SUPERSPECIAL CURVES OF GENERA TWO AND THREE

Bradley W. Brock

A dissertation presented to the faculty of
PRINCETON UNIVERSITY
in candidacy for the degree of
Doctor of Philosophy

Recommended for acceptance by the
DEPARTMENT OF MATHEMATICS

June 1993

Abstract

A superspecial curve in characteristic p is a curve whose Jacobian is a product of supersingular elliptic curves. Using Igusa's result that $h_p(\lambda)$ has only simple roots, one can calculate how many supersingular elliptic curves have each possible automorphism group. Relying on Igusa's enumeration of all automorphism groups of genus 2 curves and Hashimoto and Ibukiyama's computation of the class number of the principal genus of a quaternion hermitian space, Ibukiyama, Katsura and Oort (IKO) calculate how many superspecial curves of genus 2 have each possible automorphism group. We enumerate all automorphism groups of genus 3 curves and, relying on Hashimoto's computation of the class number for $g = 3$, calculate how many superspecial of genus 3 have each possible automorphism group. In each case the number of superspecial curves with a given automorphism group of its polarized Jacobian is a polynomial in p whose coefficients depend on p mod 12 for $g = 1$, p mod 120 for $g = 2$, and p mod 504 for $g = 3$. Its degree is the dimension of the curves in the moduli space possessing this automorphism group. Our method also provides a short, simpler proof of IKO's result, and our theorem provides insight into how the moduli of hyperelliptic curves sit in the moduli of genus 3 curves with respect to the moduli of curves with a fixed automorphism group. One implication of these results is that by taking p sufficiently large there exist both genera two and three zeta functions assumed by an arbitrarily large number of curves.

Contents

Introduction

Narasimhan and Nori (1.2A) proved that there are only finitely many curves over an algebraically closed field k with a given unpolarized abelian variety as the Jacobian. One particularly interesting abelian variety in characteristic p is the product A of g supersingular elliptic curves. Deligne (2.1A) proved that for $g \geq 2$ the isomorphism class of A does not depend on the particular choice of supersingular elliptic curves. Oort [27] calls A superspecial, and we shall also call curves with Jacobian A superspecial. Nygaard (2.3A) proved that these curves are characterized by Frobenius being zero on $H^1(X, \mathcal{O}_X)$, i.e. the Hasse-Witt matrix is zero. Ekedahl (2.13A) proved that superspecial curves can be written over $\mathbf{F}_{p^2}$, each having either the least or the most number of rational points allowed by the Weil conjectures, and that for fixed p the number of superspecial curves of arbitrary genus is finite. Ibukiyama, Katsura and Oort (3.7A) proved that the number of principal polarizations on A up to automorphisms of A is equal to the class number of a positive definite quaternion hermitian form. For $g \leq 3$ every abelian variety of dimension g with indecomposable principal polarization is the Jacobian of a curve of genus g (1.1A). Hence, using Hashimoto and Ibukiyama's calculation of these class numbers for $g = 2$ and 3 we quickly get the precise number of curves with Jacobian A. Theorem 3.10 is a more precise statement of the following results.

Theorem (Ibukiyama, Katsura, and Oort). *For every prime p the number of isomorphism classes of superspecial curves of genus 2 is*

$$\frac{p^3 + 24p^2 + 141p}{2880} + f(p)$$

where $f(p)$ depends only on p mod 120.

Proof. This is a weakening of [11, 3.3].■

Superspecial Curves

THEOREM. For every prime p the number of isomorphism classes of superspecial curves of genus 3 is

$$\frac{p^6 - p^5 + 610p^4 - 2410p^3}{1451520} + f(p)$$

where $f(p)$ is a quadratic in p whose coefficients depend only on p mod 504.

These results imply that for every N there exists p and a zeta function of a curve of genus $g = 2$ (resp. 3) over $\mathbf{F}_{p^2}$, namely one of

$$Z_X(t) = \frac{(1 \mp pt)^{2g}}{(1-t)(1-p^2t)},$$

such that at least N curves have this zeta function. It would be interesting to know if the zeta functions of superspecial curves belong to the most curves possible.

That these numbers are not uniformly bounded might not be expected because it would seem by Nygaard's result that we are imposing g^2 conditions on $3g-3$ parameters. However, we are really imposing at most $\frac{1}{2}g(g+1)$ conditions because we are selecting one Jacobian out of the $\frac{1}{2}g(g+1)$ dimensional moduli of polarized abelian varieties. It would be interesting to know if there are in fact $\frac{1}{2}g(g-1)$ explicit conditions that the Hasse-Witt matrix must satisfy.

Ihara (3.9A) proved that the number of principal polarizations on A grows as a polynomial in p of degree $\frac{1}{2}g(g+1)$, from which follows, as Ekedahl [5] makes explicit, that the number of indecomposable polarizations also grows as a polynomial in p of the same degree. One might hope that the number of superspecial curves might grow as a polynomial of degree $3g-3$. However, the moduli of hyperelliptic curves of genus 3 has dimension 5, but superspecial hyperelliptic curves of genus 3 do not appear to have quintic polynomial growth, apparently because we are indeed imposing 6 conditions. The only reason they do experience at least quadratic polynomial growth is because there are certain automorphism groups that can only be attained by the polarized Jacobian of an hyperelliptic curve. Therefore, it seems more reasonable to conjecture that the number of indecomposable principal polarizations on A with a given automorphism group is a polynomial in p with coefficients depending on p mod N for some N and of degree equal to the dimension of moduli of curves with that automorphism group. If in addition it were true that (a) there exist automorphism groups that are assumed only by Jacobians of curves and (b) the dimension of their moduli is positive, then the number of superspecial curves would grow at least polynomially of degree equal to this dimension. This would mean that for every $g \geq 1$ there exists a genus g zeta function assumed by an arbitrarily large number of curves.

If $p > 7$ there are 11 possible automorphism groups of superspecial hyperelliptic genus 3 curves, and 13 of nonhyperelliptic ones. As automorphism groups of the polarized Jacobian 6 of these coincide, for a total of essentially 18 groups. This coincidence occurs precisely when the hyperelliptic involution splits the group.

Acknowledgments

It is a pleasure to acknowledge the influence of the work of Frans Oort on this thesis. I also thank K. Hashimoto whose extremely accurate tables [9] made my work much easier, Noam Elkies who has patiently and promptly answered my questions about elliptic curves, and Charles Yeomans and Nick Katz who offered constructive criticisms to preliminary versions of this manuscript. I would like to express my gratitude to my advisor Gerd Faltings whose vast knowledge of algebraic geometry was a constant source of inspiration and guidance.

Words cannot describe the impact that the unconditional love of my wife Barbara and young daughter Katrina have had on my life and my work.

This work was supported by a Fannie and John Hertz Foundation Fellowship. For financial support during the final stages of writing I would also like to thank the Rose-Hulman Institute of Technology.

Superspecial Curves

Prerequisites, Notation and Conventions

We try to assume only a knowledge of Hartshorne [H] and generally use his notation and conventions. Other results that we quote from the literature without proof will be succeeded with an A, e.g., Theorem 2.1A. Unless we specify otherwise by a curve we mean a complete nonsingular curve over an algebraically closed field, although we often require the curve to be written over a smaller and typically finite field. We use p exclusively for the characteristic of this field when it is not zero. We denote the ring of algebraic integers by $\mathbf{A}$, a primitive nth root of unity by ω_n, and the dihedral group of order $2n$ by D_{2n}. Consequently, $D_4 \cong \mathbf{Z}/2 \times \mathbf{Z}/2$, and $D_6 \cong S_3$. If there is a nontrivial group homomorphism from G into $Aut(H)$ we denote the corresponding semidirect product by $G \ltimes H$. By an n-tuple of integers we mean, according to context, either the product of cyclic groups of those orders or the greatest common divisor. Within a proposition we use (a), (b), etc., for independent statements; (1), (2), etc., for connected statements and conditions; and (i), (ii), etc., for equivalent statements.

1 Preliminaries

We shall be using the following standard facts [H, IV.1.1.1, 5.5.2, 5.5.5, Exs. 1.7, 2.2]. A curve C over an algebraically closed field k of characteristic p is *hyperelliptic* if there exists a morphism $f : C \to \mathbf{P}^1$ of degree 2. To be consistent with the literature, e. g., [H, Ex. 1.7], we shall also require $g \geq 2$ although many hyperelliptic arguments work equally well for $g = 1$, e. g., 2.13A and 3.6. Every curve C of genus 2 is hyperelliptic, and every nonhyperelliptic curve of genus 3 is a planar quartic. An hyperelliptic curve of genus g may be embedded in $\mathbf{P}^1 \times \mathbf{P}^1$ as a curve of bidegree $(g+1, 2)$. Borrowing from the language of Riemann surfaces, we refer to the degree 2 morphism as a two-sheeted covering of $\mathbf{P}^1$. Such a curve has a unique automorphism that switches sheets, has order 2, and commutes with all other automorphisms. We shall use the term "hyperelliptic involution" exclusively for this automorphism, and since it is central we often denote it by -1. If $p > 2$, the $2g+2$ ramified points are identical with the Weierstrass points, the points fixed by the hyperelliptic involution. These points uniquely determine the curve up to automorphisms of $\mathbf{P}^1$. The function field of the curve is the extension of $k(x)$ determined by the equation $y^2 = f(x)$ where f is a monic polynomial whose roots are the affine images of the Weierstrass points. An automorphism of $\mathbf{P}^1$ is uniquely determined by its action on 3 points, so the dimension of moduli of hyperelliptic curves is $2g-1$. (The last statement is still true if $p = 2$.) If we map three points to $0, 1, \infty$ the other points form a $2g-1$-tuple determined modulo S_{2g+2}, and hence generically $(2g+2)!$ $2g-1$-tuples corresponding to the same curve, this number being reduced in proportion to the size of the automorphism group. A generalization of this last observation explains how mass formulas (3.9A) arise in a natural way.

Applying this analysis to a curve of genus 1 yields an invariant λ up to S_4 such that C is given by $y^2 = x(x-1)(x-\lambda)$. However, λ is fixed by $D_4 \leq S_4$, so λ is determined only up to $S_3 \cong S_4/D_4$. The j-invariant of C [H, p. 317] is designed to remove the S_3 ambiguity and make sense in characteristic 2. By an elliptic curve we shall mean a one-dimensional abelian variety over an algebraically closed field. This differs from a curve of genus one in that it has a distinguished point, its identity, which is invariant under automorphisms. An elliptic curve is *supersingular* if Frobenius is zero on $H^1(C, \mathcal{O}_C)$.

Theorem 1.1A. *For $g \leq 3$ every principally polarized abelian variety of dimension g with indecomposable polarization is the Jacobian of a curve of genus g.*

Proof. [22, p. 74].■

Theorem 1.2A (Narasimhan, Nori [23]). *There are, up to isomorphism, only finitely many smooth irreducible curves over an algebraically closed field k, having a given unpolarized abelian variety as the Jacobian.*

Theorem 1.3A (Torelli, Weil). *If the group of automorphisms of a curve C is G, then the group of automorphisms Γ of its polarized Jacobian is G if C is hyperelliptic and $\{\pm 1\} \times G$ otherwise.*

Proof. [22, pp. 68ff].■

Following [11] we define the *reduced automorphism group* $\overline{\Gamma}$ of a curve to be the automorphism group of its polarized Jacobian modulo $\{\pm 1\}$, i.e. $\overline{\Gamma}$ is a group of automorphisms of the projective line for an hyperelliptic curve and is equal to G, the automorphism group of the curve, otherwise.

Theorem 1.4A. *The automorphism group of a curve's polarized Jacobian has a natural, faithful representation in $SL(2g, \mathbf{Z}_l)$ for every prime $l \neq p$. The characteristic polynomial of any element has integral coefficients independent of l.*

Proof. [21, pp. 176, 180].■

Corollary 1.5 (Kulkarni [17, Corollary 3.5]). *If a prime q divides the order of the automorphism group of a curve of genus g then $q \leq 2g+1$.*

Proof. Because the representation in $SL(2g, \mathbf{Z}_l)$ is faithful a primitive qth root of unity must be a root of the characteristic polynomial of an element of order q. But this polynomial is integral and therefore must be divisible by the qth cyclotomic polynomial, which has degree $q-1$.■

In fact if $p > 2g+1$ and $g \leq 3$ the curve lifts with its automorphism group to characteristic 0 (see 3.5ff), so that this representation is realized in $SL(2g, \mathbf{Z})$ via the group's action on the singular homology of the Riemann surface. It is believed that the condition $g \leq 3$ is unnecessary.

The following are the Weil conjectures for curves and more generally in 1.7A for varieties.

Theorem 1.6A (Weil). *Let C be a nonsingular curve of genus g defined over $k = \mathbf{F}_q$, and let $N_r = N_r(C/k)$ be the number of $\mathbf{F}_{q^r}$ rational points. For all r $|1 + q^r - N_r| \leq 2g\sqrt{q^r}$.*

Proof. [H, Ex. V.1.10,C.5.7].■

Theorem 1.7A (Dwork, Grothendieck, Deligne). *Let X/k be projective and smooth of relative dimension n where $k = \mathbf{F}_q$. There exist real functions $P_i(t)$ for $0 \leq i \leq 2n$ with $P_i(0) = 1$ such that*

$$Z_X(t) = \frac{P_1(t)P_3(t)\cdots P_{2n-1}(t)}{P_0(t)P_2(t)\cdots P_{2n}(t)}$$

with the following properties.

(a) Each $P_i(t)$ is a polynomial with rational coefficients.

(b) If $1/\alpha$ is a root of P_i, α/q^n is a root of P_{2n-i} with the same multiplicity.

(c) If $P_i(1/\alpha) = 0$, $|\alpha| = q^{i/2}$ and α is an algebraic integer. Hence, $P_i(t)$ in fact has integer coefficients, and $P_{2n-i}(t) = P_i(tq^{n-i})$

(d) If furthermore X/k is geometrically connected $P_0(t) = 1 - t$ and $P_{2n}(t) = 1 - q^n t$, in which case if X is a curve P_1 has degree $2g$.

Definition. We define the hypergeometric series to be

$$F(a, b, c; z) = \sum_{n=0}^{\infty} (\Gamma(a+n)\Gamma(b+n)\Gamma(c)/\Gamma(a)\Gamma(b)\Gamma(c+n))(z^n/n!),$$

which satisfies the differential equation $z(1-z)u'' + (c-(a+b+1)z)u' - abu = 0$ and the relationship $F(a, b, c; z) = (1-z)^{c-a-b}F(c-b, c-a, c; z)$. Following [11] if a, b, and c are integers such that $1-p \leq a \leq b \leq 0$ and $1 \leq c \leq p+b$ we define $F_p(a, b, c; z)$ to be the reduction of the polynomial $F(a, b, c; z)$ modulo p. Similarly, if a, b, and c are rational we mean reduce them modulo p to the above ranges if possible, switching a and b if necessary, and compute, leaving $c > p + b$ undefined. With these conventions F is a polynomial of degree $-b$ satisfying

$$\begin{aligned} F(a, b, c; z) &= \frac{\Gamma(c-a-b)\Gamma(c)}{\Gamma(c-a)\Gamma(c-b)} F(a, b, 1+a+b-c; 1-z) \\ &= z^{-b} \frac{\Gamma(-a+1)\Gamma(c)}{\Gamma(b-a+1)\Gamma(c-b)} F(b-c+1, b, b-a+1; z^{-1}) \end{aligned}$$

where we are careful to multiply the combinatorial factors through before reducing modulo p. As a consequence of the differential equation, $F_p(a, b, c; z)$ has all simple zeros except possibly $z = 1$. We can calculate that if 1 is a zero $c - a \leq p$ and its multiplicity is $max\{0, c-a-b-p\}$. In this case $F_p(c-b, c-a, c; z)$ has the same zeros distinct from 1. If $0 \leq b \leq 2a$ the polynomial

$$G(a, b; z) = \sum \binom{a}{b-n} \binom{a}{n} z^n$$

is related to the hypergeometric series by

$$G(a,b;z) = \binom{a}{b} F(-a,-b,1+a-b;z) \text{ if } a \geq b \text{ and}$$

$$G(a,b;z) = \binom{a}{2a-b} z^{b-a} F(-a,b-2a,1+b-a;z) \text{ if } a \leq b.$$

Theorem 1.8A is essentially all that is needed to prove Theorems 3.8A(a), 3.10(a), and 3.12.

Theorem 1.8A. *The elliptic curve with invariant λ is supersingular if and only if $h_p(\lambda) = 0$, where*

$$h_p(\lambda) = \sum_{i=0}^{k} \binom{k}{i}^2 \lambda^i \quad k = \frac{1}{2}(p-1).$$

h_p has distinct roots.

Proof. [H, IV.4.22]. The last assertion, due to Igusa [12], follows from its equivalence to the characteristic p hypergeometric function $F_p(1/2,1/2,1;\lambda)$.∎

Keep in mind that an elliptic curve may be written over a field k if and only if $j \in k$ [H, Ex IV.4.4]. For example if $p > 3$ and $j \neq 0, 1728$, $y^2 = x^3 + 3j(1728-j)x + 2j(1728-j)^2$ is an elliptic curve written over any field containing its j-invariant.

Theorem 1.9A. *Every supersingular elliptic curve has $j, \lambda \in \mathbf{F}_{p^2}$, and over this field N_1 can be $1 - 2p + p^2$. In fact if $j \neq 0$ then $j^{(p^2-1)/3} = (-\lambda)^{(p^2-1)/8} = 1$. Furthermore, let h be the class number of $\mathbf{Q}(\sqrt{-p})$, $p \geq 5$. The number of supersingular elliptic curves with $j \in \mathbf{F}_p$ is*

(a) $h/2$ if $p \equiv 1 \bmod 4$,

(b) h if $p \equiv 7 \bmod 8$, and

(c) $2h$ if $p \equiv 3 \bmod 8$.

The number of supersingular elliptic curves with $\lambda \in \mathbf{F}_p$ is *(d) 0 if* $p \equiv 1 \bmod 4$ *and*

(e) 3h if $p \equiv 3 \bmod 4$*.*

Sketch of proof. Part of this proof is due to Elkies [6] who does not know with whom it originates. The last two statements arose in Gross and Zagier's work on Gauss' class number problem. Hence, there is always a supersingular elliptic curve with $j \in \mathbf{F}_p$, over which $N_1 = 1 + p$ [H, Ex. 4.16(e)] and thus $N_2 = 1 + 2p + p^2$. This N_2 becomes an N_1 over $\mathbf{F}_{p^2}$. Introducing a quadratic twist we see that N_1 can also be $1 - 2p + p^2$.

That all supersingular curves can be written over $\mathbf{F}_{p^2}$ is standard and implies that the supersingular points of the modular curves $X_0(l)$ are defined over $\mathbf{F}_{p^2}$. The second modular curve $X_0(2)$ is rational and is parameterized by a Weber function f, and hence $f \in \mathbf{F}_{p^2}$ if f corresponds to a supersingular elliptic curve. Since the cube roots of j and the eighth roots of $-\lambda$ are rational functions of the Weber functions, they are also in $\mathbf{F}_{p^2}$.∎

This theorem provides an alternate proof (at least when $p \not\equiv 3 \bmod 8$) of the fact that $h \equiv \frac{p-1}{2} \bmod 2$ and if $p \equiv 1 \bmod 4$ then $h \equiv \frac{p-1}{2} \bmod 4$. It also provides the crude bound $h \leq \frac{p+7}{6}$.

The following are some technical lemmata that will come in handy indirectly in our explicit calculations in the proof of Theorem 3.15. Lemma 1.10 was more or less discovered by Deuring [3] and according to Elkies [6] was recently rediscovered by A.O.L. Atkins.

