KYUNGPOOK Math. J. 56(2016), 1135-1140
http://dx.doi.org/10.5666/KMJ.2016.56.4.1135
pISSN 1225-6951 eISSN 0454-8124


# On the Calculation of the Number of Galois Orbits

Hyunsuk Moon
*Department of Mathematics, Kyungpook National University, Daegu 41566, Korea*
*e-mail* : hsmoon@knu.ac.kr

Abstract. Let $A$ be an abelian variety over a global field $K$. We know [6, 7] that, in many cases, the average number of $n$-torsion points of $A$ over various residue fields of $K$, takes the minimal possible value. In this article, we study several defect cases by calculating the number of Galois orbits.

## 1. Introduction

Let $K$ be a global field and $G_K$ its absolute Galois group. Let $X$ be a finite set with a continuous action of $G_K$. We suppose that $X$ is unramified outside a finite set $S$ of places of $K$ in the sense that if $\mathfrak{p} \notin S$, the inertia group $I_\mathfrak{p}$ of $\mathfrak{p}$ acts trivially on $X$. For a place $\mathfrak{p} \notin S$, we let $N_{X,\mathfrak{p}}$ be the number of fixed points of $X$ by the action of the Frobenius conjugacy class $\mathrm{Frob}_\mathfrak{p} \subset G_K$ for $\mathfrak{p}$. We define $M(X)$ to be the average number of $N_{X,\mathfrak{p}}$ where $\mathfrak{p}$ runs through the non-archimedean places in $K$, that is

$$M(X) = \lim_{x\to\infty} \frac{1}{\pi_K(x)} \sum_{\kappa(\mathfrak{p})\leq x,\ \mathfrak{p}\notin S} N_{X,\mathfrak{p}},$$

where $\kappa(\mathfrak{p})$ is the number of elements of the residue field of $\mathfrak{p}$ and $\pi_K(x)$ is the number of places of $K$ with $\kappa(\mathfrak{p}) \leq x$. It is known that the limit $M(X)$ exists and it is equal to the number of orbits of $G_K$ in $X$ ([6], cf. [3], [4]). This definition applies in particular to the case of linear representations of $G_K$.

Let $R$ be a discrete valuation ring with maximal ideal $\mathfrak{m} = (\pi)$ and finite residue field $k := R/(\pi)$. For a positive integer $n$, we let $X$ be a free $R/\mathfrak{m}^n$-module of finite rank $d \geq 1$. Consider a continuous Galois representation $\rho : G_K \to \mathrm{GL}(X)$ unramified outside a finite set $S$ of places of $K$, where $\mathrm{GL}(X)$ denotes the group of all automorphisms of $X$ as an $R/\mathfrak{m}^n$-module. Then there is a certain relationship between $M(\rho) := M(X)$ and the size of the image of $\rho$. We have $M(\rho) \geq n+1$

Received August 15, 2016; revised September 19, 2016; accepted September 22, 2016.
2010 Mathematics Subject Classification: primary 11F80; secondary 11G05, 11N45.
Key words and phrases: Galois representations, Galois image, Galois orbits.

and the equality holds when $\rho$ is surjective. Indeed, for $0 \leq i \leq n$, $X = X_0 \supset \pi X \supset \cdots \supset \pi^n X = \{0\}$ and each $\pi^i X$ is stable under the Galois action and so each $U_i = \pi^i X \smallsetminus \pi^{i+1} X$ is stable. If $\rho$ is surjective, then $G_K$ acts transitively on $U_i$ for each $0 \leq i \leq n-1$.

We note that a sufficient condition for $M(\rho)$ to have the minimal possible value $n+1$ is found for the case where $\rho$ is not necessarily surjective ([7]); we showed that for an abelian variety $A$ over $K$, in many cases, $M(X)$ takes the minimal possible value, where $X$ is the subgroup of $n$-torsion points of $A$.

In this paper, we study the defect case in the sense that $M(X)$ does not have the minimal possible value. First, we consider the case where Galois image is not too small. In [6], we obtained a upper bound of $M(\rho)$ when $\mathrm{Im}(\rho)$ is bounded below.

**Theorem 1.1.** *Let $c \geq 1$ be an integer such that $\rho(G_K) \supset 1 + \pi^c \, \mathrm{M}_d(R/\pi^n)$. Then we have*

$$M(\rho) \leq (n-c)(q^{cd} - q^{(c-1)d}) + q^{cd}, \qquad q = |R/\pi|,$$

*and the equality holds if and only if $\rho(G_K) = 1 + \pi^c \, \mathrm{M}_d(R/\pi^n)$.*

Applying this result to the $p^n$-torsion subgroup $E[p^n]$ of an elliptic curve over a number field without complex multiplication (CM), we show the following.

**Theorem A.**(=Corollary 2.4, §2) *Let $g \geq 1$ be an integer, and let $p \geq 3$ be a prime. Then there exists an integer $c \geq 1$ depending on $g$ and $p$ such that for any number field $K$ with $[K : \mathbb{Q}] \leq g$ and for any elliptic curve $E$ over $K$ without CM, we have for an integer $n > c$*

$$M(\rho) \leq (n-c)(p^{2c} - p^{2(c-1)}) + p^{2c},$$

*and the equality holds if and only if $\rho(G_K) = 1 + \pi^c \, \mathrm{M}_d(R/\pi^n)$.*

We deduce Theorem A from Theorem 1.1 by using Arai's and Cadoret-Tamagawa's results on the uniform lower bound of the Galois images associated to elliptic curves, in section 2.

