PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 135, Number 3, March 2007, Pages 617–624
S 0002-9939(06)08493-0
Article electronically published on September 15, 2006

GALOIS GROUPS VIA ATKIN-LEHNER TWISTS

PETE L. CLARK

(Communicated by Ken Ono)

ABSTRACT. Using Serre's proposed complement to Shih's Theorem, we obtain $PSL_2(\mathbb{F}_p)$ as a Galois group over $\mathbb{Q}$ for at least 614 new primes p. Assuming that rational elliptic curves with odd analytic rank have positive rank, we obtain Galois realizations for $\frac{3}{8}$ of the primes that were not covered by previous results; it would also suffice to assume a certain (plausible, and perhaps tractable) conjecture concerning class numbers of quadratic fields. The key issue is to understand rational points on Atkin-Lehner twists of $X_0(N)$. In an appendix, we explore the existence of local points on these curves.

1. INTRODUCTION

The notorious Inverse Galois Problem asks for which finite groups G there exists a Galois extension $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$ (for short, "G occurs over $\mathbb{Q}$"). The optimistic guess that every finite group occurs over $\mathbb{Q}$ is natural for at least two reasons. First, by a famous theorem of Hilbert, it is enough to realize G as the Galois group of a regular extension $L/\mathbb{Q}(t)$. Now for any field K, one says that a finite group G *occurs regularly* over K if it is the Galois group of a regular extension $L/K(t)$, and there are many fields – e.g., $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}_p, \ldots$, – over which every finite group is known to occur regularly.

There is also the lure of inductive reasoning: it is known that many finite groups – e.g., solvable, symmetric and alternating groups – occur as Galois groups over $\mathbb{Q}$ (and, of course, no finite groups have been shown *not* to occur!). Still, the progress towards realizing all groups has been anything but steady: some of the "simplest" simple groups are still not known to occur. Consider, for instance, the family of groups $PSL_2(\mathbb{F}_p)$ as p ranges over prime numbers.

Over thirty years ago, Shih showed that $PSL_2(\mathbb{F}_p)$ occurs regularly over $\mathbb{Q}$ if for some $N \in \{2, 3, 7\}$, the Kronecker symbol $(\frac{N}{p})$ is equal to -1 [9]. Later, Malle showed that $(\frac{5}{p}) = -1$ is also sufficient for $PSL_2(\mathbb{F}_p)$ to occur regularly over $\mathbb{Q}$ [4]. Note that these two results leave a density $\frac{1}{16}$ set of primes unaccounted for. To the best of my knowledge, no further occurrences of $PSL_2(\mathbb{F}_p)$ over $\mathbb{Q}$, regular or otherwise, have been established.

In 1988, Serre proposed a method of extending Shih's Theorem to realize new groups $PSL_2(\mathbb{F}_p)$ over $\mathbb{Q}$. This method is discussed in his book *Topics in Galois Theory* [11]. Referring to a calculation of Elkies, Serre remarks that the method works to realize $PSL_2(\mathbb{F}_{47})$ over $\mathbb{Q}$; notice that $p = 47$ is covered by Malle's result

Received by the editors June 30, 2005 and, in revised form, September 15, 2005.
2000 *Mathematics Subject Classification.* Primary 11G18, 12F12.

but not by Shih's. Strangely, no additional examples of the method are given or asked for.

In this paper, we analyze Serre's method and show that it works to give realizations of $PSL_2(\mathbb{F}_p)$ over $\mathbb{Q}$ for many primes p not obtainable by any previous result.

2. Analysis of Serre's method

Serre's approach [11, §5.4] begins with the following formulation of Shih's Theorem.

Theorem 1 ([9, Theorem 8])**.** *Let $p^* = (-1)^{\frac{p-1}{2}}p$, and let $N \in \mathbb{Z}^+$ be such that $(\frac{N}{p}) = -1$. Let $C(N,p)$ be the curve obtained by twisting the modular curve $X_0(N)$ using the Atkin-Lehner involution $w_N \in \mathrm{Aut}(X_0(N))$ and the quadratic extension $Q(\sqrt{p^*})/\mathbb{Q}$. Then there is a regular Galois covering $Y \to C(N,p)$, defined over $\mathbb{Q}$, with Galois group $PSL_2(\mathbb{F}_p)$.*

In the case that $C(N,p) \cong \mathbb{P}^1$, this means precisely that $PSL_2(\mathbb{F}_p)$ occurs regularly over $\mathbb{Q}$. This occurs for all p when $N \in \{2,\ 3,\ 7\}$, and we recover our earlier statement of Shih's Theorem. More generally, when $C(N,p)(\mathbb{Q}) \neq \emptyset$, there remains the possibility of finding an irreducible specialization. Indeed, we have the following.

