsion point or 7-element subgroup. In this section we describe the three classical modular curves $X_0(7)$, $X_1(7)$, and $X_0(49)$ that arise in this way. The same constructions yield for each $N > 1$ the curves $X_0(N)$, $X_1(N)$, $X_0(N^2)$ as quotients of $X(N)$, though of course for each N we face anew the problem of finding explicit coordinates and equations for these modular curves and covers.

Each of the eight 7-element subgroups T of E (equivalently, of $E[7]$) yields an isogeny of degree 7 from E to the quotient elliptic curve E/T. The T's may be regarded as points of the projective line $(E[7] - \{\mathbf{0}\})/\mathbb{F}_7^* \cong \mathbb{P}^1(\mathbb{F}_7)$, permuted by G. The stabilizer in G of a point on this $\mathbb{P}^1(\mathbb{F}_7)$ is a 21-element subgroup; for instance, $\langle g, h\rangle$ is the stabilizer of ∞. Taking $H = \langle g, h\rangle$ we conclude that $\mathcal{X}/H$ parametrizes elliptic curves E together with a 7-element subgroup T, or equivalently together with a 7-isogeny $E \to E/T$. This $\mathcal{X}/H$ is the quotient of $\mathcal{H}^*$

by the subgroup

$$\Gamma_0(7) := \left\{ \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) : c \equiv 0 \bmod 7 \right\} \tag{4.17}$$

of $\Gamma(1)$, and is called the modular curve $X_0(7)$. This curve has genus 0, with rational coordinate ("Hauptmodul")

$$j_7 = \frac{1}{q} \left(\prod_{n=1}^{\infty} (1-q^n)/(1-q^{7n}) \right)^4 = q^{-1} - 4 + 2q + 8q^2 - 5q^3 - 4q^4 \cdots . \tag{4.18}$$

Comparing this with the product expansions for $\mathsf{x}, \mathsf{y}, \mathsf{z}, \Delta$, we may express j_7 as a quotient of $\langle g, h \rangle$-invariant sextics in $\mathsf{x}, \mathsf{y}, \mathsf{z}$:

$$j_7 = \frac{(\mathsf{xyz})^2}{\Delta} = \frac{(\mathsf{xyz})^2}{\Phi_6(\mathsf{x},\mathsf{y},\mathsf{z})}. \tag{4.19}$$

Either by comparing this with (2.13), or directly from the q-expansions, we then find that the degree-8 cover $X_0(7)/X(1)$ is given by

$$j = (j_7^2 + 13j_7 + 49)(j_7^2 + 245j_7 + 7^4)^3 / j_7^7. \tag{4.20}$$

Given a 7-isogeny $E \to E/T$, the image of $E[7]$ in E/T is a 7-element subgroup of E/T and thus yields a new 7-isogeny $E/T \to E/E[7] \cong E$. This is in fact the *dual isogeny* [Silverman 1986, p. 84 ff.] of the isogeny $E \to E/T$. Thus we have a rational map $w_7 : X_0(7) \to X_0(7)$ that takes a non-cusp point of $X_0(7)$, parametrizing an isogeny $E \to E/T$, to the point parametrizing the dual isogeny $E/T \to E$. Moreover, iterating this construction recovers our original isogeny $E \to E/T$; thus w_7 is an involution of $X_0(7)$. This w_7 is known as the *Fricke involution* of $X_0(7)$. In general $X_0(N) = \mathcal{H}^*/\Gamma_0(N)$ parametrizes N-isogenies with cyclic kernel (a.k.a. "cyclic N-isogenies") between elliptic curves, and the dual isogeny yields the Fricke involution w_N of $\mathcal{X}_0(N)$. This involution can also be described over $\mathbb{C}$ as the action of the fractional linear transformation $\tau \leftrightarrow -1/N\tau$ on $\mathcal{H}^*$, which descends to an automorphism of $X_0(N)$ because it normalizes $\Gamma_0(N)$. In our case of $N = 7$ we find the formula

$$w_7(j_7) = 49/j_7 \tag{4.21}$$

for the action of w_7 on $X_0(7)$. The coefficients of the curve E/T and the 7-isogenies $E \rightleftharpoons E/T$ parametrized by $X_0(7)$ can be computed as explicit functions of j_7 by the methods of [Elkies 1998a].

The modular curve $X_1(7)$ parametrizes elliptic curves with a rational 7-torsion point. It is thus the quotient of $X(7)$ by the subgroup of G that fixes a 7-torsion point. To obtain this modular curve, and the elliptic curve it parametrizes, over $\mathbb{Q}$, we must be careful to use a 7-torsion point that generates the subgroup $\mathbb{Z}/7$ of T_7: we have already computed in (2.2) the quotient of $\mathcal{X}$ by the 7-element subgroup $\langle g \rangle$ of G, which is the stabilizer of a 7-torsion point; but this is the point (4.13), which generates the subgroup $\boldsymbol{\mu}_7$ of T_7, and so is not rational over $\mathbb{Q}$.

The $\mathbb{Z}/7$ subgroup has stabilizer $\langle sgs \rangle$, so we may obtain $X_1(7)$ as $X(7)/\langle sgs \rangle$. Alternatively we may start from $X(7)/\langle g \rangle$ and apply w_7. This second approach requires some explanation. At the level of Riemann surfaces, there is no problem: for any $N > 1$, the modular curve $X_1(N)$ is $\mathcal{H}^*/\Gamma_1(N)$ where

$$\Gamma_1(N) := \left\{ \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) : c \equiv 0,\ a, d \equiv 1 \bmod N \right\}, \tag{4.22}$$

and again $\tau \leftrightarrow -1/N\tau$ normalizes this subgroup and so yields an involution of $X_1(N)$. But over $\mathbb{Q}$ some care is required. The curve $X_1(N)$ parametrizes pairs (E, P) where E is an elliptic curve and $P \in E$ is a point of order N. The involution takes (E, P) to (E', P'), where $E' = E/\langle P \rangle$ and P' generates the image of $E[N]$ under the quotient map $E \to E'$. But to specify the generator we must use the Weil pairing: P' must be the image of a point $\tilde{P} \in E[N]$ whose Weil pairing with P is $e^{2\pi i/N}$. Once $N > 2$ the root of unity $e^{2\pi i/N}$ is not rational, so we cannot demand that both P and P' be rational N-torsion points on E, E'. Instead, P, P' must generate Galois modules such that $\langle P \rangle \otimes \langle P' \rangle \cong \boldsymbol{\mu}_N$. So, for instance, if P is rational then $\langle P' \rangle \cong \boldsymbol{\mu}_N$, and conversely if $\langle P \rangle \cong \boldsymbol{\mu}_N$ then P' is rational. The latter case applies for us: in our model of $X(7)$, the distinguished 7-torsion points on the elliptic curve E parametrized by $X(7)/\langle g \rangle$ constitute a subgroup $\cong \boldsymbol{\mu}_7$ of $E[7]$; thus the curve E' has a rational 7-torsion point.