Lemma 1.10. *An elliptic curve with* $j \neq 0, 1728$ *is supersingular if and only if* j *solves*

$$F_p(1/12, 5/12, 1; 1728/j) = 0 \text{ if } p \equiv 1 \bmod 4 \text{ and}$$

$$F_p(7/12, 11/12, 1; 1728/j) = 0 \text{ if } p \equiv -1 \bmod 4.$$

Proof. Equation (64) of [3] is proportional to

$F_p(1/12, 5/12, 1/2; 1 - 1728/j) = F_p(1/12, 5/12, 1; 1728/j)$ if $p \equiv 1 \bmod 4$ and

$F_p(7/12, 11/12, 3/2; 1 - 1728/j) = F_p(7/12, 11/12, 1; 1728/j)$ if $p \equiv -1 \bmod 4$.∎

Lemma 1.11. *Let the characteristic $p \neq 2$. If X and Y are elliptic curves with j-invariants j and k such that there exists an isogeny of degree 2 between them, then for some solution of $x^3 = jk$*

$$j + k - x^2 + 495x - 54000 = 0.$$

Proof. By the method of [H, Ex. IV.4.5] for some choice of the λ-invariants, say λ for X and μ for Y,

$$\mu = (\frac{\sqrt{\lambda}+1}{\sqrt{\lambda}-1})^2.$$

If $a = (\frac{\lambda+1}{\lambda-1})^2$ $j = 2^6\frac{(a+3)^3}{(a-1)^2}$ and $k = 2^6\frac{(4a-3)^3}{(a-1)}$. If $x = 2^4\frac{(4a-3)(a+3)}{(a-1)}$ we observe the above relation. Alternately, we can find this polynomial as a factor of the 2nd modular equation.∎

Lemma 1.12. *Assume $p \neq 2$ and $b, a^2 - b \neq 0$. The curve given by $y^2 = x^4 + 2ax^2 + b$ is isomorphic to the elliptic curve with invariant*

$$\lambda = \frac{a+\sqrt{b}}{a-\sqrt{b}}.$$

There is an isogeny of degree 2 between this elliptic curve and $y^2 = x^4 + 2ax^2 + a^2 - b$.

Proof. The first assertion is an easy consequence of the quadratic formula. The second follows from the proof of Lemma 1.11.∎

2 Supersingularity and superspecialty

For the remainder unless we say otherwise E is a supersingular elliptic curve.

Theorem 2.1A (Deligne). *All unpolarized abelian varieties of the form $E_1 \times E_2$, where E_i is a supersingular elliptic curve, are isomorphic.*

Proof. [28, Theorem 3.5].■

However, we shall be interested in the automorphism group of this abelian variety with polarization, which may vary.

Lemma 2.2A (Oort [26, p. 36]). *Let A be an abelian variety of characteristic p and of dimension $g \geq 2$, and let $E^g \to A$ be an isogeny of degree d. If $p \not| \, d$ then $A \cong E^g$.*

Definitions. For $1 \leq i \leq g$ the *Hasse invariant* $\eta(i)$ of a curve of genus g and characteristic p is the dimension of the image of $H^1(C, \mathcal{O}_C) \cong H^0(C, \Omega_C)$ under F^i where F is the p-linear map induced by the Frobenius morphism. If $\eta(g) = g$ the curve is *ordinary.* If $\eta(g) = 0$ the curve is *very special*, i.e. the Hasse-Witt matrix is nilpotent as a p-linear map. If $\eta(1) = 0$ the curve is *superspecial.* If C is written over $k = \mathbf{F}_q$, $q = p^r$, the *Newton slopes* of C are the p-adic ordinals of the reciprocal roots of $P_1(t)$, where we normalize so that $ord_p(q) = 1$. Order the Newton slopes m_j so that $m_1 \leq \cdots \leq m_{2g}$. By 1.7A(b) $m_j + m_{2g-j} = 1$. We define the *Newton polygon* to be the function on $[0, 2g]$ that passes through the points $(j, m_1 + \cdots + m_j), 0 \leq j \leq 2g$, and is linear in between. Equivalently, it is the convex hull of the points $(j, ord_p(b_j))$ where $P_1(t) = b_0 - b_1 t + \cdots + b_{2g} t^{2g}$. These definitions also make sense for abelian varieties.

Theorem 2.3A (Nygaard [24]). *The Jacobian $J(C)$ of a curve C is isomorphic to E^g if and only if C is superspecial.*

Theorem 2.4 (Oort [25]). *The following four conditions on a curve $C/\mathbf{F}_q$ of genus g are equivalent in which case we call it supersingular.*

(i) $J(C)$ is isogenous to E^g. (More generally an abelian variety isogenous to E^g is supersingular.)

(ii) For some r $|1 + q^r - N_r| = 2g\sqrt{q^r}$.

(iii) For some r $P_1(t) = (1 - q^r t)^{2g}$ over $k = \mathbf{F}_{q^{2r}}$ in Theorem 1.7A, i.e. N_1 is as small as Theorem 1.6A allows.

(iv) All Newton slopes equal $1/2$.

Proof. (i) ⇒ (iii): Because $J(C)$ and E^g are isogenous they are isogenous over some finite field over which they are both defined, and by Tate's theorem [21, p. 253] their zeta functions over this field are the same. $P_1(t)$ is the same for a curve and its Jacobian, and the statement is true for E^g [21, p. 217]. (ii) ⇔ (iii): Let $1/\alpha_i$ be the roots of P_1. $N_r(C) = q^r - a_r + 1$ where $a_r = \sum_{i=1}^{2g} \alpha_i^r$ [H, Ex. C.5.7]. Hence for the bound in 1.6A to be tight α_i^r must be the same for all i. But $a_r = 2g\alpha_i^r$ is rational and α_i is an algebraic integer. Hence, α_i^r is an integer with absolute value $q^{r/2}$, so r is even and $\alpha_i^{2r} = q^r$. The converse is trivial. (iii) ⇒ (iv): Trivial. (iv) ⇒ (i): Let $P_1(t) = b_0 - b_1 t + \cdots + b_{2g} t^{2g}$ over $k = \mathbf{F}_{q^2}$, and let $1/\alpha_i$ be its roots. Because the Newton slopes are $1/2$ q^i divides b_i. Hence, α_i/q is an algebraic integer all of whose conjugates have absolute value 1. Therefore, α_i/q is a root of unity, so over some extension $J(C)$ is isogenous to E^g by Tate's theorem. ∎

Theorem 2.5A. *$J(C)$ over an algebraically closed field has $p^{\eta(g)} - 1$ points of order p.*

Proof. [21, p. 148] or [19].∎

Corollary 2.6. *The following four conditions on a curve $C/\mathbf{F}_q$ of genus g are equivalent.*

(i) C is very special.

(ii) $J(C)$ has no points of order p.

(iii) All Newton slopes are positive.

(iv) $N_r(J(C))$ of 1.6A all satisfy $N_r \equiv 1 \bmod p$.

A necessary condition for these to hold is $N_r(C) \equiv 1 \bmod p$. This is also sufficient if $p > g$.

Proof. (i) $\Leftrightarrow$ (ii): This is 2.5A. (i) $\Rightarrow$ (iii): More generally, the Katz congruence formula says that $P_1(t) = det(1 - F^r t; H^1(C, \mathcal{O}_C)) \bmod p$ where $q = p^r$, so the number of zero Newton slopes is equal to the number of eigenvalues of the Hasse-Witt matrix with zero p-adic ordinal, which equals $\eta(g)$. (iii) $\Rightarrow$ (iv): Let $1/\alpha_i$ be the roots of P_1. $N_r(J(C)) = \prod_{i=1}^{2g}(1-\alpha_i^r)$ [21, p. 206]. (iv) $\Rightarrow$ (ii): Trivial.

For the necessity of the last condition $N_r(C) = q^r - a_r + 1$ where $a_r = \sum_{i=1}^{2g} \alpha_i^r$. For the sufficiency note that by 1.7A the coefficients of $g!P_1$ may be written as polynomials in the a_r with integral coefficients.■

For $g \leq 2$ very special curves are supersingular because there is only one Newton polygon with all slopes positive.

Naïvely we might expect the dimension of the moduli with given Hasse invariants to be analogous to the following for linear maps.

Lemma 2.7. *Let $\eta(0), \ldots, \eta(g)$ be nonnegative integers where $g = \eta(0)$ such that $\eta(i)$ is a nonincreasing convex function. Identify the matrices of order g over a field with affine g^2-space. $\{P \in A^{g^2} : \text{ rank } P^i \leq \eta(i) \text{ for every } i\}$ is an algebraic set of dimension $g^2 - \sum_{i=0}^{g-1}(\eta(i) - \eta(i+1))^2$.*

Sketch of proof. The lemma follows by induction from the following claim: The set of $m \times n$ matrices of rank $\leq r$ is algebraic of dimension $mn - (m-r)(n-r)$. We see that it is algebraic by simply setting all the subdeterminants of order $r+1$ to zero. Each of the first r rows depends generically on n parameters, and each of the last $m-r$ rows is generically a linear combination of the first rows and hence depends on r parameters. So generically a matrix depends on $rn+(m-r)r$ parameters.

Hence, the condition dim $PX \leq \eta(1)$ imposes $(g-\eta(1))^2$ independent algebraic conditions on a linear transformation P acting on a space X of dimension g. (In fact we have the additional information that these conditions are homogeneous of degree $\eta(1)+1$, the degree of the next larger subdeterminants.) Replacing X by P^iX allows one to complete the induction.∎

Remark 2.7.1. The $\{\eta(i)-\eta(i+1)\}$ form the dual partition of $g-\eta(g)$ given by the invariants of the nilpotent part of a generic P. By the invariants of a nilpotent matrix we mean those that come from its Jordan canonical form.

As mentioned in the introduction the reason this analogy is naïve is that the Hasse invariants are telling us something about the Jacobian, which exists in the $\frac{1}{2}g(g+1)$ dimensional moduli of polarized abelian varieties. Hence, a better candidate for our analogy would be to ask the same question for upper triangular matrices of order g which do form a $\frac{1}{2}g(g+1)$ dimensional space. In this case the analogous result is $(g^2+\eta(g)-\sum_{i=0}^{g-1}(\eta(i)-\eta(i+1))^2)/2$, so let us make the following conjectures. The first one would generalize 2.3A. Recall that an object is *indecomposable* if cannot be written as the product of proper subobjects, and it is *simple* if it has no proper subobjects.

Conjecture 2.8. *(a) Let A be a supersingular abelian variety and let $\{p_j\}$ be the partition of g dual to $\{\eta(i)-\eta(i+1)\}$. Then $A \cong \prod A_j$ where A_j is an indecomposable supersingular abelian variety of dimension p_j.*

(b) Let $\eta(0), \ldots, \eta(g)$ be nonnegative integers where $g=\eta(0)$ such that $\eta(i)$

is a decreasing convex function. The dimension of the moduli of g-dimensional principally polarized abelian varieties with Hasse invariants $\eta(i)$ is equal to

$$\frac{1}{2}(g^2 + \eta(g) - \sum_{i=0}^{g-1}(\eta(i) - \eta(i+1))^2).$$

(c) The dimension of the moduli of g-dimensional principally polarized abelian varieties with Newton polygon $f(i)$ is equal to the number of lattice points (a, b) satisfying $f(a) \leq b < a$ and $0 < a \leq g$.

2.8(b) gives the right answer for ordinary and for superspecial moduli. (c) also gives the right answer for ordinary moduli and gives $[\![g^2/4]\!]$ for supersingular moduli, which agrees with Oort [27]. (b) and (c) also agree with Theorem 7 of Koblitz [16].

We now give some sufficient conditions for superspecialty. The following provides a way of determining if a complete intersection is superspecial in terms of only its defining equations by noticing that $H^1(X, \mathcal{O}_X)$ can be computed as a sort of Čech homology (compare to [1, p. 186]).

Theorem 2.9. *If X is a curve which is a complete intersection in $\mathbf{P}^{r+1}$ defined by $f_1, \ldots, f_r$ of degrees $d_1, \ldots, d_r$ then*

$$0 \to H^1(X, \mathcal{O}_X) \to C^{r-1} \to \cdots \to C^0 \to 0$$

is an exact sequence where

$$C^n = \prod_{i_0 < \cdots < i_n} H^{r+1}(\mathbf{P}^{r+1}, \mathcal{O}_{\mathbf{P}^{r+1}}(-d_{i_0} - \cdots - d_{i_n}))$$

and $d : C^{n+1} \to C^n$ is defined by

$$(d\alpha)_{i_0 \cdots i_n} = \sum_i f_i \alpha_{i i_0 \cdots i_n}.$$

Here we have the usual convention that α is antisymmetric in its indices, and for $H^{r+1}(\mathbf{P}^{r+1}, \mathcal{O}_{\mathbf{P}^{r+1}}(-m))$ we are using the natural basis [H, III.5.1]

$$\{x_0^{l_0} \cdots x_{r+1}^{l_{r+1}} : l_i < 0, \sum l_i = -m\}.$$

The genus of this curve is $d_1 \cdots d_r(d_1 + \cdots + d_r - r - 2)/2 + 1$. Furthermore, if F is the Frobenius morphism on X and F_1 is Frobenius on $\mathbf{P}^{r+1}$, then under F^* this exact sequence maps to itself via F_1^* on $H^{r+1}(\mathcal{O}(-d_{i_0} - \cdots - d_{i_n}))$ followed by multiplication by $(f_{i_0} \cdots f_{i_n})^{p-1}$.

In particular let X be a planar curve defined by the homogeneous equation $f(x, y, z) = 0$ of degree d. Then X is superspecial if and only if the coefficients of $x^{kp-h}y^{ip-j}z^{(d-k-i)p+h+j-d}$ for $0 < k, h, i, j, k+i, h+j < d$ in f^{p-1} are 0.

Proof. From the short exact sequences of sheaves

$$0 \to \mathcal{O}_{V(f_{i_0} \cdots f_{i_{s-1}})}(-d_{i_s} - \cdots - d_{i_n}) \xrightarrow{f_{i_s}} \mathcal{O}_{V(f_{i_0} \cdots f_{i_{s-1}})}(-d_{i_{s+1}} - \cdots - d_{i_n})$$
$$\to \mathcal{O}_{V(f_{i_0} \cdots f_{i_s})}(-d_{i_{s+1}} - \cdots - d_{i_n}) \to 0,$$

its long exact sequence, [H, III.5.1 and Ex. III.5.5c], and induction we obtain an r-tuple complex of short exact sequences, a typical line of which looks like

$$\begin{aligned} 0 &\to H^{r-s}(\mathcal{O}_{V(f_{i_0} \cdots f_{i_s})}(-d_{i_{s+1}} - \cdots - d_{i_n})) \\ &\to H^{r-s+1}(\mathcal{O}_{V(f_{i_0} \cdots f_{i_{s-1}})}(-d_{i_s} - \cdots - d_{i_n})) \\ &\xrightarrow{f_{i_s}} H^{r-s+1}(\mathcal{O}_{V(f_{i_0} \cdots f_{i_{s-1}})}(-d_{i_{s+1}} - \cdots - d_{i_n})) \to 0. \end{aligned}$$

Going from an exact r-tuple complex to an exact sequence is completely analogous to the procedure for double complexes and yields the above exact sequence.

For the second assertion use [H, Ex. II.8.4e] to compute the degree of the canonical bundle in two different ways namely $2g-2 = d_1 \cdots d_r(d_1 + \cdots + d_r - r - 2)$. Alternately, we may calculate from our first assertion that the genus is

$$\binom{d_1 + \cdots + d_r - 1}{r+1} - \binom{d_2 + \cdots + d_r - 1}{r+1} - \cdots - \binom{d_1 + \cdots + d_{r-1} - 1}{r+1}$$

$$+\binom{d_3+\cdots+d_r-1}{r+1}+\cdots=1+\sum_{i_1=1}^{d_1}\cdots\sum_{i_r=1}^{d_r}(i_1+\cdots+i_r-r-1).$$

The third assertion follows from the proof of [H, IV.4.21] by induction.

For the last assertion write the basis of $H^2(\mathbf{P}^2,\mathcal{O}_{\mathbf{P}^2}(-d))$ as $x^{-h}y^{-j}z^{h+j-d}$ for $0<h,j,h+j<d$.∎

Theorem 2.10. *Let the curve X be embedded in $\mathbf{P}^1\times\mathbf{P}^1$ with bihomogeneous equation $f(w,z;x,y)=0$ of bidegree (a,b) and genus $(a-1)(b-1)$. Then X is superspecial if and only if the coefficients of $w^{kp-h}z^{(a-k)p+h-a}x^{ip-j}y^{(b-i)p+j-b}$ for $0<k,h<a$ and $0<i,j<b$ in f^{p-1} are 0.*

Proof. The proof is nearly identical to the planar case above except that we need to note that by a similar proof $H^1(X,\mathcal{O}_X)\cong H^2(\mathbf{P}^1\times\mathbf{P}^1,\mathcal{O}_{\mathbf{P}^1\times\mathbf{P}^1}(-a,-b))$, which has basis $w^{-h}z^{h-a}x^{-j}y^{j-b}$ for $0<h<a$ and $0<j<b$.∎

The following is an easy generalization of [11, Lemma 1.1(ii)].

Corollary 2.11. *Let X be the hyperelliptic curve whose function field is given by $y^2=f(x)$ where f is a polynomial with distinct roots of degree $2g+1$ or $2g+2$. X is superspecial if and only if the coefficients of x^{ip-j} for $1\le i,j\le g$ in $f^{(p-1)/2}$ are 0.*

Proof. Embed the hyperelliptic curve in $\mathbf{P}^1\times\mathbf{P}^1$ by the equation $w^2f_1(x,y)=z^2f_2(x,y)$ of bidegree $(2,g+1)$ where $f_1f_2=y^{2g+2}f(x/y)$ and f_i is homogeneous of degree $g+1$. Now apply Theorem 2.10 to $w^2f_1-z^2f_2$ and notice that this forces $k=h=1$, so we need only examine the terms of $w^{p-1}z^{p-1}(f_1f_2)^{(p-1)/2}$.∎

Corollary 2.12. *The following are superspecial curves, the first three of which are hyperelliptic.*

(a) $y^2=x^{2g+2}-1$ *if* $p\equiv-1 \bmod 2g+2$.

(b) $y^2 = x^{2g+1} - 1$ *if* $p \equiv -1 \bmod 2g+1$.

(c) $y^2 = x(x^{2g} - 1)$ *if* $p \equiv 2g+1, -1 \bmod 4g$.

(d) The Fermat curve $x^d + y^d + z^d = 0$ *of genus* $\binom{d-1}{2}$ *if* $p \equiv -1 \bmod d$.

Proof. We shall prove (c); the others are similar. For a coefficient to be nonzero it is necessary that $ip - j \equiv (p-1)/2 \bmod 2g$ for some $1 \leq i, j \leq g$. If $p \equiv 2g+1 \bmod 4g$ this means $i - j \equiv g \bmod 2g$, and if $p \equiv -1 \bmod 4g$ this means $i + j \equiv 1 \bmod 2g$, both of which are impossible.∎

The following generalizes part of 1.9A.

Theorem 2.13A (Ekedahl [5]). *A superspecial curve may be written over* $\mathbf{F}_{p^2}$. *If* $g > \frac{1}{2}(p^2 - p)$ *there are no superspecial curves, if* $g > \frac{1}{2}(p-1)$ *there are no superspecial hyperelliptic curves unless* $g = 1$ *and* $p = 2$*, and both of these bounds are sharp. In particular for every* p *there are only finitely many superspecial curves.*

Sketch of proof. For the first conclusion use 1.9A, and then use 1.3A to conclude that if $q = p^2$ $N_1 = 1 \pm 2gp + p^2$ with a minus sign if the curve is hyperelliptic. If the sign is minus $1 \leq N_1$ implies $g \leq p/2$. If the sign is positive $N_1 \leq N_2 = 1 - 2gp^2 + p^4$ implies $g \leq (p^2 - p)/2$. The sharpness follows from Corollary 2.12(d) with $d = p+1$, which is elliptic if $p = 2$, and 2.12(a) or (c) with $g = (p-1)/2$. For the last statement we only need to note that by 3.9A there are only finitely many superspecial curves for fixed g and p.∎

Theorem 2.14A (Ekedahl [5]). *Let* C *be a curve and* $G \leq Aut(C)$ *such that*

(1) G *is abelian,*

(2) $C/G \cong \mathbf{P}^1$ *and is ramified at* 3 *points, and*

(3) $p \equiv -1 \bmod n$ *where* n *is the exponent of* G.

Then C *is superspecial.*

Superspecial Curves

The curves in 2.14A can be realized as images of the Fermat curve of degree n. The following theorem generalizes 2.11, and its corollary generalizes 2.12.

THEOREM 2.15. *The curve defined by $y^n = f(x)$ where f is of degree r with distinct roots has genus $g = \frac{(n-1)(r-1)+1-(n,r)}{2}$ if $p \not| \, n$. It is superspecial if and only if the coefficients of x^{hp-k} for $1 \le h < ri/n, 1 \le k < rj/n$ in $f^{(ip-j)/n}$ for $1 \le i, j < n$ with $n | ip - j$ are* 0.

