Tohoku Math. J.
55 (2003), 89–98

THE NUMBER OF MONOMIAL MOD p GALOIS REPRESENTATIONS WITH BOUNDED CONDUCTOR

HYUNSUK MOON

(Received January 29, 2001, revised November 7, 2001)

Abstract. An explicit upper bound is given for (i) the number of n-dimensional monomial mod p Galois representations of $G_{\boldsymbol{Q}}$ with bounded conductor and (ii) the order of the image of such a representation in terms of n, p, and the conductor.

1. Introduction. In this paper, we give an explicit upper bound for (i) the number of monomial mod p Galois representations $\rho : G_{\boldsymbol{Q}} \to \mathrm{GL}_n(\bar{\boldsymbol{F}}_p)$ and (ii) the order of the image of the representation ρ in terms of n, p, and the conductor. Here, $G_{\boldsymbol{Q}}$ is the absolute Galois group $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ of the rational number field $\boldsymbol{Q}$, and $\bar{\boldsymbol{F}}_p$ is an algebraic closure of the prime field $\boldsymbol{F}_p$ of p elements. We say that an n-dimensional representation $\rho : G_{\boldsymbol{Q}} \to \mathrm{GL}_n(\bar{\boldsymbol{F}}_p)$ is *monomial* if it is of the form $\rho = \mathrm{Ind}_K^{\boldsymbol{Q}}\chi$, i.e., if it is induced from a one-dimensional character χ of the absolute Galois group G_K of an algebraic number field K of degree n over $\boldsymbol{Q}$.

In general, for a continuous representation $\rho : G_K \to \mathrm{GL}_n(\bar{\boldsymbol{F}}_p)$, we denote by $N(\rho)$ its *Artin conductor outside* p;

$$N(\rho) = \prod_{\mathfrak{q}\nmid p} \mathfrak{q}^{n_{\mathfrak{q}}(\rho)},$$

where $\mathfrak{q}$ runs through the non-zero prime ideals of K not dividing p, and

$$n_{\mathfrak{q}}(\rho) := \sum_{i\geq 0} \frac{1}{(G_{\mathfrak{q},0} : G_{\mathfrak{q},i})} \dim_{\bar{\boldsymbol{F}}_p}(V/V^{G_{\mathfrak{q},i}}),$$

where $G_{\mathfrak{q},i}$ is the i-th ramification group of the decomposition group of an extension of $\mathfrak{q}$ to a splitting field of ρ, and V is the representation space for ρ (cf. [Se4], [M]). We shall prove:

THEOREM. *Fix positive integers n and M. Consider n-dimensional monomial* mod p *Galois representations $\rho : G_{\boldsymbol{Q}} \to \mathrm{GL}_n(\bar{\boldsymbol{F}}_p)$ with $N(\rho) \mid M$. Then the following hold.*

(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*

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

2000 *Mathematics Subject Classification.* Primary 11F80.

A sharper estimate will be given in Theorems 4.4 and 5.2.

Now we explain the motivation for giving such an estimate. In our previous works ([M], [MT]), we studied the following Finiteness Problem for mod p Galois representations: Given an algebraic number field K, a prime number p, a positive integer n and an integral ideal M of K, do there exist only finitely many continuous semisimple representations $\rho : G_K \to \mathrm{GL}_n(\bar{\boldsymbol{F}}_p)$ with $N(\rho) \mid M$? We showed in [M] that the answer is affirmative for $K = \boldsymbol{Q}$ and a few small values of n and p. Also, in the general setting, we proved in [MT] the finiteness for those ρ's with solvable image. For more discussions on this problem, we refer the reader to the Introductions of [M] and [MT]. This problem for the general case seems very difficult. For monomial representations, however, the finiteness follows fairly easily by using the Hermite-Minkowski theorem and the finiteness of the ray class groups. So our interest is now in quantitative results as in the above Theorem. For example, Serre gave an explicit upper bound of the number of representations $\rho : G_{\boldsymbol{Q}} \to \mathrm{GL}_2(\boldsymbol{C})$ coming from modular forms of weight 1 and prime level ([Se1]).