Using $\mathcal{X}/\langle g \rangle$ for $X_1(7)$, we find that this modular curve has rational coordinate

$$d := \frac{\mathsf{y}^2\mathsf{z}}{\mathsf{x}^3} = q^{-1} + 3 + 4q + 3q^2 - 5q^4 - 7q^5 - 2q^6 + 8q^7 \cdots, \tag{4.23}$$

and that the cyclic cubic cover $X_1(7) \to X_0(7)$ is given by

$$\jmath_7 = d + \frac{1}{1-d} + \frac{d-1}{d} - 8 = \frac{d^3 - 8d^2 + 5d + 1}{d^2 - d}. \tag{4.24}$$

The elliptic curve with a 7-torsion point parametrized by $X_1(7)$ was already exhibited in extended Weierstrass form by Tate [1974, p. 195]:

$$y^2 + (1 + d - d^2)xy + (d^2 - d^3)y = x^3 + (d^2 - d^3)x^2 \tag{4.25}$$

(we chose our coordinate d so as to agree with this formula). Besides making the coefficients simpler compared to the standard Weierstrass form $y^2 = x^3 + a_4x + a_6$, Tate's formula has the advantage of putting the origin at a 7-torsion point — Tate actually obtained (4.25) starting from a generic elliptic curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 \tag{4.26}$$

tangent to the x-axis at the origin, and working out the condition for the origin to be a 7-torsion point. The equations for the curve 7-isogenous with (4.25) can again be obtained by the methods of [Elkies 1998a], or — since here the points of the isogeny's kernel are rational — already from Vélu's formulas [Vélu 1971] on which those methods are based.

From our discussion in the previous paragraph, the involution w_7 of $X_1(7)$ cannot be defined over $\mathbb{Q}$, only over K_+. (The full cyclotomic field K is not needed because $X_1(7)$ cannot distinguish a 7-torsion point from its inverse, so only the squares in $(\mathbb{Z}/7)^* = \mathrm{Gal}(K/\mathbb{Q})$ are needed, and they comprise $\mathrm{Gal}(K_+/\mathbb{Q})$; in general for each prime $p \equiv 3 \bmod 4$ the Fricke involution w_p of $X_1(p)$ is defined over the real subfield of the cyclotomic field $\mathbb{Q}(e^{2\pi i/p})$.) In fact there are three choices of w_7, cyclically permuted by $\Gamma_0(7)/\Gamma_1(7)$ (and $\mathrm{Gal}(K_+/\mathbb{Q})$); we calculate that the choice associated with $\tau \leftrightarrow -1/7\tau$ gives

$$w_7(d) = \frac{(4+3c_1+c_2)d - (3+3c_1+c_2)}{d-(4+3c_1+c_2)}, \tag{4.27}$$

where $c_j := \zeta^j + \zeta^{-j} \in K_+$ as in (4.13).

We have seen already that $\mathcal{X}/\langle h\rangle$ coincides with $X_0(49)$, and hinted that this is in fact no mere coincidence. We can now explain this: where a point on $X(7)$ specifies an elliptic curve E together with a basis $\pm\{P_1, P_2\}$ for $E[7]$, the $\langle h\rangle$-orbit of the point specifies only the two subgroups $\langle P_1\rangle$ and $\langle P_2\rangle$ generated by the basis elements. Equivalently, it specifies two elliptic curves $E_1 = E/\langle P_1\rangle$, $E_2/\langle P_2\rangle$ among the eight curves 7-isogenous with E. (Note that $\langle h\rangle$ is the stabilizer in $\mathrm{PSL}_2(\mathbb{F}_7)$ of the two points $0, \infty$ on $\mathbb{P}^1(\mathbb{F}_7)$.) But then we obtain a cyclic 49-isogeny $E_1 \to E_2$ by composing the isogenies $E_1 \to E$, $E \to E_2$. Conversely, any cyclic 49-isogeny between elliptic curves factors as a product of two 7-isogenies and thus comes from a point $\mathcal{X}/\langle h\rangle$. Thus $\mathcal{X}/\langle h\rangle$ is indeed the modular curve $X_0(49)$ parametrizing cyclic 49-isogenies. In this description of $X_0(49)$, the involution w_{49} of $\mathcal{X}/\langle h\rangle$ is the involution we have already constructed from the normalizer of $\langle h\rangle$ in G. Note that w_{49} switches the roles of E_1, E_2 but preserves E. In terms of congruence subgroups of $\Gamma(1)$, the identification of $\mathcal{X}/\langle h\rangle$ with $X_0(49)$ is explained by noting that the congruence groups $\bigl\{\pm\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{Z}) : b, c \equiv 0 \bmod 7\bigr\}$ and $\Gamma_0(49)$ are conjugate in $\mathrm{PSL}_2(\mathbb{R})$ by $\pm 7^{-1/2}\left(\begin{smallmatrix} 7 & 0 \\ 0 & 1\end{smallmatrix}\right) : \tau \mapsto 7\tau$.

Some final remarks on this curve $E_k = \mathcal{X}/\langle h\rangle = X_0(49)$: recall that we showed that its only $\mathbb{Q}$-rational points are the point at infinity and $(0,0)$. Since these are both cusps of $X_0(49)$ we conclude that there are no elliptic curves over $\mathbb{Q}$ admitting a rational cyclic 49-isogeny. However, there are infinitely many number fields, including quadratic ones such as $\mathbb{Q}(i)$ and $\mathbb{Q}(e^{2\pi i/3}) = \mathbb{Q}(\sqrt{-3})$, over which E_k is an elliptic curve of positive rank. (Take $x = -2$ or $x = -3$ in the Weierstrass equation (2.10) for E_k.) Over such a number field there are infinitely many pairs of elliptic curves with different j-invariants that admit a rational cyclic 49-isogeny. Moreover 49 is the largest integer for which this can happen: the curve $X_0(N)$ for $N > 49$ has genus > 1, and thus by Faltings only finitely many points over any given number field. See the tables and introductory remarks of [Birch and Kuyk 1975] for more information on the genera and rational points of the modular curves $X_0(N)$.

