The non-existence of certain mod 2 Galois representations of some small quadratic fields

By Hyunsuk MOON[*)] and Yuichiro TAGUCHI[**)]

(Communicated by Shigefumi MORI, M.J.A., April 14, 2008)

Abstract: For a few quadratic fields, the non-existence is proved of continuous irreducible mod 2 Galois representations of degree 2 unramified outside $\{2, \infty\}$.

Key words: Mod p Galois representation; non-existence; Serre's modularity conjecture.

1. Introduction.

In this paper, we prove the following theorem, which settles some special cases of versions (cf. Conj. 1.1 of [3]; Conj. 1 of [12]; and Question 1 of [5]) of Serre's modularity conjecture [15,17] for a few quadratic fields:

Theorem. *Let F be one of the following quadratic fields*:

$$\mathbf{Q}(\sqrt{-1}), \mathbf{Q}(\sqrt{\pm 2}), \mathbf{Q}(\sqrt{\pm 3}), \mathbf{Q}(\sqrt{\pm 5}), \mathbf{Q}(\sqrt{\pm 6}).$$

Then there exist no continuous irreducible representations $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbf{F}}_2)$ unramified outside $\{2, \infty\}$.

Here, G_F denotes the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$ of F, and $\overline{\mathbf{F}}_2$ is an algebraic closure of the finite field $\mathbf{F}_2$ of two elements.

The proof is based on the method of discriminant bound as in [1,2,7,8,11,16,19]. However, we need to improve the known upper bounds at the prime 2. This is done in Section 2. The proof of the Theorem is given in Section 3.

It is desirable to have such a theorem for mod p representations for other primes p, but this seems almost impossible at least by our method.

The first version of this paper did not include the cases of $\mathbf{Q}(\sqrt{\pm 6})$. After it was circulated, M. H. Şengün communicated to us that, combining his lower bound in [13] and our upper bound in Section 2, he could prove the non-existence in these cases. Then we examined those cases and found that our proof actually covered them as well. Thus we are grateful to him very much for his communication.

Some additional results on the finiteness and non-existence of mod 2 Galois representations of quadratic fields can be found in [8].

Convention. For a finite extension E/F of non-Archimedean local fields, we denote by $\mathcal{D}_{E/F}$ the different ideal of E/F. The 2-adic valuation v_2 is normalized by $v_2(2) = 1$, and is used to measure the order of ideals (such as $\mathcal{D}_{E/F}$) in algebraic extensions of the 2-adic field $\mathbf{Q}_2$. We denote by $\begin{pmatrix} * & * \\ & * \end{pmatrix}$ and $\begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}$ respectively the *subgroups* $\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\}$ and $\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\}$ of $\mathrm{GL}_2(\overline{\mathbf{F}}_2)$.

2. Local lemmas.

Let F be a finite extension of $\mathbf{Q}_2$, $D = G_F$ its absolute Galois group, and I its inertia subgroup. In this section, we consider mod 2 representations $\rho : D \to \mathrm{GL}_2(\overline{\mathbf{F}}_2)$ of D. Let E/F be the extension cut out by ρ. We shall estimate the different $\mathcal{D}_{E/F}$ of E/F. Let E_0 (resp. E_1) be the maximal unramified (resp. tamely ramified) subextension of E/F, and let $e_1 = [E_1 : E_0]$ be the tame ramification index of E/F. Then we have $\mathcal{D}_{E/F} = \mathcal{D}_{E/E_1}\mathcal{D}_{E_1/E_0}$, and $v_2(\mathcal{D}_{E_1/E_0}) = (1 - 1/e_1)/e_F$, where e_F is the ramification index of $F/\mathbf{Q}_2$. Thus it remains for us to calculate $\mathcal{D}_{E/E_1}$. We assume E/F is wildly ramified, with wild ramification index 2^m. Then the wild inertia subgroup G_1 of $G := \mathrm{Im}(\rho)$ is a non-trivial 2-group and, after conjugation, we may assume it is contained in $\begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}$. Since G_1 is normal in G and the normalizer of G_1 in $\mathrm{GL}_2(\overline{\mathbf{F}}_2)$ is $\begin{pmatrix} * & * \\ & * \end{pmatrix}$, we may assume that ρ is of the form

$$\rho = \begin{pmatrix} \psi_1 & * \\ & \psi_2 \end{pmatrix}, \tag{2.1}$$

where $\psi_i : D \to \overline{\mathbf{F}}_2^{\times}$ are characters of D. Note that the ψ_i's have odd order, so that they are at most tamely ramified.