Meanwhile, Ash and Sinnott ([AS]) conjectured that mod p representations of $G_{\boldsymbol{Q}}$ satisfying certain conditions should come from Hecke eigenclasses in cohomology groups of congruence subgroups of $\mathrm{GL}_n(\boldsymbol{Z})$ (this conjecture also motivates our Problem). Ash ([A]) proved this conjecture for monomial representations of degree $p-1$. In view of this result, the monomial representations would be a first tractable case, and it would be worth while counting their number. Looking at Brauer's induction theorem, we hope that monomial representations would give a supply of a good portion of all the mod p representations, so that our estimate would be not too far from the truth even for all the n-dimensional representations with conductor dividing M.

We mention also a result of Brumer and Silverman ([BS]) in the same spirit as ours, which gives an explicit bound for the number of elliptic curves over $\boldsymbol{Q}$ with bounded conductor.

The outline of the paper is as follows: In Section 2, we bound the discriminant of K and the conductor of χ when the conductor of $\rho = \mathrm{Ind}_K^{\boldsymbol{Q}} \chi$ is given. In Section 3, 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. The bound of the p-part of the discriminant is classical. Once this is done, we may employ "geometry of numbers" to bound the number of K's. In Section 4, for a given K we give an upper bound for the number of characters χ of K with a given Artin conductor M. This amounts essentially to bounding the ray class group of K of conductor pM. The most essential is to bound the class number h_K. For the product $R_K h_K$ of the regulator and class number, an upper bound is well-known. We may then use Friedman's absolute lower bound ([F]) for R_K to obtain the desired upper bound for h_K. Combining these results together, we obtain our Main Theorem 4.4. In Section 5, we derive an upper bound of the image of ρ from the bound of the ray class group in Section 4 by group-theoretic arguments (Lemma 5.1).

I would like to express my gratitude to Yuichiro Taguchi who suggested studying the quantitative version of our Finiteness Problem. I thank also the referee for useful comments.

2. Discriminant of K and conductor of χ. Let K be an algebraic number field of degree n, d_K its discriminant and $\tilde{d}_K$ the prime-to-p part of d_K. Let χ be a one-dimensional mod p Galois representation of $G_K = \mathrm{Gal}(\bar{\boldsymbol{Q}}/K)$ and $N(\chi)$ its Artin conductor outside p. We consider the set of the induced representations

$$\rho = \mathrm{Ind}_K^{\boldsymbol{Q}} \chi : G_{\boldsymbol{Q}} \to \mathrm{GL}_n(\bar{\boldsymbol{F}}_p)\,,$$

with bounded conductor. Let M be a positive integer prime to p. If $N(\rho)$ is bounded by M, the discriminant $\tilde{d}_K$ and the conductor $N(\chi)$ of χ are bounded as follows.

LEMMA 2.1. *Let $\rho = \mathrm{Ind}_K^{\boldsymbol{Q}} \chi$. If $N(\rho)$ divides M, then $\tilde{d}_K$ divides M and $N(\chi)$ divides $M/\tilde{d}_K$.*

PROOF. By [Tag], the Artin conductor of an induced representation is calculated as follows:

$$\begin{aligned} N(\mathrm{Ind}_K^{\boldsymbol{Q}} \chi) &= N_{K/\boldsymbol{Q}}(N(\chi)) \cdot (\tilde{d}_K)^{\dim \chi} \\ &= N_{K/\boldsymbol{Q}}(N(\chi)) \cdot \tilde{d}_K\,. \end{aligned}$$

Hence we have $\tilde{d}_K \mid M$ and $N(\chi) \mid (M/\tilde{d}_K)$. □

By Lemma 2.1, the number of $\rho = \mathrm{Ind}_{\boldsymbol{Q}}^K \chi$ with $N(\rho) \mid M$ is bounded by the product of the following two; (i) the number of K's with $[K : \boldsymbol{Q}] = n$ and $\tilde{d}_K \mid M$, (ii) the maximum, when K as in (i) runs, of the number of characters χ of K with $N(\chi) \mid (M/\tilde{d}_K)$. The number of (i) will be estimated in Section 3 and the number of (ii) will be estimated in Section 4.

3. Number of K's. First, we begin with estimating the discriminant of K in terms of p, n and M. The following Lemma is basically well-known (cf. [Se3]).

LEMMA 3.1. *The p-part of the discriminant of an algebraic number field K of degree n is bounded by*

$$p^{n[\log_p n]+n-1}\,.$$

Note that $p^{n[\log_p n]+n-1} \leq n^n p^{n-1}$.

