Progress in Galois Theory, pp. 25-37
H. Voelklein and T. Shaska, Editors

AUTOMORPHISMS OF THE MODULAR CURVE

Automorphisms of the modular curve $X(p)$ in positive characteristic

For John Thompson on the occasion of his seventieth birthday

Peter Bending
GCHQ, Priors Road, Cheltenham, Glos, GL52 5AJ, UK.
peter@sc98e.demon.co.uk

Alan Camina
School of Mathematics, University of East Anglia, Norwich, England, NR4 7TJ, UK.
A.Camina@uea.ac.uk

Robert Guralnick*
Department of Mathematics, University of Southern California, Los Angeles, CA, 90089.
guralnic@usc.edu

Keywords: modular curve, automorphism groups of curves

Abstract Let $p > 5$ be a prime. Let X be the reduction of the modular curve $X(p)$ in characteristic ℓ (with $\ell \neq p$). Aside from two known cases in characteristic $\ell = 3$ (with $p = 7, 11$), we show that the full automorphism group of X is $PSL(2, p)$.

1. Introduction

Let ℓ and p be distinct primes. Let $X = X_\ell(p)$ be the reduction of the modular curve $X(p)$ in characteristic ℓ. We know that $PSL(2, p)$ acts on $X(p)$.

Our main result is:

*The third author gratefully acknowledges the support of the NSF grant DMS-0140578.

Theorem 1.1. *Assume that* $p \geq 7$.

1 $Aut(X) = PSL(2,p)$ *unless* $p = 7$ *or* 11 *and* $\ell = 3$.

2 $Aut(X_3(7)) \cong PGU(3,3)$.

3 $Aut(X_3(11)) \cong M_{11}$.

In [Adl] it was shown that M_{11} is contained in $Aut(X_3(11))$. Then Rajan [Raj] showed that M_{11} is the full automorphism group.

If $p = 7$ and $\ell = 3$, then X is the Klein quartic. It is well known that X is isomorphic to the Hermitian curve and so has automorphism group as stated. See [Elk] for more details in this case.

If $p < 7$, then X has genus zero and so there is nothing to be done.

This problem was considered by Ritzenthaler [Rit] who proved the result under the additional assumptions that $p \leq 13$ or that X is ordinary (which is not always the case) and $\ell > 3$. He also obtained more information in the cases he did not settle. Goldstein and Guralnick [GG] have investigated the analagous question for the reduction of $X(n)$ with $n > 6$ composite (in any characteristic not dividing n). The result is the same -- the automorphism groups are as expected.

The note is organized as follows. In Section 2, we recall some general facts about curves and in particular some results of Stichtenoth [St1] that we will use.

In Section 3, we gather some well known facts about X and prove some preliminary results about $Aut(X)$.

In Section 4, we prove the theorem. The main ideas in the proof are to show that if $PSL(2,p)$ is not the full automorphism group, there must be a simple group containing it as a maximal subgroup. Moreover p^2 does not divide the order of this group. We also have constraints on the size and structure of this simple group. At this point, we invoke the classification of finite simple groups and show that no simple group (except in the exceptional cases) satisfies the constraints. One can prove a weaker result without the classification – for example one can show that large primes cannot divide the order of the full automorphism group, but we do not see how to prove the full result without the classification. The fact that M_{11} does come up shows that one does need to know facts about simple groups.

In fact, Ritzenhaler [Rit] did use the classification as well (but in that case, one can likely avoid its use).

We note that the only properties of the modular curve we use are that it admits an action of $PSL(2,p)$ with specified ramification data.

We refer the reader to [Ser] and [St2] for general results on coverings of curves, inertia groups and the Riemann-Hurwitz formula. See [Gor] for group theoretic notation and results.

2. Automorphism Groups of Curves

We first recall some general facts about coverings of curves. See [Ser] or [St2] for more details.