4.3. Kenku's proof of the solution of the class number 1 problem. What of the quotients of $\mathcal{X}$ by S_4 and the 2-Sylow subgroup of G? The first of these we calculate using the fact that $\pm\rho(S_4)$ is itself a reflection group, with invariant ring generated by polynomials of degrees $2, 4, 6$; we choose the elementary symmetric functions of X^2, Y^2, Z^2 as our generators:

$$\Psi_2 := X^2 + Y^2 + Z^2, \quad \Psi_4 := (XY)^2 + (XZ)^2 + (YZ)^2, \quad \Psi_6 := (XYZ)^2. \tag{4.28}$$

We then express a basis for the G-invariants in the S_4 model as polynomials in Ψ_2, Ψ_4, Ψ_6. Clearly the invariant quartic (1.11) is $\Psi_2^2 + (3\alpha - 2)\Psi_4$. The degree-6 invariant is proportional to $(1+\alpha)\Psi_2^3 + (2-3\alpha)\Psi_2\Psi_4 - (42+7\alpha)\Psi_6$. The determinant (1.14) defining the degree-14 invariant is proportional to

$$\begin{aligned}&(-9+9\alpha)\Psi_2^7 + (56-70\alpha)\Psi_2^5\Psi_4 - (294+105\alpha)\Psi_2^3\Psi_4^2 + (28+154\alpha)\Psi_2\Psi_4^3 \\ &\quad + \Psi_6\big((1008+2198\alpha)\Psi_2^4 + (1148-7014\alpha)\Psi_2^2\Psi_4 + (-12348+1078\alpha)\Psi_4^2\big) \\ &\qquad\qquad + (15778 + 15435\alpha)\Psi_2\Psi_6^2.\end{aligned} \tag{4.29}$$

Now the genus-0 curve $\mathcal{X}/S_4$ is rationally parametrized by the function $f := \Psi_2^3/\Psi_6$, which is of degree 24 on $\mathcal{X}$ and thus of degree 1 on $\mathcal{X}/S_4$. So to obtain the degree-7 cover $\mathcal{X}/S_4 \to \mathcal{X}/G$ we need only write the rational parameter Φ_{14}^3/Φ_6^7 of $\mathcal{X}/G$ as a rational function of Ψ_2^3/Ψ_6 on $\mathcal{X}$. Since $\Psi_2^2 = (2-3\alpha)\Psi_4$ on $\mathcal{X}$, our expressions for the G-invariant polynomials of degrees $6, 14$ simplify to multiples of

$$\Psi_2^3(1 + (-14+7\alpha)f), \quad \Psi_2^7\big(3 + (490+196\alpha)f + (3430+2401\alpha)f^2\big). \tag{4.30}$$

Thus $j = \Phi_{14}^3/\Phi_6^7$ is given by

$$2^6\big(3 + (490+196\alpha)f + (3430+2401\alpha)f^2\big)^3 \big/ \big(1 + (-14+7\alpha)f\big)^7, \tag{4.31}$$

in which the coefficient 2^6 may either be obtained by keeping track of all the constants of proportionality along the way, or by requiring that the third point of ramification of j (other than the points $j = 0, \infty$ forced by the factorization in (4.18)) occur at $j = 12^3$. To put (4.31) in a nicer form we replace f by the equivalent coordinate ψ, related with f by

$$f = \frac{(\alpha+3)\psi + 14 + 26\alpha}{56(\psi + 3(1+\alpha))}, \tag{4.32}$$

which puts the pole of j at $\psi = \infty$ and thus makes j a seventh-degree polynomial in ψ:

$$\begin{aligned} j &= \big(\psi - 3(1+\alpha)\big)\big(\psi - (2+\alpha)\big)^3\big(\psi + (3+2\alpha)\big)^3 \\ &= 12^3 + \big(\psi + (2+4\alpha)\big)\big(\psi^2 + 2\alpha\psi - (6+9\alpha)\big)\big(\psi^2 - 2(1+\alpha)\psi + (1-2\alpha)\big)^2. \end{aligned} \tag{4.33}$$

We noted already that the S_4 model of $\mathcal{X}$ cannot be defined over $\mathbb{Q}$ because S_4 is its own normalizer in $\mathrm{Aut}(G)$. For the same reason this polynomial (4.33) cannot have rational coefficients. Over a number field F containing k, we may choose a conjugacy class of subgroups $S_4 \subset G$, and then depending on our choice either

(4.33) or its $\mathrm{Gal}(k/\mathbb{Q})$ conjugate parametrizes elliptic curves E/F such that $\mathrm{Gal}(\bar{F})/F$ acts on $E[7]$ by a subgroup of a 24-element group in that conjugacy class.[18]

On the other hand, the 8-element dihedral subgroups D_8 of G do extend to 16-element subgroups of $\mathrm{Aut}(G)$. This is a consequence of Sylow theory, but the subgroups in question can also be seen from the interpretation of G and $\mathrm{Aut}(G)$ as $\mathrm{PSL}_2(\mathbb{F}_7), \mathrm{PGL}_2(\mathbb{F}_7)$: choose an identification of $\mathbb{F}_7^2$ with $\mathbb{F}_{49}$, and consider the action of $\Gamma\mathrm{L}_1(\mathbb{F}_{49})$ on $\mathbb{F}_{49}$. Multiplication by some $a \in \mathbb{F}_{49}^*$ and Galois conjugation are $\mathbb{F}_7$-linear transformations of determinant a^8 and -1 respectively. Using only $\mathbb{F}_{49}^*$ we obtain cyclic subgroups of orders 4, 8 in $\mathrm{PSL}_2(\mathbb{F}_7)$ and $\mathrm{PGL}_2(\mathbb{F}_7)$, the *nonsplit Cartan subgroups* of these linear groups; allowing also Galois conjugation, we obtain the normalizers of the nonsplit Cartan subgroups, which are 8- and 16-element dihedral groups and are the 2-Sylow subgroups of $\mathrm{PSL}_2(\mathbb{F}_7)$, $\mathrm{PGL}_2(\mathbb{F}_7)$ respectively. Since $D_8 \subset G$ is normalized by outer automorphisms of G, the quotient of $\mathcal{X}/D_8$ can be defined over $\mathbb{Q}$ — even though it factors through the quotient by S_4, which is only defined over k! To obtain that quotient as a degree-3 cover of the ψ-line we may either proceed as we did to obtain (4.33), namely, writing Ψ_2, Ψ_4, Ψ_6 in terms of the invariants of D_8, or locate the ramification points of the cover. This triple cover is totally ramified at the simple root $\psi = 3(1+\alpha)$ of j, and has double points at the solutions of $\psi^2 + 2\alpha\psi = (6+9\alpha)$ at which $j = 12^3$. We find that the cover is given by

$$\psi = \frac{(2+3\alpha)\phi^3 - (18+15\alpha)\phi^2 + (42+21\alpha)\phi + (14+7\alpha)}{\phi^3 - 7\phi^2 + 7\phi + 7}, \tag{4.34}$$

in which we chose the degree-1 function ϕ on $\mathcal{X}/D_8$ so that $j \in \mathbb{Q}(\phi)$:

$$\begin{aligned} j &= 64\frac{\big(\phi(\phi^2+7)(\phi^2-7\phi+14)(5\phi^2-15\phi-7)\big)^3}{(\phi^3-7\phi^2+7\phi+7)^7} \\ &= 12^3 + 56^2\frac{(\phi-3)(2\phi^4-14\phi^3+21\phi^2+28\phi+7)P^2(\phi)}{(\phi^3-7\phi^2+7\phi+7)^7}, \end{aligned} \tag{4.35}$$

where $P(\phi)$ is the polynomial

$$P(\phi) = (\phi^4 - 14\phi^2 + 56\phi + 21)(\phi^4 - 7\phi^3 + 14\phi^2 - 7\phi + 7). \tag{4.36}$$

In the modular setting ϕ parametrizes elliptic curves E such that the Galois action on $E[7]$ is contained in a subgroup $D_8 \subset G$, i.e. by the normalizer of a nonsplit Cartan subgroup; we thus refer to the ϕ-line as the modular curve $X_n(7)$.