PROOF. Let $\mathfrak{p}$ be a prime ideal of K lying above p. If F denotes the completion of K at $\mathfrak{p}$ and $\mathcal{D}_{F/\boldsymbol{Q}_p}$ the different of $F/\boldsymbol{Q}_p$, then

$$\upsilon(\mathcal{D}_{F/\boldsymbol{Q}_p}) \leq \upsilon(e) + \frac{e-1}{e}\,,$$

where υ is the valuation of F normalized by $\upsilon(p) = 1$ and e is the ramification index of F. Indeed, we may assume that $F/\boldsymbol{Q}_p$ is totally ramified. Then the extension $F/\boldsymbol{Q}_p$ is defined by an Eisenstein polynomial

$$G(X) = X^e + a_1 X^{e-1} + \cdots + a_e\,, \quad p|a_i \quad \text{and} \quad \upsilon(a_e) = 1\,,$$

and the different $\mathcal{D}_{F/\boldsymbol{Q}_p}$ is generated by $G'(\pi)$, where π is a root of $G(X)$. Hence

$$\begin{aligned}\upsilon(\mathcal{D}_{F/\boldsymbol{Q}_p}) &= \upsilon\left(e\pi^{e-1} + \sum_{i=1}^{e-1}(e-i)a_i\pi^{e-i-1}\right)\\ &\le \upsilon(e\pi^{e-1})\\ &= \upsilon(e) + \frac{e-1}{e}\,.\end{aligned}$$

In general, if we let f be the residue degree of F and $m = ef$, then

$$\begin{aligned}\upsilon(d_F) &= \upsilon(N_{F/\boldsymbol{Q}_p}\mathcal{D}_{F/\boldsymbol{Q}_p})\\ &\le m\upsilon(e) + f(e-1)\,.\end{aligned}$$

Now we globalize this. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ be all the distinct prime ideals of K lying above p. Let K_i be the completion of K at $\mathfrak{p}_i$. Then K_i is an extension of $\boldsymbol{Q}_p$ of degree $n_i = e_i f_i$, where e_i is the ramification index of $\mathfrak{p}_i$ and f_i is the residue degree of $\mathfrak{p}_i$. Finally, we obtain

$$\begin{aligned}\upsilon(d_K) &= \sum_{i=1}^{g}\upsilon(d_{K_i})\\ &\le \sum_{i=1}^{g}(n_i\upsilon(e_i) + f_i e_i - f_i)\\ &= \sum_{i=1}^{g} n_i\upsilon(e_i) + n - \sum_{i=1}^{g} f_i\\ &\le n[\log_p n] + n - 1\,.\end{aligned}$$

Here we used the inequality $\upsilon(e_i) \le [\log_p n]$. □

The following estimate follows from the existence of a "small" integer ω of K, the existence being proved by Minkowski's methods of geometry of numbers (cf. [Tak, Chap. 5, §2] or [L, Chap. 5, §4, Proof of Thm. 5]).

LEMMA 3.2. *Let n and D be positive integers. Then*

$$\#\{K\,;\,[K:\boldsymbol{Q}] = n \text{ and } |d_K| \le D\}/_{\simeq} < \frac{2^{n^2}}{n^n}\cdot(2 + D/2)^n\,,$$

where $/_{\simeq}$ means "modulo isomorphism".

PROOF. If K is totally imaginary (resp. has a real place), there exists a primitive element ω, i.e., $K = \boldsymbol{Q}(\omega)$, in the ring of integers $\mathcal{O}_K$ such that

$$|\mathrm{Re}(\omega)| < 1\,,\quad |\mathrm{Im}(\omega)| \le D^{1/2}/2\,,\quad |\omega''| < 1, \ldots, |\omega^{(n-1)}| < 1$$

$$(\text{resp.}\quad |\omega| \le D^{1/2}\,,\quad |\omega'| < 1, \ldots, |\omega^{(n-1)}| < 1)\,.$$

Here $\omega^{(i)}$ are the conjugates of ω over $\boldsymbol{Q}$. To compute the number of K's, we compute the number of possible equations

$$X^n + a_1X^{n-1} + \cdots + a_n = 0\,,\quad a_i \in \boldsymbol{Z}\,,$$

for ω. Then the problem reduces to estimating the coefficients a_i. We have a worse estimate in the totally imaginary case, which is

$$\begin{aligned}
|a_1| &= \left|\sum_i \omega^{(i)}\right| < 2|\mathrm{Re}(\omega)| + n - 2 < n < \binom{n}{1}(1 + D/4)\,, \\
|a_2| &= \left|\sum_{i\neq j} \omega^{(i)}\omega^{(j)}\right| < \binom{n}{2}(1 + D/4)\,, \\
&\cdots \\
|a_n| &= \left|\prod_i \omega^{(i)}\right| < \binom{n}{n}(1 + D/4)\,.
\end{aligned}$$