Lemma 1. *Let the notation be as above. Assume further that $F/\mathbf{Q}_2$ has ramification index*

2000 Mathematics Subject Classification. Primary 11R39, 11F80, 11R32.

[*)] Department of Mathematics, College of Natural Sciences, Kyungpook National University, Daegu 702-701, Korea.

[**)] Graduate School of Mathematics, Kyushu University 33, Fukuoka 812-8581, Japan.

2. *If E/F has ramification index 2^m (i.e. if $e_1 = 1$), then there exists a non-negative integer $m_2 \le m$ such that*

$$v_2(\mathcal{D}_{E/F}) = \begin{cases} \frac{9}{4} - \frac{2^{m_2}+1}{2^m} & \textit{and} \quad m_2 \le m-1; \textit{ or} \\ 2 - \frac{2^{m_2}+1}{2^m}. \end{cases}$$

If ρ is non-abelian, then the former case does not occur.

Here, we say ρ is (non-)abelian if the group $\mathrm{Im}(\rho)$ is (non-)abelian.

Proof. By assumption, we have $E_1 = E_0$ and the characters ψ_i are unramified. By local class field theory, the Galois group $G_1 = \mathrm{Gal}(E/E_1)$, which is an elementary 2-group, is identified with a quotient of the group $(1+\pi A)/(1+\pi A)^2$, where A is the ring $\mathcal{O}_{E_1}$ of integers of E_1, π is a uniformizer of A, and $(1+\pi A)^2$ is the subgroup of the square elements in the multiplicative group $(1+\pi A)$. The character group $X = \mathrm{Hom}(G_1, \mathbf{C}^\times)$ of G_1 is identified with a subgroup of $\mathrm{Hom}((1+\pi A)/(1+\pi A)^2, \mathbf{C}^\times)$. The subgroup X_i of X consisting of the characters with conductor dividing π^i is identified with a subgroup of $\mathrm{Hom}((1+\pi A)/(1+\pi^i A)(1+\pi A)^2, \mathbf{C}^\times)$. It is easy to see that

$$\{1\} = X_1 \subset X_2 = X_3 \subset X_4 \subset X_5 = X.$$

Indeed, the equality $X_2 = X_3$ follows from the fact that $(1+\pi^2 A) = (1+\pi^3 A)(1+\pi A)^2$, and the equality $X_5 = X$ follows from the fact that $(1+\pi^5 A) \subset (1+\pi A)^2$; cf. the proof of Lemma 2.1 of [7]. Just as in [19], we can show that the index $(X_5 : X_4)$ is 1 or 2, since the image of $(1+\pi^4 A)$ in $(1+\pi A)/(1+\pi A)^2$ has order 2. To see this, consider the equation

$$1 + a\pi^4 = (1 + x\pi^2)^2 \tag{2.2}$$

for a given $a \in A^\times$ and unknown $x \in A^\times$. If $2 = c\pi^2$ with $c \in A^\times$, then the equation (2.2) has a solution x if and only if the congruence

$$cx + x^2 \equiv a \pmod{\pi}$$

has a solution. Since the $\mathbf{F}_2$-linear map $\wp : A/\pi A \to A/\pi A$ given by $x \mapsto cx + x^2$ has $\dim_{\mathbf{F}_2} \mathrm{Coker}(\wp) = 1$, the equation (2.2) has a solution for "half" of the a's.

By assumption, X_5 has order 2^m. Suppose X_2 has order 2^{m_2}. Then the 2-adic order of the different $\mathcal{D}_{E/F} = \mathcal{D}_{E/E_1}$ can be calculated as follows by using the Führerdiskriminantenproduktformel ([14], Chap. VI, §3):

(1-i) If $(X_5 : X_4) = 2$, then

$$\begin{aligned} v_2(\mathcal{D}_{E/F}) &= \frac{1}{2} \cdot \frac{1}{2^m} \big((2^m - 2^{m-1}) \times 5 \\ &\qquad + (2^{m-1} - 2^{m_2}) \times 4 + (2^{m_2} - 1) \times 2\big) \\ &= \frac{9}{4} - \frac{2^{m_2}+1}{2^m}. \end{aligned}$$