Proof. If we think of $y^n = f(x)$ as an affine curve, its projective closure is nonsingular except for a severe singularity at infinity. After blowing up at infinity a number of times we finally get $d = (r, n)$ distinct nonsingular points at infinity. Call these $Q_1, \ldots, Q_d$, call the affine points for which $y = 0$ $P_1, \ldots, P_r$, and call the affine points for which $x = 0$ $R_1, \ldots, R_n$. Hence, if we write divisors multiplicatively

$$(x) = \frac{R_1 \cdots R_n}{(Q_1 \cdots Q_d)^{n/d}} \text{ and } (y) = \frac{P_1 \cdots P_r}{(Q_1 \cdots Q_d)^{r/d}}.$$

Because $ny^{n-1}dy = f'(x)\ dx$, $n \neq 0$, and f and f' have no common roots, we also have

$$(dx) = \frac{(P_1 \cdots P_r)^{n-1}}{(Q_1 \cdots Q_d)^{n/d+1}} \text{ and } (dy) = \frac{S_1 \cdots S_{n(r-1)}}{(Q_1 \cdots Q_d)^{r/d+1}}$$

where $S_1, \ldots, S_{n(r-1)}$ are the zeros of f'. ¿From either of these formulas we can calculate that the genus satisfies $2g-2 = nr - r - n - d$. Now let $\omega_{k,j} = x^{k-1}dx/y^j$. Because

$$(\omega_{k,j}) = (R_1 \cdots R_n)^{k-1}(P_1 \cdots P_r)^{n-1-j}(Q_1 \cdots Q_d)^{(rj-nk-d)/d},$$

this differential is holomorphic if $1 \le j \le n-1$ and $1 \le k \le (rj-d)/n < rj/n$. (There is no integer strictly between $(rj-d)/n$ and rj/n by definition of greatest common divisor.) Counting the number of lattice points in this half rectangle, we see there are $\frac{(n-1)(r-1)+1-(n,r)}{2}$ holomorphic differentials of this form. Since they are linearly independent, they form a basis of $H^0(C, \Omega_C)$.

Superspecial Curves

To conclude the proof we examine the Cartier-Manin and Hasse-Witt matrices which describe the action of Frobenius on $H^0(C, \Omega_C)$. Following Manin [19] via Yui [29] let

$$f(x)^{(ip-j)/n} = \sum_{m=0}^{N_{i,j}} c_m^{i,j} x^m$$

where $n | ip - j$.

$$\begin{aligned}\omega_{k,j} &= x^{k-1}y^{-ip}y^{ip-j}dx = y^{-ip}\sum_{m=0}^{N_{i,j}} c_m^{i,j}x^{m+k-1}dx\\ &= d(y^{-ip}\sum_{m+k\not\equiv 0 \bmod p} c_m^{i,j}\frac{x^{m+k}}{m+k}) + \sum_{1\le h<ri/n} c_{hp-k}^{i,j}\frac{x^{(h-1)p}}{y^{ip}}x^{p-1}dx.\end{aligned}$$

The definition of the Cartier operator $\mathcal{C}$ tells us that

$$\mathcal{C}(\omega_{k,j}) = \sum_{1\le h<ri/n}(c_{hp-k}^{i,j})^{1/p}\omega_{h,i},$$

which defines the Cartier-Manin matrix $A^{(1/p)}$. Because the Hasse-Witt matrix A equaling 0 is equivalent to superspecialty we are done.∎

Corollary 2.16. *The following curves of genus $g = \frac{(n-1)(r-1)+1-(n,r)}{2}$ are superspecial.*

(a) $y^n = x^r - 1$ if $p \equiv -1 \bmod \frac{nr}{(n,r)}$.

(b) $y^n = x^r - x$ if $p \equiv -1 \bmod n(r-1)$ or if $r \equiv -1 \bmod n$ and $p \equiv r \bmod n(r-1)$.

Proof. We continue with the notation of 2.15 If $p \equiv -1 \bmod n$ then $i + j = n$ and $2 \le h + k < r$. In (a) for the coefficient of x^{hp-k} to be nonzero r must divide $hp-k$. However, if $p \equiv -1 \bmod r$, $hp - k \equiv -h - k \not\equiv 0 \bmod r$. In (b) for the coefficient of x^{hp-k} to be nonzero $n(r-1)$ must divide $n(hp-k) - (ip-j)$. However, if $p \equiv -1 \bmod n(r-1)$, $n(hp-k) - (ip-j) \equiv n(-h-k) + i + j \equiv n(-h-k+1) \not\equiv 0 \bmod n(r-1)$. On the other hand, if $p \equiv r \bmod n(r-1)$ where $r \equiv p \equiv -1 \bmod n$,

$$n - jr < n(h-k) < ir - n < ir - j < ir = nr - jr = n - rj + n(r-1)$$

which makes $n(hp-k)-(ip-j) \equiv n(hr-k)-(ir-j) \equiv n(h-k)-(ir-j) \equiv 0 \bmod n(r-1)$ impossible.

Alternately, we could simply apply 2.14A to $\mathbf{Z}/n \times \mathbf{Z}/r$ in (a) and to $\mathbf{Z}/n(r-1)$ in (b) because Ekedahl actually achieved a slightly broader condition than 2.14A(3).∎

More generally we have the following corollary of 2.14A.

Corollary 2.17. *The following two curves are superspecial if* $p \equiv -1 \bmod n$.

(a) $x + y^a = x^b y^c$ *which has genus* $g = \frac{ab-a+c+1-(b,a-c)-(b-1,c)}{2}$ *for* $n = ab-a+c$.

(b) $1 + y^a = x^b y^c$ *which has genus* $g = \frac{ab-a+2-(b,a-c)-(b,c)}{2}$ *for* $n = \frac{ab}{(a,b,c)}$.

Proof. Apply 2.14A to $\mathbf{Z}/(ab-a+c)$ in (a) and to $\mathbf{Z}/\frac{ab}{(a,b,c)} \times \mathbf{Z}/(a,b,c)$ in (b).∎

The following is another corollary of 2.15.

Corollary 2.18. *The curve defined by* $y^n = (x^r-1)(x^r-a), a \neq 0, 1$ *is superspecial if and only if a satisfies* $F_p(j/n, k/r, 1-j/n+k/r; a) = 0$ *for every* $1 \leq j < n$ *and* $1 \leq k < 2rj/n$ *such that there exists* $1 \leq i < n$ *and* $1 \leq h < 2ri/n$ *with* $n|ip-j$ *and* $r|hp-k$. *Consequently, if* $ip \equiv j \bmod n$ *with* $0 < i, j < n/2$ *there are no such curves.*

The curve defined by $y^n = x(x^r-1)(x^r-a), a \neq 0, 1$ *is superspecial if and only if a satisfies* $F_p(j/n, k/r - j/nr, 1 - j/n - j/nr + k/r; a) = 0$ *for every* $1 \leq j < n$ *and* $1 \leq k < (2r+1)j/n$ *such that there exists* $1 \leq i < n$ *and* $1 \leq h < (2r+1)i/n$ *with* $n|ip-j$ *and* $r|hp-k-(ip-j)/n$.

Proof. When we apply 2.15 we find that the coefficient of x^{hp-k} is $G(\frac{ip-j}{n}, \frac{hp-k}{r}; a)$ up to a constant where G is the polynomial that appears before Theorem 1.8A. This completes the proof of all but the nonexistence statement. If $ip \equiv j \bmod n$ then $(n-i)p \equiv n-j \bmod n$ so assume instead $n/2 < i, j < n$. If we let $k = h = r$, then $F_p(j/n, 1, 2 - j/n)$ has the same roots besides 0 and 1 as $F_p(1 - j/n, 0, j/n)$ which is constant, so there are no such curves.∎

3 Automorphisms and the number of superspecial curves

The main result of this chapter is to determine the number of superspecial curves of genus 3 with a given automorphism group and to give a simpler proof of the analogous result for genus 2. First for $p > 2g+1$ we shall find all the automorphism groups of hyperelliptic curves and of genus 3 curves. To make use of Hashimoto's tables in Theorem 3.8A we then find their representations in $SL(2g, \mathbf{Z})$. We say $SL(2g, \mathbf{Z})$ instead of $SL(2g, \mathbf{Z}_l)$ as in Lemma 1.4A because if $p > 2g+1$ we shall see that the curve can be lifted with its automorphism group to characteristic zero where this representation is simply the action of the group on the singular homology of the Riemann surface. However, since we are really only interested in the characteristic polynomials in this representation we are able to avoid doing the calculations so explicitly.

Lemma 3.1. *Let f be a polynomial of degree $2g+1$ or $2g+2$ with distinct roots, let σ be an automorphism of the hyperelliptic curve $y^2 = f(x)$, let $\overline{\sigma} : x \to (ax+b)/(cx+d)$ be its image in $PGL(2)$ that permutes the roots of f and has order $n > 1$, and let μ_1 and μ_2 be the eigenvalues of $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. (Here we call ∞ a root if f has odd degree.) Up to the sign σ is given by*

$$\sigma : (x, y) \to \left(\frac{ax+b}{cx+d}, \frac{\pm\sqrt{\mu_1^{2g+2}}}{(cx+d)^{g+1}} y \right)$$

if $\overline{\sigma}$ fixes $i = 0$ roots of f,

$$\sigma : (x, y) \to \left(\frac{ax+b}{cx+d}, \frac{\pm\sqrt{\mu_1^{2g+1}\mu_2}}{(cx+d)^{g+1}} y \right)$$

if $\overline{\sigma}$ fixes $i = 1$ root r of f and $\mu_2 = a - cr$, or

$$\sigma : (x, y) \to \left(\frac{ax+b}{cx+d}, \frac{\pm\sqrt{\mu_1^{2g}\mu_1\mu_2}}{(cx+d)^{g+1}} y \right)$$

if $\overline{\sigma}$ fixes $i = 2$ roots of f. Consequently, if n is even, then $\sigma^n = (-1)^{i/2}$. If n is odd, then $\sigma^n = \pm 1$ depending on the choice of the sign above.

Proof. We shall assume f has even degree. Dealing with the infinite root requires only a slight modification of our argument. If $f(x) = e\prod(x-r)$ then

$$f(\frac{ax+b}{cx+d}) = e\prod_r(x - \frac{dr-b}{-cr+a})\prod_r\frac{a-cr}{cx+d} = f(x)\prod_r\frac{a-cr}{cx+d}$$

because $\binom{d\ -b}{-c\ a}$ is the inverse of A. When we calculate the product in the numerator for one orbit we discover that it telescopes.

$$\prod_{\text{orbit}}(a{-}cr) = \frac{(\,0 \quad ad-bc\,)\,I\begin{pmatrix} r \\ 1\end{pmatrix}}{(\,0 \quad 1\,)\,A\begin{pmatrix} r \\ 1\end{pmatrix}}\cdots\frac{(\,0 \quad ad-bc\,)\,A^{n-1}\begin{pmatrix} r \\ 1\end{pmatrix}}{(\,0 \quad 1\,)\,A^{n}\begin{pmatrix} r \\ 1\end{pmatrix}} = \frac{(ad-bc)^n}{\mu_2^n} = \mu_1^n.$$

Note here that $\mu_1^n = \mu_2^n$ by definition of n. Hence, if f has no fixed roots

$$f(\frac{ax+b}{cx+d}) = f(x)\left(\frac{\mu_1}{cx+d}\right)^{2g+2},$$

from which the result follows. For the other two cases simply note that $\frac{ar+b}{cr+d} = r$ implies that $a - cr$ is an eigenvalue of A. In case $r = \infty$ is a fixed point $c = 0$, and we should interpret $a - cr$ as d.

For the last two statements if $i = 2$ and n is even, note that $(\mu_1/\mu_2)^{n/2}$ must be -1, so σ^n yields $(x, -y)$. The other cases are even easier.■

Lemma 3.2. *The following is a complete list of reduced automorphism groups of hyperelliptic curves of genus $g \geq 2$ and characteristic $p > 2g+1$.*

(a) A_5 if $g \equiv 0, 4 \bmod 5$ and $g \equiv 0, 2 \bmod 3$.

(b) S_4 if $g \equiv 0, 2 \bmod 3$.

(c) A_4 if $g \neq 2, 3$.

(d) D_{2n} if $n|2g+2$.

(e) D_{2n} if $n|2g, g \neq 2$.

(f) $\mathbf{Z}/n$ *if* $n|2g+2, n \neq 2g+2, g+1$.

(g) $\mathbf{Z}/n$ *if* $n|2g+1$.

(h) $\mathbf{Z}/n$ *if* $n|2g, n \neq 2g, g$.

(i) D_4.

(j) $\mathbf{Z}/2$.

(k) $\mathbf{Z}/1$.

Proof. The reduced group is a subgroup of the automorphisms of $\mathbf{P}^1$ that permutes the $2g+2$ points of ramification. By Corollary 1.5 G does not have an element of order p. The only finite subgroups of $PGL(2)$ without an element of order p are the cyclic groups $\mathbf{Z}/n$, dihedral groups D_{2n}, A_4, S_4, and A_5, which have respective orbit lengths (1,1), (n,n,2), (4,4,6), (6,8,12), and (12,20,30), where here we only list lengths not equal to the order of the group.

For (a) we must be able to write $2g+2 = 12a+20b+30c+60d$ where $a, b, c = 0$ or 1 and d is nonnegative. If $g \equiv 0, 5, 9, 14 \bmod 15$, let $(a, b) = (1, 1), (1, 0), (0, 1), (0, 0)$, respectively, and choose c and d such that $c + 2d = (g + 1 - 6a - 10b)/15$.

For (b) we must be able to write $2g+2 = 6a+8b+12c+24d$ where $a, b, c = 0$ or 1 and d is nonnegative. If $g \equiv 0, 2 \bmod 3$, let $b = 1, 0$, respectively, and choose a, c and d such that $a + 2c + 4d = (g + 1 - 4b)/3$.

For (c) we must be able to write $2g + 2 = 4a + 6b + 12c$ where $a = 0, 1, 2$, $b = 0, 1$, and c is nonnegative. If $g \equiv 0, 1, 2 \bmod 3$, let $a = 2, 1, 0$, respectively, and choose b and c such that $b + 2c = (g + 1 - 2a)/3$.

The remaining cases are similar. For (d), (e), and (i) we must be able to write $2g + 2 = 2a + nb + 2nc$ where $a = 0, 1$, $b = 0, 1, 2$, and c is nonnegative. For (f), (g), (h), (j), and (k) we must be able to write $2g + 2 = a + nb$ where $a = 0, 1, 2$ and b is nonnegative. Conversely, $y^2 = f(x)$ has one of these subgroups as its reduced automorphism group if the roots of f are a union of these orbits. We make the exclusions in (c), (e), (f), and (h) because in these cases there are extra symmetries, namely S_4, S_4, D_{4g+4}, and D_{4g}, respectively. (i), (j), and (k) are actually $n = 1, 2$ in (d)-(h) and are listed separately because they occur for every g.∎

Next we would like to investigate the automorphism groups to which these lift and in particular in view of our introductory remarks to determine for which ones is $\Gamma \cong \{\pm 1\} \times \overline{\Gamma}$. Let -1 denote a central involution, and following [2, p. xviii] define

$$G(l,m,n) =< \sigma, \tau : \sigma^l = \tau^m = (\sigma\tau)^n = 1 >$$

$$G(l,m,n; \pm, \pm, \pm) =< \sigma, \tau, -1 : \pm\sigma^l = \pm\tau^m = \pm(\sigma\tau)^n = 1 > .$$

If $-1 \neq 1$ $G(l,m,n;\pm,\pm,\pm)$ has twice the order of $G(l,m,n)$. Note that the isomorphism class of a group is independent of the ordering of l, m, and n with their associated signs, and it is also independent of the sign associated to l if l is odd and m or n is even. We are interested in these groups because of the following isomorphisms

$$A_5 \cong G(2,3,5), \quad S_4 \cong G(2,3,4), \quad A_4 \cong G(2,3,3), \quad D_{2n} \cong G(2,2,n).$$

Clearly we always have $G(l,m,n;+,+,+) \cong \mathbf{Z}/2 \times G(l,m,n)$. Because A_5 has Schur multiplier $\mathbf{Z}/2$, its central extension $G(2,3,5;-,+,+) \cong SL(2,5)$ since it certainly does not split. We also have these isomorphisms in the dihedral case

$$G(2,2,n;+,+,-) \cong D_{4n}, \quad G(2,2,n;-,-,-) \cong Q_{4n},$$

$$G(2,2,n;+,-,+) \cong G(2,2,n;-,+,+), \quad G(2,2,n;+,-,-) \cong G(2,2,n;-,+,-),$$

$$G(2,2,2;+,-,+) \cong G(2,2,2;+,+,-) \cong D_8,$$

$$G(2,2,2;+,-,-) \cong G(2,2,2;-,-,+) \cong \mathbf{Z}/2 \times \mathbf{Z}/4.$$

If n is odd all four groups in the second line above are isomorphic to $G(2,2,n)$ because -1 is forced to be the identity and hence is not truly an involution. By counting the number of elements of orders 2 and 4 we can conclude that these are the only isomorphisms in the dihedral case.

Theorem 3.3. *The following is a complete list of automorphism groups of hyperelliptic curves of genus $g \geq 2$ and characteristic $p > 2g+1$.*

(a) Let $g \equiv 0, 5, 9, 14 \bmod 15$ and $\overline{\Gamma} \cong A_5$. If g is even, $\Gamma \cong G(2,3,5; -,+,+)$. If g is odd, $\Gamma \cong G(2,3,5;+,+,+)$.

(b) Let $g \equiv 0, 2 \bmod 3$ and $\overline{\Gamma} \cong S_4$. If $g \equiv 0 \bmod 4$, then $\Gamma \cong G(2,4,3; -,-,+)$. If $g \equiv 1 \bmod 4$, then $\Gamma \cong G(2,4,3;-,+,+)$. If $g \equiv 2 \bmod 4$, then $\Gamma \cong G(2,4,3;+,-,+)$. If $g \equiv 3 \bmod 4$, then $\Gamma \cong G(2,4,3;+,+,+)$.

(c) Let $g \neq 2, 3$ and $\overline{\Gamma} \cong A_4$. If g is even, $\Gamma \cong G(2,3,3;-,+,+)$. If g is odd, $\Gamma \cong G(2,3,3;+,+,+)$.

(d) Let $\overline{\Gamma} \cong D_{2n}$ where $2g+2 = nm, n > 2$. If m is even and no orbits have length n, $\Gamma \cong G(2,2,n;+,+,+)$. If $m \neq 2$ is even and two orbits have length n, $\Gamma \cong G(2,2,n;-,-,+)$. If m is odd, one orbit has length n and $\Gamma \cong G(2,2,n;+,-,+)$.

(e) Let $\overline{\Gamma} \cong D_{2n}$ where $2g = nm, n > 2, g \neq 2$. If m is even and no orbits have length n, $\Gamma \cong G(2,2,n;+,+,-)$. If $m \neq 2$ is even and two orbits have length n, $\Gamma \cong G(2,2,n;-,-,-)$. If m is odd, one orbit has length n and $\Gamma \cong G(2,2,n;+,-,-)$.

(f) If $\overline{\Gamma} \cong \mathbf{Z}/n$ for $n | 2g+2, n \neq 2g+2, g+1, 2$, then $\Gamma \cong \mathbf{Z}/2 \times \mathbf{Z}/n$.

(g) If $\overline{\Gamma} \cong \mathbf{Z}/n$ for $n | 2g+1$, then $\Gamma \cong \mathbf{Z}/2n \cong \mathbf{Z}/2 \times \mathbf{Z}/n$.

(h) If $\overline{\Gamma} \cong \mathbf{Z}/n$ for $n | 2g, n \neq 2g, g, 2$, then $\Gamma \cong \mathbf{Z}/2n$.

(i) Let $\overline{\Gamma} \cong D_4$.
If no orbits have length 2, g is odd and $\Gamma \cong G(2,2,2;+,+,+) \cong EA(8)$.
If 1 orbit has length 2, g is even and $\Gamma \cong G(2,2,2;+,+,-) \cong D_8$.
If 2 orbits have length 2, g is odd and $\Gamma \cong G(2,2,2;+,-,-) \cong \mathbf{Z}/2 \times \mathbf{Z}/4$.
If 3 orbits have length 2, $g \neq 2$ is even and $\Gamma \cong G(2,2,2;-,-,-) \cong Q_8$.

(j) Let $\overline{\Gamma} \cong \mathbf{Z}/2$. If no points are fixed, then $\Gamma \cong D_4$. If $g \neq 2$ and two points are fixed, then $\Gamma \cong \mathbf{Z}/4$.

(k) If $\overline{\Gamma} \cong \mathbf{Z}/1$, *then* $\Gamma \cong \mathbf{Z}/2$.