---

[18] Note that, since $F \supseteq k$, any $\gamma \in \mathrm{Gal}(\bar{F})/F$ must take ζ to one of ζ, ζ^2, ζ^4; thus the determinant of its action on $E[7]$ is a square in $\mathbb{F}_7^*$. Thus γ acts on $E[7]$ by a scalar multiple of a unimodular $\mathbb{F}_7$-linear transformation of $E[7]$, and may be regarded as an element of $\mathrm{PSL}_2(\mathbb{F}_7) \cong G$.

Kenku [1985] used this curve to obtain a novel proof of the Stark–Heegner theorem, which states that the only quadratic imaginary fields with unique factorization are $\mathbb{Q}(\sqrt{D})$ with $D = -3, -4, -7, -8, -11, -19, -43, -67, -163$. Let $F = \mathbb{Q}(\sqrt{D})$ be a quadratic imaginary field of discriminant $D < 0$ and class number 1. There is then an elliptic curve $E/\mathbb{Q}$ with CM by O_F, unique up to $\bar{\mathbb{Q}}$-isomorphism. Assume that the prime 7 is inert in F; this certainly happens if $|D| > 28$, else the prime(s) above 7 in F cannot be principal. (The fields with $D = -4, -8, -11$ also satisfy this condition.) Then the action of O_F on $E[7]$ gives $E[7]$ the structure of a one-dimensional vector space over $\mathbb{F}_{49}$, and $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ must respect this structure. Thus E yields a rational point of $X_n(7)$. But this point is constrained by the condition that $j_E \in \mathbb{Z}$. That is, $\phi = \phi(E)$ must be a rational number such that $j(\phi)$, given by (4.35), is an integer. Writing $\phi = m/n$ in lowest terms, we find $j(\phi) = A(m,n)/B(m,n)$ with A, B homogeneous polynomials of degree 21 without common factors. Thus $\gcd(A(m,n), B(m,n))$ is bounded given $\gcd(m,n) = 1$; one may calculate that this gcd is a factor of 56^7, and thus that $m^3 - 7m^2n + 7mn^2 + 7n^3$ divides 56. Thus if m, n are at all large then m/n must be a very good rational approximation to one of the roots $3 + 4\cos 2a\pi/7$ ($a \in \mathbb{F}_7^*$) of $\phi^3 - 7\phi^2 + 7\phi + 7$. In the present case Kenku was able to list all $\phi \in \mathbb{Q}$ such that $j(\phi) \in \mathbb{Z}$ using Nagell's list [1969] of the solutions of $x + y = 1$ in units x, y of K_+. The list can also be obtained from general bounds on rational approximation, provided all the constants are given explicitly as they are in [Bugeaud and Győry 1996]. For our specific problem of approximating elements of $K_+ \setminus \mathbb{Q}$, much better results are available, which make the computation easily tractable; for instance Michael Bennett reports that the methods of [Bennett 1997] yield the bound $\left|\cos(\pi/7) - p/q\right| > 0.099q^{-7/3}$ for all nonzero $p, q \in \mathbb{Z}$, which is more than enough to find all solutions of $|m^3 - 7mn^2 + 7mn^2 + n^3| \leq 56$. We find that the list of integral points on $X_n(7)$, however obtained, consists of the points with

$$\phi \in \left\{0, \infty, 1, -1, 2, 3, 5, -\tfrac{3}{5}, 7, \tfrac{7}{3}, \tfrac{11}{2}, \tfrac{19}{9}\right\}. \tag{4.37}$$

Of the resulting integral values of $j(\phi)$, the first eight are j-invariants of CM elliptic curves, with discriminant -3, -8, -11, -16, -67, -4, -43, -163 respectively. (The discriminant -3 occurs even though 7 is split in $\mathbb{Q}(\sqrt{-3}\,)$ thanks to the cube roots of unity in $\mathbb{Q}(\sqrt{-3}\,)$, which yield extra automorphisms of a curve of j-invariant zero; $D = -16$ occurs because the order $\mathbb{Z}[2i] \in \mathbb{Q}(i)$ still has unique factorization.) It is easy to check that none of the remaining four values $j = 10^3 7^5$, $2^{15} 7^5$, $2^6 11^3 23^3 149^3 269^3$, $2^9 17^6 19^3 29^3 149^3$ can be the j-invariants of a CM curve, and this completes Kenku's proof that the list of imaginary quadratic fields of class number 1 is complete.

[We remark that Siegel [1968] had already given a similar proof of the Stark–Heegner theorem using $X_n(5)$ together with the condition that j_E is a cube, which is tantamount to using the degree-30 cover of $X(1)$ by $X_n(15)$. An amusing feature of Siegel's argument which I have not seen mentioned elsewhere is that the Diophantine equation for an integral point on $X_n(15)$ is equivalent to the condition that a Fibonacci number be a perfect cube, and thus that Siegel in effect reduced the Stark–Heegner theorem to the fact that the only such Fibonacci numbers are $0, \pm 1, \pm 8$.]

What of the four discriminants $D = -3, -12, -19, -27$ of imaginary quadratic orders with unique factorization in which 7 splits? Let E be an elliptic curve with CM by the order of discriminant $-D$. The primes above 7 yield a distinguished pair of 7-element subgroups of E, which must be respected by the Galois group. Thus j_E lifts to a rational point on the quotient of $X(7)$ by the normalizer of the *split Cartan group* of diagonal matrices. In our case the split Cartan group is $\langle h \rangle$, and its normalizer is $\langle h, s \rangle$, so we know these quotient curves already. Since S_4 contains the normalizers of both the split and the non-split Cartan groups (note that $p = 7$ is the largest case in which $\mathrm{PSL}_2(\mathbb{F}_p)$ has a proper subgroup containing Cartan normalizers of both kinds), the j-invariant of a CM curve lifts to a rational point of $X(7)/S_4$ in both the split and inert cases. These points (necessarily rational only over k, since $X(7)/S_4$ is not defined over $\mathbb{Q}$) are as follows:

D	-3	-4	-8	-11	-12
x	$2+\alpha, 3+3\alpha, -3-2\alpha$	$-4-2\alpha$	$2+3\alpha$	$5+2\alpha$	$-3+\alpha$

D	-16	-19	-27	-43	-67	-163
x	$6+4\alpha$	$5-2\alpha$	$-3+6\alpha$	$-3-14\alpha$	$42+13\alpha$	$-283-182\alpha$

This accounts for all but two of the thirteen rational j-invariants. The remaining rational j's have $D = -7$ and $D = -28$; these are the j-invariants -15^3, 255^3 of the curves E_k, E'_k, for which 7 is ramified in the CM field $\mathbb{Q}(\sqrt{D})$, a.k.a. k. These two j's lift to rational points not on $X(7)/S_4$ but on $X_0(7)$, in fact to the fixed points $j_7 = -7$ and $j_7 = +7$ of the involution w_7.

