A REFINEMENT OF THE FALTINGS-SERRE METHOD

Nigel Boston

University of Illinois at Urbana-Champaign

August 1993

0. Introduction

In recent years the classification of elliptic curves over $\mathbf{Q}$ of various conductors has been attempted. Many results have shown that elliptic curves of a certain conductor do not exist. Later methods have concentrated on small conductors, striving to find them all and hence to verify the Shimura-Taniyama-Weil conjecture for those conductors. A typical case is the conductor 11. In [1], Agrawal, Coates, Hunt, and van der Poorten showed that every elliptic curve over $\mathbf{Q}$ of conductor 11 is $\mathbf{Q}$-isogenous to $y^2 + y = x^3 - x^2$. Their methods involved a lot of computation and the use of Baker's method. In [12], Serre subsequently applied Faltings' ideas to reprove this result in a much shorter way. He called this approach "the method of quartic fields".

In this paper I first seek to refine this method and to make it possible to classify elliptic curves over $\mathbf{Q}$ of conductor N for a large number of N. These N are all prime and so this work will indeed superceded by the work of Wiles if his gap can be fixed. The advantage of my method is that it provides a much simpler approach (when it works). Like Wiles, I am using deformations of Galois representations but in a more elementary way. The second half of the paper indicates how the Faltings-Serre method can be used to describe spaces of Galois representations and gives the first applications of the method to mod p representations with $p \neq 2$.

The main result of the first half is Theorem 1 below. Note that there are extensive tables of class numbers and units of cubic fields due to Angell [2] and that information on quartic fields is not required

Theorem (0.1) Let N be a prime $\equiv 3 (\mathrm{mod}\ 8)$, such that 3 divides neither $h(\mathbf{Q}(\sqrt{N}))$ nor $h(\mathbf{Q}(\sqrt{-N}))$. Let M be one of the cubic subfields of the unique cubic cyclic extension K of $\mathbf{Q}(\sqrt{-N})$ of conductor (2). Suppose that $h(M)$ is odd and that the minimum polynomial modulo N of a fundamental unit of M has a quadratic residue and a quadratic non-residue root.

Partially supported by NSF grant DMS 90-14522. I thank God for leading me to these results. I thank J.-P.Serre for generous sending me copies of his unpublished work.

Then there is at most one $\mathbf{Q}$-isogeny class of elliptic curves over $\mathbf{Q}$ of conductor N with given trace of Frobenius at 2, a_2.

Remarks (1) There is a unique such field K because 2 is inert in $\mathbf{Q}(\sqrt{-N})$ and 3 does not divide $h(\mathbf{Q}(\sqrt{-N}))$.

(2) By Cohen-Lenstra heuristics, 47% of N should satisfy $3 \nmid h(\mathbf{Q}(\sqrt{N}))h(\mathbf{Q}(\sqrt{-N}))$. Apparently most (but not all, e.g. 571) of these N have $h(M)$ odd. Some of these satisfy the condition on the fundamental unit (e.g. $N = 11, 67, 179, ...$); some don't (e.g. $N = 19, 43, 163, ...$).

(3) The prime N may satisfy the hypotheses of the theorem but there be no elliptic curve over $\mathbf{Q}$ of conductor N, e.g. $N = 227, 251, ...$ [5].

1. The Basic Set-up and Elementary Properties

Let E be an elliptic curve over $\mathbf{Q}$ of conductor N. Let $\overline{\rho}$:Gal$(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{F}_2)$ give the action of Galois on the 2-division points of E. The curve E has no rational points of order 2 since its conductor is neither 17 nor of the form $u^2 + 64$ (i.e. it is not a Setzer-Neumann curve) [13].

Using work of Brumer and Kramer [5] based on work of Serre [11], we can deduce various properties of E and $\overline{\rho}$. Firstly, plus or minus the discriminant of a semistable elliptic curve with no rational point of order 2 is never a perfect square. It follows that E has supersingular reduction at 2, since $\mathbf{Q}(\sqrt{\Delta})$ (Δ the discriminant of E) is $\mathbf{Q}(\sqrt{N})$ or $\mathbf{Q}(\sqrt{-N})$ and so has no unramified cyclic cubic extensions by the hypotheses of the theorem.

Secondly, since E is supersingular modulo 2, its 2-division field is a cyclic cubic extension of $\mathbf{Q}(\Delta)$ unramified outside 2 and totally ramified at 2, and moreover 2 is inert in $\mathbf{Q}(\Delta)/\mathbf{Q}$. From this it follows that $\mathbf{Q}(\sqrt{\Delta}) = \mathbf{Q}(\sqrt{-N})$, that $\overline{\rho}$ is surjective, and that the 2-division field of E (i.e. the fixed field of ker $\overline{\rho}$) is K.