Let C be a curve of genus g over an algebraically closed field of characteristic $\ell > 0$ and G a finite group of automorphisms of C. Then G has only finitely many nonregular orbits on C (i.e. orbits in which there is a nontrivial point stabilizer). Let B be a set of points of C containing one point for each nonregular G-orbit. If $b \in B$, let $I := I_b$ the inertia group (or stabilizer of b). Then the Sylow ℓ subgroup I_1 of I is normal in I and I/I_1 is cyclic. Moreover, we have a sequence of higher ramification groups $I = I_0 \geq I_1 \geq \ldots \geq I_r > I_{r+1} = 1$ with I_i/I_{i+1} an elementary abelian ℓ-group. Set

$$\rho(b) = \sum_{i=0}^{r} (|I_i|/|I| - 1/|I|).$$

Let the quotient curve C/G have genus h. Then the Riemann-Hurwitz formula is:

$$2(g-1)/|G| = 2(h-1) + \sum_{b \in B} \rho(b).$$

We next recall some bounds on automorphism groups. For the first, see [St1]. The second follows easily from the Riemann-Hurwitz formula.

Theorem 2.1. (Stichtenoth) Let C be a curve of genus $g > 1$ over an algebraically closed field of characteristic l. Let $A = Aut(C)$.

1 $|A| < 16g^4$ unless C is the Hermitian curve

$$y^{l^n} + y = x^{l^n+1} \; (n \geq 1, l^n \geq 3)$$

of genus $g = \frac{1}{2} l^n (l^n - 1)$, where n is a positive integer. In this case, $|A| < 75g^4$.

2 If C/A has positive genus or the cover $C \longrightarrow C/A$ has at least 3 branch points, 2 of the inertia groups having order larger than 2, then $|A| \leq 84(g-1)$.

Theorem 2.2. *Let C be a curve of genus $g > 1$ over an algebraically closed field of characteristic l. Let $A = Aut(C)$. Let s be a prime different from l. Let S be a subgroup of A of order s^m.*

1 If $C \longrightarrow C/S$ is unramified, then $s^m | (g-1)$.

2 If s is odd and S has exponent s^e, then $s^{m-e} | (g-1)$.

3 If $s = 2$ and S has exponent 2^e, then $s^{m-e} | 2(g-1)$.

3. The Modular Curve

Fix distinct primes ℓ, p with $p \geq 7$. Let $X = X_\ell(p)$. Then $G = PSL(2,p)$ acts on X. The following is well known (see for example [Mor]):

Lemma 3.1. *Set $Y = X/G$. Then Y has genus zero and*

1 *if $\ell > 3$, then $X \to Y$ is branched at 3 points with inertia groups of order 2,3 and p;*

2 *if $\ell = 3$, then $X \to Y$ is branched at 2 points with inertia groups S_3 and $\mathbb{Z}/p$ – moreover, in the first case the second ramification group is trivial;*

3 *if $\ell = 2$, then $X \to Y$ is branched at 2 points with inertia groups A_4 and $\mathbb{Z}/p$ – moreover, in the first case the second ramification group is trivial.*

In the two cases when G is not the full automorphism group A one can also describe the inertia and higher ramification groups. In each case $X_3(p)$ with $p = 7, 11$, there is a branch point with inertia group of order p and another branch point with inertia group $E.(\mathbb{Z}/8)$ where E is extraspecial of order 27 and exponent 3 when $p = 7$ and E is elementary abelian of order 9 when $p = 11$. Moreover, $X_3(11)$ is ordinary and the second higher ramification is trivial.

$X_3(7)$ is not ordinary. If I is the wild inertia group, then the sequence of higher ramification groups is $I, E, Z, Z, Z, 1$, where Z is the center of E (of order 3). Moreover, the Jacobian of X has no 3-torsion.

The next result is an immediate consequence of the first result and the Riemann-Hurwitz formula.

Corollary 3.2. *X has genus $g = (p+2)(p-3)(p-5)/24$. Moreover, $g - 1 = (p-1)(p+1)(p-6)/24$.*

Let A be the full automorphism group of X. Let P be a Sylow p-subgroup of G and $N = N_G(P)$ (of order $p(p-1)/2$). We note from the ramification data that P has precisely $(p-1)/2$ fixed points on X and that N acts transitively on them. Note that $N = PD$ where D is cyclic of order $(p-1)/2$ and acts transitively on the fixed points of P on X.

