Gunby *et al. Research in Number Theory* (2015) 1:3
DOI 10.1007/s40993-015-0004-8

Research in Number Theory
a SpringerOpen Journal

RESEARCH ARTICLE Open Access

Irreducible canonical representations in positive characteristic

Benjamin Gunby[1*], Alexander Smith[2] and Allen Yuan[3]

*Correspondence: bgunby314@gmail.com
[1] Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
Full list of author information is available at the end of the article

Abstract

For X a curve over a field of positive characteristic, we investigate when the canonical representation of $\mathrm{Aut}(X)$ on $H^0(X, \Omega_X)$ is irreducible. Any curve with an irreducible canonical representation must either be superspecial or ordinary. Having a small automorphism group is an obstruction to having irreducible canonical representation; with this motivation, the bulk of the paper is spent bounding the size of automorphism groups of superspecial and ordinary curves. After proving that all automorphisms of an $\mathbb{F}_{q^2}$-maximal curve are defined over $\mathbb{F}_{q^2}$, we find all superspecial curves with $g > 82$ having an irreducible representation. In the ordinary case, we provide a bound on the size of the automorphism group of an ordinary curve that improves on a result of Nakajima.

1 Introduction

Given a complete nonsingular curve X of genus $g \geq 2$, the finite group $G := \mathrm{Aut}(X)$ has a natural action on the g-dimensional k-vector space $H^0(X, \Omega_X)$, known as the *canonical representation*. It is natural to ask when this representation is irreducible. In characteristic zero, irreducibility of the canonical representation implies that $g^2 \leq |G|$, and combining this with the Hurwitz bound of $|G| \leq 84(g-1)$, one can observe that the genus of X is bounded by 82. In fact, Breuer [1] shows that the maximal genus of a Riemann surface with irreducible canonical representation is 14.

In characteristic p, the picture is more subtle when p divides $|G|$. The Hurwitz bound of $84(g-1)$ may no longer hold due to the possibility of wild ramification in the Riemann-Hurwitz formula. It is known that when $2 \leq g \leq p-2$, the Hurwitz bound holds with one exception given by Roquette [21]: the hyperelliptic curve $y^2 = x^p - x$, which has genus $\frac{p-1}{2}$ and $2p(p^2-1)$ automorphisms. In general, the problem of classifying curves with more than $84(g-1)$ automorphisms is not well understood. At present, the best general result is by Henn, who in [9] classified all curves for which $|G| \geq 8g^3$, extending the work of Stichtenoth in [22]. Recent results improve the classification for supersingular curves over characteristic 2 fields [5], for p-cyclic covers of the projective line [16], and for curves with "big actions" [17], but Henn's classification remains the best general result.

Hence, in characteristic p, the above bound of $g \leq 82$ certainly no longer applies. Indeed, Hortsch [11] shows that the Roquette curve has irreducible canonical representation, providing an example of arbitrarily high genus curves with irreducible canonical

Springer

© 2015 Gunby et al.; licensee Springer. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

representation. Dummigan [2] showed that the Fermat curve (which is equivalent to the Hermitian or Drinfeld curve after suitable change of coordinates)

$$x^{p+1} + y^{p+1} + z^{p+1} = 0$$

in characteristic p is another such example, having genus $g = \frac{p(p-1)}{2}$.

It is natural to ask whether for fixed p, there exist characteristic p curves X of arbitrarily high genus g with irreducible canonical representation. Via Observation 2.3, this question splits into two cases depending on whether the curve is *superspecial* (i.e., the Frobenius acts as 0 on $H^1(X, \mathscr{O}_X)$) or *ordinary* (i.e., the p-rank of X equals g).

In the superspecial case, we find all curves of genus $g > 82$ with irreducible canonical representations. Indeed, as we demonstrate in Theorem 3.3, any such curve must be isomorphic to either the Roquette curve or the Fermat curve given above. To prove this, we show that we may work with $\mathbb{F}_{p^2}$-maximal curves and subsequently prove a strict condition for a high genus $\mathbb{F}_{p^2}$-maximal curve to have $|\mathrm{Aut}(X)| > g^2$. Since $|\mathrm{Aut}(X)| > g^2$ is a necessary condition for irreducibility, this will give the result. To prove the condition for $\mathbb{F}_{p^2}$-maximal curves to have many automorphisms, which is given as Theorem 3.16, we rely on the new result that all automorphisms of an $\mathbb{F}_{q^2}$-maximal curve are defined over $\mathbb{F}_{q^2}$, which is given as Theorem 3.10.

We then reduce the question to considering ordinary curves, where progress is harder. Nakajima [19] bounds the automorphism group of an ordinary curve by $84g(g-1)$. In this paper, we prove the following stronger result:

Theorem 1.1. *There exists a constant $c = c(p)$ such that any ordinary curve X over a field of characteristic p with genus $g_X > c$ satisfies the inequality*

$$|\mathrm{Aut}(X)| \leq 6\left(g_X^2 + 12\sqrt{21}g_X^{\frac{3}{2}}\right).$$

Remark 1.2. From our proof, we may take $c(p)$ to be on the order of p^2.

This does not yet imply reducibility of the canonical representation, but we have the following.

Remark 1.3. An unpublished result of Guralnick and Zieve [7] states that for any prime p there is a positive constant c_p so that, if X is an ordinary curve of genus $g > 1$ over an algebraically closed field of characteristic p, the group of automorphisms of X has order bounded by $c_p g^{8/5}$. Together with the superspecial results, this would imply that for a fixed characteristic, there do not exist arbitrarily high genus curves with irreducible canonical representation. We hope that the eventual published work will give even stronger ways of characterizing ordinary curves with irreducible canonical representations.

2 Preliminaries

In this section, we present notations and basic techniques that will be used throughout the paper. Let k be an algebraically closed field of characteristic $p > 0$. Throughout, a curve is a complete connected nonsingular curve over k. For a curve X, we shall use g_X, γ_X, and $\mathrm{Aut}(X)$ to denote its genus, p-rank of Jacobian, and automorphism group, respectively. For any two curves X and Y, $\pi_{X/Y}$ will denote a (branched) covering map $X \to Y$ if there is no ambiguity with respect to the map in question.

2.1 Ramification Groups

Given a curve X, a finite subgroup $G \subset \mathrm{Aut}(X)$, and a point $P \in X$, define the ramification groups $G_i(P)$ for $i \geq 0$ as follows:

$$G_0(P) = \{\sigma \in G | \sigma P = P\} \tag{1}$$

and

$$G_i(P) = \{\sigma \in G_0(P) | \mathrm{ord}_P(\sigma \pi_P - \pi_P) \geq i + 1\} \tag{2}$$

for $i > 0$, where π_P is a uniformizer of the ring of functions on X at P and ord_P denotes the order of the zero at P.

We will use the following fact about the ramification groups, which can be found in ([19], Sections 2,3):

Proposition 2.1. *Let X be a curve, G be a subgroup of $Aut(X)$, and $P \in X$ be any point. Then the following are true:*

(1) $G_1(P)$ is a normal Sylow p-subgroup of $G_0(P)$.
(2) $G_0(P)/G_1(P)$ is a cyclic group with order prime to p.
(3) If in addition, X is ordinary (i.e. $g_x = \gamma_x$), then $G_2(P) = \{1\}$.

2.2 Galois Coverings of Curves

Let $\pi : X \to Y$ be a Galois covering of curves with Galois group G. Then, Y is the quotient of X by a finite subgroup G of automorphisms. For $Q \in Y$ and any point $P \in \pi^{-1}(Q)$, let e_Q denote the ramification index of π at P, and $d_Q := \sum_{i=0}^{\infty}(|G_i(P)| - 1)$. Note that e_Q and d_Q do not depend on the choice of P. We also have that $d_Q \geq e_Q - 1$ with equality if and only if Q is tamely ramified. The relationship between the genera of X and Y is given by the Riemann-Hurwitz formula (see [8]):

$$\frac{2g_X - 2}{|G|} = 2g_Y - 2 + \sum_{Q \in Y} \frac{d_Q}{e_Q}. \tag{3}$$

A similar formula, known as the Deuring-Šafarevič formula, relates the p-ranks of X and $Z = X/H$ when $H \subseteq G$ is a p-group (see [23], Thm 4.2) :

$$\frac{\gamma_X - 1}{|H|} = \gamma_Z - 1 + \sum_{Q \in Z} \left(1 - e_Q^{-1}\right). \tag{4}$$

2.3 Frobenius and *p*-rank

The idea of studying the canonical representation via Frobenius has appeared in [18]. It may be adapted to our situation as follows. The action of Frobenius on a curve X gives a natural action of Frobenius on $H^1(X, \mathcal{O}_X)$. In fact, for particular curves, this action can be explicitly computed on a basis of $H^1(X, \mathcal{O}_X)$ by using a Čech cover of X. In addition, by Serre duality, $H^1(X, \mathcal{O}_X)$ has a natural $k[\mathrm{Aut}(X)]$-module structure as the dual representation of the canonical representation. In fact, it is not difficult to see that the Frobenius commutes with this module structure. Since the Frobenius map does not respect scalar multiplication, it is not quite a $k[\mathrm{Aut}(X)]$-module homomorphism, but we may still observe the following:

Observation 2.2. *If X has irreducible canonical representation, then the $\mathbb{F}_p$-vector space map $F\colon H^1(X,\mathscr{O}_X) \to H^1(X,\mathscr{O}_X)$ given by Frobenius is either injective or zero.*

Proof. The kernel of this map is a k-vector space which is invariant under $\mathrm{Aut}(X)$ since automorphisms (on the function field) commute with F. Thus, the kernel is a $k[\mathrm{Aut}(X)]$-module, so if it is a proper nonzero submodule, then the canonical representation has a proper subrepresentation, contradicting the hypothesis. Hence, the kernel must either equal $H^1(X,\mathscr{O}_X)$ or zero. □

In the literature, the matrix of the action of F on $H^1(X,\mathscr{O}_X)$ is referred to as the Hasse-Witt matrix, with the corresponding dual action on $H^0(X,\Omega_X)$ being known as the Cartier operator. If the action is injective, it is immediate that the p-rank of X is equal to its maximum possible value, g; such curves are called *ordinary*. On the other hand, if the action is zero, the curve is known as *superspecial*. The typical definition of a superspecial curve is a curve whose corresponding Jacobian variety is a product of supersingular elliptic curves. However, Oort [20] shows that this condition is equivalent to the Cartier operator being zero. With this extra notation, we can restate the above observation:

Observation 2.3. *Let X be a curve. If the canonical representation of X is irreducible, then X is either superspecial or ordinary.*

Example 2.4. Let X be the genus 2 curve given by $y^2 = x^5 - x$ in positive characteristic $p > 2$. Considered as a Riemann surface, this curve is called the Bolza surface and has 48 automorphisms, the most of any genus two curve [14]. In our case, we only consider the automorphisms $\alpha(x,y) = \left(\frac{1}{x}, \frac{y}{x^3}\right)$ and $\beta(x,y) = (-x, iy)$, where $i^2 = -1$.