2. The Faltings-Serre Method [12]

Suppose that E' is another elliptic curve over $\mathbf{Q}$ with conductor N and the same trace of Frobenius at 2. Assume that E' is not isogenous to E. Let ρ, ρ' :Gal$(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{Z}_2)$ give the action of Galois on the Tate modules $T_2(E), T_2(E')$ respectively. By Faltings [7], ρ and ρ' are not isomorphic. By section 1, their reductions modulo 2 are isomorphic.

Pick the largest α such that ρ and ρ' are isomorphic modulo 2^α. Replacing ρ' by a conjugate if necessary, we can assume that they are equal modulo 2^α.

Define σ :Gal$(\overline{\mathbf{Q}}/\mathbf{Q}) \to M_2(\mathbf{F}_2)^0 \rtimes GL_2(\mathbf{F}_2)$ by

$$\sigma(x) = ((\rho'(x) - \rho(x))/2^\alpha (\text{mod } 2),\ \overline{\rho}(x)),$$

where $M_2(\mathbf{F}_2)^0$ denotes the 2×2 matrices over $\mathbf{F}_2$ of trace zero (mapped to since det ρ equals det ρ'). Let $\tilde{K}$ be the fixed field of ker σ.

3. The Proof of the Main Theorem

The idea of the Faltings-Serre method is to use it to produce a representation σ that can then be shown not to exist by methods of algebraic number theory (in particular tables of number fields). This then shows that there cannot be two non-isogenous curves with the properties stated in the main theorem.

Proposition (3.1) The extension $\tilde{K}/K$ is unramified outside N.

Proof Since E has supersingular reduction at 2, the theorem of Honda-Hill-Cartier [8] implies that the characteristic polynomial of the formal group associated to E at 2 is the same as the characteristic polynomial of the system of ℓ-adic representations at 2. This says that a_2 determines the formal group at 2 of E, which determines the 2-adic representation of a decomposition group D_2 at 2, i.e. $\rho|_{D_2} \cong \rho'|_{D_2}$. If $x \in D_2$ (so in particular if x is in an inertia group at 2), then $\sigma(x) = (0, \overline{\rho}(x))$.

It remains to show that such an extension $\tilde{K}/K$ cannot exist. The key idea is to use two results of Nicole Moser [10]. The first one is:

$$(1)\quad h(K) = (ah(M)^2 h(\mathbf{Q}(\sqrt{-N}))/3 \quad (a = 1 \text{ or } 3)$$

Proposition (3.2) The class number $h(K)$ is odd.

Proof This follows from the above formula (1), from our hypothesis that $h(M)$ is odd, and from genus theory, which tells us that $h(\mathbf{Q}(\sqrt{-N}))$ is odd (since N is prime).

Secondly, Moser showed [10] that K has a Minkowski unit, i.e. a single generator of its unit group modulo torsion as a $\mathbf{Z}[\mathrm{Gal}(K/\mathbf{Q})]$-module. To apply this, consider by global class field theory the exact sequence of $\mathbf{F}_2[\mathrm{Gal}(K/\mathbf{Q})]$-modules:

$$0 \to B \to \overline{U} \to \oplus_{\wp|N} \overline{U}_\wp \to \overline{P} \to 0,$$

where $\overline{U}$ is the global units of K modulo squares, $\overline{U}_\wp$ is the local units of $K_\wp$ modulo squares, and $\overline{P}$ is the Galois group over K of a maximal elementary 2-abelian extension L unramified outside the primes of K above N.

Now $\dim_{\mathbf{F}_2} \overline{U} = 3, \dim_{\mathbf{F}_2} \overline{U}_\wp = 1$ implying that $\dim_{\mathbf{F}_2} \overline{P} = \dim_{\mathbf{F}_2} B$. Since $\tilde{K} \subseteq L$, it remains to show that $B = 0$. The existence of a Minkowski unit implies that $\overline{U} \equiv \{\pm 1\} \oplus V$, where V is an irreducible 2-dimensional $\mathbf{F}_2[\mathrm{Gal}(K/\mathbf{Q})]$-module. So we just need an element of V which is not in one of the kernels from $\overline{U} \to \overline{U}_\wp$. The image in V of the unit in the hypotheses of the theorem satisfies this.

4. Examples

(1) $N = 11$. There is an elliptic curve over $\mathbf{Q}$ of conductor 11, namely $(11_A) y^2 + y = x^3 - x^2$. Let E be another such. Then [5], [13] $\overline{\rho}$ is determined, E has

supersingular reduction at 2, and M has odd class number. In fact M is the cubic field of discriminant -44. By [6] a fundamental unit of M has minimum polynomial x^3+x^2+x-1, which factors modulo 11 as $(x+3)^2(x+6)$. Since -3 is a quadratic non-residue modulo 11, theorem 1 shows that every elliptic curve over $\mathbf{Q}$ of conductor 11 with $a_2=-2$ is isogenous to (11_A).

