数理解析研究所講究録 1267 巻 2002 年 62-65

The Finiteness of Certain Mod p Galois Representations

九州大学 数理学研究院　文 賢淑

(Hyunsuk Moon, Kyushu Univ.)

The purpose of this contribution is to give a brief survey of some recent results of the author on the finiteness of certain mod p Galois representaions.

Let G_K be the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ of an algebraic number field K of finite degree over $\mathbb{Q}$ and $\overline{\mathbb{F}}_p$ an algebraic closure of the finite field $\mathbb{F}_p$ of p elements. We consider the following problem:

Problem. *Fix an integer $d \geq 1$ and a nonzero integral ideal N of K. Then do there exist only finitely many isomorphism classes of continuous semisimple representations $\rho : G_K \longrightarrow \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ with Artin conductor $N(\rho)$ outside p dividing N ?*

(See [M1] for the definition of $N(\rho)$.)

In the case $d = 1$, the finiteness in our Problem follows from class field theory. Also, the above Problem is reduced to the case $K = \mathbb{Q}$ by means of induction of representations.

This problem has been motivated by the celebrated conjecture of Serre ([Se]) which states that every odd and irreducible mod p representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ should arise from a modular eigenform f with conjectured level, weight and character. This implies that the set of isomorphism classes of such representations ρ with bounded conductor is finite because the space of modular forms of a bounded level and weight has a bounded dimension. A recent work of Ash and Sinnott ([A-S]), which generalize the conjecture of Serre, is also in favor of an affirmative answer to our Problem in certain cases.

This problem may be also regarded as a mod p version of the Finiteness conjecture of Fontaine-Mazur ([F-M]). Also, Khare ([Kh]) considers the same problem independently.

Now we give some remarks to explain why the conditions in the Problem are necessary:

Remarks. (1) Without any restriction on ramification outside p, we cannot expect the finiteness. For example, the set of isomorphism classes of $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_1(\overline{\mathbb{F}}_p)$ unramified outside $\ell(\neq p)$ is infinite, since we have, for each $n \geq 1$, the representation $\rho_n : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z} \hookrightarrow \overline{\mathbb{F}}_p^{\times}$ corresponding to the n-th layer of the cyclotomic $\mathbb{Z}_\ell$-extension of $\mathbb{Q}$.

(2) If we replace $\overline{\mathbb{F}}_p$ by a finite field $\mathbb{F}_{p^m}$, the finiteness follows from the Hermite-Minkowski Theorem saying that there exist only finitely many algebraic number fields which are of a given degree and unramified outside a given set of primes.

(3) The assumption of semisimplicity is necessary. In fact, there may be infinitely many (mutually unisomorphic) non-semisimple representations of a finite group G.

Now we consider the representations $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ unramified outside p, i.e., the case $K = \mathbb{Q}$ and $N(\rho) = 1$ of our Problem. For example, we obtain:

Theorem A ([M1]). *There exist only finitely many isomorphism classes of continuous semisimple Galois representations $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_4(\overline{\mathbb{F}}_2)$ unramified outside 2 such that the field $K/\mathbb{Q}$ corresponding to the kernel of ρ is totally real (in other words, ρ is unramified also at ∞).*

(For other cases, see [M1].)

The proof of this Theorem is based on comparing two estimates for discriminants of opposite directions. Using class field theory, we estimate from above the discriminant of a field K as in the Theorem in terms of the invariant "p-length" of its Galois group. For the other direction, we use the estimate of Odlyzko-Poitou-Serre which gives an asymptotic lower bound of discriminants. Then the finiteness follows from the contradiction of the two inequalities when the degree of K goes to infinity. This result extends a part of Tate's results for $d = 2$ and $p = 2$ ([Ta]).