4.4. $\mathcal{X}$ as a Shimura curve. Our identification of $\mathcal{X}$ with $X_0(7) = \mathcal{H}^*/\Gamma_0(7)$ identifies $\Gamma_0(7)$ with the fundamental group not of $\mathcal{X}$ but of $\mathcal{X}$ punctured at the 24-point orbit. We have seen already that in the hyperbolic uniformization of $\mathcal{X}$ the fundamental group $\pi_1(\mathcal{X})$ becomes a normal subgroup of the triangle group $G_{2,3,7}$. Remarkably this too is an arithmetic group: let

$$c = \zeta + \zeta^{-1} = 2\cos(2\pi/7), \tag{4.38}$$

so $O_{K_+} = \mathbb{Z}[c]$; then there exist matrices $i, j \in \mathrm{GL}_2(\mathbb{R})$ such as $c^{1/2}\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ and $c^{1/2}\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$ with

$$i^2 = j^2 = c \cdot \mathbf{1}, \quad ij = -ji \tag{4.39}$$

(this determines i, j uniquely up to $\mathrm{GL}_2(\mathbb{R})$ conjugation) such that $G_{2,3,7}$ consists of the images in $\mathrm{PSL}_2(\mathbb{R})$ of $\mathbb{Z}[c]$-linear combinations of $\mathbf{1}, i, j', ij'$ whose determinant equals 1. Here

$$j' := \tfrac{1}{2}\bigl(1 + ci + (c^2 + c + 1)j\bigr), \tag{4.40}$$

and the determinant of $a_1\mathbf{1} + a_2 i + a_3 j + a_4 ij$ $(a, b, c, d \in \mathbb{R})$ is

$$a_1^2 - ca_2^2 - ca_3^2 + c^2a_4^2. \tag{4.41}$$

For instance, $G_{2,3,7}$ is generated by the images in $\mathrm{PSL}_2(\mathbb{R})$ of

$$\begin{gathered} g_2 := ij/c, \qquad g_3 := \tfrac{1}{2}\bigl(1 + (c^2 - 2)j + (3 - c^2)ij\bigr), \\ g_7 := \tfrac{1}{2}\bigl(c^2 + c - 1 + (2 - c^2)i + (c^2 + c - 2)ij\bigr), \end{gathered} \tag{4.42}$$

with $g_2^2 = g_3^3 = g_7^7 = -1$ and $g_2 = g_7 g_3$. (Note that "$g_2 = ij/c$" is legitimate since c is a unit.] Shimura [1967] found that the quotients of $\mathcal{H}$ by arithmetic groups or their congruence subgroups also have modular interpretations, analogous to the interpretation of $\mathcal{H}^*/\Gamma(N)$ as the moduli space for elliptic curves with full level-N structure. The objects parametrized by Shimura's modular curves are more complicated than elliptic curves; for instance $\mathcal{X}$ and $\mathcal{X}/G$ parametrize families of principally polarized abelian varieties of dimension 6. These abelian sixfolds can be described precisely, but there is as yet no hope of presenting them explicitly enough to derive formulas for the sixfold parametrized by a given point of $\mathcal{X}/G$ or of $\mathcal{X}$. Still these curves hold a place in number theory comparable to that of the classical modular curves coming from congruence subgroups of $\Gamma(1)$, and limited computational investigation of these curves is now feasible (see for instance [Elkies 1998b]). For the our present purposes we content ourselves with describing the specific arithmetic groups and moduli problems connected with the Klein quartic, referring the reader to [Vignéras 1980] for the arithmetic of quaternion algebras over number fields in general, and to [Vignéras 1980; Shimura 1967] for their associated Shimura modular curves.

The K_+-algebra A generated by i, j is a *quaternion algebra* over K_+: a simple associative algebra with unit, containing K_+, such that K_+ is the center of A and $\dim_{K_+} \mathsf{A} = 4$. The ring $\mathcal{O} = O_{K_+}[i, j'] \subset \mathsf{A}$ is a maximal order in A. For each of the three real places v of K_+ we may form a quaternion algebra over $\mathbb{R}$ by tensoring A with $(K_+)_v \cong \mathbb{R}$. It is known that a quaternion algebra over $\mathbb{R}$ is isomorphic with either the algebra $M_2(\mathbb{R})$ of 2×2 real matrices, or with the Hamilton quaternions $\mathbb{H}$. We have seen that in our chosen real embedding of K_+, taking c to $2\cos(2\pi/7)$, the algebra $\mathsf{A} \otimes_{K_+} (K_+)_v$ is $M_2(\mathbb{R})$; for the other two places, in which c is $2\cos(4\pi/7)$ and $2\cos(8\pi/7)$, that algebra is isomorphic with $\mathbb{H}$ because then $i^2, j^2 < 0$. It is known that if a quaternion algebra over a number field F becomes isomorphic with $M_2(\mathbb{R})$ over at least one of F's real places then the maximal order $\mathcal{O}$ is unique up to conjugation in the algebra; moreover, that if (as in our case) there is exactly one such place and F is totally real then the group of units of norm 1 in $\mathcal{O}^* \hookrightarrow \mathrm{GL}_2(\mathbb{R})$ yields a co-compact subgroup $\Gamma \cong \mathcal{O}^*/\{\pm 1\}$ of $\mathrm{PSL}_2(\mathbb{R})$, and thus a compact Riemann surface "$X(1)$" $:= \mathcal{H}/\Gamma$, except in the classical case of the algebra $M_2(\mathbb{Q})$ over $\mathbb{Q}$. Since all maximal orders are conjugate, the resulting curve does not depend on the choice of maximal order $\mathcal{O}$. As a modular curve, "$X(1)$" parametrizes principally polarized abelian varieties of dimension $2[K:\mathbb{Q}]$ (= 6 in our case) with endomorphisms by $\mathcal{O}$. This means that the curve "$X(1)$", though constructed transcendentally, is defined over some number field; in our case that field may even be taken to be $\mathbb{Q}$ thanks to the facts that K_+ has unique factorization and is Galois over $\mathbb{Q}$. Since for us $\Gamma \cong G_{2,3,7}$, this curve is rational: the quotient of $\mathcal{H}$ by any triangle group has genus zero.