Hence the number of K's (up to isomorphism) is bounded by

$$\begin{aligned}
\prod_{i=1}^{n}\left(2\binom{n}{i}(1 + D/4) + 1\right) &\le \left(\frac{1}{n}\sum_{i=1}^{n}\left(2\binom{n}{i}(1 + D/4) + 1\right)\right)^n \\
&= \left(\frac{2(1 + D/4)(2^n - 1) + n}{n}\right)^n \\
&< (2^n/n)^n(2 + D/2)^n\,.
\end{aligned}$$

Here, in the first inequality, we used the arithmetic-geometric mean inequality. In the second line, we used the equality $\sum_{i=0}^{n}\binom{n}{i} = 2^n$. In the last inequality, we used $n < 2 + D/2$, which follows from the classical estimate of Minkowski. □

REMARK. If we use a refinement of Minkowski's methods by Hunter (cf. [C, Chap. 9.3]), then the above Lemma 3.2 will be improved.

Combining Lemma 3.1 and Lemma 3.2, we obtain the following.

PROPOSITION 3.3. *For any positive integers n and M, we have*

$$\begin{aligned}
&\#\{K\ ;\ [K : \boldsymbol{Q}] = n \text{ and } \tilde{d}_K \mid M\}/_{\simeq} \\
&\quad\le \frac{2^{n^2}}{n^n}\left(2 + \frac{1}{2}p^{n[\log_p n]+n-1}M\right)^n\,.
\end{aligned}$$

4. Number of χ's. In this section, we bound the cardinality of the set

$$\{\chi\ :\ G_K \to \bar{\boldsymbol{F}}_p^{\times} \text{ with } N(\chi) \mid M\}\,.$$

Since $\bar{\boldsymbol{F}}_p^{\times}$ is a union of finite cyclic groups of order prime to p, the character χ is tamely ramified at prime ideals $\mathfrak{p}$ ($\subset K$) lying above p. Let $\mathfrak{m} = \prod_{\mathfrak{p}|p}\mathfrak{p}$ be the product of all the distinct primes dividing p, and $K_{\mathfrak{m}M}$ the maximal abelian extension of K with conductor

$\mathfrak{m}M$. Then χ factors through the Galois group $\mathrm{Gal}(K_{\mathfrak{m}M}/K)$ of $K_{\mathfrak{m}M}/K$;

$$\begin{array}{ccc} \chi\ :\ G_K & \longrightarrow & \bar{\boldsymbol{F}}_p^{\times} \\ & \searrow \quad \nearrow & \\ & \mathrm{Gal}(K_{\mathfrak{m}M}/K) & \end{array}$$

Because $\mathrm{Gal}(K_{\mathfrak{m}M}/K)$ is a finite abelian group, we only need to bound the size of $\mathrm{Gal}(K_{\mathfrak{m}M}/K)$ instead of bounding the number of χ's;

$$\#\{\chi\} \le \#\mathrm{Gal}(K_{\mathfrak{m}M}/K)\,. \tag{4.1}$$

By class field theory, this group is isomorphic to the ray class group modulo $\mathfrak{m}M$. In the adèlic language, we have

$$\mathrm{Gal}(K_{\mathfrak{m}M}/K) \simeq \frac{K_{\boldsymbol{A}}^{\times}}{K^{\times}\prod_{\upsilon}\mathcal{U}_{\upsilon}^{n_{\upsilon}}} \quad \text{if} \quad \mathfrak{m}M = \prod \upsilon^{n_{\upsilon}}\,,$$