Let $U = X\backslash\{(0,0)\}$ and $V = X\backslash\{P_\infty\}$. Since $\{U,V\}$ is a Cech cover for the curve, we have

$$H^1(X,\mathscr{O}_X) = \Gamma(U\cap V,\mathscr{O}_X)/\left(\Gamma(U,\mathscr{O}_X)\oplus\Gamma(V,\mathscr{O}_X)\right).$$

We can easily see that y/x and y/x^2 form a basis for $H^1(X,\mathscr{O}_X)$. Then, using these automorphisms α and β, it is easy to see that the canonical representation of this curve is irreducible. For α has distinct eigenvectors $\frac{y}{x} \pm \frac{y}{x^2}$ corresponding to eigenvalues ± 1, and it is easy to see that neither of these are fixed by β.

By the above criteria, we then know that this curve is either ordinary or superspecial. To determine which it is, we apply Frobenius to the two basis elements:

$$F\left(\frac{y}{x}\right) = \frac{y^p}{x^p} = \frac{y}{x^p}\left(x^5 - x\right)^{\frac{1}{2}(p-1)} = \frac{y}{x^{\frac{1}{2}(p+1)}}\left(x^4 - 1\right)^{\frac{1}{2}(p-1)}.$$

For $i \neq 1,2$, the function y/x^i is trivial in the cohomology group, so almost every term vanishes. Indeed, we get

$$F\left(\frac{y}{x}\right) = \begin{cases} K_1\frac{y}{x} & \text{if } p \equiv 1 \\ K_2\frac{y}{x^2} & \text{if } p \equiv 3 \\ 0 & \text{if } p \equiv 5,7 \end{cases} \pmod 8$$

where K_1, K_2 are nonzero binomial coefficients, and

$$F\left(\frac{y}{x^2}\right) = \begin{cases} K_3 \frac{y}{x} & \text{if } p \equiv 3 \\ K_4 \frac{y}{x^2} & \text{if } p \equiv 1 \\ 0 & \text{if } p \equiv 5, 7 \end{cases} \pmod 8.$$

From this, we see that the Bolza surface is ordinary if $p \equiv 1, 3 \pmod 8$ and is superspecial if $p \equiv 5, 7 \pmod 8$.

3 Superspecial curves

Proposition 3.1. *If X is a superspecial curve in a field of characteristic p, then $g \leq \frac{1}{2}p(p-1)$. If X is additionally hyperelliptic, then $g \leq \frac{1}{2}(p-1)$.*

Proof. This is Theorem 1.1 of [3]. □

Both of these bounds are sharp, with the Hermitian curve $x^p - x = y^{p+1}$ giving an example of the equality case for the first bound and the hyperelliptic curve $y^2 = x^p - x$ giving an example of the equality case for the second.

These two examples can be reused for the following proposition:

Proposition 3.2. *The maximal genus of a superspecial curve with irreducible canonical representation is $\frac{1}{2}p(p-1)$, a bound attained by the Hermitian curve given by $x^p - x = y^{p+1}$. The maximal genus of a hyperelliptic superspecial curve with irreducible canonical representation is $\frac{1}{2}(p-1)$, a bound attained by the curve given by $y^2 = x^p - x$.*

Proof. Dummigan [2] and Hortsch [11] prove that the two desired curves have irreducible canonical representation, so we are done by the previous proposition. □

In fact, these are the only two infinite families of superspecial curves with irreducible canonical representation, in the sense of the following theorem:

Theorem 3.3. *If X is a superspecial curve of genus $g > 82$ over an algebraically closed field of characteristic p, then X has an irreducible canonical representation if and only if X is isomorphic to the curve given by $y^2 = x^p - x$ or to the curve given by $y^{p+1} = x^p - x$.*

This result will be proved in section 'Superspecial curves with irreducible canonical representations'. To prove this result, we transmute the problem to looking at maximal and minimal curves, which we define now.

3.1 Maximal and minimal curves

Theorem 3.4. *(Weil conjecture for curves) If X is a nonsingular curve of genus g defined over $\mathbb{F}_q$, then there are $2g$ complex constants $\omega_1, \ldots, \omega_{2g}$ of magnitude $q^{1/2}$ so that N_n, the number of $\mathbb{F}_{q^n}$-rational points on the curve, satisfies*

$$N_n = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n.$$

In particular, $q^n - 2gq^{n/2} + 1 \leq N_n \leq q^n + 2gq^{n/2} + 1$.

Definition 3.5. A curve defined over $\mathbb{F}_{q^2}$ is called $\mathbb{F}_{q^2}$-maximal if the number of $\mathbb{F}_{q^2}$-rational points is $q^2 + 2gq + 1$, and is called $\mathbb{F}_{q^2}$-*minimal* if the number of $\mathbb{F}_{q^2}$-rational points is $q^2 - 2gq + 1$.

From the Weil conjectures, we see that the number of $\mathbb{F}_{q^{2n}}$-rational points on a $\mathbb{F}_{q^2}$-maximal curve is $q^{2n} + (-1)^{n-1}2gq^n + 1$, and the number of $\mathbb{F}_{q^{2n}}$-rational points on a $\mathbb{F}_{q^2}$-minimal curve is $q^{2n} - 2gq^n + 1$. Since a curve must have at least as many $\mathbb{F}_{q^4}$-rational points as $\mathbb{F}_{q^2}$-rational points, note that a $\mathbb{F}_{q^2}$ maximal curve has genus satisfying

$$q^4 - 2gq^2 + 1 \geq q^2 + 2gq + 1$$

or $g \leq \frac{q(q-1)}{2}$.

The relevance of maximal and minimal curves is immediate from the following proposition:

Proposition 3.6. *A curve X defined over the algebraic closure of $\mathbb{F}_p$ is superspecial if and only if it is isomorphic to an $\mathbb{F}_{p^2}$-maximal curve or an $\mathbb{F}_{p^2}$-minimal curve.*

Proof. This is a consequence of Ekedahl's work in [3] and is proved as Theorem 2.6 of [15]. □

The L-functions over $\mathbb{F}_{q^2}$ corresponding to maximal and minimal curves are very simple, equaling $(qt + 1)^{2g}$ for maximal curves and $(qt - 1)^{2g}$ for minimal curves. As was noted in [4] and extended to minimal curves in [25], this is enough to imply the following result, which is known as the *fundamental equation*.

Proposition 3.7. *Suppose X is an $\mathbb{F}_{q^2}$-maximal curve over an algebraically closed field of characteristic $p > 0$. If P_0 is an $\mathbb{F}_{q^2}$-rational point, then we have the linear equivalence*

$$(q + 1)P_0 \sim qP + F(P) \tag{5}$$

where F denotes the degree q^2 Frobenius map and P is any closed point of the curve. If X is instead assumed to be an $\mathbb{F}_{q^2}$-minimal curve, we have

$$(q - 1)P_0 \sim qP - F(P). \tag{6}$$

3.2 Automorphisms of maximal curves

Proposition 3.8. *Let X be an $\mathbb{F}_{q^2}$-maximal curve of genus at least two. Then three distinct points P, Q, R satisfy*

$$(q + 1)P \sim (q + 1)Q \sim (q + 1)R \tag{7}$$

if and only if all three points are $\mathbb{F}_{q^2}$-rational.

Remark 3.6. This proposition and proof also works for minimal curves, being based off the rational point relation $(q - 1)P \sim (q - 1)Q \sim (q - 1)R$ instead of (7).

Proof. The fundamental equation 5 gives that, if P, Q, R are all $\mathbb{F}_{q^2}$-rational, they satisfy (7). Conversely, suppose (7) were satisfied for three distinct points P, Q, R. We note that if

one of these points is $\mathbb{F}_{q^2}$-rational, then all three are. For supposing P were $\mathbb{F}_{q^2}$-rational, we can write

$$qQ + F(Q) \sim (q+1)P \sim (q+1)Q,$$

where F is the q^2 Frobenius map. Then $Q \sim F(Q)$, and hence $Q = F(Q)$.

From (5), we have $qP + F(P) \sim qQ + F(Q)$, and subtracting from (7) then gives $P + F(Q) \sim Q + F(P)$. If this system is not base point free, given that $P \neq Q$, we find $P = F(P)$, so the points are $\mathbb{F}_{q^2}$-rational. Then we assume $|P + F(Q)|$ is a base-point free linear system, so X must be hyperelliptic.

This same argument shows that $|P + F(R)|$ is a base-point free linear system. Both these divisors are of degree two and dimension one, so since the genus of the curve is at least two, the divisors must be the same (see [10], p.216). Then $P + F(Q) \sim P + F(R)$, so $Q = R$. This contradicts the three points being distinct, proving the proposition. □

Theorem 3.10. *An automorphism of an $\mathbb{F}_{q^2}$-maximal or -minimal curve of genus at least two fixes the set of $\mathbb{F}_{q^2}$-rational points. More generally, automorphisms of maximal or minimal curves always commute with the q^2 Frobenius map, and are hence defined as $\mathbb{F}_{q^2}$ maps.*

Proof. Take X to be such a maximal curve, and suppose there were an automorphism σ that maps an $\mathbb{F}_{q^2}$-rational point P_1 to a non-$\mathbb{F}_{q^2}$-rational point. Choose three distinct $\mathbb{F}_{q^2}$-rational points P_1, P_2, P_3. Then $(q+1)P_1 \sim (q+1)P_2 \sim (q+1)P_3$, so

$$(q+1)(\sigma P_1) \sim (q+1)(\sigma P_2) \sim (q+1)(\sigma P_3).$$

But σP_1 being not rational contradicts the previous proposition. Then any automorphism fixes the rational points.

This implies that automorphisms commute with the degree q^2 Frobenius map. For take P an arbitrary point, σ an arbitrary automorphism, and P_0 any rational point. Then

$$F(\sigma P) \sim (q+1)P_0 - q\sigma P \sim (q+1)\sigma P_0 - q\sigma P \sim \sigma F(P).$$

This establishes the theorem in the maximal case.

The minimal curve case falls to an identical argument if there are at least three $\mathbb{F}_{q^2}$-rational points. If there are not, we must have $q^2 - 2gq + 1$ either equal to one or two. Since $q^2 - 2gq + 1$ is one mod q, it must equal one if it is less than three, with $g = q/2$. Then in this exceptional case, q must be a power of two.