Theorem 2 (Serre)**.** *With hypotheses as above, if $C(N,p)(\mathbb{Q})$ is infinite, then there are infinitely many linearly disjoint Galois extensions $L/\mathbb{Q}$ with Galois group $G \cong PSL_2(\mathbb{F}_p)$.*

In other words, whereas Shih's Theorem says that it suffices for $C(N,p) \cong \mathbb{P}^1$, Theorem 2 says that it also suffices for $C(N,p)$ to be an elliptic curve of positive rank.

$X_0(N)$ has genus one for $N \in \{11,\ 14,\ 15,\ 17,\ 19,\ 20,\ 21,\ 24,\ 27,\ 32,\ 36,\ 49\}$, so in order to realize $PSL_2(\mathbb{F}_p)$ for primes p not covered by the results of Shih and Malle, the values of N to consider are $11,\ 17$ and 19.

Theorem 3. *Let $N = 11$ or 19. For all primes p, $C(N,p)(\mathbb{Q}) \neq \emptyset$, so $C(N,p)$ can be given the structure of a rational elliptic curve. More precisely, $C(N,p)$ is the quadratic twist of $X_0(N)$ by p^*. It follows that:*

- *For primes $p \equiv 1 \pmod 4$, $(\frac{N}{p}) = -1 \iff C(N,p)$ has odd analytic rank.*
- *For primes $p \equiv -1 \pmod 4$, $(\frac{N}{p}) = -1 \iff C(N,p)$ has even analytic rank.*

Proof. Let σ denote the nontrivial element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$. Then $C(N,p)(\mathbb{Q})$ consists of those points P of $C(N,p)(\mathbb{Q}(\sqrt{p^*}))$ for which $w_N(\sigma(P)) = P$. In particular, any $P \in X_0(N)(\mathbb{Q})$ which is a fixed point of w_N remains $\mathbb{Q}$-rational on $C(N,p)$. For any squarefree N, let S_1 (resp. S_2) be the set of $\mathbb{C}$-isomorphism classes of elliptic curves with CM by the maximal order of $\mathbb{Q}(\sqrt{-N})$ (resp. by $\mathbb{Z}[\sqrt{-N}]$); these sets are distinct if and only if $-N \equiv 1 \pmod 4$. It is not hard to see that S_1 and S_2 each gives rise to a set of w_N-fixed points – the $\Gamma_0(N)$ structure is given by $E[\sqrt{-N}]$ – and that if $N > 3$, $S_1 \cup S_2$ gives all the w_N-fixed points (e.g., [6, Prop. 3]). The set S_1 (resp. S_2) forms a complete $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ orbit. So there are $\mathbb{Q}$-rational w_N-fixed points exactly when $\mathbb{Q}(\sqrt{-N})$ has class number 1, which is the case for $N = 11$ and $N = 19$ (but not for $N = 17$).

Thus, for $N = 11$ or 19, let O be the unique fixed point of w_N that parameterizes an elliptic curve with $\mathbb{Z}[\frac{1+\sqrt{-N}}{2}]$-CM, so that $(X_0(N), O)$ and $(C(N,p), O)$ are rational elliptic curves. Since the j-invariant of $X_0(N)$ is neither 0 nor 1728, the group of automorphisms of $(X_0(N), O)$ is ± 1, and it follows that under our identifications we simply have $w_N = -1$. In other words, the twist of $X_0(N)$ via w_N and $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ is just the quadratic twist by p^* in the usual sense. Finally, the sign of the functional equation for both $X_0(11)$ and $X_0(19)$ is $+1$, so the sign of the functional equation for $C(N,p)$ is $\chi_{p^*}(-N) = (\frac{-N}{p})$. The result follows. □

We get as an immediate consequence our main result:

Corollary 4. *Assume that rational elliptic curves with odd analytic rank have positive Mordell-Weil rank. Then for every p with $p \equiv 1 \pmod 4$ and which is a quadratic nonresidue* either *modulo* 11 *or modulo* 19*, $PSL_2(\mathbb{F}_p)$ occurs infinitely often as a Galois group over $\mathbb{Q}$.*

However, when $N = 17$ Serre's method fails for local reasons:

Proposition 5. *For every prime p such that $\left(\frac{17}{p}\right) = -1$, $C(N,p)(\mathbb{Q}_{17}) = \emptyset$.*

Remark. The proof that follows is purely computational. More recently we have found other approaches (see Corollary 10 and Theorem 11 in the Appendix).

Proof. For any squarefree N, the involution w_N has at least one fixed point, so that the quotient map $X_0(N) \to X_0^+(N) := X_0(N)/w_N$ is always ramified. In particular, when $X_0(N)$ has genus one, $X_0^+(N)$ has genus zero, and in fact – since $X_0(N)$ always has $\mathbb{Q}$-rational cusps – $X_0^+(N) \cong \mathbb{P}^1$. In particular, w_{17} gives a hyperelliptic involution on $X_0(17)$, and $\mathbb{Q}(X_0(17)) = \mathbb{Q}(x,y)$, where $y^2 = P(x)$ for some quartic polynomial $P \in \mathbb{Q}[x]$ and $w : (x,y) \mapsto (x,-y)$. Explicit polynomials have been computed by Elkies (unpublished) and González; by [3, p. 794], we may take $P(x) = x^4 + 2x^3 - 39x^2 - 176x - 212$. Thus $C(17,p)$ is given by the equation

$$p^* y^2 = x^4 + 2x^3 - 39x^2 - 176x - 212.$$

The condition $(\frac{17}{p}) = -1$ ensures that any two of the numbers p^* differ (multiplicatively) by an element of $\mathbb{Q}_p^{\times 2}$, hence all such curves $C(17,p)$ are $\mathbb{Q}_{17}$-isomorphic to a single curve, say $C(17,5)$, and we are reduced to deciding whether this particular hyperelliptic quartic curve has $\mathbb{Q}_{17}$-rational points.

As a general principle, one knows that all Diophantine problems over local fields are decidable; in this case an analysis involving Hensel's Lemma shows that (after ruling out rational points at infinity and projectivizing) it suffices to study a corresponding congruence modulo 17^5. Thus in practice we will want computer assistance. Luckily for us, the issue of local points on hyperelliptic quartics arises in 2-descent, so that a relatively efficient algorithm for this – first described in the early work of Birch and Swinnerton-Dyer – has been implemented in several elliptic curve software packages. For instance, a query to John Cremona's program `ratpoints` results in the instantaneous response that $C(17,5)$ fails to have points rational over $\mathbb{Q}_{17}$ (and indeed also over $\mathbb{Q}_5$). This completes the proof. □

3. Examples

Fix $N \in \{11, 19\}$. If $p \equiv 1 \pmod 4$ is a prime satisfying $(\frac{N}{p}) = -1$, then we have seen that the analytic rank of $C(N,p)$ is odd, so that it is, to say the least,

widely believed that $C(N,p)$ has infinitely many $\mathbb{Q}$-rational points. In any given case one can, in principle, verify this just by finding a rational point of infinite order. Better yet: whenever the analytic rank is equal to 1, we know – thanks to the work of Gross-Zagier and Kolyvagin – that the rank is equal to one. And it is easy to check that the analytic rank is 1: one need only check that the special value $L'(C(N,p),1)$ is nonzero, which is amenable to approximate computation. Moreover, when the sign in the functional equation is -1, the prevailing wisdom is that the analytic rank should be equal to 1 "most of the time".

Indeed, among all primes $p \leq 3 \times 10^5$ for which

$$p \equiv 1 \pmod 4, \ \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = 1,$$

it is *never* the case that the analytic rank of either $C(11,p)$ or $C(19,p)$ is odd and greater than one. This yields a list of 612 prime numbers – the smallest is $p = 1009$ – such that $PSL_2(\mathbb{F}_p)$ newly occurs as a Galois group over $\mathbb{Q}$.