Lemma 3.3. *Let P be a Sylow p-subgroup of G.*

(i) P is a Sylow p-subgroup of A. In particular, p^2 does not divide $|A|$.

(ii) $|N_A(P) : C_A(P)| = (p-1)/2$.

(iii) $|C_A(P)| < (p^2 - p)/6$.

(iv) $C_A(P)$ is contained in an inertia group.

Proof. Let M be the normalizer of P in A. Then M acts on the fixed points of P and so $M = DM_1$ where M_1 is the inertia group (in M) of some point fixed by

P. Since M_1 is an inertia group and normalizes P, it follows that M_1 centralizes P. Set $C = C_A(P)$. Then $C = M_1(C \cap D) = M_1$. Since C is normal in M, it follows that C fixes each of the $(p-1)/2$ points fixed by P. This also implies (ii) and (iv).

Now consider $X \to X/C$ and let h be the genus of X/C. We see that

$$2(g-1) \geq 2|C|(h-1) + (p-1)(|C|-1)/2,$$

whence

$$(p-1)(p+1)(p-6)/12 \geq |C|(p-5)/2 - (p-1)/2,$$

or

$$[(p-1)/2][(p^2-5p)/6] \geq |C|(p-5)/2,$$

giving the desired inequality on $|C|$ and proving (iii). In particular, p^2 does not divide $|C|$. Let $P \leq Q$ be a Sylow subgroup of A. If $P \neq Q$, then $N_Q(P) \neq P$ and so P is contained in a subgroup R of order p^2. Any group of order p^2 is abelian and so $R \leq C$, a contradiction. This gives (i). □

Note that p is the only prime of size at least $(p-1)/6$ that divides the order of the centralizer of P.

We have also shown that $C_A(P)$ is contained in the inertia group of any point fixed by P. Thus, the inertia group in A of such a point is $VC_A(P)$ where V is an ℓ-group. We shall not use this fact. We recall the following well known results about G.

Lemma 3.4. *If H is a proper subgroup of G, then $|G:H| \geq p+1$ unless $p = 11$ in which case $|G:H| \geq 11$.*

The next result applies to G but also to groups with a cyclic Sylow p-subgroup.

Lemma 3.5. *Let H be a group with a Sylow p-subgroup of order P such that $N_H(P)/C_H(P)$ has order e. If H acts faithfully as automorphisms on an r-group R for some prime $r \neq p$, then $|R| \geq r^e$.*

Proof. There is no loss in assuming that P is normal in H. We know that P acts nontrivially on $R/\Phi(R)$, where $\Phi(R) = [R,R]R^r$ is the Frattini subgroup of R (see [Gor]). So we may assume that R is an elementary abelian p-group. There is no harm in assuming that R is irreducible and P acts nontrivially on R. The hypotheses imply that if a is a generator for P, then a has e conjugates in H, whence a has e distinct eigenvalues (after extending scalars) whence $\dim R \geq e$ as desired. □

Lemma 3.6. *Let R be a subgroup of A normalized by G. Then R contains G.*

Proof. Suppose not. Since G is simple, this forces $R \cap G = 1$. We can take R to be a minimal counterexample. Thus, R is either an elementary abelian r-group for prime r or a direct product of simple groups. We consider the subgroup $B = RG$ (a semidirect product).

Now G acts faithfully on X/R. Since the automorphism group of $\mathbb{P}^1$ is $PGL(2,k)$ and the automorphism group of an elliptic curve is solvable, this implies that X/R has genus at least 2. The Riemann-Hurwitz formula then implies that $(g-1) \geq |R|(g(X/R)-1) \geq |R|$, where $g(X/R)$ is the genus of X/R.

Suppose that R does not commute with G. If R is an r-group, then $r \neq p$ (since p^2 does not divide the order of A). The smallest nontrivial module in characteristic $r \neq p$ for $PSL(2,p)$ (or even the normalizer of P) has order $r^{(p-1)/2} \geq 2^{(p-1)/2} > p^3/24 > g$, a contradiction.

If R is a direct product of nonabelian simple groups, then either P normalizes each factor, whence the simple group $PSL(2,p)$ does as well and so R is simple or there are at least p factors. In the second case, $|R| \geq 60^p > g$, a contradiction.