As in Serre's original letter [12], this classifies up to isogeny every elliptic curve over $\mathbf{Q}$ of conductor 11, because a similar argument to the above shows that an elliptic curve with good reduction outside 11 and $a_2=2$ (respectively $a_2=0$) is isogenous to (121_A) (respectively (121_D)).

(2) $N=67$. There is an elliptic curve over $\mathbf{Q}$ of conductor 67, namely $(67_A)y^2+y=x^3+x^2-12x-21$. Let E be another such. Then [5], [13] $\overline{\rho}$ is determined, E has supersingular reduction at 2, and M has odd class number. In fact M is the cubic field of discriminant -268. By [6] a fundamental unit of M has minimum polynomial $x^3-7x^2+13x-1$, which factors modulo 67 as $(x+16)^2(x+28)$. Since -16 is a quadratic non-residue modulo 67, theorem 1 shows that every elliptic curve over $\mathbf{Q}$ of conductor 67 with $a_2=2$ is isogenous to (67_A).

The same argument as for $N=11$ now applies, because the twist of (67_A) by the quadratic character associated to $\mathbf{Q}(\sqrt{-67})$ is an elliptic curve of conductor 67^2 with $a_2=-2$ and with the same $\overline{\rho}$ and the curve of CM type relative to $\mathbf{Q}(\sqrt{-67})$ is an elliptic curve of conductor 67^2 with $a_2=0$ and the same $\overline{\rho}$.

5. Deformation Spaces of Galois Representations.

The homomorphisms ρ and ρ' are lifts of the same $\overline{\rho}$ to $\mathbf{Z}_2$. They therefore lie in the deformation space of lifts of $\overline{\rho}$ [3]. The Faltings-Serre method constructs from them a third lift σ to the dual numbers $\mathbf{F}_2[\epsilon]$ $(\epsilon^2=0)$. We consider below some applications of this idea.

Let $\overline{\rho}:\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\to GL_2(\mathbf{F}_p)$ be an absolutely irreducible representation. Let $\mathcal{C}$ denote the category of complete, noetherian local rings with residue field $\mathbf{F}_p$. Objects of this category are rings of the form $\mathbf{Z}_p[[T_1,...,T_r]]/I$. If R is such a ring, then two representations $\rho_1,\rho_2:\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\to GL_2(R)$ will be called *strictly equivalent* if conjugate by an element of $\Gamma_2(R):=\ker(GL_2(R)\to GL_2(\mathbf{F}_p)$. A strict equivalence class of lifts of $\overline{\rho}$ is called a *deformation* of $\overline{\rho}$. Fix a finite set of rational primes S containing the primes ramified in $\overline{\rho}$.

Define a functor $\mathcal{F}:\mathcal{C}\dashrightarrow \mathit{Sets}$ by:

$\mathcal{F}(R)=\{\text{deformations of }\overline{\rho}\text{ to }R\text{ unramified outside }S\}$

Mazur [9] proved that $\mathcal{F}$ is representable, i.e. that there exists a representation $\xi:\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\to GL_2(\mathcal{R})$ (the universal deformation) lifting $\overline{\rho}$ and parametrizing lifts of $\overline{\rho}$ to R in $\mathcal{C}$ unramified outside S up to strict equivalence via $\mathrm{Hom}(\mathcal{R},R)$. The set $\mathrm{Hom}(\mathcal{R},\overline{\mathbf{Z}}_p)$ will be called the deformation space of lifts of $\overline{\rho}$.

At the joint AMS-LMS conference in Cambridge, England, in 1992, I suggested that deformation spaces of Galois representations should have some special properties. In particular, it appears that they are often coordinatized by their restrictions to various inertia subgroups I_ℓ $(\ell\in S)$, namely (i) the restrictions to I_ℓ $(\ell\in S-\{p\})$ should indicate which component the lift is on and (ii) the restriction to I_p should

indicate where the lift is on that component. This idea is now to use the Faltings-Serre method to prove some cases of (ii). The novelty of this approach lies in replacing the prime 2 by more general primes. See [3] for a further discussion of this.