Let X be an $\mathbb{F}_{q^2}$-minimal curve in characteristic 2 with a single $\mathbb{F}_{q^2}$-rational point. Suppose there were an automorphism σ of the curve that did not fix the unique $\mathbb{F}_{q^2}$-rational point P_0. Let $P_1 = \sigma^{-1}P_0$. Then (6) applied to P_0 and σP_0 gives

$$(q-1)P_0 \sim q\sigma P_0 - F(\sigma P_0).$$

Similarly, applying (6) to P_0 and P_1 gives $(q-1)P_0 \sim qP_1 - F(P_1)$, and applying σ to this equation gives

$$(q-1)\sigma P_0 \sim q\sigma P_1 - \sigma F(P_1) \sim qP_0 - \sigma F(P_1).$$

Then

$$F(\sigma P_0) + \sigma F(P_1) \sim P_0 + \sigma P_0.$$

But P_0 is neither $\sigma F(P_1)$ nor $F(\sigma P_0)$, so since the curve is not rational, $|P_0 + \sigma P_0|$ is base-point free. We similarly find that $|\sigma P_0 + \sigma^2 P_0|$ is base-point free, so again by the uniqueness of such a linear system, we have $\sigma P_0 + \sigma^2 P_0 \sim P_0 + \sigma P_0$, for $P_0 = \sigma^2 P_0$.

Next, since X is an $\mathbb{F}_{q^4}$-minimal curve too, and since $q^4 - 2gq^2 + 1 = q^4 - q^3 + 1 \geq 3$, we can use what we have already proved to say that σ fixes the set of $\mathbb{F}_{q^4}$-rational points, of which there are an odd number. Write the order of σ as $2^l \cdot r$ with r odd. Then σ^r still switches P_0 and P_1, but in addition has order a power of two. Since there are an odd number of $\mathbb{F}_{q^4}$-rational points, this implies that σ^r fixes some $\mathbb{F}_{q^4}$-rational point. Call this point P_2. Then

$$(q-1)P_0 \sim qP_2 - F(P_2)$$

and

$$(q-1)\sigma^r P_0 \sim q\sigma^r P_2 - \sigma^r F(P_2)$$

for

$$(q-1)P_1 \sim qP_2 - \sigma^r F(P_2).$$

Then

$$(q-1)P_0 + F(P_2) \sim (q-1)P_1 + \sigma^r F(P_2)$$

so that

$$F(P_2) + P_1 \sim \sigma^r F(P_2) + F(P_1).$$

This must be another base-point free divisor of degree two. From the uniqueness of such a divisor, we have $F(P_2) + P_1 \sim P_0 + P_1$, for $F(P_2) \sim P_0$. This is impossible, implying that the automorphism group of X fixes the unique $\mathbb{F}_{q^2}$-rational point. Then the automorphism group of an $\mathbb{F}_{q^2}$-minimal curve fixes the $\mathbb{F}_{q^2}$-rational points. That automorphisms commute with Frobenius is proved exactly as it was before. □

Remark 3.11. This result has been observed before for specific curves. In [6], for instance, the automorphism group of a family of maximal curves is calculated, and it is observed that all automorphisms are defined over $\mathbb{F}_{q^2}$.

3.3 Consequences of Theorem 3.10

Theorem 3.10 is a very strong result for understanding the structure of the automorphism groups of maximal and minimal curves, telling us that if X is $\mathbb{F}_{q^2}$-maximal or -minimal, the group of automorphisms fixes the set of $\mathbb{F}_{q^{2n}}$-rational points for any n, a set whose cardinality we already knew. This can be exploited.

Proposition 3.12. *Let X be an $\mathbb{F}_{q^2}$-maximal or -minimal curve of genus $g \geq 2$. Take H to be a p-subgroup of automorphisms. Then H fixes a unique point and acts freely on all other points, and $|H|$ divides q^3.*

Proof. Maximal and minimal curves are known to have p-rank 0, so the first part of this proposition follows from Lemma 11.129 and Remark 11.128 of [10]. Explicitly, from the Deuring-Šafarevič formula, we have

$$\frac{-1}{|H|} = -1 + \sum_{Q \in Z} \left(1 - e_Q^{-1}\right),$$

where $Z = X/H$, and this relation can only hold if the map ramifies with index $|H|$ at a single point.

To prove the bound, we first deal with the case where X is $\mathbb{F}_{q^2}$-maximal. The action of H on the $\mathbb{F}_{q^2}$ rational points splits into one orbit of size one and some number of free orbits by the first part, so

$$|H| \mid \left(q^2 + 2gq\right)$$

But $g \leq \frac{q(q-1)}{2}$, so $|H| \leq q^3$. The same argument works for minimal curves unless $q^2 - 2gq = 0$, or rather unless $g = q/2$. In this case we consider the action of H on the $\mathbb{F}_{q^4}$ rational points. This gives

$$|H| \mid q^3(q-1)$$

so again $|H| \leq q^3$. □

From here forward, we will use the term *short orbit* to denote any non-free orbit of G in X, that is, an orbit where each point has nontrivial stabilizer in G.

Proposition 3.13. *Suppose X is a $\mathbb{F}_{q^2}$-maximal curve of genus $g \geq 2$, and suppose the automorphism group G of X has only free orbits outside of the $\mathbb{F}_{q^2}$-rational points. Then*

$$|G| \mid 2q^3\left(q^2 - 1\right)(q+1).$$

If X is instead a $\mathbb{F}_{q^2}$-minimal curve of genus $g \geq 2$, and the automorphism group G has only free orbits outside the $\mathbb{F}_{q^2}$-rational points, then

$$|G| \mid 2q^3\left(q^2 - 1\right)(q-1).$$

Proof. First suppose X is maximal. By Theorem 3.10, for a pair of integers $a \geq 1$ and $b \geq 2$, we can say the set $S_{(a,b)}$ of $\mathbb{F}_{q^{2ab}}$-rational points that are not $\mathbb{F}_{q^{2a}}$-rational is stabilized under G. If G has no short orbits outside the $\mathbb{F}_{q^2}$-rational points, then we know that $|G|$ will divide $|S_{(a,b)}|$, so for all $a, b \geq 1$,

$$|G| \mid \left(q^{2ab} + (-1)^{ab-1}2gq^{ab} - q^{2a} + (-1)^a 2gq^a\right). \tag{8}$$

Take T to be the maximal divisor of $|G|$ not divisible by p. From the above expression, we get

$$T \mid \left(q^{a(b-1)} + (-1)^{a(b-1)-1}\right)\left((-1)^{ab-1}2g + q^{ab} + (-1)^{a(b-1)}q^a\right).$$

Write $m = a(b-1)$, and take a, a' to be different factors of m with $a > a'$. If m is odd, we get

$$T \mid \left(q^m + 1\right)\left(-2g + q^{m+a} - q^a\right). \tag{9}$$

Subtracting this from the similar expression for a' gives, for m odd,

$$T \mid \left(q^{2m} - 1\right)\left(q^{a-a'} - 1\right). \tag{10}$$

From $m = 3$, we get $T \mid (q^6 - 1)(q^2 - 1)$. From $m = 5$, we get $T \mid (q^{10} - 1)(q^4 - 1)$. $1 + q^2 + q^4$ is coprime to $q^2 + 1$ and $1 + q^2 + q^4 + q^6 + q^8$, so we get $T \mid (q^2 - 1)^2$. If $m = a(b - 1)$ is even, we use the same process, first getting

$$T \mid \left(q^m - 1\right)\left((-1)^{a-1}2g + q^{m+a} + q^a\right). \tag{11}$$

If a, a' are divisors of m, we get

$$T \mid \left(q^{2m} - 1\right)\left(q^{a-a'} - (-1)^{a-a'}\right).$$

From $m = 2$, $T \mid (q^4 - 1)(q + 1)$, and the GCD of $q^2 + 1$ and $q - 1$ is at most two, so we have that T is a factor of $2(q^2 - 1)(q + 1)$. The relation on $|G|$ then follows from Proposition 3.12.

In the minimal case, (10) holds for all m. Taking the GCD for $m = 2, 3$ gives the result. □

Proposition 3.14. *Suppose X is a $\mathbb{F}_{q^2}$-maximal curve of genus at least two, and suppose the automorphism group G of X has only free orbits outside of the $\mathbb{F}_{q^2}$-rational points. Then*

$$|G| \mid 2q^3(q + 1) \cdot \gcd(2g - 2, q + 1) \cdot \gcd(4g, q - 1).$$

For minimal curves, the relation is instead

$$|G| \mid 2q^3(q - 1) \cdot \gcd(2g - 2, q - 1) \cdot \gcd(4g, q + 1).$$

Proof. We start with the maximal case. From (9),

$$\gcd\left((q + 1)^2, |G|\right) \mid \left(q^m + 1\right)\left(-2g + q^{m+a} - q^a\right)$$

for m odd. Choose m coprime to $q + 1$. Then we get

$$\gcd\left((q + 1)^2, |G|\right) \mid (q + 1)\gcd\left(q + 1, -2g + q^{m+a} - q^a\right)$$

or

$$\gcd\left((q + 1)^2, |G|\right) \mid (q + 1)\gcd\left(q + 1, 2g - 2\right).$$

Next, we have

$$\gcd\left(q - 1, |G|\right) \mid \left(q^m + 1\right)\left(-2g + q^{m+a} - q^a\right)$$

for

$$\gcd\left(q - 1, |G|\right) \mid 4g.$$

Together with the previous proposition, these two relations imply the result for maximal curves. For minimal curves, we start instead with

$$|G| \mid \left(q^{m+a} - q^a\right)\left(-2g + q^{m+a} + q^a\right)$$

to derive the other result. □

The next technical lemma is a direct application of Proposition 3.14, and allows us to bound the size of automorphism groups for some curves with relatively small genus.

Lemma 3.15. *Suppose X is a $\mathbb{F}_{p^2}$-maximal curve of genus at least two over a field with characteristic an odd prime, and suppose the automorphism group G of X has only free*

orbits outside of the $\mathbb{F}_{q^2}$-rational points. Suppose the genus of X can be written as $g = \frac{1}{2}c(p-1) + dp$. Then

$$|G| \mid 16q^3(q+1)d(c+d+1).$$

3.4 $\mathbb{F}_{p^2}$-maximal curves with many automorphisms

In this section we prove the following theorem:

Theorem 3.16. *Let X be a $\mathbb{F}_{p^2}$-maximal curve of genus g at least 2, where $p > 7$, and let $|G|$ be the group of automorphisms of X. If $|G| > g^2$ and $|G| > 84(g-1)$, X must be isomorphic to a curve of the form $y^m = x^p - x$, where $m > 1$ and m divides $p+1$.*

As a first step, we determine the structure of a Sylow subgroup of G.

Proposition 3.17. *Let X be a $\mathbb{F}_{p^2}$-maximal curve of positive genus, and suppose G has order divisible by p. Then we can write*

$$g = \frac{1}{2}c(p-1) + dp.$$

Furthermore, unless X is isomorphic to the Hermitian curve, we must have that p^2 does not divide $|G|$.