On the other hand, when $p \equiv -1 \pmod 4$, the analytic rank of $C(N,p)$ is noticeably less averse to being *even* and greater than zero.[1] Elkies' computation of $\operatorname{rank} C(11,47) = 2$ is an example of this. Among $p < 1000$, $C(11,p)$ also has (apparent) analytic rank 2 for 103, 599, and 683. The phenomenon is robust enough to persist upon enforcing the congruence conditions $(\frac{2}{p}) = (\frac{3}{p}) = (\frac{5}{p}) = (\frac{7}{p}) = 1$; for

$$p = 4079,\ 5591,\ 6719,\ 10391,\ 19319,\ 24359,\ 26759, \tag{1}$$

either $C(11,p)$ or $C(19,p)$ has (apparent) analytic rank 2.

Example 1.

$[513624381660076268297 03 : -4948233782238353787199293 : 5697234033382001683]$

is a nontorsion point on the curve

$$C(11,4079) : Y^2Z + YZ^2 = X^3 - X^2Z - 171928490XZ^2 + 1571689994520Z^3,$$

so $PSL_2(\mathbb{F}_{4079})$ occurs as a Galois group over $\mathbb{Q}$.

Example 2. $[-99184162 : 21162527913 : 10648]$ is a nontorsion point on the curve

$$C(19,5591) : Y^2Z + YZ^2 = X^3 + X^2Z - 291753289XZ^2 + 2040511796399Z^3,$$

so $PSL_2(\mathbb{F}_{5591})$ occurs as a Galois group over $\mathbb{Q}$.

On the basis of these computations, it seems reasonable to conjecture that $C(N,p)$ has positive rank for infinitely many primes $p \equiv -1 \pmod 4$.

4. Some remarks

There is a large literature on the variation of ranks of elliptic curves in a family of quadratic twists, but comparatively little has been said about the case of restricting to twists by prime numbers. Worth mentioning in this regard is the work of Ono and Skinner [7], which shows that for certain rational elliptic curves a positive proportion of prime twists have rank zero. There is as yet no analogous result for positive rank. Note however that Vatsal has shown that a positive proportion of all quadratic twists of $X_0(19)$ has rank 1 [12]. His argument could be readily adapted to the case of twists by primes in a given congruence class – and hence to give,

[1] At least apparently: approximate calculation can strongly suggest, but not prove, that an elliptic curve has analytic rank ≥ 2.

unconditionally, a new positive density set of primes p for which $PSL_2(\mathbb{F}_p)$ occurs over $\mathbb{Q}$ – provided we knew the following.

Conjecture 6. *Fix coprime positive integers m and M, and let $F(X)$ be the number of primes satisfying $p \leq X$, $p \equiv m \pmod{M}$, and such that the class number of $\mathbb{Q}(\sqrt{-3p})$ is indivisible by 3. Then $F(X) \gg X/\log X$.*

This conjecture may be within reach; by taking $M = 4$ and replacing $\mathbb{Q}(\sqrt{-3p})$ with $\mathbb{Q}(\sqrt{p})$, we get a theorem of Belabas and Fouvry [1].

Professor Shih has made me aware of the relevance of his later paper [10] to the present work. In particular, this note can be viewed as responding to [10, Remark 4]. What does not figure in [10] is the dichotomy between $N = 11, 19$ and $N = 17$ arising from the fact that the curves $C(N, p)$ have $\mathbb{Q}$-rational points in the former case but not in the latter case. Deciding which Atkin-Lehner twists of $X_0(N)$ have points rational over $\mathbb{Q}$ (or even over all of its completions) is an interesting Diophantine problem which we address in the Appendix of this paper.

The calculations of Section 3 have been extended, thanks to the help of Nick Rogers: in particular, for all the primes p in (1), $\operatorname{rank} C(11, p) + \operatorname{rank} C(19, p) > 0$. Conversely, after a wider search, we have still not been able to find any primes for which either $C(11, p)$ or $C(19, p)$ has odd analytic rank ≥ 3. It has been suggested to me by several people that it is "implausible" for, e.g., the ranks to be bounded in a family of quadratic twists by *prime numbers*. In response to this, I would like to say that I do not necessarily agree: although I am too far from being sufficiently expert in this matter to have an opinion of my own, I was not able to find in the literature any conjecture, heuristic or model (let alone any theorem) which would rule out, e.g., the statement that $\operatorname{rank} C(19, p) = 1$ for all primes $p \equiv 1 \pmod 4$. In any case, the phenomenon seems to be worthy of further investigation.