(1-ii) If $(X_5 : X_4) = 1$, then

$$\begin{aligned} v_2(\mathcal{D}_{E/F}) &= \frac{1}{2} \cdot \frac{1}{2^m} ((2^m - 2^{m_2}) \times 4 + (2^{m_2} - 1) \times 2) \\ &= 2 - \frac{2^{m_2}+1}{2^m}. \end{aligned}$$

Let ψ_i be the characters in (2.1). If ρ is non-abelian (or equivalently, if $\psi_1 \ne \psi_2$ as characters on D), then $\mathrm{Gal}(E_0/F) = G/G_1$ acts on G_1 (identified with a subgroup of $\left(\begin{smallmatrix}1 & * \\ & 1\end{smallmatrix}\right)$) via $\psi_1\psi_2^{-1}$ (cf. [11], Proof of Prop. 2.3). This induces a similar action on X which respects the filtration X_i. Each orbit in $X_5 \smallsetminus X_4$ by this action has odd cardinality $|\mathrm{Im}(\psi_1\psi_2^{-1})|$, while $X_5 \smallsetminus X_4$ has 2-power cardinality if it is non-empty. Thus we must have $X_5 = X_4$, and we are in the case (1-ii) above. □

Specializing the $F/\mathbf{Q}_2$, we calculate the value of $v_2(\mathcal{D}_{E/F})$ more precisely as follows:

Lemma 2. *Assume $F/\mathbf{Q}_2$ is a totally ramified quadratic extension. Then the extension E/F has ramification index 2^m. If ρ is non-abelian, then there exists a non-negative integer $m_2 \le m$ such that*

$$v_2(\mathcal{D}_{E/F}) = 2 - \frac{2^{m_2}+1}{2^m}.$$

If ρ is abelian, then we have $m \le 3$ and $v_2(\mathcal{D}_{E/F}) \le 15/8$. In fact, more precisely, we have:

$$v_2(\mathcal{D}_{E/F}) = \begin{cases} 15/8 & \textit{if } m = 3, \\ 7/4, 3/2 \textit{ or } 5/4 & \textit{if } m = 2, \\ 5/4, 1 \textit{ or } 1/2 & \textit{if } m = 1. \end{cases}$$

Proof. $F/\mathbf{Q}_2$ being totally ramified, any abelian extension of F has no non-trivial tame ramification since $\mathcal{O}_F^\times$ is a pro-2 group. Thus the characters ψ_i in (2.1) are unramified, and E/F has ramification index 2^m.

If ρ is non-abelian, then $v_2(\mathcal{D}_{E/F})$ has the second value in Lemma 1. If ρ is abelian (or equivalently, if $\psi_1 = \psi_2$ as characters on D), then G_1 is identified with a quotient of $\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^2$. The group $\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^2$ has order 8. The different is the largest in the case where $G_1 \simeq \mathcal{O}_F^\times/(\mathcal{O}_F^\times)^2$, in which case $m = 3$, $(X_5 : X_4) = (X_4 : X_3) = (X_2 : X_1) = 2$, and

$$v_2(\mathcal{D}_{E/F}) = \frac{1}{2} \cdot \frac{1}{8}(4 \times 5 + 2 \times 4 + 1 \times 2) = \frac{15}{8}.$$

Other cases can be calculated similarly. Note that $(X_{i+1} : X_i) = 1$ or 2 since the residue field of $\mathcal{O}_F$ is $\mathbf{F}_2$. □

Recall that $e_1 = [E_1 : E_0]$ denotes the tame ramification index of E/F.

Lemma 3. *If $F/\mathbf{Q}_2$ is the unramified quadratic extension, then we have $e_1 = 1$ or 3. If ρ is non-abelian, there exist non-negative integers $m_2 \leq m_4 \leq m$ such that*

$$v_2(\mathcal{D}_{E/F}) = \begin{cases} 2 - \frac{1}{2^{m-1}} & \textit{if } e_1 = 1, \\ \frac{8}{3} - \frac{2^{m_4}+2^{m_2}+1}{3 \cdot 2^{m-1}} & \textit{if } e_1 = 3. \end{cases}$$

If ρ is abelian, then $m \leq 3$ and $v_2(\mathcal{D}_{E/F}) \leq 35/12$. In fact, more precisely, we have:

$$v_2(\mathcal{D}_{E/F}) = \begin{cases} 35/12 & \textit{if } m = 3, \\ 8/3 \textit{ or } 13/6 & \textit{if } m = 2, \\ 13/6 \textit{ or } 5/3 & \textit{if } m = 1, \end{cases}$$

if $e_1 = 3$. If $e_1 = 1$, then the values of $v_2(\mathcal{D}_{E/F})$ are the above values minus $2/3$.