Proof. Because $g+1 = 6a+10b+15c+30d$ in the proof of 3.2(a) g is divisible by 2 (resp. 3, 5) if and only the orbit of length 30 (resp. 20, 12) is among the roots of f. Every element of order 2 in A_5 fixes two of the points of the orbit of length 30, so by 3.1 we are done. Because $g+1 = 3a+4b+6c+12d$ in (b) $g \equiv 0 \bmod 2$ (resp. $\equiv 0 \bmod 3$, $\equiv 0, 1 \bmod 4$) if and only if the orbit of length 6 (resp. 8, 12) is among the roots of f. Every element of order 4 in S_4 fixes two of the points of the orbit of length 6, and every odd element of order 2 in S_4 fixes two of the points of the orbit of length 12, so by 3.1 we are done. Because $g+1 = 2a+3b+6c$ in (c) g is even if and only if the orbit of length 6 is among the roots of f. Every element of order 2 in A_4 fixes two of the points of the orbit of length 6, so by 3.1 we are done. If n is even every noncentral element of order 2 in D_{2n} fixes two of the points of one of the orbits of length n, and the two elements of order 2 appearing in the representation of $G(2,2,n)$ fix points from distinct orbits. If n is odd every noncentral element of order 2 in D_{2n} fixes one point from each of the orbits of length n. Every element of order n in D_{2n} fixes both points from the orbit of length 2. These three observations and 3.1 suffice to prove (d), (e), and (i). A direct application of 3.1 proves (f), (g), (h), (j), and (k). We make the additional exclusions in (d), (e), (i), and (j) because again there are extra symmetries. ∎

As we mentioned in the first chapter nonhyperelliptic curves of genus 3 are planar quartic. Furthermore, since the embedding in $\mathbf{P}^2$ is canonical its automorphisms can be thought of as elements of $PGL(3)$ [H, IV.5.5.6]. A complete list of the finite subgroups of $PGL(3)$ and their fundamental invariants is a classical result of Blichfeldt, Dickson, and others. The list is independent of characteristic except when p divides the order, so we shall assume that we are in characteristic zero. For the following discussion we restrict our attention to three dimensions, but the generalization to n dimensions should be obvious. Elements of $PGL(3)$ are of course determined only modulo scalar matrices, so suppose we are given a set of representatives in $GL(3)$ of a finite subgroup of $PGL(3)$. By dividing by the cube root of the determinant we can assume our representatives are in $SL(3)$. Furthermore, since $SL(3)$ only contains three scalar matrices, the linear group generated by these representatives is a central extension of degree 1 or 3 of our original group. In the classical terminology our group is a collineation group of the linear group. An *invariant* of our group is a homogeneous polynomial in three variables preserved up to a constant by the action of the linear group elements. It is easy to see that this constant is a 1-dimensional group character, and we call an *absolute invariant* one whose character is trivial.

Given a linear representation calculating the number of invariants is straightforward. Let the element g_i have characteristic polynomial $p_i(z)$ normalized so that $p_i(0) = 1$. The generating function whose ith coefficient is the number of linearly independent invariants of character χ is given by

$$\frac{1}{|G|}\sum_i \frac{\chi(g_i)}{p_i(z)}$$

where the sum is over the linear group G. Consequently, the generating function of the number of all invariants is given by

$$\frac{1}{|G'|}\sum \frac{1}{p_i(z)}$$

where the sum is over G', the commutator subgroup. Bear in mind that only invariants of a given degree with the same character form a vector space; invariants with different characters may not be added. The reason these formulas work is that the natural action of the group on the $\binom{d+2}{2}$-dimensional space of homogeneous polynomials of degree d has character that is the sum of the $\binom{d+2}{2}$ monomials of degree d in the eigenvalues, and the generating function of these sums is just the reciprocal of the characteristic polynomial. Typically all invariants can be built up as polynomials in four *fundamental* invariants. Because we only have transcendence degree three there will be an algebraic relationship satisfied by the fundamental invariants, which is often nontrivial to find. For example, for the natural permutation representation of S_n this relationship describes how to write the discriminant in terms of the elementary symmetric functions.

Our task is to find those invariants which are irreducible nonsingular quartics in order to complete the classification of the automorphism groups of genus 3 curves. In the following theorem we shall only list the degrees of the fundamental invariants, and when necessary in the proof of the subsequent theorem we shall describe them more explicitly for a particular representation. (a) through (e) correspond to groups that are intransitive in the sense that they can be block diagonalized, (f) and (g) are imprimitive, and the remainder are primitive. We shall use $G_k(l, m, n; \pm, \pm, \pm)$ to denote $< \sigma, \tau, \omega_{2k} : \pm\sigma^l = \pm\tau^m = \pm(\sigma\tau)^n = 1 >$ where ω_{2k} is a central element of order $2k$ and $-1 = \omega^k$. Note that if k is odd $G_k(l, m, n; \pm, \pm, \pm) \cong \mathbf{Z}/k \times G(l, m, n; \pm, \pm, \pm)$.

Theorem 3.4A (Blichfeldt [20, pp. 236-254]). *The following is a complete list of the finite subgroups G of $PGL(3)$, for which the characteristic p does not divide the order of the group, preceded by the degrees of their fundamental invariants.*

(a) (1,1,1) $\mathbf{Z}/m \times \mathbf{Z}/n$.

(b) (1,2,n,n) $G_m(2, 2, n, -, -, -)$ *and some of its subgroups.*

(c) (1,4,4,6) $G_m(2, 3, 3, -, +, +)$ *and some of its subgroups.*

(d) (1,6,8,12) $G_m(2, 4, 3, -, -, +)$ *and some of its subgroups.*

(e) (1,12,20,30) $G_m(2, 3, 5, -, +, +)$ *and some of its subgroups.*

(f) (3,n,n,n) $\mathbf{Z}/3 \ltimes \mathbf{Z}/n \times \mathbf{Z}/n$ *and some of its subgroups which may have*

more invariants.

(g) (3,n,2n,3n) $S_3 \ltimes \mathbf{Z}/n \times \mathbf{Z}/n$ *and some of its subgroups.*

(h) (3,3,6,9) $\mathbf{Z}/4 \ltimes \mathbf{Z}/3 \times \mathbf{Z}/3$.

(i) (6,6,6,9) a group of order 72 containing the above group.

(j) (6,9,12,12) a group of order 216 containing the above group.

(k) (2,6,10,15) A_5.

(l) (4,6,14,21) $PSL(2,7)$.

(m) (6,12,30,45) A_6.

We immediately observe that only (a), (b), (c), (f), (g), and (l) could produce irreducible quartics. Of these all but (c) and (l) can be described as the semidirect product of a permutation group and a diagonal abelian group. The idea of the following proof is to find the diagonal abelian groups, account for the groups in (c) and (l), and then see which semidirect products are possible. Kuribayashi and Komiya [18] have a considerably longer proof of the following.

Theorem 3.5. *The following is a complete list of automorphism groups of nonhyperelliptic curves of genus 3 and characteristic* $p > 7$.

(a) $\mathbf{Z}/1$.

(b) $\mathbf{Z}/2$ *for* $x^4 + y^4 + dy^2z^2 + z^4 + x^2(ay^2 + byz + cz^2)$.

(c) $\mathbf{Z}/3$ *for* $x^3(y + bz) + y^4 + ay^2z^2 + z^4$.

(d) D_4 *for* $x^4 + y^4 + z^4 + ax^2y^2 + bx^2z^2 + cy^2z^2$.

(e) $\mathbf{Z}/6$ *for* $x^4 + y^4 + z^3y + ax^2y^2$.

(f) D_6 *for* $x^3z + y^3z + z^4 + axyz^2 + bx^2y^2$.

(g) D_8 *for* $x^4 + y^4 + z^4 + ax^2y^2 + bx^2z^2 + by^2z^2$.

(h) $\mathbf{Z}/9$ *for* $x^4 + y^3x + z^3y$.

(i) $G_2(2,2,2,-,-,-)$ *of order* 16 *for* $x^4 + y^4 + ay^2z^2 + z^4$.

(j) $S_4 \cong S_3 \ltimes \mathbf{Z}/2 \times \mathbf{Z}/2$ *for* $x^4 + y^4 + z^4 + a(x^2y^2 + x^2z^2 + y^2z^2)$.

(k) $G_2(2,3,3,-,+,+)$ *of order* 48 *for* $x^4+y^4+z^3y$.

(l) $S_3 \ltimes \mathbf{Z}/4 \times \mathbf{Z}/4$ *for* $x^4+y^4+z^4$.

(m) $PSL(2,7)$ *for* $x^3y+y^3z+z^3x$.

Proof. When we mention an invariant we of course mean for a particular representation of the group. Because $p > 2g+1$ p does not divide the order of the automorphism group. A nonsingular irreducible quartic must have at least one of the terms x^4, x^3y, and x^3z because otherwise $(1,0,0)$ is a singular point. Similarly, it must have one of y^4, y^3x, and y^3z and one of z^4, z^3x, and z^3y. Let us determine what cyclic groups may arise. If i and j are relatively prime, then one of i, j, or $i-j$ must be relatively prime to an integer n that has no more than two prime factors. Hence, if n has no more than two prime factors, we can without loss of generality assume that a cyclic group of order n in $PGL(3)$ is generated by $(x,y,z) \to (\omega_n x, \omega_n^i y, z)$. Applying this automorphism to the above monomials and setting the characters of one of each triple equal, we have twenty-seven possibilities. For two possibilities $n|12$ and $i=4$ or -3, for two $n|8$ and $i=4,-3$, for four $n|9$ and $i=4,-3,3,-2$, for two $n|7$ and $i=3,-2$, for two $n|6$ and $i=3,-2$, for three $n|4$ and i is arbitrary, for three $n|2$ and i is arbitrary, and for nine $n|3$ and i is arbitrary. Because of the obvious symmetry between i and $1-i$ we shall only need to consider half of these cases. If $n=7$ none of the other twelve monomials have the same character, so we must have the Klein curve, the quartic in 3.4A(l), which gives (m). Hence, for all other groups only the two primes 2 and 3 can divide the order, so we need not consider any other cyclic groups. If $i=4$ and $n=12, 9$, or 8 the characters of the other monomials again tell us that we can only have a trinomial, namely $x^4+y^4+z^3y$ for $n=12$, $x^4+y^3x+z^3y$ for $n=9$, and $x^4+y^3z+z^3y$ for $n=8$. If $n=6$ we can pick up an additional monomial to obtain $x^4+y^4+z^3y+ax^2y^2$. If $n=4$ the most general curve is $x^4+f(y,z)$ where f is a homogeneous quartic with distinct factors. If $n=3$ the most general curve is $f(x,y)+z^3x+z^3y$ where again

f is a homogeneous polynomial with distinct factors. If $n = 2$ the most general curve is $x^4 + f(y,z) + x^2(ay^2 + byz + cz^2)$. If $i = 3$ and $n = 9, 3$ or 2 we get isomorphic curves, and if $n = 6$ we get $x^3z + y^3z + z^3y$, which is reducible. The only case that remains is $i = -1, n = 3$, in which case the most general curve is $x^3z + y^3z + z^4 + axyz^2 + bx^2y^2$ up to isomorphism.

Now we need to check which of these groups may be extended to a diagonal noncyclic group. This consists of scaling x and y by roots of unity and then seeing if we can get any group elements other than those already listed for some choice of the arbitrary coefficients. Essentially the same calculations show that the cyclic groups of orders $n = 12, 9, 8$, and 6 cannot be extended to such a noncyclic group. Applying this analysis to $n = 4$ we find that the only way to get a noncyclic group is to exclude the y^3z and yz^3 terms, in which case we see that $x^4 + y^4 + z^4 + ax^2y^2$ has $\mathbf{Z}/4 \times \mathbf{Z}/2$ diagonal symmetries and that $x^4 + y^4 + z^4$ has $\mathbf{Z}/4 \times \mathbf{Z}/4$ diagonal symmetries. The other extensions turn out to be the cyclic groups of orders $n = 12$ and 8. Similarly for $n = 2$, $x^4 + y^4 + z^4 + ax^2y^2 + bx^2z^2 + cy^2z^2$ has $\mathbf{Z}/2 \times \mathbf{Z}/2$ diagonal symmetries, and all other extensions are cyclic. For $n = 3$ and $i = 4$ or -1 the only possible noncyclic diagonal extension is $\mathbf{Z}/3 \times \mathbf{Z}/3$, which corresponds up to isomorphism to the reducible curve $x^3z + y^3z + z^4$, and the only other extensions are the cyclic groups of orders $n = 12, 9$ and 6, the last being the one that gave rise to a reducible curve.

Before we determine which of the above curves allow semidirect products with permutations of x, y, and z, let us note that the curve with cyclic group of order 12 is one of the quartic invariants in 3.4A(c). The linear invariant is x and the quartic invariants are $y^4 + z^3y$ and $z^4 - 8y^3z$ for some representation of a $G_m(2, 3, 3, -, +, +)$. Hence, with x^4 there are three linearly independent quartics, and from them we can only create this curve up to isomorphism. To create this curve x^4 and $y^4 + z^3y$ must have the same character, and this determines which particular group we have. One linear group in $GL(3)$ whose collineations are the automorphisms of this curve is the direct product of $\mathbf{Z}/4$ and $G(2,3,3,-,+,+)$, and the kernel of the projection is $\mathbf{Z}/2$, which yields the group in (k). Also note that the curves from above with groups $\mathbf{Z}/8$ and $\mathbf{Z}/4 \times \mathbf{Z}/4$ are isomorphic to the Fermat curve, which is case (l).

The only curve that remains in which x, y, and z can be permuted evenly is $x^4+y^4+z^4+ax^2y^2+ax^2z^2+ay^2z^2$ with D_4 symmetry, in which case all permutations are allowed, which is case (j). All the rest permit some transposition of x, y, and z for some choice of the coefficients. x and y can be switched in $x^4+y^4+z^4+ax^2y^2$ which yields case (i). x and y can also be switched in $x^4+y^4+z^4+ax^2y^2+bx^2z^2+by^2z^2$ which yields case (g). Switching y and z in $x^4+f(y,z)$ for a symmetric f with cyclic group $\mathbf{Z}/4$ can be diagonalized to yield a $\mathbf{Z}/4 \times \mathbf{Z}/2$. Similarly, switching y and z in $x^4+f(y,z)+x^2(ay^2+byz+az^2)$ can be diagonalized to yield a D_4, switching x and y in $f(x,y)+z^3x+z^3y$ can be diagonalized to yield a $\mathbf{Z}/6$. Finally switching x and y in $x^3z+y^3z+z^4+axyz^2+bx^2y^2$ yields case (f). This concludes the proof of the theorem.∎

In the diagram after Theorem 3.15 is the lattice of reduced automorphism groups of genus 3 curves and the dimension of their moduli. The arrows point in the direction of specialization. The intersection indicates that in a natural way some reduced automorphism groups are assumed by both hyperelliptic and nonhyperelliptic curves. The labeling is consistent with that in Theorem 3.15.

It is now apparent why we can lift curves of genus 3 with their automorphisms for $p > 7$ to characteristic zero. We can explicitly write down the curves with a given automorphism group in terms of some parameters, and conversely curves with the given parameterization have the given automorphism group. Hence, to lift to characteristic zero simply lift the parameters. To make use of Hashimoto's tables in Theorem 3.8A we need to find the representation of these groups in singular homology. We could proceed in a number of different ways. We could calculate a $2g$-dimensional representation in singular homology or in a Weil cohomology, or we could calculate a g-dimensional representation in the space of differentials and take the direct sum with its complex conjugate or equivalently its image under the Rosati involution. The reason these methods lead to the same result is that the action on the period matrix of the Jacobian is the same as the action on homology on one hand and the same as the action on the underlying real structure of the complex torus on the other.

In the following lemma we shall abbreviate $(2,2)$ by D_4 and cyclic groups by their order, except 16 and 48 shall abbreviate $G_2(2,2,2,-,-,-)$ and $G_2(2,3,3,-,+,+)$, respectively. We also include genera 1 and 2, and for the sake of completeness we list those special groups with $p \leq 2g+1$. Note that $PGL(2,5) \cong S_5$, $S_3 \ltimes (4,4)$ is a semidirect product, and $PU(3,9)$ is the projective unitary group, which is simple of order 6048. We shall abuse the language slightly by saying that an automorphism has characteristic polynomial f_i if it has characteristic polynomial $f_i(x)$ or $f_i(-x)$.

Lemma 3.6. *In the representation of Theorem 1.4A the proportion of the automorphism group with a given characteristic polynomial is given by the following tables. (For the sake of convenience the polynomials f_i will be listed in Theorem 3.8A.)*

(a) For elliptic curves

$\overline{\Gamma}$	f_1	f_2	f_3
1	1		
2	$\frac{1}{2}$	$\frac{1}{2}$	
3	$\frac{1}{3}$		$\frac{2}{3}$
$D_6(p=3)$	$\frac{1}{6}$	$\frac{1}{2}$	$\frac{1}{3}$
$A_4(p=2)$	$\frac{1}{12}$	$\frac{1}{4}$	$\frac{2}{3}$

(b) For genus 2 curves

$\overline{\Gamma}$	f_1	f_2	f_6	f_7	f_9	f_{10}	f_{11}
1	1						
2	$\frac{1}{2}$	$\frac{1}{2}$					
D_4	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$				
5	$\frac{1}{5}$					$\frac{4}{5}$	
D_6	$\frac{1}{6}$	$\frac{1}{2}$		$\frac{1}{3}$			
D_{12}	$\frac{1}{12}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{6}$		
S_4	$\frac{1}{24}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{3}$			$\frac{1}{4}$
$PGL(2,p=5)$	$\frac{1}{120}$	$\frac{1}{12}$	$\frac{1}{8}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{5}$	$\frac{1}{4}$

(c) For hyperelliptic genus 3 *curves*

$\overline{\Gamma}$ (Γ)	f_1	f_2	f_8	f_9	f_{10}	f_{11}	f_{15}	f_{25}	f_{26}	f_{30}	f_{31}	f_{32}
1	1											
$2\ (4)$	$\frac{1}{2}$		$\frac{1}{2}$									
$2\ (2,2)$	$\frac{1}{2}$	$\frac{1}{2}$										
$D_4\ (2,4)$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$									
$D_4\ (EA(8))$	$\frac{1}{4}$	$\frac{3}{4}$										
D_6	$\frac{1}{6}$	$\frac{1}{2}$				$\frac{1}{3}$						
7	$\frac{1}{7}$										$\frac{6}{7}$	
D_8	$\frac{1}{8}$	$\frac{5}{8}$			$\frac{1}{4}$							
D_{12}	$\frac{1}{12}$	$\frac{1}{4}$	$\frac{1}{3}$			$\frac{1}{6}$			$\frac{1}{6}$			
D_{16}	$\frac{1}{16}$	$\frac{5}{16}$	$\frac{1}{4}$		$\frac{1}{8}$			$\frac{1}{4}$				
S_4	$\frac{1}{24}$	$\frac{3}{8}$			$\frac{1}{4}$	$\frac{1}{3}$						
$PGL(2,p=7)$	$\frac{1}{336}$	$\frac{1}{16}$	$\frac{1}{12}$		$\frac{1}{8}$	$\frac{1}{6}$		$\frac{1}{4}$	$\frac{1}{6}$		$\frac{1}{7}$	

(d) For nonhyperelliptic genus 3 *curves*

$\overline{\Gamma}$	f_1	f_2	f_8	f_9	f_{10}	f_{11}	f_{15}	f_{25}	f_{26}	f_{30}	f_{31}	f_{32}
1	1											
2	$\frac{1}{2}$	$\frac{1}{2}$										
3	$\frac{1}{3}$			$\frac{2}{3}$								
D_4	$\frac{1}{4}$	$\frac{3}{4}$										
6	$\frac{1}{6}$	$\frac{1}{6}$		$\frac{1}{3}$			$\frac{1}{3}$					
D_6	$\frac{1}{6}$	$\frac{1}{2}$				$\frac{1}{3}$						
D_8	$\frac{1}{8}$	$\frac{5}{8}$			$\frac{1}{4}$							
9	$\frac{1}{9}$			$\frac{2}{9}$								$\frac{2}{3}$
16	$\frac{1}{16}$	$\frac{7}{16}$			$\frac{1}{2}$							
S_4	$\frac{1}{24}$	$\frac{3}{8}$			$\frac{1}{4}$	$\frac{1}{3}$						
48	$\frac{1}{48}$	$\frac{7}{48}$		$\frac{1}{6}$	$\frac{1}{6}$		$\frac{1}{6}$			$\frac{1}{3}$		
$S_3 \ltimes (4,4)$	$\frac{1}{96}$	$\frac{5}{32}$			$\frac{1}{4}$	$\frac{1}{3}$		$\frac{1}{4}$				
$PSL(2,7)$	$\frac{1}{168}$	$\frac{1}{8}$			$\frac{1}{4}$	$\frac{1}{3}$					$\frac{2}{7}$	
$PU(3,p^2=9)$	$\frac{1}{6048}$	$\frac{1}{96}$		$\frac{1}{108}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{1}{12}$	$\frac{1}{4}$		$\frac{1}{6}$	$\frac{2}{7}$	

Proof. We can treat the hyperelliptic curves in general using Lemma 3.1. A basis for the space of differentials is $\{dx/y, \ldots, x^{g-1}dx/y\}$, and $d(\frac{ax+b}{cx+d}) = \frac{ad-bc}{(cx+d)^2}dx$. Hence, using the notation of Lemma 3.1 an automorphism without fixed points

$$\sigma : (x, y) \to \left(\frac{ax+b}{cx+d}, \frac{\pm\sqrt{\mu_1^{2g+2}}}{(cx+d)^{g+1}}y\right)$$

takes $x^{i-1}dx/y$ to

$$\pm\frac{(ad-bc)(ax+b)^{i-1}(cx+d)^{g-i}}{\sqrt{\mu_1^{2g+2}}y}dx,$$

and therefore by diagonalizing, the set of characteristic roots of this representation is

$$\pm\frac{\{\mu_1^g\mu_2, \mu_1^{g-1}\mu_2^2, , \ldots, \mu_1\mu_2^g\}}{\sqrt{\mu_1^{2g+2}}}.$$

If $\overline{\sigma}$ has order n, then $\mu_2/\mu_1 = \omega_n$ for some primitive root of unity ω_n. Since $n \mid 2g+2$ the direct sum of this representation of σ and its complex conjugate has characteristic roots $\omega_n, \omega_n^2, \ldots, \omega_n^g, \omega_n^{g+2}, \ldots, \omega_n^{2g+1}$ up to a sign. Similarly, if the automorphism has one fixed point, $n \mid 2g+1$ and the representation has characteristic roots $\omega_n, \omega_n^2, \ldots, \omega_n^{2g}$ up to a sign, and if the automorphism has two fixed points, $n \mid 2g$ and the representation has characteristic roots $\omega_{2n}, \omega_{2n}^3, \ldots, \omega_{2n}^{4g-1}$ up to a sign.