Appendix: Local points on $C(N, p)$

We suppose that N is squarefree and p is a prime number such that $(\frac{N}{p}) = -1$.

The cusps of $X_0(N)$ are $\mathbb{Q}$-rational but freely permuted by w_N, so that if $\mathbb{Q}(\sqrt{-N})$ has class number greater than one, there are no "obvious" $\mathbb{Q}$-rational points on $C(N, p)$. Indeed, Shih found that in certain cases $C(N, p)$ fails to have points even over certain completions of $\mathbb{Q}$.

In this appendix we will begin a systematic study of the "deficient places" of $C(N, p)$, i.e., the primes $\ell \leq \infty$ such that $C(N, p)(\mathbb{Q}_\ell) = \emptyset$. This is the special case $m = p^*$ of a problem of Ellenberg [2, Problem A], which is concerned with twists of $X_0(N)$ by w_N and an arbitrary quadratic field $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$.

Proposition 7. *$C(N, p)(\mathbb{R}) \neq \emptyset$.*

Proof. Let $\mathcal{O}$ be the ring of integers of $\mathbb{Q}(\sqrt{-N})$. Then $E := \mathbb{C}/\mathcal{O}$ is an elliptic curve over the complex numbers such that $P = (E, E[\sqrt{-N}])$ gives a w_N-fixed point. But complex conjugation on $\mathbb{C}$ induces an antiholomorphic involution on E, and it follows easily that $j(E) \in \mathbb{R}$ and that $P \in X_0(N)(\mathbb{R})$. Thus, every Atkin-Lehner twist of $X_0(N)$ has $\mathbb{R}$-rational points.

Recall that a (nonsingular, projective) curve $C_{/\mathbb{Q}_\ell}$ is said to have *good reduction* if there exists a smooth arithmetic surface $\mathcal{C}_{/\mathbb{Z}_\ell}$ with generic fiber isomorphic to C. If C has positive genus, then it admits a unique minimal model $\mathcal{C}_{/\mathbb{Z}_\ell}$, whose smoothness is equivalent to the good reduction of C. On the other hand, there

are only two curves of genus zero over $\mathbb{Q}_\ell$: $\mathbb{P}^1$ (which has good reduction), and the twisted form corresponding to the unique division quaternion algebra over $\mathbb{Q}_l$ (which does not have good reduction). □

Proposition 8. *Fix ℓ prime to Np. Then $C(N,p)$ has good reduction over $\mathbb{Q}_\ell$. In particular, if $X_0(N)$ has genus at most one, $C(N,p)(\mathbb{Q}_\ell) \neq \emptyset$.*

Proof. When $X_0(N)$ has genus zero – i.e., when $N \in \{2,\ 3,\ 5,\ 6,\ 7,\ 10,\ 13\}$ – work of Shih gives a more precise result. Indeed, the genus zero curve $C(N,p)_{/\mathbb{Q}}$ is classified up to isomorphism by a quaternion algebra. By [9, Prop. 10], this quaternion algebra is given by the Hilbert symbol $\langle c_N, p^* \rangle$, where

$$c_2 = c_3 = 1,\ c_5 = 125,\ c_6 = 18,\ c_7 = 49,\ c_{10} = 5,\ c_{13} = 13.$$

The genus zero case follows (after a small calculation, when $\ell = 2$).

Let us now assume that $X_0(N)$ has positive genus. By a well-known theorem of Igusa, $X_0(N)$ has good reduction over $\mathbb{Z}_\ell$, so $C(N,p)_{/\mathbb{Q}(\sqrt{p^*})}$ has good reduction at the places over ℓ. Moreover ℓ is unramified in $\mathbb{Q}(\sqrt{p^*})$, so that $C(N,p)_{/\mathbb{Q}_\ell}$ has good reduction after an unramified base change. Since formation of the minimal model commutes with unramified base change and smoothness can be checked on geometric fibers, this means that the minimal model $\mathcal{C}(N,p)_{/\mathbb{Z}_\ell}$ is itself smooth.