Our quaternion algebra A over K_+ has the remarkable property that, for each *finite* place v of K_+, the quaternion algebra $\mathsf{A} \otimes_{K_+} (K_+)_v$ over $(K_+)_v$ is isomorphic with $M_2((K_+)_v)$. (In other words, A is *unramified* at each finite prime v.) Using this isomorphism, one may define arithmetic subgroups of Γ and modular curves covering "$X(1)$" analogous to the classical modular curves $X(N)$, $X_0(N)$ etc. For instance if $\wp$ is a prime of O_K then the units of $\mathcal{O}$ congruent to 1 mod $\wp$ constitute a normal subgroup of $\mathcal{O}^*$ that maps to a normal subgroup $\Gamma(\wp)$ of Γ. Thanks to the isomorphism of $\mathsf{A} \otimes_{K_+} (K_+)_v$ with $M_2((K_+)_v)$ we have $\Gamma/\Gamma(\wp) \cong \mathrm{PSL}_2(k_\wp)$ [where $k_\wp$ is the residue field $O_{K_+}/\wp$ of $\wp$]. The Riemann surface "$X(\wp)$" $:= \mathcal{H}/\Gamma(\wp)$ is then a normal cover of "$X(1)$" with Galois group $\mathrm{PSL}_2(k_\wp)$. This too is a Shimura modular curve, parametrizing principally polarized abelian sixfolds with endomorphisms by $\mathcal{O}$ and complete level-$\wp$ structure — this last makes sense because $O_{K_+} \subset \mathcal{O}$ acts on the sixfold so we may speak about the sixfold's $\wp$-torsion points. The isomorphism $\Gamma/\Gamma(\wp) \cong \mathrm{PSL}_2(k_\wp)$ lets us define groups $\Gamma_0(\wp), \Gamma_1(\wp)$ intermediate between Γ and $\Gamma(\wp)$, and thus Shimura modular curves "$X_0(\wp)$" and "$X_1(\wp)$", which parametrize $\mathcal{O}$-sixfolds with partial level-$\wp$ structure. The curves "$X(\wp)$", "$X_0(\wp)$" and "$X_1(\wp)$" are defined over K_+, and even over $\mathbb{Q}$ if $\wp$ is Galois-stable. Note that the Galois-stable primes of K_+ are those that lie over an inert rational prime, i.e. a prime $\equiv \pm 2$ or ± 3 mod 7, and the prime $\wp_7 = (2-c)$ lying over the ramified prime 7.

We remarked already that Hurwitz curves come from normal subgroups of $G_{2,3,7}$. Shimura observed [1967, p. 83] that since each of the groups $\Gamma(\wp)$ is a normal subgroup of Γ, and $\Gamma \equiv g_{2,3,7}$, the resulting curves "$X(\wp)$" are Hurwitz curves. In particular "$X(\wp_7)$" is a Hurwitz curve of genus 3. We already know what this means: "$X(\wp_7)$" is none other than the Klein quartic $\mathcal{X}$. Furthermore, its fundamental group $\pi_1(\mathcal{X})$ is the congruence subgroup of Γ consisting of the images in $\mathrm{PSL}_2(\mathbb{R})$ of $\mathbb{Z}[c]$-linear combinations $a_1\mathbf{1} + a_2 i + a_3 j' + a_4 ij'$ of norm 1 with $2-c$ dividing a_2, a_3, a_4.

[The four Hurwitz curves of the next smallest genera also arise as "$X(\wp)$" for primes $\wp$ of K_+: the prime above 2 yields the Fricke–Macbeath curve [Fricke 1899; Macbeath 1965] of genus 7 and automorphism group $(\mathrm{P})\mathrm{SL}_2(\mathbb{F}_8)$, and the primes above 13 yield three curves of genus 14 with automorphisms by $\mathrm{PSL}_2(\mathbb{F}_{13})$ first found by Shimura. The next two Hurwitz curves have genus 17 and come from non-arithmetic quotients of $G_{2,3,7}$. See [Conder 1990] for more information on the groups that can arise as automorphism groups of Hurwitz curves, and [Conder 1987] for the list of all such groups of order less than 10^6.]

The quotient curves $X_0(7)$, $X_1(7)$, $X_0(49)$ of $\mathcal{X}$ now reappear as Shimura modular curves "$X_0(\wp_7)$", "$X_1(\wp_7)$", "$X_0(\wp_7^2)$". These curves have involutions $w_{\wp_7}$ and $w_{\wp_7^2}$ analogous to the Fricke involutions of the classical modular curves. However, the involutions of "$X_0(\wp_7)$" and "$X_1(\wp_7)$" are not the same as the involutions of the same quotients of $\mathcal{X}$ when considered as the classical modular curves $X_0(7)$ and $X_1(7)$. For instance, on $X_0(7)$ the involution $w_7 : j_7 \leftrightarrow 49/j_7$ switched the two cusps $j_7 = 0, \infty$, and also the elliptic points of order 3, at which

$$j_7^2 + 13j_7 + 49 = 0.$$

On "$X_0(\wp_7)$", the elliptic points of order 3 remain the same and are still switched by $w_{\wp_7}$; but there are no cusps — instead, the simple pole $j_7 = \infty$ of j is the unique elliptic point of order 7 of "$X_0(\wp_7)$", and must thus be fixed by $w_{\wp_7}$. Therefore $w_{\wp_7}$ takes j_7 not to $49/j_7$ but to $-13 - j_7$. In this setting the three Fricke involutions of "$X_1(\wp_7)$" are defined over $\mathbb{Q}$, and take d to $1-d$, $1/d$, and $d/(d-1)$.

We have seen already that the Fermat curve $\mathcal{F}_7$ is an unramified cover of $\mathcal{X}$. It follows that $\pi_1(\mathcal{F}_7)$ is a subgroup of $\pi_1(\mathcal{X})$, and thus of $G_{2,3,7}$. That subgroup obligingly turns out to be a congruence subgroup, with the result that $\mathcal{F}_7$, like $\mathcal{X}$, is a Shimura modular curve. That subgroup — call it Γ_7 — is intermediate between $\Gamma(\wp_7)$ and $\Gamma(\wp_7^2)$, and may be described as follows: under an identification of $\Gamma/\Gamma(\wp_7^2)$ with $\mathrm{PSL}_2(O_{K_+}/\wp_7^2)$, the group $\Gamma_7/\Gamma(\wp_7^2)$ consists of matrices congruent to the identity mod $\wp$ whose bottom left entry vanishes. Clearly Γ_7, thus defined, contains $\Gamma(\wp_7)$ as a normal subgroup of index 7, so $\mathcal{H}/\Gamma_7$ is a degree-7 unramified cyclic cover of $\mathcal{X}$. This is not yet enough to identify $\mathcal{H}/\Gamma_7$ with $\mathcal{F}_7$, but we obtain more automorphisms of $\mathcal{H}/\Gamma_7$ by observing that $\Gamma_0(\wp_7)$ is also a normal subgroup. Thus the quotient group $\Gamma_0(\wp_7)/\Gamma_7$ acts on $\mathcal{H}/\Gamma_7$. This group of automorphisms contains as an index-3 normal subgroup $\Gamma_1(\wp_7)/\Gamma_7$, which is an elementary abelian group of order 7^2. The quotient of $\mathcal{H}/\Gamma_7$ by this subgroup is the genus-zero curve $\mathcal{H}/\Gamma_1(\wp_7) =$ "$X_1(\wp_7)$", which we have already described as $X_1(7) = \mathcal{X}/\langle h\rangle$; and the ramification behavior of this quotient map $(\mathcal{H}/\Gamma_7)\to$"$X_1(\wp_7)$" *does* suffice to identify $\mathcal{H}/\Gamma_7$ with $\mathcal{F}_7$. The 147-element group $\Gamma_0(\wp_7)/\Gamma_7$ is then an index-2 subgroup of $\mathrm{Aut}(\mathcal{F}_7)$, generated by diagonal 3×3 matrices and cyclic coordinate permutations; extending $\Gamma_0(\wp_7)$ by $w_{\wp_7}$ yields the full group of automorphisms of $\mathcal{F}_7$.