For $g = 1$ if $\overline{\sigma}$ has order 2 it has two fixed points and characteristic polynomial f_2, and if $\overline{\sigma}$ has order 3 it has one fixed point and characteristic polynomial f_3, which concludes the proof of (a). For $g = 2$ if $\overline{\Gamma} \cong S_4$ we can refer to Theorem 3.3(b) and its proof to conclude that the 6 odd involutions have no fixed points and characteristic polynomial f_2, the 3 even involutions have two fixed points and characteristic polynomial f_6, the 8 elements of order 3 have no fixed points and characteristic polynomial f_7, and the 6 elements of order 4 have two fixed points and characteristic polynomial f_{11}, which concludes the proof of this line in table (b). If $\overline{\Gamma} \cong D_{12}$ we can refer to Theorem 3.3(d) and its proof to conclude that elements in the cyclic subgroup of order 6 have no fixed points and characteristic polynomials f_1, f_2, f_7, and f_9, depending on whether the elements have order 1, 2, 3, or 6, respectively. Half the involutions outside this subgroup have no fixed points and characteristic polynomial f_2, and half have two fixed points and characteristic polynomial f_6, which concludes the proof of this line in table (b). If $\overline{\Gamma} \cong \mathbf{Z}/5$ we can refer to Theorem 3.3(g) and its proof to conclude that the 4 elements of order 5 have one fixed point and characteristic polynomials f_{10}, which concludes the proof of this line in table (b). The remaining groups are naturally contained in one of these three groups, so their proofs are similar.

For hyperelliptic curves with $g = 3$ if $\overline{\Gamma} \cong S_4$ we can refer to Theorem 3.3(b) and its proof to conclude that the 9 elements of order 2 have no fixed points and characteristic polynomial f_2, the 8 elements of order 3 have two fixed points and characteristic polynomial f_{11}, and the 6 elements of order 4 have no fixed points and characteristic polynomial f_{10}, which proves that line in table (c). If $\overline{\Gamma} \cong D_{16}$ we can refer to Theorem 3.3(d) and its proof to conclude that elements in the cyclic subgroup of order 8 have no fixed points and characteristic polynomials f_1, f_2, f_{10}, and f_{25}, depending on whether the elements have order 1, 2, 4, or 8, respectively. Half the involutions outside this subgroup have no fixed points and characteristic polynomial f_2, and half have two fixed points and characteristic polynomial f_8, which concludes the proof of this line in table (c). If $\overline{\Gamma} \cong D_{12}$ we can refer to Theorem 3.3(e) and its proof to conclude that elements in the cyclic subgroup of order 6 have two fixed points and characteristic polynomials f_1, f_8, f_{11}, and f_{26}, depending on whether the elements have order 1, 2, 3, or 6, respectively. Half the involutions outside this subgroup have no fixed points and characteristic polynomial f_2, and half have two fixed points and characteristic polynomial f_8, which concludes the proof of this line in table (c). If $\overline{\Gamma} \cong \mathbf{Z}/7$ we can refer to Theorem 3.3(g) and its proof to conclude that the 6 elements of order 7 have one fixed point and characteristic polynomials f_{31}, which concludes the proof of this line in table (c). The remaining groups are naturally contained in one of these four groups, so their proofs are similar.

We can treat the nonhyperelliptic curves of genus 3 by examining the action of the automorphism group on $H^0(X, \Omega_X) \cong H^1(X, \mathcal{O}_X) \cong H^2(\mathbf{P}^2, \mathcal{O}_{\mathbf{P}^2}(-4))$. A basis for $H^2(\mathbf{P}^2, \mathcal{O}_{\mathbf{P}^2}(-4))$ is $\{1/x^2yz, 1/xy^2z, 1/xyz^2\}$. Hence, if $\sigma \in PGL(3)$ has eigenvalues μ_1, μ_2, μ_3 up to a constant and f is an invariant planar quartic such that $\sigma(f) = \mu f$, then the action on homology has eigenvalues $\mu/\mu_1^2\mu_2\mu_3$, $\mu/\mu_1\mu_2^2\mu_3$, $\mu/\mu_1\mu_2\mu_3^2$, $\mu_1^2\mu_2\mu_3/\mu$, $\mu_1\mu_2^2\mu_3/\mu$, and $\mu_1\mu_2\mu_3^2/\mu$. In all cases we can and shall choose f to be an absolute invariant, i.e. with $\mu = 1$. If $\overline{\Gamma} \cong PSL(2,7)$ the 21 elements of order 2 have eigenvalues $1, -1, -1$ and characteristic polynomial $f_2(-x)$, the 56 elements of order 3 have eigenvalues $1, \omega_3, \omega_3^2$ and characteristic polynomial f_{11}, the 42 elements of order 4 have eigenvalues $1, i, -i$ and characteristic polynomial f_{10}, and the 48 elements of order 7 have eigenvalues $\omega_7, \omega_7^2, \omega_7^4$ or their complex conjugates and characteristic polynomial f_{31}, which concludes the proof of this line in table (d). If $\overline{\Gamma} \cong S_3 \ltimes \mathbf{Z}/4 \times \mathbf{Z}/4$ the 15 elements of order 2 have eigenvalues $1, -1, -1$ and characteristic polynomial $f_2(-x)$, the 32 elements of order 3 have eigenvalues $1, \omega_3, \omega_3^2$ and characteristic polynomial f_{11}, the 24 elements of order 4 have eigenvalues $1, i, -i$ and characteristic polynomial f_{10}, and the 24 elements of order 8 have eigenvalues $i, \omega_8, -\omega_8$ or their complex conjugates and characteristic polynomial f_{25}, which concludes the proof of this line in table (d). If $\overline{\Gamma} \cong G_2(2,3,3,-,+,+)$ the 7 elements of order 2 have eigenvalues $1, -1, -1$ and characteristic polynomial $f_2(-x)$, the 8 elements of order 3 have eigenvalues $1, 1, \omega_3$ or their complex conjugates and characteristic polynomial f_9, the 8 elements of order 4 have eigenvalues $1, i, -i$ or $-1, i, i$ and characteristic polynomial $f_{10}(x)$ or $f_{10}(-x)$, respectively, the 8 elements of order 6 have eigenvalues $1, -1, \omega_3$ or their complex conjugates and characteristic polynomial $f_{15}(-x)$, and the 16 elements of order 12 have eigenvalues $1, i, \omega_3$ or their conjugates and characteristic polynomial $f_{30}(-x)$, which concludes the proof of this line in table (d). If $\overline{\Gamma} \cong \mathbf{Z}/9$ the 2 elements of order 3 have eigenvalues $1, 1, \omega_3$ or their complex conjugates and characteristic polynomial f_9, and the 6 elements of order 9 have eigenvalues $1, \omega_9, \omega_9^6$ or their conjugates and characteristic polynomial $f_{32}(x)$, which concludes the proof of this line in table (d). The remaining groups are naturally contained in one of these four groups, so their proofs are similar.

We can summarize the results of the last paragraph with the following table. In the left column are the characteristic polynomials in $SL(6, \mathbf{Z})$ and in the right column are the eigenvalues, up to a constant and conjugation, of elements in $PGL(3)$.

$f_1(x) = (x-1)^6$	$1, 1, 1$
$f_2(-x) = (x-1)^2(x+1)^4$	$1, 1, -1$
$f_9(x) = (x^2+x+1)^3$	$1, 1, \omega_3$
$f_{11}(x) = (x-1)^2(x^2+x+1)^2$	$1, \omega_3, \omega_3^2$
$f_{10}(x) = (x-1)^2(x^2+1)^2$	$1, -1, i$
$f_{10}(-x) = (x+1)^2(x^2+1)^2$	$1, 1, i$
$f_{15}(-x) = (x^2+x+1)(x^2-x+1)^2$	$1, -1, \omega_3$
$f_{31}(x) = x^6+x^5+x^4+x^3+x^2+x+1$	$\omega_7, \omega_7^2, \omega_7^4$
$f_{25}(x) = (x^2+1)(x^4+1)$	$1, -1, \omega_8$
$f_{32}(x) = x^6+x^3+1$	$1, \omega_9, \omega_9^6$
$f_{30}(-x) = (x^2-x+1)(x^4-x^2+1)$	$1, i, \omega_3$

We can compute the five special lines in the lemma by consulting character tables [2]. In each case all but one possible representation can be quickly ruled out.■

The following theorem allows us to translate Hashimoto and Ibukiyama's results on quaternion hermitian spaces into results on principal polarizations of E^g.

Theorem 3.7A (Serre, Ibukiyama, Katsura, Oort). *The number of principal polarizations H on $A = E^g$ $(g \geq 2)$ up to automorphisms of A is equal to the class number $H_g(p, 1)$ of the principal genus of the quaternion hermitian space B^g where $B = End(E) \otimes_{\mathbf{Z}} \mathbf{Q}$ is the definite quaternion algebra over $\mathbf{Q}$ with discriminant p.*

Proof. [11, Proposition 2.10].∎

The center of the automorphism group of a principally polarized abelian variety contains -1 and hence the number of elements with characteristic polynomial $f_i(x)$ equals the number with $f_i(-x)$. Because we ultimately need to lift curves to their Jacobians this explains our abuse of language in Lemma 3.6. Denote the proportion of the automorphism group of the jth principal polarization with characteristic polynomial $f_i(x)$ or $f_i(-x)$ by H_{ij}, and let $H_i = \sum_j H_{ij}$. The next theorem calculates the H_i and therefore H because

$$H = \sum_j 1 = \sum_j \sum_i H_{ij} = \sum_i \sum_j H_{ij} = \sum_i H_i.$$

THEOREM 3.8A. *For $p > 2g+1$ the class number H of the principal genus of the quaternion hermitian space B^g is the sum of the H_i given below.*

(a) (Eichler [4]) *For $g = 1$*

$f_1(x) = (x-1)^2, f_1(-x)$	$H_1 = \frac{p-1}{12}$
$f_2(x) = x^2+1$	$H_2 = \frac{1}{4}(1-(\frac{-1}{p}))$
$f_3(x) = x^2+x+1, f_3(-x)$	$H_3 = \frac{1}{3}(1-(\frac{-3}{p}))$

(b) (Hashimoto and Ibukiyama [10]) *For $g = 2$*

$f_1(x) = (x-1)^4, f_1(-x)$	$H_1 = \frac{(p-1)(p^2+1)}{2880}$
$f_2(x) = (x-1)^2(x+1)^2$	$H_2 = \frac{7(p-1)^2}{576}$
$f_3(x) = (x-1)^2(x^2+1), f_3(-x)$	$H_3 = \frac{p-1}{48}(1-(\frac{-1}{p}))$
$f_4(x) = (x-1)^2(x^2+x+1), f_4(-x)$	$H_4 = \frac{p-1}{72}(1-(\frac{-3}{p}))$
$f_5(x) = (x-1)^2(x^2-x+1), f_5(-x)$	$H_5 = \frac{p-1}{72}(1-(\frac{-3}{p}))$
$f_6(x) = (x^2+1)^2$	$H_6 = \frac{5(p-1)}{96} + \frac{1}{32}(1-(\frac{-1}{p}))$
$f_7(x) = (x^2+x+1)^2, f_7(-x)$	$H_7 = \frac{p-1}{18} + \frac{1}{36}(1-(\frac{-3}{p}))$
$f_8(x) = (x^2+1)(x^2+x+1), f_8(-x)$	$H_8 = \frac{1}{12}(1-(\frac{-1}{p}))(1-(\frac{-3}{p}))$
$f_9(x) = (x^2+x+1)(x^2-x+1)$	$H_9 = \frac{2}{9}(1-(\frac{-3}{p}))$
$f_{10}(x) = (x^4+x^3+x^2+x+1), f_{10}(-x)$	$H_{10} = (\frac{4}{5}\ \mathit{if}\ p \equiv 4 \bmod 5)$
$f_{11}(x) = x^4+1$	$H_{11} = \frac{1}{8}(1-(\frac{-1}{p})) + \frac{1}{8}(1-(\frac{-2}{p}))$
$f_{12}(x) = x^4-x^2+1$	$H_{12} = \frac{1}{12}(1-(\frac{-3}{p}))$

(c) (Hashimoto [9]) *For* $g = 3$

$$\begin{array}{ll}
f_1(x) = (x-1)^6, f_1(-x) & H_1 = \frac{(p-1)^2(p^2+1)(p^2+p+1)}{1451520} \\
f_2(x) = (x-1)^4(x+1)^2, f_2(-x) & H_2 = \frac{31(p-1)^2(p^2+1)}{69120} \\
f_3(x) = (x-1)^4(x^2+1), f_3(-x) & H_3 = \frac{(p-1)(p^2+1)}{11520}(1-(\frac{-1}{p})) \\
f_4(x) = (x-1)^4(x^2+x+1), f_4(-x) & H_4 = \frac{(p-1)(p^2+1)}{17280}(1-(\frac{-3}{p})) \\
f_5(x) = (x-1)^4(x^2-x+1), f_5(-x) & H_5 = \frac{(p-1)(p^2+1)}{17280}(1-(\frac{-3}{p})) \\
f_6(x) = (x-1)^2(x+1)^2(x^2+1), & H_6 = \frac{7(p-1)^2}{2304}(1-(\frac{-1}{p})) \\
f_7(x) = (x-1)^2(x+1)^2(x^2+x+1), f_7(-x) & H_7 = \frac{7(p-1)^2}{1728}(1-(\frac{-3}{p})) \\
f_8(x) = (x^2+1)^3 & H_8 = \frac{(p^2-p+2)}{384}(1-(\frac{-1}{p})) \\
f_9(x) = (x^2+x+1)^3, f_9(-x) & H_9 = \frac{(p^2-p+2)}{648}(1-(\frac{-3}{p})) \\
f_{10}(x) = (x-1)^2(x^2+1)^2, f_{10}(-x) & H_{10} = \frac{23(p-1)^2}{1152} + \frac{(p-1)}{128}(1-(\frac{-1}{p})) \\
f_{11}(x) = (x-1)^2(x^2+x+1)^2, f_{11}(-x) & H_{11} = \frac{13(p-1)^2}{432} + \frac{(p-1)}{864}(1-(\frac{-3}{p})) \\
f_{12}(x) = (x-1)^2(x^2-x+1)^2, f_{12}(-x) & H_{12} = \frac{(p-1)^2}{432} + \frac{(p-1)}{864}(1-(\frac{-3}{p})) \\
f_{13}(x) = (x^2+x+1)(x^2+1)^2, f_{13}(-x) & H_{13} = (\frac{5(p-1)}{288} + \frac{1}{96}(1-(\frac{-1}{p})))(1-(\frac{-3}{p})) \\
f_{14}(x) = (x^2+1)(x^2+x+1)^2, f_{14}(-x) & H_{14} = (\frac{(p-1)}{72} + \frac{1}{144}(1-(\frac{-3}{p})))(1-(\frac{-1}{p})) \\
f_{15}(x) = (x^2+x+1)^2(x^2-x+1), f_{15}(-x) & H_{15} = \frac{(5p+9)}{216}(1-(\frac{-3}{p})) \\
f_{16}(x) = (x-1)^2(x^2+1)(x^2+x+1), f_{16}(-x) & H_{16} = \frac{(p-1)}{288}(1-(\frac{-1}{p}))(1-(\frac{-3}{p})) \\
f_{17}(x) = (x-1)^2(x^2+1)(x^2-x+1), f_{17}(-x) & H_{17} = \frac{(p-1)}{288}(1-(\frac{-1}{p}))(1-(\frac{-3}{p})) \\
f_{18}(x) = (x-1)^2(x^2+x+1)(x^2-x+1), f_{18}(-x) & H_{18} = \frac{(p-1)}{54}(1-(\frac{-3}{p})) \\
f_{19}(x) = (x^2+1)(x^2+x+1)(x^2-x+1) & H_{19} = \frac{1}{18}(1-(\frac{-1}{p}))(1-(\frac{-3}{p})) \\
f_{20}(x) = (x-1)^2(x^4+x^3+x^2+x+1), f_{20}(-x) & H_{20} = \frac{(p-1)}{24}(\frac{4}{5}\ \textit{if}\ p \equiv 4 \bmod 5) \\
f_{21}(x) = (x-1)^2(x^4-x^3+x^2-x+1), f_{21}(-x) & H_{21} = \frac{(p-1)}{24}(\frac{4}{5}\ \textit{if}\ p \equiv 4 \bmod 5) \\
f_{22}(x) = (x-1)^2(x^4+1), f_{22}(-x) & H_{22} = \frac{(p-1)}{96}(1-(\frac{-1}{p})+1-(\frac{-2}{p})) \\
f_{23}(x) = (x-1)^2(x^4-x^2+1), f_{23}(-x) & H_{23} = \frac{(p-1)}{144}(1-(\frac{-3}{p})) \\
f_{24}(x) = (x^2+1)(x^4+x^3+x^2+x+1), f_{24}(-x) & H_{24} = \frac{1}{4}(1-(\frac{-1}{p}))(\frac{4}{5}\ \textit{if}\ p \equiv 4 \bmod 5) \\
f_{25}(x) = (x^2+1)(x^4+1) & H_{25} = \frac{3}{16}(1-(\frac{-1}{p})) + \frac{3}{32}(1-(\frac{-1}{p}))(1-(\frac{-2}{p})) \\
f_{26}(x) = (x^2+1)(x^4-x^2+1) & H_{26} = \frac{1}{6}(1-(\frac{-1}{p})) + \frac{1}{48}(1-(\frac{-1}{p}))(1-(\frac{-3}{p})) \\
f_{27}(x) = (x^2+x+1)(x^4+x^3+x^2+x+1), f_{27}(-x) & H_{27} = \frac{1}{6}(1-(\frac{-3}{p}))(\frac{4}{5}\ \textit{if}\ p \equiv 4 \bmod 5) \\
f_{28}(x) = (x^2+x+1)(x^4-x^3+x^2-x+1), f_{28}(-x) & H_{28} = \frac{1}{6}(1-(\frac{-3}{p}))(\frac{4}{5}\ \textit{if}\ p \equiv 4 \bmod 5) \\
f_{29}(x) = (x^2+x+1)(x^4+1), f_{29}(-x) & H_{29} = \frac{1}{24}(1-(\frac{-3}{p}))(1-(\frac{-1}{p})+1-(\frac{-2}{p})) \\
f_{30}(x) = (x^2+x+1)(x^4-x^2+1), f_{30}(-x) & H_{30} = \frac{1}{18}(1-(\frac{-3}{p})) + \frac{1}{12}(1-(\frac{-1}{p}))(1-(\frac{-3}{p})) \\
f_{31}(x) = x^6+x^5+x^4+x^3+x^2+x+1, f_{31}(-x) & H_{31} = \frac{1}{7}(1-(\frac{-7}{p})) + (\frac{6}{7}\ \textit{if}\ p \equiv 6 \bmod 7) \\
f_{32}(x) = x^6+x^3+1, f_{32}(-x) & H_{32} = \frac{1}{9}(1-(\frac{-3}{p})) + (\frac{2}{3}\ \textit{if}\ p \equiv 8 \bmod 9)
\end{array}$$

The number of principal polarizations on E^g up to automorphisms of E^g is given for small primes in the following table.

g \ p	2	3	5	7	11	13	17	19	23	29	31	37	41
1	1	1	1	1	2	1	2	2	3	3	3	3	4
2	1	1	2	2	5	4	8	10	16	24	26	37	50
3	1	2	3	5	19	23	70	109	262	755	1047	2586	4526

The H_1 term is given by the following theorem.