Second, we obtained the finiteness in the solvable image case of our Problem:

Theorem B ([M-T]). *Given an integer $d \geq 1$ and a nonzero integral ideal N of K, there exist only finitely many isomorphism classes of continuous semisimple representations $\rho : G_K \longrightarrow \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ with solvable image and with $N(\rho)$ dividing*

The finiteness statement holds true also for classical Artin representations, i.e., if we replace $\overline{\mathbb{F}}_p$ by the complex number field $\mathbb{C}$ and $N(\rho)$ by the usual Artin conductor. This can be proved by using the finiteness of ideal class groups (or global class field theory) and the Hermite-Minkowski theorem. This suggests us to view our Problem, if answered affirmatively, as a generalization of these two. Also, the Problem can be reduced to a special case in which the image of ρ is a finite simple group of Lie type in characteristic p. This is based on a theorem of Larsen and Pink ([L-P]) on the structure of finite subgroups of $\mathrm{GL}_d(\overline{\mathbb{F}}_p)$. Furthermore, these results hold also for function fields K under a reasonable condition that there are no constant field extensions.

Third, we consider the set of n-dimensional monomial mod p representations of $G_{\mathbb{Q}}$ with bounded conductor. We say that a representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ is *monomial* if it is of the form $\rho = \mathrm{Ind}_K^{\mathbb{Q}}\chi$, i.e. if it is induced from a character $\chi : G_K \to \overline{\mathbb{F}}_p^{\times}$ of the absolute Galois group G_K of an algebraic number field K of degree n over $\mathbb{Q}$. From the construction together with the Hermite-Minkowski theorem and the finiteness of ray class groups, it follows easily that this set is finite. We shall give an explicit upper bounds for (i) the number of elements of this set and (ii) the order of the image of a $\rho = \mathrm{Ind}_K^{\mathbb{Q}}\chi$ as above in terms of n, p and the conductor:

Theorem C ([M2]). *Fix positive integers n and M. Consider n-dimensional monomial mod p Galois representations $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ with $N(\rho) \mid M$.*
(i) *The number of isomorphism classes of such ρ's is bounded by*

$$\frac{2^{n^2+n+1}\cdot(11.1)}{\pi^n}\left(2+\frac{1}{2}n^n p^{n-1}M\right)^n p^{2n-1}M^n.$$

(ii) *The order of the image of such a ρ is bounded by*

$$\frac{2^{n(n+1)}(11.1)^n}{\pi^{n^2}}n!n^{n^2}p^{n(2n-1)}M^{n^2}.$$

(A sharper estimate is given in [M2].)

The outline of the proof is:

First, we bound the discriminant of K and the conductor of χ when the conductor of $\rho = \mathrm{Ind}_K^{\mathbb{Q}}\chi$ is given. We give an upper bound of the number of algebraic number fields K of degree n and discriminant (outside p) dividing D in terms of n, p and D. For a given K, we give an upper bound for the number of characters χ of G_K with a given Artin conductor M. Combining these results together, we obtain the above Theorem (i). This is a quantitative result on our Problem. Finally, we deduce the estimate of the order of the image of $\mathrm{Ind}_K^{\mathbb{Q}}\chi$ from that of the image of χ by means of a group theoretic lemma. Such a statement (estimate of the order of the image of ρ) may be thought of as an effective result on our Problem.

References

[A-S] A. Ash and W. Sinnott, *An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod-p cohomology of* $\mathrm{GL}(n, \mathbb{Z})$, Duke Math. J. **105** (2000), 1–24.

[F-M] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, Elliptic Curves, Modular forms and Fermat's Last Theorem, 2nd ed. (J. Coates, S. T. Yau, eds.), International Press, 1997, pp. 190–227.

[Kh] C. Khare, *Conjectures on finiteness of mod p Galois representations*, J. Ramanujan Math. Soc. **15** (2000), 23–42.

[L-P] M. J. Larsen and R. Pink, *Finite subgroups of algebraic groups*, preprint (1998).

[M] H. Moon, *On the finiteness of mod p Galois representations*, Thesis, Tokyo Metropolitan University, 2000.

[M1] H. Moon, *Finiteness results on certain mod p Galois representations*, J. Number Theory **84** (2000), 156–165.

[M2] H. Moon, *The number of monomial mod p Galois representations with bounded conductor*, to appear in Tohoku Math. J.

[M-T] H. Moon and Y. Taguchi, *Mod p Galois representations of solvable image*, Proc. Amer. Math. Soc. **129** (2001), 2529–2534.

[Se] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.

[Ta] J. Tate, *The non-existence of certain Galois extensions of* $\mathbb{Q}$ *unramified outside 2*, Contemp. Math. **174** (1994), 153–156.