Finally, if $X_0(N)$ has genus one, then, since every smooth curve of genus at most one over the finite field $\mathbb{F}_\ell$ has an ℓ-rational point (e.g., by the Weil bounds), $C(N,p)(\mathbb{Q}_\ell) \neq \emptyset$ by Hensel's Lemma. □

The next result is a generalization of [9, Prop. 10].

Theorem 9 (González)**.** *$C(N,p)_{/\mathbb{Q}}$ admits a finite morphism to the genus zero curve with corresponding quaternion algebra $\langle c_N,\ p^* \rangle$, where $c_N = N^{\frac{12}{\gcd(12,N-1)}}$.*

Proof. See [8, Thm. 6.2]. The argument is analytic in nature: one constructs a $\Gamma_0(N)$-automorphic function G (which is a Hauptmodul when $X_0(N)$ has genus zero) with $\mathbb{Q}$-rational Fourier coefficients, and such that $w_N(G) = c_N/G$. To see that this gives the theorem as we have stated it, apply the Exercise in [11, § 5.3]. □

Thus, if c_N is not a norm from $\mathbb{Q}(\sqrt{p^*})$, we deduce that $C(N,p)$ has at least *two* deficient places. In particular we get the following sharpening of Proposition 5.

Corollary 10. *The deficient places of $C(17,p)$ are precisely $\ell = p$ and $\ell = 17$.*

Proof. By Theorem 9, $C(17,p)$ maps to the genus zero curve V with corresponding quaternion algebra $\langle 17^3,\ p^* \rangle \cong \langle 17,\ p^* \rangle$. Since $V(\mathbb{Q}_\ell) = \emptyset$ for $\ell = p$ and 17, *a fortiori* the same holds for $C(17,p)$. That there are no other deficient places follows from Propositions 7 and 8. □

Theorem 11. *Suppose N is prime. Then $C(N,p)(\mathbb{Q}_N) = \emptyset \iff N \equiv 1 \pmod 4$.*

Proof. Because $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-3})$ have class number one, we may assume that $N \geq 5$. We shall apply the work of Mazur and Rapoport on the structure of the minimal regular model for $X_0(N)_{/\mathbb{Q}_N}$ [5] (especially relevant is the picture on [5, p. 177]). Recall that the special fiber $M_0(N)_{/\mathbb{F}_p}$ of the coarse moduli space consists of two rational curves intersecting tranversely along the supersingular points, with each supersingular point on $X(1)_{/\overline{\mathbb{F}_N}}$ getting glued to its Galois conjugate under the quadratic Frobenius map $\sigma : \mathbb{F}_{N^2} \to \mathbb{F}_{N^2}$. The Atkin-Lehner involution w_N has the effect of interchanging the two branches, and the assumption that p^* is a

quadratic nonresidue modulo N – note that $(\frac{N}{p}) = (\frac{p^*}{N})$ – means that $C(N,p)$ is the generic fiber of an arithmetic surface $M(N,p)_{/\mathbb{Z}_N}$ which is the twist of $M_0(N)_{/\mathbb{Z}_N}$ by σ. In particular, the only $\mathbb{F}_N$-rational points on the special fiber of $M(N,p)$ are the supersingular points, which are singular.

However, as alluded to above, $M_0(N)_{/\mathbb{Z}_N}$ is not necessarily a *regular* model of $X_0(N)_{/\mathbb{Q}_N}$. More precisely, if $N \equiv -1 \pmod 3$, then $j = 0$ must be blown up twice leading to a chain of two rational curves; and similarly if $N \equiv -1 \pmod 4$, $j = 1728$ must be blown up once leading to a single rational curve. Now a similar procedure can be performed on $M(N,p)_{/\mathbb{Z}_N}$ to get a(n in fact minimal) regular model of $C(N,p)_{/\mathbb{Q}_N}$, which we shall denote by $\mathcal{C}(N,p)_{/\mathbb{Z}_N}$; we need only keep track of the effect of the twisted $\mathrm{Gal}(\mathbb{F}_{N^2}/\mathbb{F}_N)$ action on these rational curves. In the $j = 0$ case, the Galois action interchanges the two rational curves, hence leads to no new $\mathbb{F}_N$-rational points. However, in the $j = 1728$ case, the unique rational curve is evidently stabilized by the Galois action, yielding a smooth $\mathbb{F}_N$-rational curve of genus zero. But, as above, it is well known that every smooth genus zero curve over a finite field is isomorphic to the projective line, giving $N + 1$ rational points on the special fiber of $\mathbb{F}_N$. In summary, we have that a (minimal) regular model for $C(N,p)$ over $\mathbb{Z}_N$ has $\mathbb{F}_N$-rational points if and only if $N \equiv -1 \pmod 4$. We are done by Hensel's Lemma. □