Theorem 3.9A (Y. Ihara). *The mass formula for principal polarizations on E^g is*

$$\sum_{i=1}^{h_g} 1/|\Gamma_i| = \prod_{i=1}^{g} \frac{-B_{2i}}{4i}(1+(-p)^i)$$

where h_g = the number of principal polarizations on E^g, Γ_i = the group of automorphisms of the ith principally polarized abelian variety, and B_i is the ith Bernoulli number given by the generating function

$$\frac{x}{e^x-1} = \sum_{i=0}^{\infty} \frac{B_i}{i!}x^i.$$

Proof. [10, Proposition 9].∎

We define a *mass formula* for curves to be the sum of the reciprocals of the orders of the reduced automorphism groups of the superspecial curves of a given genus as a function of p. The following theorem improves Theorem 1.2A for E^g and expands on the theorems in the Introduction. Note that 3.10(c) corrects an error in [5, 1.7.4].

Theorem 3.10.

(a) (Eichler [4], Deuring [3]) *The mass formula for elliptic curves is*

$$\sum 1/|\overline{\Gamma}| = \frac{p-1}{12}.$$

The number of superspecial elliptic curves is 1 *if* $p = 2$ *or* 3 *and*

$$\frac{p-1}{12} + \frac{1-(\frac{-1}{p})}{4} + \frac{1-(\frac{-3}{p})}{3}$$

otherwise and hence is a polynomial depending on p mod 12.

(b) (Ibukiyama, Katsura, Oort [11, 3.1 and 3.3]) *The mass formula for genus 2 curves is*

$$\sum 1/|\overline{\Gamma}| = \frac{(p-1)(p-2)(p-3)}{2880}.$$

The number of superspecial curves of genus 2 is 0 *if* $p = 2, 3$, 1 *if* $p = 5$ *and*

$$\frac{p^3+24p^2+141p-166}{2880}-\frac{1-(\frac{-1}{p})}{32}+\frac{1-(\frac{-2}{p})}{8}+\frac{1-(\frac{-3}{p})}{18}+(\frac{4}{5}\ \textit{if}\ p\equiv 4 \bmod 5)$$

otherwise and hence is a polynomial depending on $p \bmod 120$*.*

(c) (Ekedahl [5]) *The mass formula for genus 3 curves is*

$$\sum 1/|\overline{\Gamma}| = \frac{(p-1)^2(p-2)((p+5)(p+1)(p-3)+60)}{1451520}.$$

(d) The number of curves of genus 3 is 0 *if* $p = 2$, 1 *if* $p = 3$, 3 *if* $p = 7$ *and*

$$\frac{p^6-p^5+610p^4-2410p^3+67789p^2-171109p+105120}{1451520}+\frac{(p^2-4p+87)(1-(\frac{-1}{p}))}{384}$$

$$+\frac{(p^2+2p-35)(1-(\frac{-3}{p}))}{648}+\frac{(1-(\frac{-1}{p}))(1-(\frac{-3}{p}))}{12}+\frac{(1-(\frac{-1}{p}))(1-(\frac{-2}{p}))}{16}+\frac{1-(\frac{-7}{p})}{7}$$

$$+(\frac{6}{7}\ \textit{if}\ p\equiv 6 \bmod 7)+(\frac{2}{3}\ \textit{if}\ p\equiv 8 \bmod 9)$$

otherwise and hence is a polynomial depending on $p \bmod 504$*.*

Proof. We shall denote by $H_1(a)$ the H_1 in 3.8A(a), etc. We can read 3.10(a) off from $H_1(a)$ and the sum $H(a)$ in 3.8A(a). By 1.1A and Ekedahl [5, 1.7.2.1] $2((H_1(b)/2)-(H_1(a)/2)^2/2)$ gives the mass formula in (b). By combinatorics $H(b)-\binom{H(a)+1}{2}$ gives the number of curves in (b). Similarly, $H_1(c)-a_1b_1/2-a_1^3/24$ gives (c) where a_1 and b_1 are the mass formulas in (a) and (b), and $H(c)-ab-\binom{a+2}{3}$ gives (d), where a and b are the number of curves in (a) and (b).∎

The following is a table of the number of superspecial curves.

g \ p	2	3	5	7	11	13	17	19	23	29	31	37	41
1	1	1	1	1	2	1	2	2	3	3	3	3	4
2	0	0	1	1	2	3	5	7	10	18	20	31	40
3	0	1	1	3	11	19	56	91	222	691	977	2483	4346

Hashimoto's formulas actually give us more information which we intend to utilize.

Theorem 3.11. *The only conjugacy classes that contribute to the formulas in Theorem 3.10 are those with characteristic polynomials listed below. The contribution from $f_i(\pm x)$ is H_i when $p > 2g+1$.*

(a) (Eichler [4]) *For elliptic curves.*

$$\begin{array}{ll}
f_1(x) = (x-1)^2, f_1(-x) & H_1 = \frac{p-1}{12} \\
f_2(x) = x^2+1 & H_2 = \frac{1}{4}(1-(\frac{-1}{p})) \\
f_3(x) = x^2+x+1, f_3(-x) & H_3 = \frac{1}{3}(1-(\frac{-3}{p}))
\end{array}$$

(b) For genus 2 curves.

$$\begin{array}{ll}
f_1(x) = (x-1)^4, f_1(-x) & H_1 = \frac{(p-1)(p-2)(p-3)}{2880} \\
f_2(x) = (x-1)^2(x+1)^2 & H_2 = \frac{(p-1)(p-3)}{96} \\
f_6(x) = (x^2+1)^2 & H_6 = \frac{p-1}{32} - \frac{1}{32}(1-(\frac{-1}{p})) \\
f_7(x) = (x^2+x+1)^2, f_7(-x) & H_7 = \frac{p-1}{18} - \frac{1}{36}(1-(\frac{-3}{p})) \\
f_9(x) = (x^2+x+1)(x^2-x+1) & H_9 = \frac{1}{12}(1-(\frac{-3}{p})) \\
f_{10}(x) = (x^4+x^3+x^2+x+1), f_{10}(-x) & H_{10} = (\frac{4}{5} \ \mathit{if}\, p \equiv 4 \bmod 5) \\
f_{11}(x) = x^4+1 & H_{11} = \frac{1}{8}(1-(\frac{-2}{p}))
\end{array}$$

(c) For genus 3 curves.

$$\begin{array}{ll}
f_1(x) = (x-1)^6, f_1(-x) & H_1 = \frac{(p-1)^2(p-2)((p+5)(p+1)(p-3)+60)}{1451520} \\
f_2(x) = (x-1)^4(x+1)^2, f_2(-x) & H_2 = \frac{(p-1)^2(p^2-2p+3)}{2304} \\
f_8(x) = (x^2+1)^3 & H_8 = \frac{(p-3)^2}{384}(1-(\frac{-1}{p})) \\
f_9(x) = (x^2+x+1)^3, f_9(-x) & H_9 = \frac{(p-2)(p-5)}{648}(1-(\frac{-3}{p})) \\
f_{10}(x) = (x-1)^2(x^2+1)^2, f_{10}(-x) & H_{10} = \frac{(p-1)^2}{64} + \frac{(p-1)}{192}(1-(\frac{-1}{p})) \\
f_{11}(x) = (x-1)^2(x^2+x+1)^2, f_{11}(-x) & H_{11} = \frac{(p-1)(p-2)}{36} \\
f_{15}(x) = (x^2+x+1)^2(x^2-x+1), f_{15}(-x) & H_{15} = \frac{(p-5)}{72}(1-(\frac{-3}{p})) \\
f_{25}(x) = (x^2+1)(x^4+1) & H_{25} = (\frac{1}{8} + \frac{1}{16}(1-(\frac{-2}{p})))(1-(\frac{-1}{p})) \\
f_{26}(x) = (x^2+1)(x^4-x^2+1) & H_{26} = \frac{1}{12}(1-(\frac{-1}{p})) \\
f_{30}(x) = (x^2+x+1)(x^4-x^2+1), f_{30}(-x) & H_{30} = \frac{1}{12}(1-(\frac{-1}{p}))(1-(\frac{-3}{p})) \\
f_{31}(x) = x^6+x^5+x^4+x^3+x^2+x+1, f_{31}(-x) & H_{31} = \frac{1}{7}(1-(\frac{-7}{p})) + (\frac{6}{7} \ \mathit{if}\, p \equiv 6 \bmod 7) \\
f_{32}(x) = x^6+x^3+1, f_{32}(-x) & H_{32} = (\frac{2}{3} \ \mathit{if}\, p \equiv 8 \bmod 9)
\end{array}$$

Proof. This will follow via Theorem 1.1A by “subtracting” Lemma 3.13 from Theorem 3.8A.∎

Theorem 3.12 (Eichler [4]). *The number of superspecial elliptic curves in Theorem 3.10(a) breaks down as follows. For $p = 2$ there is one such curve, and $\overline{\Gamma} \cong A_4$. For $p = 3$ there is one such curve, and $\overline{\Gamma} \cong D_6$. For $p \geq 5$ the number of curves with reduced automorphism group $\overline{\Gamma}$ is*

(a) if $|\overline{\Gamma}| = 1$

$$\frac{p-1}{12} - \frac{1-(\frac{-1}{p})}{4} - \frac{1-(\frac{-3}{p})}{6},$$

(b) if $|\overline{\Gamma}| = 2$

$$\frac{1-(\frac{-1}{p})}{2}, \text{ and}$$

(c) if $|\overline{\Gamma}| = 3$

$$\frac{1-(\frac{-3}{p})}{2}.$$

Proof. Combine [H, IV.4.7] with 1.8A, or apply the inverse of the first three rows of the matrix in Lemma 3.6(a) to the vector given by the H_i in Theorem 3.11(a).■

Lemma 3.13. *The decomposable contributions to Theorem 3.8A for $p > 2g+1$ are given below.*

(a) For $g = 2$ the product of two elliptic curves.

$$\begin{array}{ll}
f_1(x) = (x-1)^4, f_1(-x) & H_1 = \frac{(p-1)^2}{576} \\
f_2(x) = (x-1)^2(x+1)^2 & H_2 = \frac{(p-1)(p+11)}{576} \\
f_3(x) = (x-1)^2(x^2+1), f_3(-x) & H_3 = \frac{p-1}{48}(1-(\frac{-1}{p})) \\
f_4(x) = (x-1)^2(x^2+x+1), f_4(-x) & H_4 = \frac{p-1}{72}(1-(\frac{-3}{p})) \\
f_5(x) = (x-1)^2(x^2-x+1), f_5(-x) & H_5 = \frac{p-1}{72}(1-(\frac{-3}{p})) \\
f_6(x) = (x^2+1)^2 & H_6 = \frac{(p-1)}{48} + \frac{1}{16}(1-(\frac{-1}{p})) \\
f_7(x) = (x^2+x+1)^2, f_7(-x) & H_7 = \frac{1}{18}(1-(\frac{-3}{p})) \\
f_8(x) = (x^2+1)(x^2+x+1), f_8(-x) & H_8 = \frac{1}{12}(1-(\frac{-1}{p}))(1-(\frac{-3}{p})) \\
f_9(x) = (x^2+x+1)(x^2-x+1) & H_9 = \frac{5}{36}(1-(\frac{-3}{p})) \\
f_{11}(x) = x^4+1 & H_{11} = \frac{1}{8}(1-(\frac{-1}{p})) \\
f_{12}(x) = x^4-x^2+1 & H_{12} = \frac{1}{12}(1-(\frac{-3}{p}))
\end{array}$$

(b) For $g = 3$ the product of three elliptic curves.

$f_1(x) = (x-1)^6, f_1(-x)$	$H_1 = \frac{(p-1)^3}{41472}$
$f_2(x) = (x-1)^4(x+1)^2, f_2(-x)$	$H_2 = \frac{(p-1)^2(p+23)}{13824}$
$f_3(x) = (x-1)^4(x^2+1), f_3(-x)$	$H_3 = \frac{(p-1)^2}{2304}(1-(\frac{-1}{p}))$
$f_4(x) = (x-1)^4(x^2+x+1), f_4(-x)$	$H_4 = \frac{(p-1)^2}{3456}(1-(\frac{-3}{p}))$
$f_5(x) = (x-1)^4(x^2-x+1), f_5(-x)$	$H_5 = \frac{(p-1)^2}{3456}(1-(\frac{-3}{p}))$
$f_6(x) = (x-1)^2(x+1)^2(x^2+1),$	$H_6 = \frac{(p-1)(p+11)}{2304}(1-(\frac{-1}{p}))$
$f_7(x) = (x-1)^2(x+1)^2(x^2+x+1), f_7(-x)$	$H_7 = \frac{(p-1)(p+11)}{1728}(1-(\frac{-3}{p}))$
$f_8(x) = (x^2+1)^3$	$H_8 = \frac{(p+1)}{192}(1-(\frac{-1}{p}))$
$f_9(x) = (x^2+x+1)^3, f_9(-x)$	$H_9 = \frac{1}{162}(1-(\frac{-3}{p}))$
$f_{10}(x) = (x-1)^2(x^2+1)^2, f_{10}(-x)$	$H_{10} = \frac{(p-1)^2}{576} + \frac{(p-1)}{192}(1-(\frac{-1}{p}))$
$f_{11}(x) = (x-1)^2(x^2+x+1)^2, f_{11}(-x)$	$H_{11} = \frac{p-1}{36} + \frac{(p-1)}{432}(1-(\frac{-3}{p}))$
$f_{12}(x) = (x-1)^2(x^2-x+1)^2, f_{12}(-x)$	$H_{12} = \frac{(p-1)}{432}(1-(\frac{-3}{p}))$
$f_{13}(x) = (x^2+x+1)(x^2+1)^2, f_{13}(-x)$	$H_{13} = (\frac{(p-1)}{144} + \frac{1}{48}(1-(\frac{-1}{p})))(1-(\frac{-3}{p}))$
$f_{14}(x) = (x^2+1)(x^2+x+1)^2, f_{14}(-x)$	$H_{14} = \frac{1}{72}(1-(\frac{-1}{p}))(1-(\frac{-3}{p}))$
$f_{15}(x) = (x^2+x+1)^2(x^2-x+1), f_{15}(-x)$	$H_{15} = \frac{2}{27}(1-(\frac{-3}{p}))$
$f_{16}(x) = (x-1)^2(x^2+1)(x^2+x+1), f_{16}(-x)$	$H_{16} = \frac{(p-1)}{288}(1-(\frac{-1}{p}))(1-(\frac{-3}{p}))$
$f_{17}(x) = (x-1)^2(x^2+1)(x^2-x+1), f_{17}(-x)$	$H_{17} = \frac{(p-1)}{288}(1-(\frac{-1}{p}))(1-(\frac{-3}{p}))$
$f_{18}(x) = (x-1)^2(x^2+x+1)(x^2-x+1), f_{18}(-x)$	$H_{18} = \frac{5(p-1)}{432}(1-(\frac{-3}{p}))$
$f_{19}(x) = (x^2+1)(x^2+x+1)(x^2-x+1)$	$H_{19} = \frac{5}{144}(1-(\frac{-1}{p}))(1-(\frac{-3}{p}))$
$f_{22}(x) = (x-1)^2(x^4+1), f_{22}(-x)$	$H_{22} = \frac{(p-1)}{96}(1-(\frac{-1}{p}))$
$f_{23}(x) = (x-1)^2(x^4-x^2+1), f_{23}(-x)$	$H_{23} = \frac{(p-1)}{144}(1-(\frac{-3}{p}))$
$f_{25}(x) = (x^2+1)(x^4+1)$	$H_{25} = \frac{1}{16}(1-(\frac{-1}{p}))$
$f_{26}(x) = (x^2+1)(x^4-x^2+1)$	$H_{26} = (\frac{1}{12} + \frac{1}{48}(1-(\frac{-3}{p})))(1-(\frac{-1}{p}))$
$f_{29}(x) = (x^2+x+1)(x^4+1), f_{29}(-x)$	$H_{29} = \frac{1}{24}(1-(\frac{-3}{p}))(1-(\frac{-1}{p}))$
$f_{30}(x) = (x^2+x+1)(x^4-x^2+1), f_{30}(-x)$	$H_{30} = \frac{1}{18}(1-(\frac{-3}{p}))$
$f_{32}(x) = x^6+x^3+1, f_{32}(-x)$	$H_{32} = \frac{1}{9}(1-(\frac{-3}{p}))$

(c) For $g = 3$ the product of an elliptic curve and an abelian surface with indecomposable polarization.

$f_1(x) = (x-1)^6, f_1(-x)$	$H_1 = \frac{(p-1)^2(p-2)(p-3)}{69120}$
$f_2(x) = (x-1)^4(x+1)^2, f_2(-x)$	$H_2 = \frac{(p-1)^2(p-3)(p+58)}{69120}$
$f_3(x) = (x-1)^4(x^2+1), f_3(-x)$	$H_3 = \frac{(p-1)(p-2)(p-3)}{11520}(1-(\frac{-1}{p}))$
$f_4(x) = (x-1)^4(x^2+x+1), f_4(-x)$	$H_4 = \frac{(p-1)(p-2)(p-3)}{17280}(1-(\frac{-3}{p}))$

$f_5(x) = (x-1)^4(x^2-x+1), f_5(-x)$	$H_5 = \frac{(p-1)(p-2)(p-3)}{17280}(1-(\frac{-3}{p}))$
$f_6(x) = (x-1)^2(x+1)^2(x^2+1),$	$H_6 = \frac{(p-1)(p-3)}{384}(1-(\frac{-1}{p}))$
$f_7(x) = (x-1)^2(x+1)^2(x^2+x+1), f_7(-x)$	$H_7 = \frac{(p-1)(p-3)}{288}(1-(\frac{-3}{p}))$
$f_8(x) = (x^2+1)^3$	$H_8 = \frac{(p-3)}{384}(1-(\frac{-1}{p}))$
$f_9(x) = (x^2+x+1)^3, f_9(-x)$	$H_9 = \frac{(p-2)}{108}(1-(\frac{-3}{p}))$
$f_{10}(x) = (x-1)^2(x^2+1)^2, f_{10}(-x)$	$H_{10} = \frac{(p-1)^2}{384} - \frac{(p-1)}{384}(1-(\frac{-1}{p}))$
$f_{11}(x) = (x-1)^2(x^2+x+1)^2, f_{11}(-x)$	$H_{11} = \frac{(p-1)^2}{432} - \frac{(p-1)}{864}(1-(\frac{-3}{p}))$
$f_{12}(x) = (x-1)^2(x^2-x+1)^2, f_{12}(-x)$	$H_{12} = \frac{(p-1)^2}{432} - \frac{(p-1)}{864}(1-(\frac{-3}{p}))$
$f_{13}(x) = (x^2+x+1)(x^2+1)^2, f_{13}(-x)$	$H_{13} = (\frac{(p-1)}{96} - \frac{1}{96}(1-(\frac{-1}{p})))(1-(\frac{-3}{p}))$
$f_{14}(x) = (x^2+1)(x^2+x+1)^2, f_{14}(-x)$	$H_{14} = (\frac{(p-1)}{72} - \frac{1}{144}(1-(\frac{-3}{p})))(1-(\frac{-1}{p}))$
$f_{15}(x) = (x^2+x+1)^2(x^2-x+1), f_{15}(-x)$	$H_{15} = \frac{(p+4)}{108}(1-(\frac{-3}{p}))$
$f_{18}(x) = (x-1)^2(x^2+x+1)(x^2-x+1), f_{18}(-x)$	$H_{18} = \frac{(p-1)}{144}(1-(\frac{-3}{p}))$
$f_{19}(x) = (x^2+1)(x^2+x+1)(x^2-x+1)$	$H_{19} = \frac{1}{48}(1-(\frac{-1}{p}))(1-(\frac{-3}{p}))$
$f_{20}(x) = (x-1)^2(x^4+x^3+x^2+x+1), f_{20}(-x)$	$H_{20} = \frac{(p-1)}{24}(\frac{4}{5}\ \mathit{if}\, p \equiv 4 \bmod 5)$
$f_{21}(x) = (x-1)^2(x^4-x^3+x^2-x+1), f_{21}(-x)$	$H_{21} = \frac{(p-1)}{24}(\frac{4}{5}\ \mathit{if}\, p \equiv 4 \bmod 5)$
$f_{22}(x) = (x-1)^2(x^4+1), f_{22}(-x)$	$H_{22} = \frac{(p-1)}{96}(1-(\frac{-2}{p}))$
$f_{24}(x) = (x^2+1)(x^4+x^3+x^2+x+1), f_{24}(-x)$	$H_{24} = \frac{1}{4}(1-(\frac{-1}{p}))(\frac{4}{5}\ \mathit{if}\, p \equiv 4 \bmod 5)$
$f_{25}(x) = (x^2+1)(x^4+1)$	$H_{25} = \frac{1}{32}(1-(\frac{-1}{p}))(1-(\frac{-2}{p}))$
$f_{27}(x) = (x^2+x+1)(x^4+x^3+x^2+x+1), f_{27}(-x)$	$H_{27} = \frac{1}{6}(1-(\frac{-3}{p}))(\frac{4}{5}\ \mathit{if}\, p \equiv 4 \bmod 5)$
$f_{28}(x) = (x^2+x+1)(x^4-x^3+x^2-x+1), f_{28}(-x)$	$H_{28} = \frac{1}{6}(1-(\frac{-3}{p}))(\frac{4}{5}\ \mathit{if}\, p \equiv 4 \bmod 5)$
$f_{29}(x) = (x^2+x+1)(x^4+1), f_{29}(-x)$	$H_{29} = \frac{1}{24}(1-(\frac{-3}{p}))(1-(\frac{-2}{p}))$

Proof. The proof proceeds in the following order. Use 3.12 to prove (a) and (b). Subtract (a) from 3.8A(b) and use the matrix in 3.6(b) to prove 3.14. Now use 3.12 and 3.14 to prove (c).