where $K_{\boldsymbol{A}}^{\times}$ is the idèle group of K and $\mathcal{U}_{\upsilon}$ is the unit group of the completion K_{υ} of K at a place υ (resp. the connected component of $K_{\upsilon}^{\times}$) if υ is a finite place (resp. an infinite place). Also, $\mathcal{U}_{\upsilon}^{n_{\upsilon}}$ is the group of local units of $\mathcal{U}_{\upsilon}$ which are congruent to 1 modulo the n_{υ}-th power of the maximal ideal at υ. Now the ray class group $K_{\boldsymbol{A}}^{\times}/(K^{\times}\prod_{\upsilon}\mathcal{U}_{\upsilon}^{n_{\upsilon}})$ sits in the following exact sequence:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \dfrac{\prod\mathcal{U}_{\upsilon}}{(K^{\times}\cap\prod\mathcal{U}_{\upsilon})\prod\mathcal{U}_{\upsilon}^{n_{\upsilon}}} & \longrightarrow & \dfrac{K_{\boldsymbol{A}}^{\times}}{K^{\times}\prod\mathcal{U}_{\upsilon}^{n_{\upsilon}}} & \longrightarrow & \dfrac{K_{\boldsymbol{A}}^{\times}}{K^{\times}\prod\mathcal{U}_{\upsilon}} & \longrightarrow & 0\,. \\ & & \uparrow & & \wr| & & \wr| & & \\ & & \prod_{\upsilon|\mathfrak{m}M}\left(\dfrac{\mathcal{U}_{\upsilon}}{\mathcal{U}_{\upsilon}^{n_{\upsilon}}}\right) & & \mathrm{Gal}(K_{\mathfrak{m}M}/K) & & \widetilde{\mathcal{C}\ell}_K & & \end{array}$$

Here the left vertical arrow is surjective and $\widetilde{\mathcal{C}\ell}_K$ denotes the narrow ideal class group of K. If we let q_{υ} be the cardinality of the residue field of υ, then

$$\#\left(\frac{\mathcal{U}_{\upsilon}}{\mathcal{U}_{\upsilon}^{n_{\upsilon}}}\right) = (q_{\upsilon}-1)q_{\upsilon}^{n_{\upsilon}-1} < q_{\upsilon}^{n_{\upsilon}}\,.$$

Therefore

$$\#\left(\prod_{\upsilon|\mathfrak{m}M}\frac{\mathcal{U}_{\upsilon}}{\mathcal{U}_{\upsilon}^{n_{\upsilon}}}\right) < \prod_{\upsilon|\mathfrak{m}M} q_{\upsilon}^{n_{\upsilon}} \le p^n M^n\,.$$

LEMMA 4.1. *Let K be a number field of degree n. Then we have*

$$\#\mathrm{Gal}(K_{\mathfrak{m}M}/K) < 2^n \cdot h_K \cdot p^n \cdot M^n\,,$$

where h_K is the class number of K.

PROOF. By the above exact sequence, we have

$$\#\mathrm{Gal}(K_{\mathfrak{m}M}/K) \le \#(\widetilde{\mathcal{C}\ell}_K)\#\left(\prod_{\upsilon|\mathfrak{m}M}\frac{\mathcal{U}_{\upsilon}}{\mathcal{U}_{\upsilon}^{n_{\upsilon}}}\right) < 2^n \cdot h_K \cdot p^n \cdot M^n\,.$$

□

Since this result involves the class number, we need to estimate the class number only in terms of n, p and M. To estimate h_K, we first estimate the product of the class number h_K and the regulator R_K by using the integral expression of the zeta function.

LEMMA 4.2. *Let R_K be the regulator of a number field K and w_K the number of roots of unity in K. Then we have*

$$h_K R_K < 2\pi^{-n} w_K d_K .$$

PROOF. Let $\Lambda(s) = (2^{-2r_2}\pi^{-n}d_K)^{s/2}\Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\zeta_K(s)$. Then it satisfies the functional equation $\Lambda(1-s) = \Lambda(s)$, and the residue of $\Lambda(s)$ at $s = 1$ is

$$\lambda = \frac{2^{r_1} h_K R_K}{w_K} .$$

The function $\Lambda(s)$ has an integral expression of the form

$$\Lambda(s) = \frac{\lambda}{s(s-1)} + (\text{integral of a positive function}) .$$

(See, e.g., [L, Chap. 13, §4, Thm. 3 and Chap. 14, §8, Thm. 15].) From this, it follows that, for $s > 1$,

$$\frac{\lambda}{s(s-1)} \le (2^{-2r_2}\pi^{-n}d_K)^{s/2}\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta_K(s). \tag{4.2}$$

Now take a real number $s = 1 + 1/\alpha$, $\alpha \ge 1$. Then we have the inequalities

$$\zeta_K\left(1+\frac{1}{\alpha}\right) \le \zeta_{\boldsymbol{Q}}\left(1+\frac{1}{\alpha}\right)^n < (1+\alpha)^n ,$$

where the first inequality follows from the product expansion for the zeta function and the second one follows from $\sum_{n=1}^{\infty} n^{-s} < 1 + \int_1^{\infty} x^{-s}dx$. Putting $\alpha = 1$ in (4.2), we obtain that

$$\begin{aligned} h_K R_K &\le 2^{1-n}\pi^{-n} w_K d_K \zeta_K(2) \\ &< 2\pi^{-n} w_K d_K . \end{aligned}$$

□

REMARK. If we take other values of α, the estimate may possibly be refined.