Proof. Let H be a Sylow p-subgroup of G, and let H' be a subgroup of H of size p. Per Proposition 3.12, H' stabilizes a single point P. Then

$$\frac{2g-2}{p} = 2d - 2 + \frac{(c+2)(p-1)}{p},$$

where $i = c+1$ is the final index so $G_i(P)$ has order p and d is the genus of X/H'. This gives g in the form $\frac{1}{2}c(p-1) + dp$.

Next, we recall that the Hermitian curve is the only $\mathbb{F}_{p^2}$-maximal curve attaining the maximal genus $\frac{1}{2}p(p-1)$. Then, unless the curve X is Hermitian, $p^2 + 2gp < p^3$. Then, if H is not of order p, it is of order p^2. But then we can write

$$\frac{2g-2}{p^2} = 2f - 2 + \frac{1}{p^2}\left((c+2)(p^2-1) + bp(p-1)\right)$$

for some nonnegative integers f, b, c. We are here using the fact that, for $a_1, a_2 \geq 1$, if $G_{a_1+1}(P)$ is distinct from $G_{a_1}(P)$ and $G_{a_2+1}(P)$ is distinct from $G_{a_2}(P)$, then $a_1 - a_2 \equiv 0 \pmod{p}$, see ([10], Lemma 11.75(v)). Simplifying gives

$$2g = 2fp^2 + c(p^2-1) + bp(p-1).$$

But $2g < p(p-1)$ for X not the Hermitian curve, so we get $f = c = b = g = 0$ unless the curve is Hermitian. □

We will use the notation $g = \frac{1}{2}c(p-1) + dp$ throughout this section. In this notation, d is the genus of the quotient curve from dividing by an order p subgroup.

As is traditional when studying large automorphism groups (see [9] or [19]), we use the following lemma to split into cases. For this lemma, a *wild* short orbit is an orbit where each point has nontrivial stabilizer of order dividing p, and a *tame* short orbit is an

orbit where each point has nontrivial stabilizer of order not dividing p. For a proof of the lemma, see [10], Theorem 11.56.

Lemma 3.18. *Let G be the automorphism group of a genus $g \geq 2$ curve X defined over an algebraically closed field of characteristic p. If $|G| > 84(g-1)$, then X/G is rational and one of the following four cases applies.*

(I) *$p \neq 2$ and G has precisely three short orbits in X, one wild and two tame, with each point in the tame orbits having an order-two stabilizer.*
(II) *G has precisely two short orbits, both wild.*
(III) *G has one wild short orbit and no other short orbits.*
(IV) *G has one wild short orbit, one tame short orbit, and no other short orbits.*

The first two cases are easily dealt with.

Lemma 3.19. *There is no $\mathbb{F}_{p^2}$-maximal curve X of Type I of Lemma 3.18.*

Proof. The Hermitian curve is of Type IV, so by Proposition 3.17 we can assume that a maximal p-subgroup of X is of order p. Recall the notation $g = \frac{1}{2}c(p-1) + dp$. The size of the wild orbit is in the form $1 + np$ for some integer n by Proposition 3.12. Letting s denote the size of the stabilizer for the wild orbit, the Riemann-Hurwitz formula gives

$$\frac{2g-2}{(1+np)s} = \frac{(c+1)(p-1)-1}{s} = \frac{(c+1)(p-1)-1}{s}.$$

Then

$$(1+np)(cp+p-c-2) = 2g-2.$$

If $n > 0$, the only case where genus is at most $\frac{1}{2}p(p-1)$ is $n = 1, c = 0$, and no case has genus strictly less than this. Since the Hermitian curve is not of this type, we have $n = 0$ and get

$$p = 2dp,$$

which cannot happen. □

For Type II, we in fact have a result for $\mathbb{F}_{q^2}$-maximal curves instead of just $\mathbb{F}_{p^2}$-maximal curves.

Proposition 3.20. *There is no $\mathbb{F}_{q^2}$-maximal curve X of Type II of Lemma 3.18.*

Proof. From Proposition 3.12, we see each wild orbit is of size congruent to one modulo p. One wild orbit must be a subset of the $\mathbb{F}_{q^2}$-rational points, since the number of such points is congruent to one modulo p. The number of remaining $\mathbb{F}_{q^2}$-rational points is then divisible by p, so the other wild orbit cannot lie among the $\mathbb{F}_{q^2}$-rational points. The other wild orbit must then lie in the set of $\mathbb{F}_{q^{2n}}$-rational points that are not $\mathbb{F}_{q^2}$-rational. However, these sets of points also have order divisible by p, so this is again impossible. □

The following lemma allows our divisibility-based methods to become precise at the end.

Lemma 3.21. *Let X be a $\mathbb{F}_{p^2}$-maximal curve of genus at least two. If X/H is rational for some subgroup $H \subset G$ of order p, then X is isomorphic to $y^m = x^p - x$ for some m dividing $p+1$.*

Proof. The main theorem of [12] states that any Artin-Schreier curve with zero Hasse-Witt map must be of the form $y^m = x^p - x$ with m dividing $p+1$. Since $\mathbb{F}_{p^2}$-maximal curves are superspecial, they by definition have zero Hasse-Witt map. Since X/H is rational, X is an Artin-Schreier curve, and the theorem applies. □

At this point in the proof of Theorem 3.16, we can assume that there at most one short tame orbit and a unique wild orbit in the action of G on X. There are three cases to consider. First, for relatively low genus curves, it is possible there is a free orbit among the $\mathbb{F}_{p^2}$ points. Otherwise, the $\mathbb{F}_{p^2}$-rational points either consist of just one wild orbit, a case dealt with in Lemma 3.23, or are the union of a tame orbit with a wild orbit, a case dealt with in Lemma 3.24.

Lemma 3.22. *Suppose X is a $\mathbb{F}_{p^2}$-maximal curve of genus $g \geq 2$ and $p > 7$. Suppose $X \to X/G$ is wildly ramified and that there is a free orbit among the $\mathbb{F}_{p^2}$-rational points. Then $|G| \leq g^2$ or $|G| \leq 84(g-1)$.*

Proof. Write $g = dp + \frac{1}{2}c(p-1)$ and write $np+1$ for the length of the wild orbit.

First, we deal with the case that $d > 0$ and $n > 1$. In this case, there must be a free orbit of size at most $(2d+c+1)p^2 - (c+n)p$, which is less than g^2 for $d > 2$, $d = 2$ and $c > 0$, or $d = 1$ and $c > 2$. We also have a lower bound of $p(np+1)$ on the size of the group. Then, if $|G| > g^2$, we must have

$$5p^2 - np \geq np^2 + p,$$

so $n < 5$.

If the tame orbit is outside the $\mathbb{F}_{p^2}$-rational points, we must have the wild orbit size dividing the number of other points in $\mathbb{F}_{p^2}$. Then $np+1$ divides $(2d+c+1)p - (c+n)$, so

$$np+1 \mid (n(n+c) + 2d + c + 1).$$

For $2 \leq n \leq 4$, $d > 0$, and $2d + c \leq 4$, it is a quick computation to verify this only has solutions for $p = 2, 3, 5, 7$.

Now, if the tame orbit is among the $\mathbb{F}_{p^2}$-rational points, we use Lemma 3.15 to say

$$np+1 \mid 16(p+1)d(c+d+1)$$

which, from $p(n-1) = (np+1) - (p+1)$ gives

$$np+1 \mid 16(n-1)d(c+d+1).$$

For $2d+c \leq 4$, we then have $np+1 \mid 96(n-1)$ or $np+1 \mid 64(n-1)$. Checking for p with $n = 2, 3, 4$ is another easy computation. The only p that can satisfy these congruences for n in this range are $p = 2, 5$, and the case is done.

Now suppose that $n = 1$ with $d > 0$. In this case, the stabilizer of each point of the wild orbit is necessarily transitive on the other points, so that G acts double transitively on the wild orbit. Take $\bar{G}$ to be the permutation group G induces on these $p+1$ points. By element counting, no $\alpha \in \bar{G}$ that fixes two points of the orbit can have order more

than $p-1$. But subgroups of the stabilizer of a point of size not dividing p are necessarily cyclic, so the stabilizer of any pair of points is cyclic.

Then, by [13], and since the 2-transitive action is on a set of size $p+1$ and not p^k+1 for some larger k, we know that $\bar{G}$ is either isomorphic to $\mathrm{PSL}(2,p)$, $\mathrm{PGL}(2,p)$, or has a regular normal subgroup. But $\mathrm{PSL}(2,p)$ is of size $\frac{1}{2}(p^3-p)$ and $\mathrm{PGL}(2,p)$ is still larger, while $g < \frac{5}{2}p$ being necessary for $|G| > g^2$ implies the number of $\mathbb{F}_{p^2}$ points outside this orbit is at most $6p^2-2p$, so $p-1 < 12$. Then exceptions can only exist for $p \leq 11$. We can deal with the case $p = 11$ by noting $\mathrm{PGL}(2,11)$ is too large, and $\mathrm{PSL}(2,11)$ has size equal to $p^2+2gp-p$ only when g is exactly $\frac{1}{2}5(p-1)$, outside the case $d \neq 0$.

If $\bar{G}$ instead has some regular normal subgroup, or a subgroup acting freely and transitively on the $p+1$ points, we know that the regular normal subgroup must be a elementary p-group. Excepting $p = 2$ to $p+1 = 3$, we then get that p must be a Mersenne prime, of the form 2^k-1 for some k.

Taking an alternative tack, we can also write

$$\frac{2g-2}{rp(p+1)} = \frac{-k}{t} + \frac{(c+1)(p-1)-1}{rp}$$

in this case for some positive integers r, t and with k either 0 or 1. Then

$$\frac{k|G|}{t} = p(c+1)(p-1) - 2dp$$

Then, for $d \leq 2$, $k \neq 0$ for $p > 5$. But this tame orbit size must divide the number of $\mathbb{F}_{p^2}$-rational points that are not among the $p+1$, so

$$((c+1)(p-1)-2d) \mid ((2d+c+1)p-(c+1)).$$

In fact, unless the tame orbit is among the $\mathbb{F}_{p^2}$-rational points, we see that $p+1 \mid (2d+c+1)p-(c+1)$ too, so $p+1 \mid 2d+2c+2$, which is impossible for $2d+c \leq 5$, $d \geq 1$, and $p > 7$ (should $2d+c > 5$ with $d \geq 1$, $|G|$ is forced to be less than g^2). Then the tame orbit is $\mathbb{F}_{p^2}$-rational, so we also have that $(c+1)(p-1)-2d$ divides $2(p^2-1)(p+1)$, so

$$((c+1)(p-1)-2d) \mid 32d(c+d+1)^2,$$

where the relation comes from considering the greatest common denominator of $p-1, p+1$ with the left hand side. This relation doubles as an inequality. If $c+2d > 4$, $d > 0$, and $|G| > g^2$, we have from counting the number of points in the free orbit of $\mathbb{F}_{p^2}$-points that $p^2-14p+9 < 0$ for $p < 17$. Otherwise, for $c+2d \leq 4$, $d > 0$, we get $p \leq 9 \cdot 64 + 3$. The only Mersenne primes of interest are then $p = 3, 7, 31, 127$. Checking $31, 127$ for $(c,d) = (0,1), (1,1), (2,1), (0,2)$, we see that they cannot be examples, so for $p > 7$ we again have no examples.