Remark. The proof still goes through when $N = 2$ or $N = 3$. In each case there is a unique supersingular point on the special fiber. The desingularization performed by successive blowups of this point leads to a chain of 11 rational curves when $N = 2$ and 5 rational curves when $N = 3$. Since these numbers are odd, the Galois action stabilizes the middle element of the chain.

Moreover, we have assumed N to be prime only for simplicity of exposition: for any squarefree N and ℓ dividing N, the argument gives a necessary and sufficient condition for $C(N,p)(\mathbb{Q}_\ell) = \emptyset$; namely that $(\frac{p^*}{\ell}) = -1$ and that there does not exist a supersingular point on $X_0(N/\ell)_{/\mathbb{F}_\ell}$ whose automorphism group is divisible by 4. We leave the task of converting this into an explicit congruence condition to the interested reader.

Theorem 11 gives a third proof of Proposition 5. The relationship between Theorems 9 and 11 (whose proofs seem very different) is interesting: neither encompasses the other, although there is a substantial overlap: the implication $\Longleftarrow$ of Theorem 11 also follows from Theorem 9.

At present, I do not know whether there is a similarly simple necessary and sufficient condition for $C(N,p)(\mathbb{Q}_p) = \emptyset$; whether there is ever a deficient prime ℓ not dividing Np; or whether $C(N,p)$ can have no deficient places but still fail to have $\mathbb{Q}$-rational points.[2]

Acknowledgements

I thank Dr. Nick Rogers for performing additional calculations and Professor Shih for making me aware of the connections with his work. As usual, I am grateful to Noam Elkies for rapid and helpful replies to my questions.

[2] *Added in proof* (August 2006): I have recently obtained an affirmative answer to the last question.

References

[1] K. Belabas and E. Fouvry, *Sur le* 3*-rang des corps quadratiques de discriminant premier ou presque premier*, Duke Math. J. 98 (1999), 217-268. MR1695199 (2000i:11167)

[2] J. Ellenberg, $\mathbb{Q}$*-curves and Galois representations*, Progr. Math. 224, 93-103. MR2058645 (2005g:11088)

[3] J. González. *Equations of hyperelliptic modular curves*, Ann. Inst. Fourier (Grenoble) 41 (1991), 779-795. MR1150566 (93g:11064)

[4] G. Malle, *Genus zero translates of three point ramified Galois extensions*, Manuscripta Math. 71 (1991), 97-111. MR1094741 (92f:12009)

[5] B. Mazur, *Modular elliptic curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. 47 (1988), 33-186.

[6] A. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France 102 (1974), 449-462. MR0364259 (51:514)

[7] K. Ono and C. Skinner, *Nonvanishing of quadratic twists of modular L-functions*, Invent. Math. 134 (1998), 651-660. MR1660945 (2000a:11077)

[8] J. Quer, $\mathbb{Q}$*-curves and abelian varieties of* GL_2*-type*, Proc. London Math. Soc. (3) 81 (2000), 285-317. MR1770611 (2001j:11040)

[9] K.-y. Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. 207 (1974), 99-120. MR0332725 (48:11051)

[10] K.-y. Shih, *p-division points on certain elliptic curves*, Comp. Math. 36 (1978), 113-129. MR0515041 (80d:10042)

[11] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics 1, Jones and Bartlett, 1992. MR1162313 (94d:12006)

[12] V. Vatsal, *Rank-one twists of a certain elliptic curve*, Math. Ann. 311 (1998), 791-794. MR1637976 (99i:11050)

Department of Mathematics and Statistics, 1126 Burnside Hall, McGill University, 805 Sherbrooke West, Montreal, QC, Canada H3A 2K6

E-mail address: clark@math.mcgill.ca

Current address: Department of Mathematics, University of Georgia, Athens, Georgia 30602

E-mail address: pete@math.uga.edu