We shall show how to calculate (b) from 3.12; (a) and (c) are analogous and easier. Let $E_i, i = 1, 2, 3$ be three distinct supersingular elliptic curves. The automorphism group of E_1^3 with its induced principal polarization is the semidirect product of S_3 and $(AutE_1)^3$, and its 6 dimensional representation is simply the tensor of the 3 dimensional representation of S_3 as permutation matrices and the natural 2 dimensional representation of $AutE_1$ in 1.4A. The automorphism group of $E_1 \times E_2 \times E_3$ is $AutE_1 \times AutE_2 \times AutE_3$, and its 6 dimensional representation is the product of the three 2 dimensional representations in 1.4A. The automorphism group of $E_1^2 \times E_2$ is the product of $AutE_2$ and the semidirect product of S_2 and $(AutE_1)^2$. Its 6 dimensional representation is the direct sum of the 2 dimensional representation of $AutE_2$ and the tensor of the 2 dimensional permutation representation of S_2 and the 2 dimensional representation of $AutE_1$. ¿From these observations we can calculate the number of elements with given characteristic polynomials in the 6 dimensional representations from the numbers of elements with given characteristic polynomials in the 2 dimensional representations even without knowing what these representations look like explicitly.∎

Our approach now gives a new and very short proof of the following result.

Theorem 3.14 (Ibukiyama, Katsura, Oort [11, Theorem 3.3]). *The number of superspecial curves of genus* 2 *in Theorem 3.10(b) breaks down as follows. For* $p = 2, 3$ *there are no such curves. For* $p = 5$ *there is one such curve, and* $\overline{\Gamma} \cong PGL(2,5)$. *For* $p \geq 7$ *the number of curves with reduced automorphism group* $\overline{\Gamma}$ *is*

(a) if $|\overline{\Gamma}| = 1$

$$\frac{(p-1)(p^2-35p+346)}{2880} - \frac{1-(\frac{-1}{p})}{32} - \frac{1-(\frac{-2}{p})}{8} - \frac{1-(\frac{-3}{p})}{9} - (\frac{1}{5} \text{ if } p \equiv 4 \bmod 5),$$

(b) if $|\overline{\Gamma}| = 2$

$$\frac{(p-1)(p-17)}{48} + \frac{1-(\frac{-1}{p})}{8} + \frac{1-(\frac{-2}{p})}{2} + \frac{1-(\frac{-3}{p})}{2},$$

(c) if $\overline{\Gamma} \cong D_4$

$$\frac{p-1}{8} - \frac{1-(\frac{-1}{p})}{8} - \frac{1-(\frac{-2}{p})}{4} - \frac{1-(\frac{-3}{p})}{2},$$

(d) if $|\overline{\Gamma}| = 5$

$$(1 \text{ if } p \equiv 4 \bmod 5),$$

(e) if $\overline{\Gamma} \cong D_6$

$$\frac{p-1}{6} - \frac{1-(\frac{-2}{p})}{2} - \frac{1-(\frac{-3}{p})}{3},$$

(f) if $\overline{\Gamma} \cong D_{12}$

$$\frac{1-(\frac{-3}{p})}{2}, \text{ and}$$

(g) if $\overline{\Gamma} \cong S_4$

$$\frac{1-(\frac{-2}{p})}{2}.$$

Proof. Apply the inverse of the first seven rows of the matrix in 3.6(b) to the vector given by the H_i in Theorem 3.11(b).∎

So far we have been fortunate because the number of characteristic polynomials has been equal to the number of groups, thus making the matrix in 3.6 square and hence possible to invert. For $g = 3$ we have only twelve characteristic polynomials but twenty-four groups. However, six groups are essentially repeated between the hyperelliptic and nonhyperelliptic cases because the hyperelliptic involution splits. This still leaves us with eighteen groups, so we have some work to do, which is the subject of our main theorem. I(b), I(d), or I(i) replaces [27, 5.12.3] where a slight error was made in the proof that there are superspecial hyperelliptic curves of genus 3 if $p \equiv 3 \bmod 4$ and $p > 3$. Probably the most interesting part is how I(e) and II(d) fit together.

Theorem 3.15. *The number of superspecial curves of genus* 3 *in Theorem 3.10(d) breaks down as follows.*

(I) The hyperelliptic case where $\overline{\Gamma} \leq PGL(2)$.

For $p = 2, 3, 5$ *there are no such curves. For* $p = 7$ *there is one such curve, and* $\overline{\Gamma} \cong PGL(2, 7)$. *For* $p \geq 11$ *the number of curves with automorphism group* Γ *is* *(a) if $\overline{\Gamma} \cong \mathbf{Z}/1$, the number of equivalence classes of size $8!/5!$ of monic polynomials of degree 7 with roots 0 and 1 satisfying the conditions of 2.11 modulo the action of S_8,*

(b) if $\overline{\Gamma} \cong \mathbf{Z}/2$ and $\Gamma \cong \mathbf{Z}/4$

$$\frac{(p-7)(p-11)}{192}(1-(\frac{-1}{p})),$$

(c) if $\overline{\Gamma} \cong \mathbf{Z}/2$ and $\Gamma \cong D_4$, the number of equivalence classes of size 8 of monic polynomials $f(x)$ of degree 4 with root 1 with $f(x^2)$ satisfying the conditions of 2.11 modulo scaling the roots and taking reciprocals,

(d) if $\overline{\Gamma} \cong D_4$ and $\Gamma \cong \mathbf{Z}/2 \times \mathbf{Z}/4$

$$\frac{p-11}{16}(1-(\frac{-1}{p})) - \frac{1}{8}(1-(\frac{-1}{p}))(1-(\frac{-2}{p})),$$

(e) if $\overline{\Gamma} \cong D_4$ and $\Gamma \cong EA(8)$, the number of 3-element sets $\{\lambda_1, \lambda_2, \lambda_3\}$ such that $\lambda_1\lambda_2\lambda_3 = 1$ and $h_p(\lambda_i) = 0$ modulo taking the reciprocal of all three elements,

(f) if $\overline{\Gamma} \cong D_6$, the number of supersingular elliptic curves, $j \neq 1728, 2^{11}/3$, such that λ also satisfies $h_p((\frac{\lambda+\omega_3^2}{\lambda+\omega_3})^3) = 0$,

(g) (Oort [27, 5.15]) *if $\overline{\Gamma} \cong \mathbf{Z}/7$*

$$(1 \textit{ if } p \equiv 6 \bmod 7),$$

(h) if $\overline{\Gamma} \cong D_8$,the number of ordered pairs (λ_1, λ_2) such that $\lambda_1 \neq 3 \pm 2\sqrt{2}$ or ω_3^i, $\lambda_1^2\lambda_2 = 1$, and $h_p(\lambda_i) = 0$ modulo taking reciprocals,

(i) if $\overline{\Gamma} \cong D_{12}$

$$\frac{1}{2}(1-(\frac{-1}{p})),$$

(j) if $\overline{\Gamma} \cong D_{16}$

$$\frac{1}{4}(1-(\frac{-1}{p}))(1-(\frac{-2}{p})), \textit{ and}$$

(k) if $\overline{\Gamma} \cong S_4$

$$(1 \text{ if } h_p(-3) = 0).$$

(II) The nonhyperelliptic case where the automorphism group $G \cong \overline{\Gamma}$.

For $p = 2$ *there are no such curves. For* $p = 3$ *there is one such curve, and* $G \cong PU(3,9)$. *For* $p = 5$ *there is only the Klein curve. For* $p = 7$ *there is the Fermat curve and a curve with* S_4 *symmetry. For* $p \geq 11$ *the number of curves with automorphism group* G *is*

(a) if $G \cong \mathbf{Z}/1$

$$\frac{(p-1)(p-9)(p-11)(p^3+20p^2-349p-3200)}{1451520} - \frac{(p^2-18p+77)}{384}(1-(\frac{-1}{p}))$$

$$-\frac{(p-5)(p-11)}{1296}(1-(\frac{-3}{p})) + \frac{1}{7}(1-(\frac{-7}{p})) - (\frac{1}{7} \text{ if } p \equiv 6 \bmod 7) - a,$$

where a *is the number in I(a) above,*

(b) if $G \cong \mathbf{Z}/2$

$$\frac{(p-1)(p-9)(p^2-3p-82)}{1152} - \frac{(7p-67)}{192}(1-(\frac{-1}{p})) - \frac{(p-5)}{72}(1-(\frac{-3}{p}))$$

$$+\frac{1}{16}(1-(\frac{-1}{p}))(1-(\frac{-2}{p})) + \frac{1}{24}(1-(\frac{-1}{p}))(1-(\frac{-3}{p})) - \frac{1}{2}(1-(\frac{-7}{p})) - c,$$

where c *is the number in I(c) above,*

(c) if $G \cong \mathbf{Z}/3$

$$\frac{(p-5)(p-11)}{432}(1-(\frac{-3}{p})) - (\frac{1}{3} \text{ if } p \equiv 8 \bmod 9),$$

(d) if $G \cong D_4$

$$\frac{(p-1)(p-5)(p-9)}{192} + \frac{(p-5)}{32}(1-(\frac{-1}{p})) - e,$$

where e *is the number in I(e) above,*

(e) if $G \cong \mathbf{Z}/6$

$$\frac{(p-5)}{24}(1-(\frac{-3}{p})) - \frac{1}{8}(1-(\frac{-1}{p}))(1-(\frac{-3}{p})),$$

(f) if $G \cong D_6$

$$\frac{(p-1)(p-8)}{12} - \frac{1}{4}(1-(\frac{-1}{p})) + \frac{1}{2}(1-(\frac{-7}{p})) - f,$$

where f *is the number in I(f) above,*

(g) if $G \cong D_8$

$$\frac{(p-1)(p-9)}{16} - \frac{(p-9)}{16}(1-(\frac{-1}{p})) - \frac{1}{8}(1-(\frac{-1}{p}))(1-(\frac{-2}{p})) + \frac{1}{2}(1-(\frac{-7}{p})) - h,$$

where h *is the number in I(h) above,*

(h) if $G = \mathbf{Z}/9$

$$(1 \textit{ if } p \equiv 8 \bmod 9),$$

(i) if $|G| = 16$

$$\frac{(p-7)}{24}(1-(\frac{-1}{p})) - \frac{1}{12}(1-(\frac{-1}{p}))(1-(\frac{-3}{p})),$$

(j) if $G \cong S_4$

$$\frac{p-1}{2} - \frac{1}{2}(1-(\frac{-1}{p})) - (1-(\frac{-7}{p})) - (1 \textit{ if } h_p(-3) = 0),$$

(k) if $|G| = 48$

$$\frac{1}{4}(1-(\frac{-1}{p}))(1-(\frac{-3}{p})),$$

(l) if $G \cong S_3 \ltimes (\mathbf{Z}/4 \times \mathbf{Z}/4)$

$$\frac{1}{2}(1-(\frac{-1}{p})), \textit{ and}$$

(m) if $G \cong PSL(2,7)$

$$\frac{1}{2}(1-(\frac{-7}{p})).$$

REMARK 3.15.1. The smallest primes for which $h_p(-3) = h_p(-8) = h_p(\omega_3) = 0$ are $p = 7$, 47, 191, 383, 439, 1151, 1399, 2351, 2879, 3119, 3511, 3559, 4127, 5087, 5431, 6911, 8887, 9127, 9791, 9887. Note that for all of these primes $p \equiv 7$ or 47 mod 48. The 7 mod 8 behavior is due to 8-torsion over $\mathbf{Q}$ for the curve with $\lambda = -8$. The smallest primes for which there exists nontrivial curves in I(f) are $p = 31$, 59, 61, 71(2), 73(2), 79, 83. If $p = 23$ $h_p(-2) = h_p(-1) = h_p(1/2) = h_p(2) = h_p(1/3) = h_p(3/2) = 0$, and in general a sufficient condition for I(e) is $h_p(\lambda) = h_p(-\lambda) = 0$ because then $-\lambda\frac{1}{1-\lambda}\frac{\lambda-1}{\lambda} = \lambda\frac{1}{1+\lambda}\frac{\lambda+1}{\lambda} = 1$. The following is a table of the number of superspecial curves in I(e) and I(h).

p	17	23	31	41	47	71	73	79	89	97
I(e)	0	2	3	0	4	10	2	9	0	4
I(h)	2	0	2	2	5	0	6	2	2	2

The reason that the above primes are never congruent to 3 or 5 mod 8 is that by Theorem 1.9A $\lambda_1\lambda_2\lambda_3 = 1 = (-1)^{(p^2-1)/8}$. In [27, 5.15] Oort raises the question of whether there exist superspecial hyperelliptic curves for all $p \geq 7$. If I(e) and I(h) persist in being nonzero for $p \equiv 1$ mod 8, then in light of I(g) and I(i) one would only need to construct curves for $p \equiv 5$ mod 8 when $p \not\equiv 6$ mod 7. The only primes $7 \leq p < 100$ for which existence is in question are $p = 29$, 37, and 53.

One could argue heuristically à la Lang-Trotter that the number in I(e) grows as p as follows. The number of supersingular pairs (λ_1, λ_2) is $O(p^2)$, and the probability that $\lambda_3 = 1/(\lambda_1, \lambda_2) \in \mathbf{F}_{p^2}$ is supersingular is $O(p/p^2) = O(1/p)$.

Proof. (of 3.15) For $p \leq 7$ except when $p = 7$ and $G \cong S_4$ we can conclude by 2.9 and 2.11 that the curves listed are indeed superspecial and by 3.10 that there are no others. That the curve with $p = 7$ and $G \cong S_4$ is superspecial is similar to the general proof for $G \cong S_4$, so assume now that $p > 7$.

As mentioned earlier we need to add 12 new calculations to the 12 calculations in 3.11(c) in order to use 3.6(c,d) to calculate the 24 quantities in this theorem. Six of the calculations will consist of verifying the quantities in I(a,c,e,f,h,k) of the hyperelliptic case, which will fill in the holes in II(a,b,d,f,g,j) of the nonhyperelliptic case. The other six calculations will consist of verifying the quantities in I(d) and II(d,i,j,l,m). To complete the proof at this point simply subtract the information obtained thus far from 3.11(c) and apply the inverse of the pertinent 12×12 submatrix of 3.6(d) to fill in the rest of the theorem.

I(a) and (c) say no more than what is contained in 2.11, so we shall begin with I(e). An hyperelliptic curve C with $EA(8) \leq \Gamma$ can be written as

$$y^2 = (x^4 - (d^2 + 1/d^2)x^2 + 1)(x^4 - (e^2 + 1/e^2)x^2 + 1)$$

with $d, e \neq 0, \pm 1, \pm i$. Generically 192 choices for the ordered pair (d, e) produce isomorphic curves. 32 are just reorderings of the Weierstrass points, and we get 6 times this via $(d, e) \rightarrow (id, ie)$ and $(d, e) \rightarrow (\frac{d+1}{d-1}, \frac{e+1}{e-1})$. This curve has $EA(8) < \Gamma$ if and only if we can take $d = ie$ which has reduced automorphism group D_8, $d^8 = -1$ which has reduced group D_{16}, or $d = \pm\sqrt{\pm 2 \pm \sqrt{3}}$ which has reduced group S_4. Let $\alpha : (x, y) \rightarrow (1/x, y/x^4)$ with $v = y/x^2$ and $u = x + 1/x$, $\beta : (x, y) \rightarrow (-1/x, y/x^4)$ with $v = y/x^2$ and $u = x - 1/x$, and $\gamma : (x, y) \rightarrow (-x, y)$ with $v = y$ and $u = x^2$. If E_i $i = 1, 2, 3$ is the curve $C/ < \sigma_i >$ for $\sigma_i = \alpha, \beta, \gamma$, then by Hurwitz [H, IV.2.4] E_i is elliptic because each involution fixes exactly four points and therefore $g(C) - 1 = 2(g(E_i) - 1) + 4/2$. E_1 is given by

$$v^2 = (u^2 - 2 - d^2 - 1/d^2)(u^2 - 2 - e^2 - 1/e^2)),$$

E_2 is given by

$$v^2 = (u^2 + 2 - d^2 - 1/d^2)(u^2 + 2 - e^2 - 1/e^2)),$$

E_3 is given by

$$v^2 = (u^2 - (d^2 + 1/d^2)u + 1)(u^2 - (e^2 + 1/e^2)u + 1).$$

Because the natural isogeny from $J(C)$ to $E_1 \times E_2 \times E_3$ has degree a power of 2, 2.2A implies C is superspecial if and only if all three E_i are supersingular. After applying an isogeny of degree 2 to each of these three elliptic curves we can obtain elliptic curves with $\lambda_1 = ((d+1/d)/(e+1/e))^2$, $\lambda_2 = ((e-1/e)/(d-1/d))^2$, and remarkably $\lambda_3 = 1/(\lambda_1\lambda_2)$. The 192 ordered pairs yield 12 ordered triples $(\lambda_1, \lambda_2, \lambda_3)$ corresponding to permutations and taking the reciprocal of all three. $\overline{\Gamma} \cong D_8$ symmetry corresponds to being able to take $\lambda_1 = \lambda_2$, D_{16} to $\lambda_1 = \lambda_2 = 3 + 2\sqrt{2}$, and S_4 to $\lambda_1 = \lambda_2 = -3$, which is 2-isogenous to both $\lambda = \omega_3$ and $\lambda = 9, -8$. This process is reversible via

$$d = \frac{\sqrt{\lambda_1(1-\lambda_2)} + \sqrt{\lambda_1 - 1}}{\sqrt{1-\lambda_1\lambda_2}}, e = \frac{\sqrt{1-\lambda_2} + \sqrt{\lambda_2(\lambda_1-1)}}{\sqrt{1-\lambda_1\lambda_2}},$$

thus completing the proof of I(a,c,e,h,k).