Now, suppose $d \neq 0$ and the wild orbit is of size 1. In this case we can write

$$\frac{2g-2}{rp} = \frac{-k}{t} + \frac{(c+1)(p-1)-1}{rp}$$

for k either 0 or 1. For $k = 0$, we get $2dp - p = 0$, which is impossible. For $k = 1$, we have

$$\frac{2dp-p}{rp} = \frac{-1}{t},$$

which is impossible for $d > 0$.

This just leaves all cases where $d = 0$. In this case, we know by Lemma 3.21 that any possible curve is isomorphic to one of the form $y^m = x^p - x$ with m dividing $p+1$. But

these do not have the specified type, as the automorphism group for each partitions the set of $\mathbb{F}_{p^2}$-rational points into either one or two short orbits. The lemma is proved. □

Lemma 3.23. *For $p \geq 7$, the only $\mathbb{F}_{p^2}$-maximal curve of genus at least two with all of the $\mathbb{F}_{p^2}$-rational points forming a single wild orbit is the Hermitian curve.*

Proof. We first deal with the case where the maximal p-group has order p. Write $g = dp + \frac{1}{2}c(p-1)$, and write the size of the stabilizer for a point of the wild orbit as rp. Suppose $d \neq 0$. Then $r \leq 4d+2$, as r is the order of a cyclic group in X/H, where H is a p-group, and X/H has genus $d > 0$. Write $p^2 + 2gp + 1 = N$. Assuming that there is at most one other tamely ramified orbit, we can write

$$\frac{2g-2}{rpN} = \frac{-k}{t} + \frac{cp+p-c-2}{rp}.$$

But the magnitude of the right hand side, if nonzero, has a lower bound of

$$\frac{cp+p-c-2}{(rp)(rp+1)},$$

so

$$\frac{1}{rp^2} \geq \frac{2g-2}{2rgp^2} \geq \frac{2g-2}{rpN} \geq \frac{cp+p-c-2}{(rp)(rp+1)},$$

so $rp+1 \geq cp^2+p^2-cp-2p$, and so $(4d+2)p+1 \geq p(cp+p-c-2)$, and finally

$$d \geq \frac{1}{4}\left(cp^2+p^2-cp-4p-1\right).$$

If $c=0$, we get $d \geq \frac{1}{4}(p-4)$. But then the genus is at least $\frac{1}{4}p(p-4)$ and is divisible by p, and no maximal curve fits this bill for $p \geq 7$ by checking against Theorem 10.48 of [10]. If $c > 0$, the only curve in the range is the Hermitian curve.

Then we can assume $d = 0$. This case falls immediately to Lemma 3.21. The Hermitian curve is the only example of a curve of the form $y^m = x^p - x$, where m divides $p+1$, whose automorphism group acts transitively on the $\mathbb{F}_{p^2}$-rational points. □

Lemma 3.24. *Let X be a $\mathbb{F}_{p^2}$-maximal curve of genus at least two. Then G has two short orbits in X, one wild and one tame, that have union equal to the set of $\mathbb{F}_{p^2}$-rational points if and only if X is isomorphic to a curve given by the equation $y^m = x^p - x$, where $m \mid p+1$, $m \neq 1, p+1$.*

Proof. Write $1+np$ for the size of the wild orbit and write $g = dp + \frac{1}{2}c(p-1)$. Then Riemann-Hurwitz gives

$$2g-2 = -(p^2+(2g-n)p) + (1+np)((c+1)(p-1)-1),$$

which reduces to

$$2d(p+1) = (c+1)(n-1)(p-1).$$

But $p-1$ and $p+1$ have greatest common factor at most 2, so $d \geq \frac{1}{4}(p-1)$ unless the right hand side of this expression vanishes. But the only $\mathbb{F}_{p^2}$-maximal curve with genus at least $\frac{1}{4}p(p-1)$ is the Hermitian curve, so the right hand vanishes. Then n must be 1 and d must be zero.

By Lemma 3.21, we have that such a curve is of the form $y^m = x^p - x$ with m dividing $p+1$. Taking away the cases $m = 1$ for being rational and $m = p+1$ for being Hermitian and not of this form, we have one direction of the lemma.

However, the curve $y^m = x^p - x$ with m dividing $p+1$ is covered by the Hermitian curve. It is a twist of a maximal curve. Further, per Theorem 12.11 of [10], if $m \neq p+1$, the curve has two short orbits, one of size $p+1$ and the other of size $(c+1)p(p-1)$. These partition the rational points between them. For genus $g \geq 2$, we only need that $m > 1$. Then we have the converse. □

At this point we have exhausted all possibilities. Theorem 3.16 is true.

3.5 Superspecial curves with irreducible canonical representations

We can now prove Theorem 3.3.

Proof. X is isomorphic either to a $\mathbb{F}_{p^2}$-maximal or $\mathbb{F}_{p^2}$-minimal curve. In the latter case, since the genus of a $\mathbb{F}_{p^2}$-minimal curve is at most $\frac{1}{2}(p-1)$, as a curve cannot have negatively many points, we have that the only possible examples of an exception to $|G| \leq 84(g-1)$ come from curves isomorphic to the Roquette curve from equation $y^2 = x^p - x$. Then X can be assumed to be $\mathbb{F}_{p^2}$-maximal. But then, if $g > 82$ and $|G| > g^2$, then $|G| > 84(g-1)$ too. Further, if $p \leq 7$, then we have $g \leq 3 \cdot 7 = 21$. Then we can apply Theorem 3.16 to say that if X has irreducible canonical representation, has $g > 82$, and is not isomorphic to the Roquette curve from $y^2 = x^p - x$, then it is isomorphic to $y^m = x^p - x$ for some $m \mid p+1$. The following proposition then implies the theorem.

Proposition 3.25. *Let X be the smooth projective model of $y^m = x^p - x$, where $m|p+1$. Then X has an irreducible canonical representation if and only if $m \in \{2, p+1\}$.*

We first recall a basis for $H^0(X, \Omega^1)$. From [24], Lemma 1, we know that such a basis is given by

$$x^i y^j dy \text{ with } 0 \leq i, j \text{ and } im + jp \leq (p-1)(m-1) - 2.$$

where i and j are integers. Alternatively, via $my^{m-1}dy = -dx$, we can write this basis as

$$\frac{x^i dx}{y^j} \text{ with } 0 \leq i \text{ and } j \leq m-1 \text{ and } im + (m-1-j)p \leq (p-1)(m-1) - 2$$

Take $m' = (p+1)/m$. We claim that the subspace generated by $\frac{x^i dx}{y}$ with $0 \leq i \leq m'-2$ is invariant under the automorphism group provided that $m < p+1$. We recall that, by ([10], Thm 12.11), the automorphism group of X is generated by the following two elements:

(1) An mth root of unity ζ_m acting via $(x, y) \to (x, \zeta_m y)$.

(2) An element $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{F}_p)$ acting via

$$(x, y) \to \left(\frac{ax+b}{cx+d}, \frac{y}{(cx+d)^{m'}} \right).$$

We have that ζ_m acts on the basis vectors as a scalar, so it fixes the subspace. Next, σ acts on the basis for the subspace by

$$\sigma\left(\frac{x^i dx}{y}\right) = (ax+b)^i(cx+d)^{m'-2-i}\frac{dx}{y}.$$

This result is a linear combination of terms of the form $\frac{x^i dx}{y}$ with $i \leq m'-2$. Then the generators fix the subspace. This is a proper subspace when $m > 2$. Thus, when $2 < m < p+1$, the canonical representation is not irreducible. When $m \in \{2, p+1\}$, the canonical representation is irreducible as stated in Proposition 3.2. □

4 Automorphisms of Ordinary Curves

In this section, we prove Theorem 1.1, improving upon a bound by Nakajima [19] on the automorphisms of ordinary curves. The proof of the theorem borrows many techniques from the similar theorem in [19], but improves the bound by using asymptotics and some more detailed arguments.

Proof of Theorem 1.1. Let $G = \mathrm{Aut}(X)$ and $Y = X/G$. If $|G| > 84(g-1)$, then Y has genus zero and Lemma 3.18 applies. This splits the proof of the theorem into four cases, each corresponding to a type of curve from this Lemma.

Case I. This case has p an odd prime, with one point $P \in Y$ wildly ramified, two points Q, Q' tamely ramified with ramification index 2, and no other ramified points. Choose $P_1 \in X$ over P. Then we can write $|G^{(0)}_{P'}| = Eq$, with q a power of p and $p \nmid E$. Hurwitz gives

$$2\left(\frac{g-1}{|G|}\right) = -2 + \frac{2}{2} + \frac{Eq+q-2}{Eq} = \frac{q-2}{Eq}.$$

But Eq is the size of a subgroup of G, so we have that

$$2\left(\frac{g-1}{q-2}\right) = \frac{|G|}{Eq}$$

is an integer. Since $q-2$ is odd, we have $(q-2)|(g-1)$. Write $a = \frac{g-1}{q-2}$. Also, E divides $q-1$ by ([19], Proposition 1), so write $q-1 = dE$. Then

$$|G| = 2aEq = \frac{2a}{d}\left(\frac{g-1}{a}+1\right)\left(\frac{g-1}{a}+2\right) = \frac{2(g+a-1)(g+2a-1)}{ad}.$$

But $1 \leq a < g$, so this equation forces $|G| \leq 2(2g-1)(g+1) \leq 5g^2$, finishing this case.

Case II. In this case, there are two wildly ramified points in Y and no other ramified points. Renaming the points if necessary, we write $e_{Q_1} = E_1 q$, $e_{Q_2} = E_2 qq'$ with E_1, E_2 integers not divisible by p. Then Hurwitz gives

$$2\left(\frac{g-1}{|G|}\right) = -2 + \frac{E_1 q + q - 2}{E_1 q} + \frac{E_2 qq' + qq' - 2}{E_2 qq'}.$$

If $qq' = q = 2$, this equation forces X to be an elliptic curve, against our assumption $g_X \geq 2$. We then assume $qq' > 2$.