Proof. By local class field theory, the characters ψ_i in (2.1) are identified with characters of $F^\times/(1 + 2\mathcal{O}_F)^\times$. Since $\mathcal{O}_F^\times/(1 + 2\mathcal{O}_F)^\times \simeq \mathbf{F}_4^\times$, the tamely ramified extension E_1/E_0 has degree either 1 or 3.

As in the proof of Lemma 1, identify the Galois group $G_1 = \mathrm{Gal}(E/E_1)$ (resp. the character group $X = \mathrm{Hom}(G_1, \mathbf{C}^\times)$) with a quotient of $(1 + \pi A)/(1 + \pi A)^2$ (resp. a subgroup of $\mathrm{Hom}((1 + \pi A)/(1 + \pi A)^2, \mathbf{C}^\times)$), where $A = \mathcal{O}_{E_1}$ and π is a uniformizer of A. Let X_i be the subgroup of X consisting of the characters of G_1 with conductor dividing π^i.

If $e_1 = 1$, then the value of $v_2(\mathcal{D}_{E/F})$ can be calculated as in Proposition 2.3 of [11]; we have $\{1\} = X_1 \subset X_2 \subset X_3 = X$ and $(X_3 : X_2) \leq 2$. If ρ is abelian (i.e. $\psi_1 = \psi_2$), then X is in fact identified with a subgroup of the character group of $(1 + 2\mathcal{O}_F)/(1 + 2\mathcal{O}_F)^2$, and one has $(X_2 : X_1) \leq 4$ since F has residue field $\mathbf{F}_4$. Thus $|X_3| \leq 8$, and

(2.3)
$$v_2(\mathcal{D}_{E/F}) = \begin{cases} \frac{1}{8}(4 \times 3 + 3 \times 2) = \frac{9}{4} & \text{if } m = 3, \\ \frac{1}{4}(2 \times 3 + 1 \times 2) = 2 \text{ or} & \\ \frac{1}{4}(3 \times 2) = \frac{3}{2} & \text{if } m = 2, \\ \frac{3}{2} \text{ or } \frac{2}{2} = 1 & \text{if } m = 1. \end{cases}$$

If ρ is non-abelian (i.e. $\psi_1 \neq \psi_2$), then as in the last part of the proof of Lemma 1, we have $X_3 = X_2$, and hence

$$v_2(\mathcal{D}_{E/F}) = \frac{1}{2^m}((2^m - 1) \times 2) = 2 - \frac{1}{2^{m-1}}.$$

Assume $e_1 = 3$. Then as in the proof of Lemma 1, one can show that

$$\{1\} = X_1 \subset X_2 = X_3 \subset X_4 = X_5 \subset X_6 \subset X_7 = X,$$

with $(X_7 : X_6) = 1$ or 2. By assumption, X_7 has order 2^m. Suppose $|X_2| = 2^{m_2}$ and $|X_4| = 2^{m_4}$. If ρ is abelian, then X is identified with a subgroup of the character group of $(1 + 2\mathcal{O}_F)/(1 + 2\mathcal{O}_F)^2$ (so $X_1 = X_2$ and $X_5 = X_6$), and $v_2(\mathcal{D}_{E/E_1})$ is calculated to have the same values as in (2.3). Adding the tame part $v_2(\mathcal{D}_{E_1/E_0}) = 2/3$, we see that $v_2(\mathcal{D}_{E/F})$ has the values as in the statement of the lemma. If ρ is non-abelian, then as in the former case, we have $X_7 = X_6$, and hence

$$\begin{aligned} v_2(\mathcal{D}_{E/E_1}) &= \frac{1}{3} \cdot \frac{1}{2^m}\big((2^m - 2^{m_4}) \times 6 \\ &\quad + (2^{m_4} - 2^{m_2}) \times 4 + (2^{m_2} - 1) \times 2\big) \\ &= 2 - \frac{2^{m_4} + 2^{m_2} + 1}{3 \cdot 2^{m-1}}. \end{aligned}$$

Adding the tame part, we obtain

$$v_2(\mathcal{D}_{E/F}) = \frac{8}{3} - \frac{2^{m_4} + 2^{m_2} + 1}{3 \cdot 2^{m-1}}.$$

□

3. Proof of the Theorem.

Suppose there were a continuous irreducible representation $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbf{F}}_2)$ unramified outside $\{2, \infty\}$. Let K/F be the extension cut out by ρ and $G = \mathrm{Im}(\rho)$ its Galois group. As in [19], we distinguish the two cases where G is solvable and non-solvable.