So assume that R is simple. We could invoke the Schreier conjecture (and so the classification of simple groups at this point) by noting that G cannot act nontrivially on a simple group other than by inner automorphisms because the group of outer automorphisms is solvable. On the other hand p does not divide $|R|$ and so G cannot act on R via inner automorphisms.

We give an elementary argument avoiding this. Let $W = RD$ where $D = N_G(P)$ is the Borel subgroup of G. Let S be a Sylow s-subgroup of R for some prime s dividing $|R|$ (in particular, $s \neq p$). By the Frattini argument (or Sylow's theorem), $W = RN_W(S)$. In particular, we may assume that $P \leq N_W(S)$ and that the normalizer of P in $N_W(S)$ acts as a group of order $(p-1)/2$ on P. It follows by the previous lemma that either P centralizes S or $|S| \geq s^{(p-1)/2}$. The last possibility is a contradiction as before. The first possibility implies that P centralizes a Sylow s-subgroup. Repeating this argument for each prime s dividing $|R|$ implies that P centralizes R, whence the normal closure of P does as well. Thus, G centralizes R, a contradiction to the minimality of R.

So we may assume that R commutes with G and so by minimality has prime order r.

We consider the possibilities for the inertia groups of G on X/R. These are precisely $IR/R \leq GR/R$ where I is an inertia group of RG on X. We identify GR/R with G. First consider the case where $P \leq I$. Then IR/R contains P, whence by the structure of inertia groups and the subgroup structure of G, $IR/R = P$.

Similarly, if $\ell = 2$, we see that the other inertia group in $G = GR/R$ will be A_4. This implies that the genus of X/R is at least that of X, whence $R = 1$, a contradiction.

So $\ell > 2$. If $r > 3$, then the other inertia groups are either contained in G or are $R \times J$ with $J \leq G$. It follows that they project onto J in G. So G has the same inertia groups on X/R as on X, a contradiction as above (because the second ramification groups are trivial).

So $r \leq 3$ and $\ell > 2$. If $\ell > 3$, it follows that all ramification is tame and an easy computation using Riemann-Hurwitz shows that $R = 1$, a contradiction.

So $r \leq 3$ and $\ell = 3$. If $JR/R = S_3$, we argue as above. The only remaining possibility is that JR/R has order $6r$ and normalizes the subgroup of order 3. If $r = 3$, this implies that JR/R is dihedral of order 18. The Riemann-Hurwitz formula implies that X/R has genus larger than X, a contradiction. If $r = 2$, then since the Sylow 3-subgroup T of the inertia group has order 3, it is contained in G. Since we know the higher ramification groups for G, $T_2 = 1$ (on X). It follows that T_2 is self centralizing in the inertia group (see [Ser]), whence the inertia group has order 6, a case we have already handled. □

Corollary 3.7. $G = N_A(G)$.

Proof. The previous result shows that $C_A(G) = 1$. Thus, $N_A(G)$ embeds in the automorphism group of G. This is $PGL(2,p)$. So $N_A(G) = G$ or is $PGL(2,p)$. The latter implies that $N_A(P)/C_A(P)$ has order $p-1$, contradicting Lemma 3.3. □

We can now show that A is almost simple – we will not use this in the rest of the paper.

Corollary 3.8. *Let A_1 be any overgroup of G in A. Then A_1 has a unique minimal normal subgroup S_1 that is simple and contains G. In particular, A_1 embeds in the automorphism group of S_1.*

Proof. Let N be a minimal normal subgroup of A_1. This is normalized by G and so contains G. This shows it is unique (since the intersection of two distinct minimal normal subgroups is trivial). Since N is characteristically simple, it must be a direct product of nonabelian simple groups. Since $G \leq N$, it follows that G normalizes each of the factors of N and so each must contain G. Since the factors intersect trivially, there is only one such factor, whence N is a simple nonabelian group containing G. □

4. Proof of the Theorem

We continue notation from the previous section.

Lemma 4.1. $|A| \leq 16g^4$ *or* $\ell = 3$ *and* $p = 7$.