Define b_1 and b_2 so $b_1 E_1 = q-1$, $b_2 E_2 = qq'-1$. b_1 and b_2 are positive integers by ([19], Proposition 1, Lemma 2). We then rewrite the above equation as

$$\frac{|G|}{qq'} = \frac{2(g-1)(q-1)(qq'-1)}{b_2(q-1)(qq'-2) + b_1(qq'-1)q'(q-2)}.$$

Then

$$\frac{|G|}{qq'} \leq \frac{2(g-1)(qq'-1)}{b_2(qq'-2)},$$

with equality if and only if $q = 2$. If $3 \leq qq' \leq 14$, this gives

$$|G| \leq \frac{14 \cdot 13(g-1)}{6b_2},$$

which is less than g^2 for $g \geq 30$. Assuming $qq' \geq 15$ for the rest of this case, we have

$$|G| \leq \frac{15qq'(g-1)}{7b_2}. \tag{12}$$

We now split into three subcases. First, suppose $q \neq 2$ and $q' \neq 1$. E_2qq' is the size of a subgroup of G, so

$$\frac{b_2|G|}{qq'(qq'-1)} = \frac{2b_2(g-1)(q-1)}{b_2(q-1)(qq'-2) + b_1(qq'-1)q'(q-2)}$$

is an integer. But the greatest common denominator of $q-1$ and the denominator will need to divide $b_1(q'-1)$, so

$$\frac{2b_2b_1(g-1)(q'-1)}{b_2(q-1)(qq'-2) + b_1(qq'-1)q'(q-2)}$$

is also an integer. Then

$$\frac{2b_2(g-1)(q'-1)}{q'(qq'-1)(q-2)} \geq 1,$$

so $\frac{1}{b_2}(qq'-1) \leq 2(g-1)$ for $q > 2$. Then Equation 12 gives

$$|G| \leq \frac{32}{7}(g-1)^2.$$

For the next subcase, take $q = 2$ and $q' \neq 1$. In this case, our equation is

$$\frac{|G|}{2q'} = \frac{(g-1)(2q'-1)}{b_2(q'-1)}.$$

The left is an integer, so we find that $(q'-1)|(g-1)$. Write $a(q'-1) = (g-1)$. We find

$$|G| = 2aq'\frac{2q'-1}{b_2} = \frac{1}{ab_2}2(g+a-1)(2g+a-2),$$

which from $1 \leq a < g$ gives $|G| \leq 6g^2$.

If $q = 2$ and $q' = 1$, we would have $qq' = 2$, which we already dealt with.

Finally, suppose $q' = 1$. We have that

$$\frac{b_2|G|}{q(q-1)} = \frac{2b_2(g-1)}{(b_1+b_2)(q-2)}$$

and

$$\frac{b_1|G|}{q(q-1)} = \frac{2b_1(g-1)}{(b_1+b_2)(q-2)}$$

are integers. Adding these, we see $a(q-2) = 2(g-1)$ for some a. Then

$$|G| = 2(g-1)\frac{q(q-1)}{(b_1+b_2)(q-2)} \leq \frac{15}{14}(g-1)2g \leq 3g^2,$$

where we are using $q = qq' \geq 15$. This finishes Case II.

Case III. [19] shows that this case is impossible for ordinary curves.

Case IV. Let $e_{Q_1} = Eq$ and $e_{Q_2} = e$, where $q = p^n$ and $(E,p) = (e,p) = 1$. This implies that $\frac{d_{Q_1}}{e_{Q_1}} = \frac{Eq+q-2}{Eq}$ and $\frac{d_{Q_2}}{e_{Q_2}} = \frac{e-1}{e}$. Applying the Riemann-Hurwitz formula, we have

$$\frac{2g_X - 2}{|G|} = \frac{(e-E)q - 2e}{Eqe}. \tag{13}$$

By ([19], Lemmas 1,2), it suffices to consider when $E > (\frac{g_X}{21})^{\frac{1}{2}}$, and thus, we take E to be large in the following analysis. Our strategy for the remainder of Case III is to first prove two bounds on $|G|$ in terms of E, q, and g_X in Lemma 4.1. Then, we bound E and q in terms of g_X to finish the proof.

Lemma 4.1. *If $E \geq 444$, we have the following estimates of $|G|$:*

$$|G| \leq 2(1 + 7E^{-1})Eq(g_X - 1) \tag{14}$$

and

$$|G| \leq 2(3 + 37E^{-1})E^2(g_X - 1). \tag{15}$$

Proof. Define $d = (q-1)/E$ and $\varepsilon = e - E$. It is shown in ([19], Proposition 1, Lemma 2) that d, ε are positive integers. We then define the variables

$$\lambda = \frac{dE\varepsilon - 2E - \varepsilon}{E + \varepsilon}$$

and

$$\mu = \frac{dE\varepsilon - 2E - \varepsilon}{(d + E^{-1})(E + \varepsilon)},$$

so that (13) gives us

$$|G| = \frac{2Eq}{\lambda}(g_X - 1) = \frac{2E^2}{\mu}(g_X - 1). \tag{16}$$

First, we bound λ from below. If $\varepsilon \geq 4$, then certainly $\lambda \geq \frac{E\varepsilon}{E+\varepsilon} - 2 > 1$. Otherwise, we have that $\lambda = (d\varepsilon - 2) - (d\varepsilon - 1)\frac{\varepsilon}{E+\varepsilon}$ and $\varepsilon \leq 3$. But $\lambda > 0$ implies that $d\varepsilon - 2$ is a positive integer, and thus

$$\lambda = (d\varepsilon - 2) - (d\varepsilon - 1)\frac{\varepsilon}{E + \varepsilon} \geq 1 - \frac{6}{E}.$$

Next, we claim that $\mu \geq \frac{1}{3} - \frac{4}{E}$. As before, it is easy to see that if $\varepsilon \geq 3$, then we are done. Thus, assume that $\varepsilon < 3$ and we have

$$\mu = \frac{d\varepsilon - 2}{d + E^{-1}} - \frac{\varepsilon(d\varepsilon - 1)}{(d + E^{-1})(E + \varepsilon)} \geq \frac{d\varepsilon - 2}{d} - \frac{4}{E}.$$

Since $\mu > 0$, we have $d\varepsilon > 2$. Hence, this is minimized at $d = 3$, $\varepsilon = 1$, in which case we get our desired bound of

$$\mu \geq \frac{1}{3} - \frac{4}{E}.$$

Finally, we have the bounds

$$\frac{1}{\mu} \leq \left(\frac{1}{3} - \frac{4}{E}\right)^{-1} \leq 3 + \frac{37}{E}$$

$$\frac{1}{\lambda} \leq \left(1 - \frac{6}{E}\right)^{-1} \leq 1 + \frac{7}{E}$$

for all $E \geq 444$, and the result follows. □

Now we bound E^2 and Eq by a multiple of g_X. Let $P_1 \in X$ be such that $\pi_{X/Y}(P_1) = Q_1$. Let $Z = X/G_1(P_1)$ and $W = X/G_0(P_1)$. We have a sequence of maps $X \to Z \to W$ such that $|\mathrm{Gal}(X/Z)| = q$ and W is the quotient of Z by $G_0(P_1)/G_1(P_1)$, which is a cyclic group

of order E by Proposition 2.1. We now have two cases depending on whether or not Z is rational.

Lemma 4.2. *Theorem 1.1 holds in the case* $g_Z \geq 1$.

Proof. Observing that the point P_1 is totally wildly ramified in $\pi_{X/Z}$, we have by the Riemann-Hurwitz formula:

$$2g_X - 2 \geq q(2g_Z - 2) + 2(q-1),$$

which implies that $g_X \geq qg_Z$.

We now bound g_Z from below by a multiple of E so that we may apply Lemma 4.1 to get:

$$|G| \leq 2\left(1 + 7E^{-1}\right) Eq\left(g_X - 1\right) \leq 2\left(1 + 7E^{-1}\right)\left(\frac{E}{g_Z}\right) g_X(g_X - 1). \tag{17}$$

To do so, we examine the quotient map $Z \to W = Z/C_E$ where $C_E \cong G_0(P_1)/G_1(P_1)$ denotes the cyclic group of order E. Hereafter, for any positive integer $a|E$, we identify C_a with the unique order a cyclic subgroup of C_E. Let the lengths of the short orbits of C_E acting on Z (that is, the orbits of size less than E) be $l_1, \cdots, l_{s+1}$. We have that $l_i|E$. We may assume that $l_{s+1} = 1$ corresponding to the image of the point P_1 in Z, which is fixed by all of $G_0(P_1)/G_1(P_1)$. Applying the Riemann-Hurwitz formula to the map $Z \to W$ yields

$$2g_Z - 2 = E(2g_W - 2) + \sum_{i=1}^{s+1}(E - l_i). \tag{18}$$

If $g_W > 0$, then we have $2g_Z - 2 \geq E - l_{s+1} = E - 1$ which implies the result by (17). Thus, we assume $g_W = 0$. Then, we note that $2g_Z - 2 \geq 0$ and $\frac{E}{2} \leq E - l_i \leq E - 1$. By 18, we conclude that $s \geq 2$. If $s \geq 4$, we have that

$$\begin{aligned} 2g_Z - 2 = -2E + (E-1) + \sum_{i=1}^{s}(E - l_i) &\geq -2E + (E-1) + 4\left(\frac{E}{2}\right) \\ &= E - 1 \end{aligned}$$

and we are done as before. Hence, we have two remaining cases, $s = 2$ and $s = 3$.

Subcase 1: $s = 2$. We have that $2g_Z - 2 = E - l_1 - l_2 - 1$. We let $a = \operatorname{lcm}\left(\frac{E}{l_1}, \frac{E}{l_2}\right)$ and let $Z' = Z/C_a$. Then, we observe that by the choice of a, the map $\pi_{Z'/W}$ is a map of degree $\frac{E}{a}$ which is only ramified at $\pi_{X/W}(P_1)$, where it is totally ramified. It follows that by the Riemann-Hurwitz formula on $\pi_{Z'/W}$, we have that $2g_{Z'} - 2 = -\frac{2E}{a} + (\frac{E}{a} - 1) = -\frac{E}{a} - 1$. But $g_{Z'} \geq 0$, so it follows that $a = E$ and therefore, $(l_1, l_2) = 1$. Assume without loss of generality that $l_1 \geq l_2$. It follows from the fact that l_1 and l_2 are relatively prime integers dividing E that $l_1 l_2 \leq E$. Hence, we have that either $l_1 + l_2 \leq \frac{E}{3} + 3$ or $l_1 = \frac{E}{2}$. In the former case, we immediately have that $E \leq 3g_Z + 3$ and thus $\frac{E}{g_Z} \leq 3(1 - \frac{3}{E})^{-1} \leq 3(1 + \frac{4}{E})$. Thus, we have that by (17),

$$\begin{aligned} |G| \leq 6\left(1 + 12E^{-1}\right) g_X\left(g_X - 1\right) &\leq 6\left(1 + 12\sqrt{\frac{21}{g_X}}\right) g_X\left(g_X - 1\right) \\ &\leq 6\left(g_X^2 + 12\sqrt{21}g_X^{\frac{3}{2}}\right), \end{aligned} \tag{19}$$

as desired.