For the regulator R_K, Silverman [S] proved that, for some positive constants c_n, d_n depending only on the degree n, one has

$$R_K > c_n(\log d_n|d_K|)^{r-\lambda} ,$$

where r is the rank of the unit group of K, and λ is the maximum of the ranks of the unit groups of proper subfields of K. Friedman improved the estimate of constants c_n and d_n. In particular, he found the smallest regulator and that all number fields satisfy $R_K/w_K \ge 0.09058 > 1/11.1$ (cf. [F, Thm. B]). Thus we have

$$h_K < \frac{2\pi^{-n} w_K d_K}{R_K} < \frac{2(11.1)d_K}{\pi^n} .$$

Putting this into Lemma 4.1 with $M/\tilde{d}_K$ in place of M, we obtain:

$$\#\mathrm{Gal}(K_{\mathfrak{m}_{M/\tilde{d}_K}}/K) < \frac{2^{n+1}(11.1)d_K}{\pi^n}\cdot p^n\cdot\left(\frac{M}{\tilde{d}_K}\right)^n \le \frac{2^{n+1}(11.1)}{\pi^n}p^{n[\log_p n]+2n-1}\frac{M^n}{(\tilde{d}_K)^{n-1}}.$$

Noticing (4.1), the number of χ is bounded as follows:

PROPOSITION 4.3. *Let K be an algebraic number field of degree n with $\tilde{d}_K \mid M$. Then we have*

$$\#\{\chi : G_K \to \bar{\boldsymbol{F}}_p^{\times} \text{ with } N(\chi)\mid(M/\tilde{d}_K)\} \le \#\mathrm{Gal}(K_{\mathfrak{m}_{M/\tilde{d}_K}}/K) < \frac{2^{n+1}(11.1)}{\pi^n}p^{n[\log_p n]+2n-1}M^n\,.$$

Taking the "product" of Propositions 3.3 and 4.3, we obtain our main result.

THEOREM 4.4. *The number of isomorphism classes of n-dimensional monomial* mod *p representations with conductor dividing M is bounded by*

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

REMARK. Noticing the inequality $p^{n[\log_p n]+n-1} < n^n p^{n-1}$, we obtain the "rounded" result as in the Introduction.

5. Order of the image of ρ. An effective version of our Finiteness Problem is to give an explicit upper bound of the order of the image of ρ. In this section, we give an explicit upper bound of $\mathrm{Im}(\rho)$ for monomial representations ρ.

LEMMA 5.1. *Let G be a group, and H a subgroup of G with $(G : H) = n$. Let $\chi : H \to \mathrm{GL}_k(W)$ be a linear representation of H on a finite-dimensional vector space W over a field k, and let $\rho = \mathrm{Ind}_H^G\chi$. Suppose that the image of χ is finite. Then we have the following*:

(i) *If H is normal in G, then $\#\rho(G) \le n\cdot\#\chi(H)^n$.*

(ii) *In general, we have $\#\rho(G) \le n!\cdot\#\chi(H)^n$.*

PROOF. By Mackey's theorem ([Se2, Chap. 7, Prop. 22]), we know that

$$\rho|_H = \bigoplus_{s\in H\backslash G/H}\mathrm{Ind}_{H_s}^H\chi^s\,, \tag{5.1}$$

where $H_s = sHs^{-1}\cap H$ and $\chi^s : H_s \to \mathrm{GL}_k(W)$ is defined by $x \mapsto \chi(s^{-1}xs)$. Put $n_s := (H : H_s)$. Then by comparing the dimensions of both sides of (5.1), we have

$$n = \sum_{s\in H\backslash G/H} n_s\,.$$

(i) If H is normal in G, i.e., $n_s = 1$ for all s, then

$$\rho|_H \simeq \bigoplus_{s \in G/H} \chi^s ,$$

and

$$\chi^s(H) = \chi(H) .$$

Hence we have

$$\#\rho(G) \leq n \cdot \#\rho(H) = n \cdot \#\chi(H)^n .$$

(ii) We prove the statement by induction on n. The case $n = 1$ is trivial. Suppose $n > 1$. We may assume that $n_s < n$ for all s, since otherwise $H = G$. By the induction hypothesis, we have

$$\#\mathrm{Im}(\mathrm{Ind}_{H_s}^H \chi^s) \leq n_s! \cdot \#\chi^s(H_s)^{n_s} .$$