References

[Adler 1981] A. Adler, "Some integral representations of $\mathrm{PSL}_2(\mathbf{F}_p)$ and their applications", *J. Algebra* **72**:1 (1981), 115–145.

[Adler 1997] A. Adler, "The Mathieu group M_{11} and the modular curve $X(11)$", *Proc. London Math. Soc.* (3) **74**:1 (1997), 1–28.

[Arbarello et al. 1985] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves, I*, Grundlehren der mathematischen Wissenschaften **267**, Springer, New York, 1985.

[Bennett 1997] M. A. Bennett, "Effective measures of irrationality for certain algebraic numbers", *J. Austral. Math. Soc. Ser. A* **62**:3 (1997), 329–344.

[Benson 1993] D. J. Benson, *Polynomial invariants of finite groups*, London Math. Soc. Lecture Note Series, Cambridge University Press, Cambridge, 1993.

[Birch and Kuyk 1975] B. J. Birch and W. Kuyk (editors), *Modular functions of one variable, IV*, edited by B. J. Birch and W. Kuyk, Lecture Notes in Math. **476**, Springer, Berlin, 1975.

[Bourbaki 1968] N. Bourbaki, *Groupes et algèbres de Lie, IV–VI*, Actualités scientifiques et industrielles **1337**, Hermann, Paris, 1968. Reprinted by Masson, Paris, 1981.

[Bugeaud and Győry 1996] Y. Bugeaud and K. Győry, "Bounds for the solutions of unit equations", *Acta Arith.* **74**:1 (1996), 67–80.

[Buser and Sarnak 1994] P. Buser and P. Sarnak, "On the period matrix of a Riemann surface of large genus", *Invent. Math.* **117**:1 (1994), 27–56. With an appendix by J. H. Conway and N. J. A. Sloane.

[Buser et al. 1994] P. Buser, J. Conway, P. Doyle, and K.-D. Semmler, "Some planar isospectral domains", *Internat. Math. Res. Notices* **1994**:9 (1994), 391–399.

[Clemens 1980] C. H. Clemens, *A scrapbook of complex curve theory*, Plenum, New York, 1980.

[Conder 1987] M. Conder, "The genus of compact Riemann surfaces with maximal automorphism group", *J. Algebra* **108**:1 (1987), 204–247.

[Conder 1990] M. Conder, "Hurwitz groups: a brief survey", *Bull. Amer. Math. Soc.* (*N.S.*) **23**:2 (1990), 359–370.

[Conway et al. 1985] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Oxford, 1985.

[Coolidge 1931] J. L. Coolidge, *A treatise on algebraic plane curves*, Clarendon, Oxford, 1931.

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

[Darmon and Granville 1995] H. Darmon and A. Granville, "On the equations $z^m = F(x,y)$ and $Ax^p + By^q = Cz^r$", *Bull. London Math. Soc.* **27**:6 (1995), 513–543.

[Dickson 1934] L. E. Dickson, *History of the theory of numbers, II: Diophantine analysis*, Stechert and Co., New York, 1934.

[Ekedahl and Serre 1993] T. Ekedahl and J.-P. Serre, "Exemples de courbes algébriques à jacobienne complètement décomposable", *C. R. Acad. Sci. Paris Sér. I Math.* **317**:5 (1993), 509–513.

[Elkies 1994] N. D. Elkies, "Mordell-Weil lattices in characteristic 2, I: Construction and first properties", *Internat. Math. Res. Notices* **1994**:8 (1994), 343–361.

[Elkies 1998a] N. D. Elkies, "Elliptic and modular curves over finite fields and related computational issues", pp. 21–76 in *Computational perspectives on number theory*

(Chicago, 1995), edited by D. A. Buell and J. T. Teitelbaum, AMS/IP Stud. Adv. Math., Amer. Math. Soc., Providence, RI, 1998.

[Elkies 1998b] N. D. Elkies, "Shimura curves computations", pp. 1–47 in *Algorithmic number theory* (ANTS-III: Portland, 1998), edited by J. Buhler, Lecture Notes in Computer Science **1423**, Springer, New York, 1998.

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. Erratum in **75** (1984), 381.

[Faltings 1991] G. Faltings, "Diophantine approximation on abelian varieties", *Ann. of Math.* (2) **133**:3 (1991), 549–576.

[Fricke 1899] R. Fricke, "Über eine einfache Gruppe von 504 Operationen", *Math. Annalen* **52** (1899), 321–339.

[Fulton and Harris 1991] W. Fulton and J. Harris, *Representation theory*, Graduate Texts in Math. **129**, Springer, New York, 1991.

[Genocchi 1864] A. Genocchi, "Intorno all'equazione $x^7+y^7+z^7=0$", *Annali di Mat. Pura ed Applicata* **6** (1864), 287–288.

[Gordon et al. 1992] C. Gordon, D. L. Webb, and S. Wolpert, "One cannot hear the shape of a drum", *Bull. Amer. Math. Soc.* (*N.S.*) **27**:1 (1992), 134–138.

[Gross 1978] B. H. Gross, "On the periods of abelian integrals and a formula of Chowla and Selberg", *Invent. Math.* **45**:2 (1978), 193–211. With an appendix by David E. Rohrlich.

[Gross 1990] B. H. Gross, "Group representations and lattices", *J. Amer. Math. Soc.* **3**:4 (1990), 929–960.

[Gross and Rohrlich 1978] B. H. Gross and D. E. Rohrlich, "Some results on the Mordell-Weil group of the Jacobian of the Fermat curve", *Invent. Math.* **44**:3 (1978), 201–224.

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Math. **52**, Springer, New York, 1977.

[Hirzebruch 1983] F. Hirzebruch, "Arrangements of lines and algebraic surfaces", pp. 113–140 in *Arithmetic and geometry, II*, edited by M. Artin and J. Tate, Progr. Math. **36**, Birkhäuser, Boston, 1983. Reprinted as #69 (pp. 679–706) of his *Gesammelte Abhandlungen* vol. 2, Springer, 1987.