We now assume that E is even and $l_1 = \frac{E}{2}$. It follows that l_2 is either 1 or 2. We claim that Z is not ordinary in both cases. This would contradict the Deuring-Šafarevič formula applied to $\pi_{X/Z}$. Let $Z'' = Z/C_2$ so that the map $\pi_{Z''/W}$ is a degree $\frac{E}{2}$ map with exactly two ramification points, $R_1 = \pi_{X/W}(P_1)$ and another point $R_2 \in W$. By the Riemann-Hurwitz formula applied to $\pi_{Z''/W}$, we have that

$$2g_{Z''} - 2 = \frac{E}{2}(-2) + 2(E-1),$$

which implies that $g_{Z''} = 0$. Therefore, since $\pi_{Z/Z''}$ has degree 2, Z is hyperelliptic. In fact, since $g_{Z''} = g_W = 0$ and $\pi_{Z''/W}$ is a degree $\frac{E}{2}$ map which is totally ramified over 2 points, we may assume up to automorphisms of Z'' and W that $\pi_{Z''/W}$ is the map $z \mapsto z^{\frac{E}{2}}$. Let Z be the hyperelliptic curve given by $y^2 = f(x)$ such that the map $Z \to Z''$ is given by $(x, y) \mapsto x$. Then, $\mathrm{Gal}(Z''/W) \in \mathrm{Aut}(Z'')$ is a cyclic group of order $\frac{E}{2}$ such that any element $\gamma \in \mathrm{Gal}(Z''/W)$ fixes 0 and ∞ and has the property that $(\gamma z)^{\frac{E}{2}} = z^{\frac{E}{2}}$. Hence, γ is multiplication by an $\frac{E}{2}$-th root of unity. In fact, if γ is chosen to be a generator of this cyclic group, then γ is multiplication by a primitive $\frac{E}{2}$-th root of unity. It follows that the map $Z \to Z'$ is branched over 0, possibly ∞ depending on whether l_2 is 1 or 2, and $\frac{E}{2}$ other points which are permuted by $\mathrm{Gal}(Z''/W)$. Hence, these points must be related by multiplication by some $\frac{E}{2}$-th root of unity. Thus, we have that $f(x) = x\left(x^{\frac{E}{2}} - a\right)$ and Z is the hyperelliptic curve given by the equation $y^2 = x\left(x^{\frac{E}{2}} - a\right)$ for some $a \in k$. We show that this curve is not ordinary for sufficiently large E.

This is a standard computation; we simply compute the action of Frobenius on a basis of $H^1(Z, \mathcal{O}_Z)$ and show that the matrix of Frobenius is not invertible. For this hyperelliptic curve, a basis of $H^1(Z, \mathcal{O}_Z)$ is given by $\left\{\frac{y}{x^i}\right\}$ for $i = 1, 2, \cdots, \left\lfloor \frac{E}{4} \right\rfloor$.

If $p = 2$, then Frobenius sends $\frac{y}{x^i}$ to $\frac{x^{\frac{E}{2}} - a}{x^{2i}} = 0$ in $H^1(Z, \mathcal{O}_Z)$, so in fact Z is supersingular and we can ignore this case. Otherwise, assume that $p > 2$ and Frobenius sends

$$\frac{y}{x^i} \mapsto \frac{y^p}{x^{pi}} = \frac{y\left(x\left(x^{\frac{E}{2}} - a\right)\right)^{\frac{p-1}{2}}}{x^{pi}}.$$

Therefore, the (i, j) entry of the matrix of Frobenius with respect to this basis, known as the *Hasse-Witt matrix*, is

$$[pi - j]\left(x\left(x^{\frac{E}{2}} - a\right)\right)^{\frac{p-1}{2}} = \left[pi - j - \frac{p-1}{2}\right]\left(x^{\frac{E}{2}} - a\right)^{\frac{p-1}{2}},$$

where $[n]f(x)$ refers to the x^n coefficient of $f(x)$. Thus the (i, j) entry is nonzero if and only if $\frac{E}{2}$ divides $pi - j - \frac{p-1}{2}$, or in other words, $pi - \frac{p-1}{2} \equiv j \pmod{\frac{E}{2}}$.

Suppose Z is ordinary. Then for each i, row i must have some nonzero entry. Thus, since $1 \le j \le \left\lfloor \frac{E}{4} \right\rfloor$, we have that for each i, the smallest positive integer n such that

$$pi - \frac{p-1}{2} \equiv n \left(\mathrm{mod}\ \frac{E}{2}\right)$$

satisfies $1 \le n \le \left\lfloor \frac{E}{4} \right\rfloor$.

Let $i = \left\lfloor \frac{E}{2p} \right\rfloor$. First assume that $i \neq 0$. Then, $pi - \frac{p-1}{2}$ is between $\frac{E}{2} - p + 1 - \frac{p-1}{2}$ and $\frac{E}{2} - \frac{p-1}{2}$. Since its value modulo $\frac{E}{2}$ must be between 1 and $\left\lfloor \frac{E}{4} \right\rfloor$, we have $\frac{E}{2} - p + 1 - \frac{p-1}{2} \le \frac{E}{4}$, so $E \le 6(p-1)$ and $g_X \le 21E^2 = 756(p-1)^2$. Thus, g_X is bounded by some $c = c(p)$

on the order of p^2 and we have finished this case. Now, note that if $i = 0$, we trivially have the same bounds.

Subcase 2: $s = 3$. We have that $2g_Z - 2 = 2E - l_1 - l_2 - l_3 - 1$. By the same argument as above, we obtain $(l_1, l_2, l_3) = 1$ and thus $l_1 + l_2 + l_3 \leq E + 2$ and we are done by the same bounds as in (19). □

For the remainder of the proof, we assume that $g_Z = 0$, which implies that $g_W = 0$. Applying the Riemann-Hurwitz formula to the cyclic cover $\pi_{Z/W}$ immediately yields that there must be exactly two ramification points, and they both must be totally ramified. Let them be $R_1, R_2 \in W$ such that $\pi_{X/W}(P_1) = R_1$. We have the following lemma:

Lemma 4.3. *If there exists $R_3 \in W$, $R_3 \neq R_1, R_2$, which is ramified under $\pi_{X/W}$, then Theorem 1.1 holds.*

Proof. In $\pi_{X/W}$, R_1 is totally ramified by definition, so $d_{R_3} = Eq + q - 2$ and $e_{R_3} = Eq$. Since R_2 is totally ramified in $\pi_{Z/W}$, we have that $e_{R_2} \geq E$ and thus $\frac{d_{R_2}}{e_{R_2}} \geq \frac{e_{R_2}-1}{e_{R_2}} \geq 1 - \frac{1}{E}$. Finally, since R_3 is unramified in $\pi_{Z/W}$, e_{R_3} divides $q = \deg \pi_{X/Z}$. Hence, $d_{R_3} = 2e_{R_3} - 2$ so we have that $\frac{d_{R_3}}{e_{R_3}} = 2 - \frac{2}{e_{R_3}} \geq 2 - \frac{2}{p}$. Finally, we apply the Riemann-Hurwitz formula to $\pi_{X/Z}$ which yields:

$$\frac{2g_X - 2}{Eq} \geq -2 + \frac{d_{R_1}}{e_{R_1}} + \frac{d_{R_2}}{e_{R_2}} + \frac{d_{R_3}}{e_{R_3}} \geq 2 - \frac{2}{Eq} - \frac{2}{p}.$$

Rearranging and using (14), we have

$$|G| \leq 2Eq\left(1 + 7E^{-1}\right)\left(g_X - 1\right) \leq 2\left(\frac{1 + 7E^{-1}}{1 - \frac{1}{Eq} - \frac{1}{p}}\right)\left(g_X - 1\right)^2.$$

The conclusion follows by letting E grow large and using $p \geq 2$. □

Now suppose that R_1 and R_2 are the only ramification points of $\pi_{X/W}$ in W. In this final case, we will show a stronger result; that is, that $|G| \leq g_X^2$ for g_X sufficiently large, except possibly for one particular family of cases. As before, assume $E \geq 1$. Also assume $|G| > g_X^2$, and as usual we can and will also assume that $21E^2 > g_X$.

Lemma 4.4. *In this case, $d \geq E - 2$.*

Proof. Again letting $H = G_1(P_1)$, we have that since $G_2(P_1) = \{1\}$ by Proposition 2.1 (3), $H = G_1(P_1)/G_2(P_1)$, which is an elementary abelian p-group of order q. Choose some P_2 mapping to R_2. Let $N = H_0(P_2) = H_1(P_2)$. As in [19], we let $q' = |N|$ and $q'' = |H/N|$. Then $q'q'' = q$.

By the argument in Lemma 5 of [19], E divides both $q' - 1$ and $q'' - 1$, and $q' \neq 1$. Therefore, either

$$q'' = 1$$

or

$$E^2 \leq (q' - 1)(q'' - 1) < q'q'' = q.$$

In the former case, ([19], p. 606) shows that $E \leq \sqrt{q}+1$. This implies that $E^2-2E \leq q-1$, and so $d = \frac{q-1}{E} \geq E-2$, so Lemma 4.4 holds. In the latter case, $E^2 \leq q-1$, which implies that $d = \frac{q-1}{E} \geq E$. Thus Lemma 4.4 holds here as well. □

Lemma 4.5. *If* $\epsilon \geq 3$, *then* $g_X \leq 364$.