Proof. We note that for $p > 7$, G does not have a 3-dimensional projective representation in characteristic ℓ. In particular, it cannot embed in the automorphism group of the Hermitian curve and so X is not the Hermitian curve.

So we can apply the Stichtenoth result. If $p = 7$, we just note that the only Hermitian curve of genus 3 occurs in characteristic 3. □

If $p = 7$, X is the Klein quartic and the result is well known in this case. If $p < 7$, there is nothing to prove. So we assume that $p \geq 11$. Since the case $\ell = 3$ and $p = 11$ is done [Raj], we assume that $\ell \neq 3$ if $p = 11$.

Let R be a minimal overgroup of G in A. Then, every nontrivial normal subgroup of R contains G. It follows by minimality that either R is a minimal normal subgroup of R (i.e. R is simple) or that G is normal in R. However, G is self normalizing in A. Thus, R is simple.

We now go through the families of nonabelian simple groups and show (that aside from the exceptional cases) that no such R can exist. So we'll assume that $p \geq 13$ or $l \neq 3$ (and, of course, that $p \geq 11$ and $l \neq p$). We will frequently refer to the ATLAS for the information we need.

1 $R \neq A_n$.

The smallest A_n containing G is with $n = p + 1$ except that $PSL(2, 11)$ embeds in A_{11}. In that case though any subgroup of A_{11} isomorphic to $PSL(2, 11)$ is contained in one isomorphic to M_{11}, i.e. R is not a minimal overgroup.

Note that A_{p+1} contains an elementary abelian subgroup of order $2^{(p-1)/2}$, so by Theorem 2.2, either $l = 2$ or $2^{(p-3)/2} | \frac{1}{12}(p-1)(p+1)(p-6)$. Similarly, if s is odd, then either $l = s$ or $s^{\lfloor (p+1)/s \rfloor - 1} | \frac{1}{24}(p-1)(p+1)(p-6)$. A quick check tells us that $l = 2$ or $p = 7$, and that $l = 3$. Therefore $l = 3$ and $p = 7$, which we're assuming not to be the case.

2 R is not a Chevalley group in characteristic p.

Proof. The only Chevalley group in characteristic p that does not have order divisible by p^2 is $PSL(2, p)$.

3 R is not a sporadic group (recall we're assuming that $p \geq 13$ or $l \neq 3$).

Our first test is as follows. If (R, p) is a valid pair, then $|R|$ must be exactly divisible by p and divisible by $\frac{1}{2}p(p-1)(p+1)$. By Theorem 2.1, we must also have $|R| < 16g^4$. A quick computation leaves us with the following possibilities:

R	M_{11}	M_{12}	J_1	M_{22}	M_{23}	J_2	J_3	M_{24}	He	Ru	$O'N$
p	11	11	11	11	23	17	19	23	17	29	31

Our plan now is to try to use Theorem 2.2 in order to show that l must be simultaneously two values (which of course is absurd) for as many of the above possibilities as we can. We will refer to the ATLAS for the information we need. For example, if $R = M_{12}$ and $p = 11$, then $g - 1 = 25$; however, M_{12} has an elementary abelian subgroup of order 2^3 (implying that $l = 2$ since $2^2 \nmid 50$) and an elementary abelian subgroup of order 3^2 (implying that $l = 3$ since $3 \nmid 25$). The table below lists each possibility (R, p) with appropriate subgroups S and the associated critical quantities s^{m-e}:

R	p	$g-1$	S	s^{m-e}	S	s^{m-e}
M_{11}	11	25	C_3^2	3		
M_{12}	11	25	C_2^3	2^2	C_3^2	3
J_1	11	25	C_2^3	2^2		
M_{22}	11	25	C_2^3	2^2	C_3^2	3
M_{23}	23	374	C_2^4	2^3	C_3^2	3
J_3	17	132	$C_2^2C_2^4$	2^4	C_3^3	3^2
J_3	19	195	$C_2^2C_2^4$	2^4	C_3^3	3^2
M_{24}	23	374	C_2^4	2^3	C_3^2	3
He	17	132	C_2^5	2^4	C_5^2	5
Ru	29	805	C_2^3	2^2	$E_{5^3,+}$	5^2
$O'N$	31	1000	C_3^2	3	C_7^2	7

Here, we use the notation $C_2^2C_2^4$ to mean a group having a normal subgroup C_2^2 with corresponding quotient C_2^4, and $E_{5^n,+}$ denotes the extraspecial group of order 5^n and exponent 5.