First we deal with the solvable case. If G is solvable, then it sits in an exact sequence

$$1 \to H \to G \to \mathbf{Z}/2\mathbf{Z} \to 1, \quad H \subset \overline{\mathbf{F}}_2^\times \times \overline{\mathbf{F}}_2^\times,$$

as in Theorem 1 in §22 of [18]. Hence K is an abelian

extension of odd degree, unramified outside $\{2,\infty\}$, over the quadratic extension K'/F corresponding to H. By using class field theory and noticing that $\mathbf{Q}(\sqrt{3})$ and $\mathbf{Q}(\sqrt{6})$ have narrow class number 2 (resp. $\mathbf{Q}(\sqrt{-5})$ and $\mathbf{Q}(\sqrt{-6})$ have class number 2), we can show that, for each $F=\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{6})$ (resp. $F=\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{-5})$, $\mathbf{Q}(\sqrt{-6})$), there are 7 possibilities (resp. 3 possibilities) for such K'. By examining Jones' tables [6], we find them as follows:
If $F=\mathbf{Q}(\sqrt{2})$, then
$K'=\mathbf{Q}(\sqrt{\pm\sqrt{2}})$, $\mathbf{Q}(\sqrt{1\pm\sqrt{2}})$, $\mathbf{Q}(\sqrt{2},\sqrt{-1})$, $\mathbf{Q}(\sqrt{2+\sqrt{2}})$, $\mathbf{Q}(\sqrt{-2+\sqrt{2}})$;
If $F=\mathbf{Q}(\sqrt{3})$, then
$K'=\mathbf{Q}(\sqrt{1\pm\sqrt{3}})$, $\mathbf{Q}(\sqrt{-1\pm\sqrt{3}})$, $\mathbf{Q}(\sqrt{3},\sqrt{-1})$, $\mathbf{Q}(\sqrt{3},\sqrt{2})$, $\mathbf{Q}(\sqrt{3},\sqrt{-2})$;
If $F=\mathbf{Q}(\sqrt{5})$, then
$K'=\mathbf{Q}(\sqrt{(1\pm\sqrt{5})/2})$, $\mathbf{Q}(\sqrt{-1\pm\sqrt{5}})$, $\mathbf{Q}(\sqrt{5},\sqrt{-1})$, $\mathbf{Q}(\sqrt{5},\sqrt{2})$, $\mathbf{Q}(\sqrt{5},\sqrt{-2})$;
If $F=\mathbf{Q}(\sqrt{6})$, then
$K'=\mathbf{Q}(\sqrt{2\pm\sqrt{6}})$, $\mathbf{Q}(\sqrt{-2\pm\sqrt{6}})$, $\mathbf{Q}(\sqrt{6},\sqrt{-1})$, $\mathbf{Q}(\sqrt{6},\sqrt{2})$, $\mathbf{Q}(\sqrt{6},\sqrt{-2})$;
If $F=\mathbf{Q}(\sqrt{-1})$, then
$K'=\mathbf{Q}(\sqrt{-1},\sqrt{2})$, $\mathbf{Q}(\sqrt{1\pm\sqrt{-1}})$;
If $F=\mathbf{Q}(\sqrt{-2})$, then
$K'=\mathbf{Q}(\sqrt{-2},\sqrt{-1})$, $\mathbf{Q}(\sqrt{\pm\sqrt{-2}})$;
If $F=\mathbf{Q}(\sqrt{-3})$, then
$K'=\mathbf{Q}(\sqrt{-3},\sqrt{-1})$, $\mathbf{Q}(\sqrt{-3},\sqrt{2})$, $\mathbf{Q}(\sqrt{-3},\sqrt{-2})$;
If $F=\mathbf{Q}(\sqrt{-5})$, then
$K'=\mathbf{Q}(\sqrt{-5},\sqrt{-1})$, $\mathbf{Q}(\sqrt{-5},\sqrt{2})$, $\mathbf{Q}(\sqrt{-5},\sqrt{-2})$;
If $F=\mathbf{Q}(\sqrt{-6})$, then
$K'=\mathbf{Q}(\sqrt{-6},\sqrt{-1})$, $\mathbf{Q}(\sqrt{-6},\sqrt{2})$, $\mathbf{Q}(\sqrt{-6},\sqrt{-2})$.
All these K' have class number either 1 or 2. Let $\mathcal{O}_{K',2}=\mathcal{O}_{K'}\otimes_{\mathbf{Z}}\mathbf{Z}_2$ denote the 2-adic completion of the integer ring $\mathcal{O}_{K'}$ of K'. Then its multiplicative group $\mathcal{O}_{K',2}^{\times}$ is isomorphic to the direct-product of $\mathbf{Z}_2^{\oplus 4}$ and a cyclic group of order dividing 12 (A nontrivial 3-torsion subgroup appears only if K' contains $\mathbf{Q}(\sqrt{-3})$ or $\mathbf{Q}(\sqrt{5})$). Thus there can exist an abelian extension K/K' of odd degree at most 3. But in each case, the 3-torsion subgroup of $\mathcal{O}_{K',2}^{\times}$ is killed (when the reciprocity map is applied) by the global unit $\zeta_3=(-1+\sqrt{-3})/2$ or $\varepsilon^2=(3+\sqrt{5})/2$ (N.B. The latter is totally positive). Thus there is no abelian extension K/K' of odd degree unramified outside $\{2,\infty\}$.