Proof. By definition,

$$\mu = \frac{dE\epsilon - 2E - \epsilon}{(d+E^{-1})(E+\epsilon)} = \frac{E\epsilon}{E+\epsilon}\frac{d}{d+E^{-1}} - \frac{2E+\epsilon}{(d+E^{-1})(E+\epsilon)},$$

which is an increasing function in d. Therefore, we can substitute $d \geq E-2$ to obtain

$$\mu \geq \frac{(E-2)E\epsilon - 2E - \epsilon}{(E-2+E^{-1})(E+\epsilon)}.$$

Using $2E \leq 2E\epsilon$ in the numerator and $E^{-1} \leq 1$ in the denominator, we have that

$$\mu \geq \frac{(E-4)E\epsilon - \epsilon}{(E-1)(E+\epsilon)} = \frac{\epsilon(E^2-4E-1)}{(E-1)(E+\epsilon)}.$$

This last expression is increasing in ϵ, so if $\epsilon \geq 3$,

$$\mu \geq \frac{3\left(E^2-4E-1\right)}{E^2+2E-3}.$$

Substituting into the expression $|G| = \frac{2E^2}{\mu}(g_X-1)$,

$$|G| \leq \frac{2E^2\left(E^2+2E-3\right)}{3\left(E^2-4E-1\right)}\left(g_X-1\right).$$

(Here we assume that this expression is positive, i.e. $E \geq 5$.)
Now, since $|G| > g_X^2$, this means

$$\frac{2E^2\left(E^2+2E-3\right)}{3\left(E^2-4E-1\right)} \geq \frac{|G|}{g_X-1} \geq \frac{g_X^2}{g_X-1} > g_X+1.$$

However, [19] also shows that if $q'' \neq 1$, then $E^2 < g_X$, and if $q'' = 1$, then $E \leq \sqrt{g_X+1}+1$. Either way, $g_X+1 \geq (E-1)^2$. Therefore,

$$\frac{2E^2\left(E^2+2E-3\right)}{3\left(E^2-4E-1\right)} > (E-1)^2.$$

Therefore, $E \leq 20$.
Since $g_X+1 < \frac{2E^2(E^2+2E-3)}{3(E^2-4E-1)}$ for $E \geq 5$, this means that if $5 \leq E \leq 20$, $g_X+1 < 366$. Thus if $E \geq 5$, $g_X \leq 364$, so the lemma holds. If $E \leq 4$, we have the bound $E \geq \sqrt{\frac{g}{21}}$, so in this case, $g \leq 21 \cdot 4^2 = 336$, so the lemma also holds here. □

We now consider the case $\epsilon \leq 2$. Recall that $\epsilon = e - E$. We rearrange the expression

$$\frac{2g_X-2}{|G|} = \frac{(e-E)q-2e}{Eqe}$$

into

$$\frac{|G|}{Eqe} = \frac{2g_X-2}{(e-E)q-2e} = \frac{2g_X-2}{dE\epsilon-2E-\epsilon}.$$

Now, note that since both Eq and e are the size of the stabilizer of a point in X under G, $|G|$ is divisible by both Eq and e. Now, $\gcd(q,e) = 1$, as $p \nmid e$, and $\gcd(E,e)$ divides $e - E = \epsilon$. Therefore, Eqe divides $\epsilon|G|$, and so

$$\frac{\epsilon(2g_X - 2)}{dE\epsilon - 2E - \epsilon}$$

is a positive integer.

We first consider the case $q'' = 1$. Then [19] shows that $g_X = q - 1 = dE$. Therefore,

$$\frac{2dE\epsilon - 2\epsilon}{dE\epsilon - 2E - \epsilon}$$

is an integer. Subtracting 2,

$$\frac{4E}{dE\epsilon - 2E - \epsilon}$$

is an integer. But $dE\epsilon - 2E - \epsilon \geq dE - 2E - 1 \geq E^2 - 4E - 1 > 4E$ for $E \geq 9$. Therefore, $E \leq 9$. Thus $g_X < 21E^2 = 1701$.

Now, suppose $q'' \neq 1$. We have that E divides both $q' - 1$ and $q'' - 1$. Let $q' = p^{a'}$ and $q'' = p^{a''}$. Then E divides $\gcd(q'-1, q''-1) = p^{\gcd(a',a'')} - 1$. Therefore, $E \leq p^{\gcd(a',a'')} - 1$. Suppose $a' \neq a''$. Then $E^3 < (p^{\gcd(a',a'')} - 1)(p^{2\gcd(a',a'')} - 1) \leq (q'-1)(q''-1)$, since one of a' or a'' must be at least $2\gcd(a',a'')$. By the argument in Lemma 5 of [19], we have that $g_X \geq (q'-1)(q''-1)$. Therefore, $g_X \geq E^3$. But $21E^2 > g_X$, so $E \leq 20$, implying that $g_X < 21 \cdot 20^2 = 8400$. Therefore, if $g_X \geq 8400$, then $q' = q'' = \sqrt{q}$.

In this case, $\sqrt{q} = p^n$ for some positive integer n, and $q' = q'' = p^n$. Then the argument in Lemma 5 of [19] (applying the Hurwitz formula to the map $X \to Z$) shows that $g_X = p^{2n} - p^n$. Therefore,

$$\frac{\epsilon\left(2g_X - 2\right)}{(\epsilon q - 2e)} = \frac{2\epsilon\left(p^{2n} - p^n - 1\right)}{\epsilon p^{2n} - 2e}$$

is an integer, so subtracting 2,

$$\frac{2(2e - \epsilon p^n - \epsilon)}{\epsilon p^{2n} - 2e}$$

is an integer. Now, since E divides $q' - 1 = p^n - 1$, $E \leq p^n - 1$ and thus $e = E + \epsilon \leq p^n + 1$, as $\epsilon \leq 2$. Therefore,

$$|2(2e - \epsilon p^n - \epsilon)| \leq \max\left(4e, 2\epsilon p^n + 2\epsilon\right) \leq 4p^n + 4.$$

Therefore, if $2e - \epsilon p^n - \epsilon \neq 0$,

$$4p^n + 4 \geq \epsilon p^{2n} - 2e \geq p^{2n} - 2p^n - 2.$$

Therefore, $p^n < 7$, so $p^n \leq 5$. Thus $E \leq p^n - 1 = 4$, so $g_X \leq 21 \cdot 4^2 = 336 < 8400$.

Therefore, if $g_X \geq 8400$, then $2e - \epsilon p^n - \epsilon = 0$. This implies that $e = \frac{\epsilon}{2}(p^n + 1)$, and thus $E = e - \epsilon = \frac{\epsilon}{2}(p^n - 1)$. This also means that the integer

$$\frac{\epsilon|G|}{Eqe} = \frac{\epsilon(2g_X - 2)}{(\epsilon q - 2e)}$$

must in fact be equal to 2. Thus if $\epsilon = 1$, then $|G| = 2Eqe = 2\frac{p^n - 1}{2} \cdot p^{2n} \cdot \frac{p^n + 1}{2} = \frac{p^{4n} - p^{2n}}{2}$. But if $|G| > g_X^2 = (p^{2n} - p^n)^2$, we have that

$$p^{4n} - p^{2n} > 2\left(p^{2n} - p^n\right)^2,$$

so $p^n = 2$. But then $E = 1$, a contradiction. Therefore, $\epsilon = 2$. Thus $E = p^n - 1$, and $e = p^n + 1$. Since $\frac{2|G|}{Eqe} = 2$, $|G| = Eqe = p^{4n} - p^{2n}$.

Therefore, if $g_X \geq 8400$ and $|G| > g_X^2$, then $E = p^n - 1$, $e = p^n + 1$, $q = p^{2n}$, $g_X = p^{2n} - p^n$, and $|G| = p^{4n} - p^{2n}$ for some positive integer n. Theorem 1.1 trivially follows from this stronger result in this case. □

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
BG, AS, and AY contributed equally to the thought and execution of sections 1, 2, and 4. AS was the primary force behind the new ideas in section 3. All authors read and approved the final manuscript.

Acknowledgments
This research was supported by an REU at Emory University under the mentorship of David Zureick-Brown. We would also like to thank Ken Ono, Rachel Pries, and David Yang for advice and helpful comments.

Author details
[1]Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA. [2]Department of Mathematics, Princeton University, Fine Hall, Washington Road, Princeton, NJ 08544, USA. [3]Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02138, USA.

Received: 26 September 2014 Accepted: 19 November 2014
Published online: 29 May 2015

References

1. Breuer, T: Characters and Automorphism Groups of Compact Riemann Surfaces, vol. 280. Cambridge University Press (2000)
2. Dummigan, N: The determinants of certain Mordell-Weil lattices. Am. J. Math, 1409–1429 (1995)
3. Ekedahl, T: On supersingular curves and abelian varieties. Math. Scand. **60**, 151–178 (1987)
4. Fuhrmann, R, Garcia, A, Torres, F: On maximal curves. J. Number Theory. **67**(1), 29–51 (1997)
5. Giulietti, M, Korchmaros, G: Automorphism groups of algebraic curves with p-rank zero. J. Lond. Math. Soc. **81**(2), 227–296 (2010)
6. Guralnick, R, Malmskog, B, Pries, R: The automorphism groups of a family of maximal curves. J. Algebra. **361**, 92–106 (2012)
7. Guralnick, R, Zieve, M: Automorphism groups of curves with ordinary Jacobians. In preparation
8. Hartshorne, R: Algebraic Geometry Springer (1977)
9. Henn, H-W: Funktionenkörper mit großer Automorphismengruppe. Journal für die reine und angewandte Mathematik. **302**, 96–115 (1978)
10. Hirschfeld, JWP, Korchmáros, G, Torres, F: Algebraic Curves Over a Finite Field. Princeton University Press (2013)
11. Hortsch, R: On the canonical representation of curves in positive characteristic. New. York. J. Math. **18**, 911–924 (2012)
12. Irokawa, S, Sasaki, R: A remark on Artin-Schreier curves whose Hasse-Witt maps are the zero maps. Tsukuba J. Math. **15**(1), 185–192 (1991)
13. Kantor, WM, O'Nan, ME, Seitz, GM: 2-transitive groups in which the stabilizer of two points is cyclic. J. Algebra. **21**(1), 17–50 (1972)
14. Katz, K, Katz, M, Schein, M, Vishne, U: Bolza quaternion order and asymptotics of systoles along congruence subgroups. arXiv preprint arXiv: 1405.5454 (2014)
15. Kazemifard, A, Naghipour, AR, Tafazolian, S: A note on superspecial and maximal curves. Bull. Iran. Math. Soc. **39**(3) (2013)
16. Lehr, C, Matignon, M: Automorphism groups for p-cyclic covers of the affine line. Compositio Math. **141**(5), 1213—1237 (2005)
17. Matignon, M, Rocher, M: Smooth curves having a large automorphism p-group in characteristic $p > 0$. Algebra Number Theory. **2**(8), 887–926 (2008)
18. Nakajima, S: Equivariant form of the Deuring-Šafarevič formula for Hasse-Witt invariants. Mathematische Zeitschrift. **190**(4), 559–566 (1985)
19. p-ranks and automorphism groups of algebraic curves. Trans. Am. Math. Soc. **303**(2), 595–607 (1987)
20. Oort, F: Which abelian surfaces are products of elliptic curves Mathematische Annalen. **214**, 35–47 (1975)
21. Roquette, P. Abschä Mathematische Zeitschrift. **117**, 157–163 (1970)
22. Stichtenoth, H: Über die automorphismengruppe eines algebraischen funktionenkörpers von primzahlcharakteristik. I. eine abschätzung der ordnung der automorphismengruppe. Archiv Der Mathematik. **24**, 527–544 (1973)
23. Subrao, D: The p-rank of Artin-Schreier curves. Manuscripta Mathematica. **16**(2), 169–193 (1975)
24. Sullivan FJ: p-torsion in the class group of curves with too many automorphisms. Archiv der Mathematik. **26**(1), 253–261 (1975)
25. Viana, PH, Rodriguez, JEA: Eventually minimal curves. Bull. Braz. Math. Soc. **36**(1), 39–58 (2005)