We are left with the possibilities $(M_{11}, 11)$ and $(J_1, 11)$. For the former, the table tells us that $l = 3$, which we're assuming not to be the case since $p = 11$. So let us consider $(J_1, 11)$. J_1 has subgroups of order $3, 7, 19$, none of which divide $2(g-1)$, therefore each of them fixes a point on X. Now at least two fix a point in common by the second part of Theorem 2.1, since $|J_1| > 84(g-1)$. Suppose that the subgroups of order 3 and 7 do (the other two cases are similar). By Hall's theorem the corresponding inertia group contains a cyclic group of order 21; however, J_1 contains no such group.

4 R is not an exceptional Chevalley group in characteristic $s \neq p$.

There are ten families of these: $G_2, F_4, E_6, E_7, E_8, {}^2B_2, {}^3D_4, {}^2G_2, {}^2F_4, {}^2E_6$, whose orders are as follows. Here q is a power of s.

Group	Order	Restriction on q
G_2	$q^6(q^6-1)(q^2-1)$	None
F_4	$q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$	None
E_6	$q^{36}(q^{12}-1)(q^9-1)(q^8-1)$ $(q^6-1)(q^5-1)(q^2-1)/\gcd(3,q-1)$	None
E_7	$q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)$ $(q^8-1)(q^6-1)(q^2-1)/\gcd(2,q-1)$	None
E_8	$q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)$ $(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1)$	None
${}^2B_2$	$q^2(q^2+1)(q-1)$	$q=2^{2m+1}$
${}^3D_4$	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$	None
${}^2G_2$	$q^3(q^3+1)(q-1)$	$q=3^{2m+1}$
${}^2F_4$	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$	$q=2^{2m+1}$
${}^2E_6$	$q^{36}(q^{12}-1)(q^9+1)(q^8-1)$ $(q^6-1)(q^5+1)(q^2-1)/\gcd(3,q+1)$	None

All the groups in this table are simple, except for $G_2(2), {}^2B_2(2), {}^2G_2(3)$ and ${}^2F_4(2)$, which have simple subgroups of indices $2,4,3,2$ respectively.

Note that we can ignore ${}^2B_2$, since the order of ${}^2B_2(q)$ is not divisible by 3, implying that ${}^2B_2(q)$ does not contain $PSL(2,p)$.

Our first test is basically the same as our first test for the sporadic groups. The main difference is that we need some mechanism for bounding p; this is provided by the fact that $PSL(2,p)$ has no faithful linear representation in $\overline{\mathrm{GF}(s)}$ of degree less than $(p-1)/2$. Therefore, if $PSL(2,p)$ embeds into a group R having a faithful linear representation of degree d, we must have $p \leq 2d+1$. The table below lists, for each of the exceptional Chevalley groups (apart from ${}^2B_2$ of course), the degree of a faithful linear representation it possesses, and the resulting bound on p:

Group	Degree (d)	Bound ($2d+1$)
G_2	7	15
F_4	26	53
E_6	27	55
E_7	56	113
E_8	248	497
${}^3D_4$	8	17
${}^2G_2$	7	15
${}^2F_4$	26	53
${}^2E_6$	27	55

Given a group R and a prime p, we need a bound on q, but this is easily provided by Theorem 2.1.

Carrying out the test leaves just one possibility:

$$R = G_2(3), p = 13.$$

Fortunately this group is documented in the ATLAS, therefore we can easily eliminate it by playing the same game as we did for the surviving sporadic groups: $G_2(3)$ has elementary abelian subgroups of order 2^3 and 3^2, but $2(g-1) = 98$ is not divisible by either 2^2 or 3.

5 R is not a classical group in characteristic $s \neq p$.

There are six families of these: $A_n, B_n, C_n, D_n, {}^2A_n, {}^2D_n$, whose orders are as follows. Here q is a power of s.