Remark. The quadratic fields F in the Theorem do not have abelian extensions of odd degree which are unramified outside $\{2,\infty\}$. Thus if a representation $\rho: G_F\to \mathrm{GL}_2(\overline{\mathbf{F}}_2)$ unramified outside $\{2,\infty\}$ has solvable image, then the image is unipotent, and the extension K/F cut out by ρ is contained in the compositum of the above seven (resp. three) quadratic extensions K' of F.

Next we prove the non-solvable case. This is done by the comparison of the Tate and Odlyzko bounds for discriminants. We denote by $d_{K/\mathbf{Q}}$ the discriminant of $K/\mathbf{Q}$, and $d_K^{1/n}=|d_{K/\mathbf{Q}}|^{1/n}$ the root discriminant of K, where $n=[K:\mathbf{Q}]$. By the Odlyzko bound [10], we have

$$d_K^{1/n}>\begin{cases}17.020 & \text{if } n\geq 120,\\ 20.895 & \text{if } n\geq 1000.\end{cases}$$

If $G=\mathrm{Gal}(K/F)$ is non-solvable, then $n=2|G|\geq 120$. On the other hand, by Lemmas 2 and 3, we have

$$d_K^{1/n}\leq\begin{cases}2\cdot 2^2=8 & \text{if } F=\mathbf{Q}(\sqrt{-1}),\\ 2\sqrt{2}\cdot 2^2<11.314 & \text{if } F=\mathbf{Q}(\sqrt{\pm 2}),\\ 2\sqrt{3}\cdot 2^2<13.857 & \text{if } F=\mathbf{Q}(\sqrt{3}),\\ \sqrt{3}\cdot 2^{35/12}<13.079 & \text{if } F=\mathbf{Q}(\sqrt{-3}),\\ \sqrt{5}\cdot 2^{35/12}<16.885 & \text{if } F=\mathbf{Q}(\sqrt{5}),\\ 2\sqrt{5}\cdot 2^2<17.889 & \text{if } F=\mathbf{Q}(\sqrt{-5}),\\ 2\sqrt{6}\cdot 2^2<19.596 & \text{if } F=\mathbf{Q}(\sqrt{\pm 6}).\end{cases}$$

Thus we have a contradiction in all cases but $F=\mathbf{Q}(\sqrt{-5})$ and $\mathbf{Q}(\sqrt{\pm 6})$. To deal with these three cases, let 2^m be the wild ramification index of K/F at 2. Then the 2-Sylow subgroup of G has order $\geq 2^m$. If $m\leq 2$, then by Lemma 2 applied to a 2-adic completion of K/F, we have $v_2(\mathcal{D}_{K/F})\leq 7/4$, and hence

$$d_K^{1/n}\leq\begin{cases}2\sqrt{5}\cdot 2^{7/4}<15.043 & \text{if } F=\mathbf{Q}(\sqrt{-5}),\\ 2\sqrt{6}\cdot 2^{7/4}<16.479 & \text{if } F=\mathbf{Q}(\sqrt{\pm 6}),\end{cases}$$

which contradicts the Odlyzko bound. If $m\geq 3$, then by §§251–253 of [4], the image of G in $\mathrm{PGL}_2(\overline{\mathbf{F}}_2)$ contains a conjugate of $\mathrm{PSL}_2(\mathbf{F}_8)$, which has order 504. Hence the Odlyzko bound applies with $n=2|G|>1000$, whence a contradiction in the remaining cases as well. □