[Hoffmann 1991] D. W. Hoffmann, "On positive definite Hermitian forms", *Manuscripta Math.* **71**:4 (1991), 399–429.

[Hurwitz 1893] A. Hurwitz, "Über algebraische Gebilde mit eindeutigen Transformationen in sich", *Math. Annalen* **41** (1893), 403–442.

[Kemper 1996] G. Kemper, "A constructive approach to Noether's problem", *Manuscripta Math.* **90**:3 (1996), 343–363.

[Kenku 1985] M. A. Kenku, "A note on the integral points of a modular curve of level 7", *Mathematika* **32**:1 (1985), 45–48.

[Klein 1879a] F. Klein, "Ueber die Erniedrigung der Modulargleichungen", *Math. Annalen* **14** (1879), 417–427. Reprinted as [Klein 1923, LXXXIII, pp. 76–89].

[Klein 1879b] F. Klein, "Ueber die Transformationen siebenter Ordnung der elliptischen Funktionen", *Math. Annalen* **14** (1879), 428–471. Reprinted as [Klein 1923, LXXXIV, pp. 90–136]. Translated in this collection.

[Klein 1923] F. Klein, *Gesammelte Mathematische Abhandlungen, 3: Elliptische Funktionen* etc., edited by R. Fricke et al., Springer, Berlin, 1923. Reprinted by Springer, 1973.

[Kneser 1967] M. Kneser, "Über die Ausnahme-Isomorphismen zwischen endlichen klassischen Gruppen", *Abh. Math. Sem. Univ. Hamburg* **31** (1967), 136–140.

[Kubert and Lang 1981] D. S. Kubert and S. Lang, *Modular units*, Grundlehren der mathematischen Wissenschaften **244**, Springer, New York, 1981.

[Macbeath 1965] A. M. Macbeath, "On a curve of genus 7", *Proc. London Math. Soc.* (3) **15** (1965), 527–542.

[MacWilliams and Sloane 1977] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Mathematical Library **16**, North-Holland, Amsterdam, 1977.

[Mazur 1986] B. Mazur, "Arithmetic on curves", *Bull. Amer. Math. Soc.* (*N.S.*) **14**:2 (1986), 207–259.

[Nagell 1960] T. Nagell, "The Diophantine equation $x^2+7=2^n$", *Ark. Mat.* **4** (1960), 185–187.

[Nagell 1969] T. Nagell, "Sur un type particulier d'unités algébriques", *Ark. Mat.* **8** (1969), 163–184.

[Perlis 1977] R. Perlis, "On the equation $\zeta_K(s) = \zeta_{K'}(s)$", *J. Number Theory* **9**:3 (1977), 342–360.

[Poonen 1996] B. Poonen, "Computational aspects of curves of genus at least 2", pp. 283–306 in *Algorithmic number theory: Second International Symposium* (Talence, 1996), edited by H. Cohen, Lecture Notes in Comput. Sci. **1122**, Springer, Berlin, 1996.

[Selberg and Chowla 1967] A. Selberg and S. Chowla, "On Epstein's zeta-function", *J. Reine Angew. Math.* **227** (1967), 86–110.

[Serre 1967] J.-P. Serre, "Complex multiplication", pp. 292–296 in *Algebraic Number Theory* (Brighton, 1965), edited by J. W. S. Cassels and A. Fröhlich, Thompson and Academic Press, Washington, D.C., and London, 1967. Reprinted as #76, (pp. 455–459) of his *Oeuvres*, vol. 2, Springer, Berlin, 1986.

[Serre 1973] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Math. **7**, Springer, New York, 1973. Translation of *Cours d'arithmétique*, Presses univ. de France, Paris, 1970.

[Serre 1983a] J.-P. Serre, "Nombres de points des courbes algébriques sur $\mathbf{F}_q$", pp. Exp. No. 22, 8 in *Séminaire de théorie des nombres de Bordeaux* (Talence, 1982/1983), Univ. Bordeaux I, Talence, 1983. Reprinted as #129 (pp. 664–668) of his *Oeuvres*, vol. 3, Springer, Berlin, 1986.

[Serre 1983b] J.-P. Serre, "Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini", *C. R. Acad. Sci. Paris Sér. I Math.* **296**:9 (1983), 397–402. Reprinted as #128 (pp. 658–663) of his *Oeuvres*, vol. 3, Springer, Berlin, 1986.

[Serre 1984] J.-P. Serre, "Résumés des cours de 1983–1984", pp. 79–83 in *Annuaire*, Collège de France, Paris, 1984. Reprinted as #132 (pp. 701–705) of his *Oeuvres*, vol. 3, Springer, Berlin, 1986.

[Shephard and Todd 1954] G. C. Shephard and J. A. Todd, "Finite unitary reflection groups", *Canadian J. Math.* **6** (1954), 274–304.

[Shimura 1967] G. Shimura, "Construction of class fields and zeta functions of algebraic curves", *Ann. of Math.* (2) **85** (1967), 58–159.

[Siegel 1968] C. L. Siegel, "Zum Beweis des Starkschen Satzes", *Invent. Math.* **5** (1968), 180–191.

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math. **106**, Springer, New York, 1986.

[Stark 1973] H. M. Stark, "On the Riemann hypothesis in hyperelliptic function fields", pp. 285–302 in *Analytic number theory* (St. Louis, MO, 1972), edited by H. G. Diamond, Proc. Sympos. Pure Math. **24**, Amer. Math. Soc., Providence, 1973.

[Stichtenoth 1973] H. Stichtenoth, "Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik", *Arch. Math.* (*Basel*) **24** (1973), 527–544, 615–631.

[Sunada 1985] T. Sunada, "Riemannian coverings and isospectral manifolds", *Ann. of Math.* (2) **121**:1 (1985), 169–186.

[Suzuki 1982] M. Suzuki, *Group theory, I*, Grundlehren der mathematischen Wissenschaften, Springer, Berlin, 1982. Translated from the Japanese by the author.

[Tate 1974] J. T. Tate, "The arithmetic of elliptic curves", *Invent. Math.* **23** (1974), 179–206.

[Thompson 1976] J. G. Thompson, "Finite groups and even lattices", *J. Algebra* **38**:2 (1976), 523–524.

[Vélu 1971] J. Vélu, "Isogénies entre courbes elliptiques", *C. R. Acad. Sci. Paris Sér. A-B* **273** (1971), A238–A241.

[Vignéras 1980] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math. **800**, Springer, Berlin, 1980.

[Weil 1964] A. Weil, "Sur certains groupes d'opérateurs unitaires", *Acta Math.* **111** (1964), 143–211.

Noam D. Elkies
Department of Mathematics
Harvard University
Cambridge, MA 02138
United States
elkies@math.harvard.edu