Group	Order	Restrictions on n
A_n	$q^{n(n+1)/2}\prod_{i=1}^{n}(q^{i+1}-1)$ / $\gcd(n+1, q-1)$	None
B_n	$q^{n^2}\prod_{i=1}^{n}(q^{2i}-1)$ / $\gcd(2, q-1)$	$n > 1$
C_n	$q^{n^2}\prod_{i=1}^{n}(q^{2i}-1)$ / $\gcd(2, q-1)$	$n > 2$
D_n	$q^{n(n-1)}(q^n-1)\prod_{i=1}^{n-1}(q^{2i}-1)$ / $\gcd(4, q^n-1)$	$n > 3$
${}^2A_n$	$q^{n(n+1)/2}\prod_{i=1}^{n}(q^{i+1}-(-1)^{i+1})$ / $\gcd(n+1, q+1)$	$n > 1$
${}^2D_n$	$q^{n(n-1)}(q^n+1)\prod_{i=1}^{n-1}(q^{2i}-1)$ / $\gcd(4, q^n+1)$	$n > 3$

All the groups in this table are simple, except for $A_1(2), B_2(2), {}^2A_2(3)$ and ${}^2A_2(2)$. But we can safely ignore these since all their orders have largest prime factor less than 7.

Our first test is basically the same as our first test for the exceptional Chevalley groups. This time the degrees of the faithful linear representations, and the resulting bounds on p, are as follows:

Group	Degree (d)	Bound ($2d+1$)
A_n	$n+1$	$2n+3$
B_n	$2n+1$	$4n+3$
C_n	$2n$	$4n+1$
D_n	$2n$	$4n+1$
${}^2A_n$	$n+1$	$2n+3$
${}^2D_n$	$2n$	$4n+1$

The main difference is that we need some mechanism for bounding n. But we simply note that each group R has order at least $2^{n(n+1)/2}$ and that each prime p is at most $4n+3$; therefore, we obtain the crude inequality

$$2^{n(n+1)/2} < 16g^4 < 16[(4n+3)^3/24]^4,$$

which implies that $n \leq 9$.

Carrying out the test eliminates all possibilities.

References

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

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

[Elk] Noam Elkies, The Klein quartic in number theory in The Eightfold Way – The Beauty of Klein's Quartic Curve, S. Levy, Ed., MSRI Publications, Cambridge University Press, Cambridge, 1999.

[GG] D. Goldstein and R. Guralnick, Automorphisms of the modular curve $X(n)$ in positive characteristic II. n composite, preprint.

[Gor] Daniel Gorenstein, *Finite Groups*, Harper and Row, 1968.

[GLS] D. Gorenstein, R. Lyons and R. Solomon, The Classification of Finite Simple Groups, Number 3, Mathematical Surveys and Monographs, Amer. Math. Soc., Providence, RI, 1998.

[Har] R. Hartshorne, *Algebraic Geometry*, GTM 52, Springer-Verlag, 1977.

[Gur] R. Guralnick, Monodromy groups of curves in L. Schneps, Ed, The MSRI Semester on Fundamental and Galois Groups, to appear.

[Igu] J. Igusa, Arithmetic variety of moduli for genus two, Annals Math. 72 (1960), 612-649.

[Mor] C. J. Moreno, Algebraic Curves over Finite Fields, Cambridge Tracts in Mathematics 97, CUP, 1991.

[Raj] C. Rajan, Automorphisms of $X(11)$ over characteristic 3 and the Mathieu group M_{11}, J. Ramanujan Math. Soc. 13 (1998), 63–72.

[Rit] C. Ritzenthaler, Automorphismes des courbes modulaires $X(n)$ en caractéristique p, Manuscripta Math. 109 (2002), 49–62.

[Ser] Jean-Pierre Serre, *Local Fields*, GTM 67, 1979.

[Sil] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, 1986.

[St1] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik*, Archiv. der Math. 24 (1973), 527–544.

[St2] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Universitext, 1993.

http://www.springer.com/978-0-387-23533-2

Progress in Galois Theory
Proceedings of John Thompson's 70th Birthday Conference
Voelklein, H.; Shaska, T. (Eds.)
2005, X, 168 p., Hardcover
ISBN: 978-0-387-23533-2