Then from this and (5.1), we see

$$\begin{aligned} \#\rho(H) &\leq \prod_{s \in H\backslash G/H} n_s! \cdot \#\chi^s(H_s)^{n_s} \\ &\leq \left(\prod_{s \in H\backslash G/H} n_s! \right) (\#\chi(H))^{\sum n_s} \\ &\leq (n-1)! \cdot \#\chi(H)^n . \end{aligned}$$

Hence we have

$$\#\rho(G) \leq n \cdot \#\rho(H) \leq n! \cdot \#\chi(H)^n .$$

The proof is complete. □

By the above Lemma (with $H = \mathrm{Gal}(K_{\mathfrak{m}M/\tilde{d}_K}/K)$) together with Proposition 4.3, we conclude:

THEOREM 5.2. *Let $\rho = \mathrm{Ind}_K^{\boldsymbol{Q}} \chi : G_{\boldsymbol{Q}} \to \mathrm{GL}_n(\bar{\boldsymbol{F}}_p)$ be an n-dimensional monomial representation with $N(\rho) \mid M$. Then we have*

$$\#\mathrm{Im}(\rho) \ < \ n! \cdot \left(\frac{2^{n+1}(11.1)}{\pi^n} p^{n[\log_p n]+2n-1} M^n \right)^n .$$

REFERENCES

[A] A. ASH, Monomial Galois representations and Hecke eigenclasses in the mod-p cohomology of GL($(p-1)$, $\boldsymbol{Z}$), Math. Ann. 315 (1999), 263–280.

[AS] A. ASH AND W. SINNOTT, An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod-p cohomology of GL(n, $\boldsymbol{Z}$), Duke Math. J. 105 (2000), 1–24.

[BS] A. BRUMER AND J. H. SILVERMAN, The number of elliptic curves over $\boldsymbol{Q}$ with conductor N, manuscripta math. 91 (1996), 95–102.

[C] H. COHEN, Advanced Topics in Computational Number Theory, Grad. Texts in Math. 193 Springer-Verlag, New York, (2000).

[F] E. FRIEDMAN, Analytic formulas for the regulator of a number field, Invent. Math. 98 (1989), 599–622.

[L] S. LANG, Algebraic Number Theory, Grad. Texts in Math. 110, Springer-Verlag, New York, 1994.

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

[MT] H. MOON AND Y. TAGUCHI, Mod p Galois representations of solvable image, Proc. Amer. Math. Soc. 129 (2001), 2529–2534.

[Se1] J.-P. SERRE, Modular forms of weight one and Galois representations, Algebraic Number Fields: L-functions and Galois properties (A. Fröhlich, ed.), Proc. Sympos., Univ. Durham, Durham, 1975, 193–268, Academic Press, London, 1977.

[Se2] J.-P. SERRE, Linear Representations of Finite Groups, Grad. Texts in Math. 42, Springer-Verlag, New York-Heidelberg, 1977.

[Se3] J.-P. SERRE, Quelques applications du théorème de densité de Chebotarev, Inst. Hautes Études Sci. Publ. Math. 54 (1981), 323–401.

[Se4] J.-P. SERRE, Sur les représentations modulaires de degré 2 de Gal($\bar{\boldsymbol{Q}}/\boldsymbol{Q}$), Duke Math. J. 54 (1987), 179–230.

[S] J. H. SILVERMAN, An inequality relating the regulator and the discriminant of a number field, J. Number Theory 19 (1984), 437–442.

[Tag] Y. TAGUCHI, Induction formula for the Artin conductor of mod ℓ Galois representation, Proc. Amer. Math. Soc. 130 (2002), 2865–2869.

[Tak] T. TAKAGI, Algebraic Number Theory, 2nd ed., Iwanami Shoten, 1971. (in Japanese)

GRADUATE SCHOOL OF MATHEMATICS
KYUSHU UNIVERSITY 33
FUKUOKA 812–8581
JAPAN

E-mail address: moon@math.kyushu-u.ac.jp