Acknowledgments. The writing of this paper was greatly encouraged by "Ecole d'été sur la conjecture de modularité de Serre", Luminy, 9–20, July, 2007. We thank its organizers, especially J.-M. Fontaine, and speakers for their big efforts. We thank also A. Ash, F. Diamond, S. Hattori, C.

Khare, K. Klosin, T. Saito, J.-P. Serre and R. Taylor for their information on the literature on various versions of Serre's modularity conjecture and/or comments on the first version of this paper.

The first author was supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD) (KRF-2006-531-C00004). The main part of this work was done while the second author was visiting Pohang University of Science and Technology; he thanks YoungJu Choie and POSTECH for their hospitality, and the Brain-Pool of KOFST for financial support. He thanks also Makoto Matsumoto for financial support by the JSPS Core-to-Core Program 18005.

References

[1] S. Brueggeman, The nonexistence of certain Galois extensions unramified outside 5, J. Number Theory **75** (1999), no. 1, 47–52.

[2] S. Brueggeman, The nonexistence of certain nonsolvable Galois extensions of number fields of small degree, Int. J. Number Theory **1** (2005), no. 1, 155–160.

[3] K. Buzzard, F. Diamond and F. Jarvis, On Serre's conjecrure for mod ℓ Galois representations over totally real fields. (Preprint). `http://www.unet.brandeis.edu/~fdiamond/bdj12.pdf`

[4] L. E. Dickson, *Linear Groups*, Teubner, 1901, Leibzig.

[5] L. M. Figueiredo, Serre's conjecture for imaginary quadratic fields, Compositio Math. **118** (1999), no. 1, 103–122.

[6] J. Jones, Tables of number fields with prescribed ramification. `http://math.asu.edu/~jj/numberfields/`

[7] H. Moon, Finiteness results on certain mod p Galois representations, J. Number Theory **84** (2000), no. 1, 156–165.

[8] H. Moon and Y. Taguchi, Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations, Doc. Math., Extra Vol. (2003), 641–654. (Electronic).

[9] H. Moon and Y. Taguchi, On the finiteness and non-existence of certain mod 2 Galois representations of quadratic fields, Kyungpook Math. J. **48** (2008), 323–330.

[10] A. M. Odlyzko, Discriminant bounds, (unpublished manuscript, 1976), available at: `http://www.dtc.umn.edu/~odlyzko/unpublished/index.html`

[11] K. Ono and Y. Taguchi, 2-adic properties of certain modular forms and their applications to arithmetic functions, Int. J. Number Theory **1** (2005), no. 1, 75–101.

[12] M. Schein, Weights in Serre's conjecture for Hilbert modular forms: the ramified case. (Preprint). `http://arxiv.org/abs/math.NT/0610488`

[13] M. H. Şengün, The non-existence of certain representations of the absolute Galois group of quadraticfields. (Preprint).

[14] J.-P. Serre, *Corps Locaux*, Deuxieme edition, Hermann, Paris, 1968.

[15] J.-P. Serre, Valeurs propres des opérateurs de Hecke modulo l, in *Journées Arithmétiques de Bordeaux* (*Conf., Univ. Bordeaux,* 1974), 109–117. Astérisque, Nos. 24–25, Soc. Math. France, Paris, 1975.

[16] J.-P. Serre, Note $229._2$ on p. 710, Œuvres III, Springer-Verlag, 1986.

[17] J.-P. Serre, Sur les représentations modulaires de degré 2 de Gal$(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.

[18] D. A. Suprunenko, *Matrix Groups*, Translated from the Russian, Translation edited by K. A. Hirsch, Amer. Math. Soc., Providence, R.I., 1976.

[19] J. Tate, The non-existence of certain Galois extensions of $\mathbf{Q}$ unramified outside 2, in *Arithmetic Geometry* (*Tempe, AZ,* 1993), 153–156, Contemp. Math., 174, Amer. Math. Soc., Providence, RI, 1994.