An hyperelliptic curve C with $D_6 \leq \overline{\Gamma}$ can be written as $y^2 = x(x^3-1)(x^3-a^3)$ with $a^3 \neq 0, 1$. The only other choice for a^3 that produces an isomorphic curve is $1/a^3$, and the curve has $D_6 < \overline{\Gamma}$ if and only if $a^3 = -1$ which has reduced automorphism group D_{12} or $a^3 = -8, -1/8$ which has reduced group S_4. Let $\alpha : (x, y) \rightarrow (a/x, a^2y/x^4)$ with $u = x + a/x$, and $v = y/x^2$, $\beta : (x, y) \rightarrow (a\omega/x, a^2\omega^2y/x^4)$ with $u = \omega x + a\omega^2/x$, and $v = y/x^2$, and $\gamma : (x, y) \rightarrow (\omega x, \omega^2 y)$ be their product with $u = x^3$, and $v = yx$, where $\omega = \omega_3$ is a cube root of unity. If E_i $i = 1, 2, 3$ is the curve $C/ < \sigma_i >$ for $\sigma_i = \alpha, \beta, \gamma$, then E_i is elliptic because again the involutions α and β fix exactly four points and γ of order 3 fixes exactly 2 points and therefore $g(C) - 1 = 3(g(E_3) - 1) + 2 * 2/2$. E_1 and E_2 are both given by $v^2 = u^3 - 3au - a^3 - 1$, which has $\lambda = \frac{-\omega a + 1}{a - \omega}$, and E_3 is given by $v^2 = u(u-1)(u-a^3)$, which has $\lambda_3 = a^3$. Because the natural isogeny from $J(C)$ to $E_1 \times E_2 \times E_3$ has degree a product of powers of 2 and 3, 2.2A again implies C is superspecial if and only if all three E_i are supersingular. The maps $a \rightarrow \omega a$ and $a \rightarrow 1/a$ induce the maps $\lambda \rightarrow 1/(1-\lambda)$ and $\lambda \rightarrow 1/\lambda$, and $\overline{\Gamma} \cong D_{12}$ symmetry corresponds to being able to take $\lambda = -1$ and hence $j = 1728$, and S_4 to $\lambda = \omega$ and hence $j = 2^{11}/3$. Given λ we can recover a by $a = \frac{\omega\lambda+1}{\lambda+\omega}$, and hence $\lambda_3 = (\frac{\omega\lambda+1}{\lambda+\omega})^3$, thus completing the proof of I(f).

Superspecial Curves

An hyperelliptic curve C with $\mathbf{Z}/2 \times \mathbf{Z}/4 \leq \Gamma$ can be written as

$$y^2 = (x^4 - 1)(x^4 - (a^2 + 1/a^2)x^2 + 1)$$

with $a \neq 0, \pm 1, \pm i$. Generically 8 choices for a, generated by $a \to ia$ and $a \to 1/a$, produce isomorphic curves. This curve has $\mathbf{Z}/2 \times \mathbf{Z}/4 < \Gamma$ if and only if we can take $a = 2 + \sqrt{3}$ which has reduced automorphism group D_{12} or $a^4 = -1$ which has reduced group D_{16}. Let $\alpha : (x, y) \to (-x, y)$ with $v = y$ and $u = x^2$ and $\beta : (x, y) \to (-x, -y)$ with $v = yx$ and $u = x^2$. $E_1 = C/ < \alpha >$ is elliptic because the involution α fixes four points, and $Y = C/ < \beta >$ has genus 2 because the involution β does not fix any points so $g(C) - 1 = 2(g(Y) - 1) + 0/2$. E_1 is given by $v^2 = (u^2 - 1)(u - a^2)(u - 1/a^2)$, which has $j = 1728$ and the curve Y is given by $v^2 = u(u^2 - 1)(u - a^2)(u - 1/a^2)$. Under the transformation $u \to i\frac{(u-1)\sqrt{a^2+1}}{(u+1)\sqrt{a^2-1}}$, Y becomes $v^2 = u(u^2 + (\frac{a^2-1}{a^2+1}))(u^2 + (\frac{a^2+1}{a^2-1}))$. Following [11], on Y let $\gamma : (u, v) \to (1/u, v/u^3)$ with $s = v(1 + u)/u^2$ and $t = u + 1/u$ and $\delta : (u, v) \to (1/u, -v/u^3)$ with $s = iv(1 - u)/u^2$ and $t = -u - 1/u$. If E_i $i = 2, 3$ is the curve $Y/ < \sigma_i >$ for $\sigma_i = \gamma, \delta$, then E_i is elliptic because each involution fixes exactly two points and therefore $g(Y) - 1 = 2(g(E_i) - 1) + 2/2$. E_2 and E_3 are both given by $s^2 = (t + 2)(t^2 + 1/(a^4 - 1))$, which has λ that satisfies $\lambda^2 - \lambda + a^4/4 = 0$. Because the natural isogeny from $J(C)$ to $E_1 \times E_2 \times E_3$ has degree a power of 2, 2.2A implies C is superspecial if and only if $p \equiv 3 \bmod 4$ and $h_p(\lambda) = 0$. E_2 undergoes an isogeny of degree 2 under $a \to 1/a$ and is fixed by $a \to ia$. $\overline{\Gamma} \cong D_{12}$ symmetry corresponds to a 3-isogeny with E_1, and D_{16} to $\lambda = (1 + \sqrt{2})/2$, which is supersingular when $p \equiv 5, 7 \bmod 8$. Hence, every C gives rise to 4 λ's and each of the $(p - 1)/2$ λ's appearing in 1.8A gives rise to a curve C with $\mathbf{Z}/2 \times \mathbf{Z}/4$ symmetry, except when $\lambda = 1/2$ which gives a singular C, when $a = 2 + \sqrt{3}$ which gives 4 λ's but symmetry D_{12}, and when $a^4 = -1$ which gives only 2 λ's and symmetry D_{16}. Therefore, the number of such curves is $(p - 1)/8 - 5/4$ if $p \equiv 3 \bmod 8$ and $(p - 1)/8 - 7/4$ if $p \equiv 7 \bmod 8$, from which we can conclude I(d).

Superspecial Curves

By 3.5(d) a nonhyperelliptic curve C with automorphism group $D_4 \leq G$ can be written as $x^4 + y^4 + 1 + ax^2y^2 + bx^2 + cy^2$. A singularity occurs in the Jacobian matrix if and only if $abc - a^2 - b^2 - c^2 + 4 = 0$ or a, b, or $c = \pm 2$ Generically 24 choices for (a, b, c), generated by permutations and changing the sign of any two of them, produce isomorphic curves. This curve has $D_4 < G$ if and only if we can take $a = b$ which has $D_8 \leq G$. If E_i $i = 1, 2, 3$ is the curve $C/ < \sigma_i >$ for $\sigma_i = \alpha, \beta, \gamma$, where α, β, and γ are the three involutions of D_4, then E_i is elliptic because each involution fixes exactly four points. If γ is the map $(x, y) \to (-x, y)$ and $z = 2x^2 + ay^2 + b$, then E_3 is given by $z^2 = (a^2 - 4)y^4 + (2ab - 4c)y^2 + b^2 - 4$, which by 1.12 is 2-isogenous to an elliptic curve with invariant

$$\lambda_3 = \frac{ab - 2c + 2\sqrt{a^2 + b^2 + c^2 - abc - 4}}{ab - 2c - 2\sqrt{a^2 + b^2 + c^2 - abc - 4}},$$

and similarly we can determine λ_1 and λ_2 corresponding to E_1 and E_2 by permuting a, b, and c cyclicly. By Oort [27, p. 39] the natural isogeny from $J(C)$ to $E_1 \times E_2 \times E_3$ has degree a power of 2, and therefore 2.2A implies C is superspecial if and only if $h_p(\lambda_i) = 0$. Permutations of (a, b, c) induce similar permutations on $(\lambda_1, \lambda_2, \lambda_3)$, and $(a, b, c) \to (-a, -b, c)$ induces $(\lambda_1, \lambda_2, \lambda_3) \to (1/\lambda_1, 1/\lambda_2, \lambda_3)$, and the D_8 symmetry $a = b$ implies $\lambda_1 = \lambda_2$. This transformation is reversible via

$$a = \frac{-2(\lambda_2 + 1)(\lambda_3 + 1) + 4(\lambda_1 + 1)\sqrt{\lambda_2\lambda_3/\lambda_1}}{(\lambda_2 - 1)(\lambda_3 - 1)}$$

and cyclic permutations for b and c, except that some nonsingular λ's yield singular (a, b, c). This is to be expected because $(a, b, c) = (\pm 2, \pm 2, \pm 2)$ with an even number of minus signs gives indeterminate $(\lambda_1, \lambda_2, \lambda_3)$. In particular, we find that if $\lambda_1 = 1/\lambda_2\lambda_3$, $\lambda_2\lambda_3$, λ_2/λ_3, or λ_3/λ_2 then $(a, b, c) = (2, 2, 2)$, $(2, -2, -2)$, $(-2, 2, -2)$, and $(-2, -2, 2)$, respectively. Hence, we see that the number of equivalence classes of triples $(\lambda_1, \lambda_2, \lambda_3)$ not corresponding to a nonsingular quartic is precisely the number that correspond to an hyperelliptic curve in I(e).

It remains to count the number of classes of supersingular triples $(\lambda_1, \lambda_2, \lambda_3)$ and therefore the number of curves with $\overline{\Gamma} \cong D_4$. The curve has no more symmetry provided no λ_i is equal to another one or its reciprocal, and there are 24 triples for each curve. Hence, by 1.8A if $p \equiv 1 \bmod 4$ there are $k(k-2)(k-4)/24$ curves where $k = (p-1)/2$. If $p \equiv 3 \bmod 4$ we must treat the root -1 differently because it is its own reciprocal. There are $(k-1)(k-3)(k-5)$ ordered triples without -1 and $3(k-1)(k-3)$ with -1 for a total of $(k-1)(k-2)(k-3)/24$ curves, thus completing the proof of II(d).

By 3.5(i) a nonhyperelliptic curve C with automorphism group $G_2(2,2,2; -,-,-) \leq G$ can be written as $x^4 + y^4 + 1 + ax^2y^2$ with $a \neq \pm 2$. Generically 6 choices for a, generated by $a \to -a$ and $a \to \frac{2a+12}{a-2}$, produce isomorphic curves. This curve has $16 < |G|$ if and only if we take $a^2 = -12$ which has $|G| = 48$ or we take $a = 0, \pm 6$ which is the Fermat curve. Using the notation of II(d) with $b = c = 0$ and without the additional 2-isogeny $\lambda_1 = (a-2)/(a+2)$ and $\lambda_2 = \lambda_3 = -1$, we can recover a by $a = -2(\lambda_1 - 1)/(\lambda_1 + 1)$, and C is superspecial if and only if $h_p(\lambda_i) = 0$. The maps $a \to -a$ and $a \to \frac{2a+12}{a-2}$ induce the maps $\lambda_1 \to 1/\lambda_1$ and $\lambda_1 \to 1 - \lambda_1$. $|G| = 48$ symmetry implies $\lambda_1 = \omega_6$, which is supersingular when $p \equiv 5 \bmod 6$, and Fermat symmetry implies $\lambda_1 = -1$, $1/2$, or 2. Since we have 6 λ's for all but these two exceptional curves this calculation is the same as 3.12(a) for $p \equiv 3 \bmod 4$, which concludes the proof of II(i).

By 3.5(j) a nonhyperelliptic curve C with automorphism group $S_4 \leq G$ can be written as $x^4 + y^4 + 1 + ax^2y^2 + ax^2 + ay^2$ with $a \neq -1, \pm 2$. a uniquely determines the curve, unless $a^2 + 3a + 18 = 0$ and C is the Klein curve. The only other curve with $S_4 < G$ is the Fermat curve with $a = 0$. Again using the notation of II(d) with $a = b = c$ and without the additional 2-isogeny, $\lambda_1 = \lambda_2 = \lambda_3 = -a - 1$, we can recover a by $a = -1 - \lambda_1$, and C is superspecial if and only if $h_p(\lambda_i) = 0$. The Fermat curve has $\lambda_1 = -1$, and the Klein curve has $\lambda_1^2 - \lambda_1 + 16 = 0$, which is supersingular when $p \equiv 3, 5, 6 \bmod 7$ by [H, 4.23.4 and Ex. IV.4.12(b)] for example. The hole when $a = 2$ and $\lambda_1 = -3$ is fortunately filled by I(k), thus concluding the proof of II(j). By either this or 2.17 II(l,m) are also proved, which concludes the proof of the theorem.∎

Remark 3.15.2. The following is a sketch of a possible alternate proof of the II(f) that would follow the proof of II(d) above. Assume C is not hyperelliptic with $D_6 \leq Aut(C)$. Let E_i $i = 1, 2, 3$ be the curve $C/ < \sigma_i >$ for $\sigma_i = \alpha, \beta, \gamma$, two distinct involutions and their product in D_6. The E_i are elliptic, and C is superspecial if and only if all three E_i are supersingular. By 3.15(f) the curve C can be written as $x^3 + y^3 + 1 + axy + bx^2y^2$. If $\alpha : (x, y) \to (y, x)$, $u = x + y$, and $z = 2bxy - 3x - 3y + a$, E_1 is given by $z^2 = -4b(u^3 + 1) + (3u - a)^2$. If $\beta : (x, y, z) \to (\omega y, \omega^2 x)$, $u = \omega x + \omega^2 y$, and $z = 2bxy - 3\omega x - 3\omega^2 y + a$, E_2 is also given by $z^2 = -4b(u^3 + 1) + (3u - a)^2$. If $\gamma : (x, y, z) \to (\omega x, \omega^2 y)$, where ω is a cube root of unity, $v = xy$, and $z = 2x^3 + 1 + axy + bx^2y^2$, E_3 is given by $z^2 = -4v^3 + (bv^2 + av + 1)^2$. Now we would need to know what ordered pairs (a, b) give the same curve, what effect this has on the elliptic curves, and how to get from the elliptic curves back to C. It is possible to show that C has S_4 symmetry (resp. is Fermat, or is Klein) if and only if

$$a^3 + 8a^2b^2 + 45ab + 27 = 16b^3 + a^4b$$

(resp. $ab = 9/2$ and $a^3 = 108$, or $ab = -9/7$ and $a^3 = 27/7$).

Remark 3.15.3. We could also prove II(e) as follows. By 3.5(e) the curve C can be written as $y^3 = (x^2 - 1)(x^2 - a)$. By Corollary 2.18 with $i = j = 1$ $p \not\equiv 1 \bmod 3$. If $p \equiv 2 \bmod 3$ a only needs to solve $F_p(2/3, 1/2, 5/6; a) = F_p(1/3, 1/2, 7/6; a) = 0$. However, because

$$F(a, b, c; z) = \frac{\Gamma(1-a)\Gamma(1-b)\Gamma(c)}{\Gamma(c-a)\Gamma(c-b)\Gamma(2-c)} z^{1-c}(1-z)^{c-a-b} F(1-a, 1-b, 2-c; z)$$

we can conclude that these two polynomials have the same $(p-5)/6$ simple zeros distinct from 0 and 1. If a is a root so is $1/a$, which is the only other value that corresponds to the same curve, and the curve has higher symmetry only if $a=-1$ and $p \equiv 11 \bmod 12$. Hence, we are done.

We could also prove II(i) as follows. By 3.5(i) the curve C can be written as $y^4=(x^2-1)(x^2-a)$ or $y^4=x(x-1)(x-\lambda)$. By Corollary 2.18 with $i=j=1$ for the first curve $p \not\equiv 1 \bmod 4$. If $p \equiv 3 \bmod 4$ a only needs to solve $F_p(1/2,1/2,1;a)=0$ or equivalently λ only needs to solve $F_p(1/2,1/2,1;\lambda)=0$. Hence, the calculation is identical to that for 3.12(a) as noted earlier.

Remark 3.15.4. We can restate I(f) as: the number of simultaneous solutions to $h_p(a)=F_p(1/2,1/6,2/3;a)=0, a \neq -1,-8,-1/8$, up to taking the reciprocal. This follows from 2.18 applied to the curve $y^2=x(x^3-1)(x^3-a)$. It would be interesting to know what the connection is between the roots of $F_p(1/2,1/6,2/3;\lambda)=0$ and the roots of $h_p((\frac{\lambda+\omega^2}{\lambda+\omega})^3)=0$.

We can restate I(h) as: the number of simultaneous solutions to $h_p(a)=F_p(1/2,1/4,3/4;a)=0, a \neq -1,(2\pm\sqrt{3})^4$, up to taking the reciprocal. This follows from 2.18 applied to the curve $y^2=(x^4-1)(x^4-a)$. It would be interesting to know what the connection is between the roots of $F_p(1/2,1/4,3/4;\lambda)=0$ and the roots of $h_p(\lambda^2)=0$.

Bibliography

1. R. Bott and L. W. Tu, *Differential Forms in Algebraic Topology*, Graduate Texts in Mathematics **82**, Springer-Verlag, New York (1982), xiv + 331 pp.

2. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups*, Oxford University Press, New York (1985), xxxiii + 252 pp.

3. M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Univ. Hamburg* **14** (1941), 197-272.

4. M. Eichler, Úber die Idealklassenzahl total definiter Quaternionenalgebren, *Math. Z.* **43** (1938), 102-109.

5. T. Ekedahl, On supersingular curves and abelian varieties, *Math. Scand.* **60** (1987), 151-178.

6. N. Elkies, private communication.

7. W. Feit, The current situation in the theory of finite simple groups, *in Actes du Congrès International des Mathématiciens, Vol. I*, Gauthier-Villars (1970), 55-93.

H. R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer-Verlag, New York (1977), xvi + 496 pp.

9. K. Hashimoto, Class numbers of positive definite ternary quaternion hermitian forms, *Proceed. Japan Acad.* **59** Ser. A (1983), 490-493.

10. K. Hashimoto and T. Ibukiyama, On class numbers of positive definite binary quaternion hermitian forms (I), *J. Fac. Sci. Univ. Tokyo Sect IA* **27** (1980), 549-601.

11. T. Ibukiyama, T. Katsura, and F. Oort, Supersingular curves of genus two and class numbers, *Compositio Mathematica* **57** (1986), 127-152.

12. J. Igusa, Class number of a definite quaternion with prime discriminant, *Proc. Nat. Acad. Sci. U.S.A.* **44** (1958), 312-314.

13. J. Igusa, Arithmetic variety of moduli for genus two, *Ann. of Math.* **72** (1960), 612-649.

14. T. Katsura and F. Oort, Supersingular abelian varieties of dimension two and three and class numbers, *in Algebraic Geometry, Sendai, 1985* (T. Oda, ed.),

Advanced Studies in Pure Mathematics **10**, North-Holland, New York (1987), 253-281.

15. N. Katz, Slope filtration of F-crystals, *in Journées de Géométrie Algébrique de Rennes (Juillet 1978) (I)*, Astérisque **63**, Société Mathématique de France, Paris (1979), 113-164.

16. N. Koblitz, p-adic variation of the zeta-function over families of varieties defined over finite fields, *Compositio Mathematica* **31** (1975), 119-218.

17. R. S. Kulkarni, Symmetries of surfaces, *Topology* **26** (1987), 195-203.

18. A. Kuribayashi and K. Komiya, On Weierstrass points and automorphisms of curves of genus three, *in Algebraic Geometry: Proceedings, Copenhagen 1978* (K. Lønsted, ed.), Lecture Notes in Mathematics **732**, Springer-Verlag, New York (1979), 253.

19. Ju. I. Manin, The Hasse-Witt matrix of an algebraic curve, *Am. Math. Soc. Translations, Ser. 2* **45** (1965), 245-264.

20. G. A. Miller, H. F. Blichfeldt, L. E. Dickson, *Theory and Applications of Finite Groups*, Dover, New York (1961), 390 pp.

21. D. Mumford, *Abelian Varieties*, Oxford University Press (1970), 279 pp.

22. D. Mumford, *Curves and Their Jacobians*, University of Michigan Press, Ann Arbor, 104 pp.

23. M. S. Narasimhan and M. V. Nori, Polarizations on an abelian variety, *in Geometry and Analysis: Papers Dedicated to the Memory of V. K. Patodi*, Springer-Verlag, New York (1981), 125-128.

24. N. O. Nygaard, Slopes of powers of frobenius on crystalline cohomology, *Ann. Sci. École Norm. Sup., 4 sér.,* **14** (1981), 369-401.

25. F. Oort, Subvarieties of moduli spaces, *Invent. Math.* **24** (1974), 95-119.

26. F. Oort, Which abelian surfaces are products of elliptic curves?, *Math. Ann.* **214** (1975), 35-47.

27. F. Oort, Hyperelliptic supersingular curves, *in Arithmetic Algebraic Geometry* (G. van der Geer, F. Oort, J. Steenbrink, eds.), Progress in Mathematics **89**, Birkhäuser, Boston (1991), 247-284.

28. T. Shioda, Supersingular K3 surfaces, *in Algebraic Geometry: Proceedings, Copenhagen 1978* (K. Lønsted, ed.), Lecture Notes in Math. **732**, Springer-Verlag, New York (1979), 564-591.

29. N. Yui, On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$, *Journal of Algebra* **52** (1978), 378-410.