Example (1) Let E be the elliptic curve $X_0(49)$. This is an elliptic curve over $\mathbf{Q}$ of conductor 49. In [4], it is calculated that the universal deformation ring of the Galois representation given by the 3-division points of E with $S = \{3, 7\}$ is $\mathbf{Z}_3[[T_1, T_2, T_3, T_4]]/((1 + T_4)^3 - 1)$. Thus its deformation space splits into three explicitly given components $\{T_4 = 0\}, \{T_4 = \omega - 1\}, \{T_4 = \omega^2 - 1\}$, where ω is a primitive 3rd root of unity, and as shown in [4] any lift to $\mathbf{Z}_3$ lies on the first component. Also, (i) above holds. In other words, the image of an inertia group at 7 determines on which component a representation over $\overline{\mathbf{Z}}_3$ lies.

Now let ρ and ρ' be two lifts of $\overline{\rho}$ to $\mathbf{Z}_3$ (so lying on the first component). Suppose that they agree on inertia at 3. We shall show that they are actually strictly equivalent (so give the same point in the deformation space).

Assume for now they are not strictly equivalent. Since $\overline{\rho}$ is absolutely irreducible, two lifts are strictly equivalent if and only if they are isomorphic. For suppose that $\rho' = A^{-1}\rho A$ with $A \in GL_2(\mathbf{Z}_p)$. Then A centralizes the image of $\overline{\rho}$ and so by Schur the image of A in $GL_2(\mathbf{F}_p)$ is a scalar matrix, i.e. $A = BC$ where B is scalar and $C \in \Gamma_2(\mathbf{Z}_p)$. But then $\rho' = C^{-1}\rho C$.

Since ρ and ρ' are not isomorphic, σ defines a homomorphism from $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ into the semidirect product $M_2(\mathbf{F}_3) \rtimes GL_2(\mathbf{F}_3) (\cong GL_2(\mathbf{F}_3[\epsilon]), \epsilon^2 = 0)$ unramified outside $S = \{3, 7\}$. Letting K and $\tilde{K}$ denote, as before, the fixed fields of $\overline{\rho}$ and σ respectively, we get that $\tilde{K}/K$ is unramified outside 7. It is also unramified outside 3 because (i) holds, i.e. ρ and ρ' agree on inertia at 3. Such an everywhere unramified field extension of K does not exist, since its Galois group would be a quotient of the ideal class group killed by 3 with $\mathrm{Gal}(K/\mathbf{Q})$ acting via the adjoint action. This is excluded as explained in [4] by the work of Coates and Flach since 3 does not divide the numerator of a certain special value of the L-function of the symmetric square of E.

(2) Following [9], let p be a prime number of the form $27 + 4a^3$ and K be a splitting field over $\mathbf{Q}$ for $x^3 + ax + 1$. Embedding $\mathrm{Gal}(K/\mathbf{Q}) \cong S_3$ in $GL_2(\mathbf{F}_p)$, we obtain a representation $\overline{\rho}$:$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{F}_p)$ unramified outside p. Letting $S = \{p\}$, Mazur showed that $\mathcal{R} \cong \mathbf{Z}_p[[T_1, T_2, T_3]]$.

Let ρ and ρ' be lifts of $\overline{\rho}$ to $\mathbf{Z}_p$ unramified outside S. Suppose that they agree on inertia at p, but are not strictly equivalent. Then they produce, as in (1), an unramified p-extension of the fixed field of $\ker \overline{\rho}$, but as Mazur showed in [9], $p \nmid h(K)$, a contradiction thereby proving (ii) in this case.

References

1. M.Agrawal, J.Coates, D.Hunt, and A.van der Poorten, *Elliptic curves of conductor* 11, Math. Comp. **35** (1980), 991-1002.
2. I.O.Angell, *A table of complex cubic fields.*

3. N.Boston, *Deformations of Galois representations*, (a monograph), in preparation.
4. N.Boston and S.V.Ullom, *Representations related to CM elliptic curves*, Math. Proc. Camb. Phil. Soc. **113** (1993), 71-85.
5. A.Brumer and K.Kramer, *The rank of elliptic curves*, Duke Math. J. **44, no. 4** (1977), 715-742.
6. B.N.Delone and D.K.Faddeev, *The theory of irrationalities of the third degree*, AMS, Providence, RI, 1964.
7. G.Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern* **73** (1983), 349-366.
8. W.Hill, *Formal groups and zeta-functions of elliptic curves*, Invent. Math. **12** (1971), 321-336.
9. B.Mazur, *Deforming Galois representations*, Proceedings of the March 1987 Workshop on "Galois groups over **Q**" held at MSRI, Berkeley, California.
10. N.Moser, *Unités et nombre de classes d'une extension galoisienne diédrale de* **Q**, Abh. Math. Sem. Univ. Hamburg **48** (1979), 54-75.
11. J.-P.Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.
12. J.-P.Serre, letter to Tate, Oct. 26, 1984.
13. B.Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. **10** (1975), 367-378.