Second, we deal with typical mod $p$ Galois image cases. It is well known that there are six cases of subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ that can arise as the image of mod $p$ Galois representation attached to an elliptic curve defined over $\mathbb{Q}$: Borel subgroup, split Cartan subgroup, normalizer of a split Cartan subgroup, non-split Cartan subgroup, normalizer of a non-split Cartan subgroup, and exceptional subgroup. In section 3, we calculate the invariant $M(\rho)$ for three cases with typical mod $p$ Galois images. For instance, we obtain the following.

**Theorem B.**(=Theorem 3.4, §3) *Let $N_+$ be the normalizer of a split Cartan subgroup in $\mathrm{GL}_d(k)$. If $G = \rho(G_K)$ is the inverse image of $N_+$ by the mod $\pi$ reduction, then*

$$M(\rho) = nd + 1.$$

## 2. Open Galois Image

For a prime $p$ and an elliptic curve $E$ over $K$, let $T_pE$ denote the $p$-adic Tate module of $E$, and let

$$\rho_{E,p} : G_K \to \mathrm{Aut}(T_pE) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

be the $p$-adic Galois representation determined by the action of $G_K$ on $T_pE$. Since $\rho_{E,p}$ reflects arithmetic and geometric properties of $E$, it is important to understand the Galois representation $\rho_{E,p}$. The following theorem asserts that the representation has large image if $E$ has no CM.

**Theorem 2.1.**([8], IV-11) *Let $K$ be a number field, $E$ an elliptic curve over $K$ without CM, and $p$ a prime number. Then the representation $\rho_{E,p} : G_K \to \mathrm{GL}_2(\mathbb{Z}_p)$ has an open image in $\mathrm{GL}_2(\mathbb{Z}_p)$, i.e., there exists an integer $c \geq 1$ depending on $K$, $E$, and $p$ such that*

$$\rho_{E,p}(G_K) \supseteq 1 + p^c\,\mathrm{M}_2(\mathbb{Z}_p).$$

Theorem 2.1 is generalized by Arai to the following: the image $\rho_{E,p}(G_K)$ has an uniform bound.

**Theorem 2.2.**([1], Theorem 1.2) *Let $K$ be a number field, and let $p$ be a prime. Then there exists an integer $c \geq 1$ depending on $K$ and $p$ such that for any elliptic curve $E$ over $K$ without CM, we have*

$$\rho_{E,p}(G_K) \supseteq 1 + p^c\,\mathrm{M}_2(\mathbb{Z}_p).$$

Theorem 2.2 is generalized by Cadoret and Tamagawa to the following: not fixing $K$, but bounding the degree of $K$.

**Theorem 2.3.**(Corollary of Theorem 1.1, [2]) *Let $g \geq 1$ be an integer, and let $p$ be a prime. Then there exists an integer $c \geq 1$ depending on $g$ and $p$ such that for any number field $K$ with $[K : \mathbb{Q}] \leq g$ and for any elliptic curve $E$ over $K$ without CM, we have*

$$\rho_{E,p}(G_K) \supseteq 1 + p^c\,\mathrm{M}_2(\mathbb{Z}_p).$$

Denote by $\rho_{E,p,n}$ be the reduction mod $p^n$ of $\rho_{E,p}$. By combining Theorems 1.1 and 2.3, we deduce

**Corollary 2.4.** *Let $g \geq 1$ be an integer, and let $p \geq 3$ be a prime. Then there exists an integer $c \geq 1$ depending on $g$ and $p$ such that for any number field $K$ with $[K : \mathbb{Q}] \leq g$ and for any elliptic curve $E$ over $K$ without CM, we have for an integer $n > c$*

$$M(\rho_{E,p,n}) \leq (n - c)(p^{2c} - p^{2(c-1)}) + p^{2c},$$

*and the equality holds if and only if $\rho_{E,p,n}(G_K) = 1 + \pi^c\,\mathrm{M}_d(R/\pi^n)$.*

## 3. Image of the Mod $p$ Reduction

It is well known that there are six cases of subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ that can arise as the image of the mod $p$ Galois representation $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ attached to an elliptic curve defined over $\mathbb{Q}$ ([5], p. 115-116): Borel subgroup, Split Cartan subgroup, Normalizer of a split Cartan subgroup, Non-split Cartan subgroup, Normalizer of a non-split Cartan subgroup, and Exceptional subgroup. In this section, we deal with three cases of these. We prepare a lemma.

We use the same notation as in §1. For a continuous representation $\rho : G_K \to \mathrm{GL}_d(R/\pi^n)$, we let $G := \mathrm{Im}(\rho) \subset \mathrm{GL}_d(R/\pi^n)$ and $\varpi_m : \mathrm{GL}_d(R/\pi^n) \to \mathrm{GL}_d(R/\pi^m)$ a mod $\pi^m$ reduction map for an integer $1 \leq m < n$. We denote the reduction of $\rho$ modulo $\pi$ by $\bar{\rho} := \varpi_1 \circ \rho$. **Lemma 3.1.** *Let $G_1$ be a subgroup in $\mathrm{GL}_d(k)$. If $G$ is the inverse image of $G_1$ by $\varpi_1$, then we have*

$$M(\rho) = n(M(\bar{\rho}) - 1) + 1.$$

*Proof.* Let $V_n = (R/\pi^n)^{\oplus d}$. For each $0 \leq i \leq n-1$, $U_{n,i} = \pi^i V_n \smallsetminus \pi^{i+1} V_n$ is stable under the action of $G$. So, we calculate the number of orbits of $G$ in each $U_{n,i}$. On the other hand, the action of $G$ on $U_{n,i}$ and $G_{n-i}$ on $U_{n-i,0}$ are compatible in the sense that

$$g(\pi^i v) = \pi^i(\bar{g} v)$$

for all $g \in G$ and $v \in V_{n-i}$, where $\bar{g}$ is the mod $\pi^{n-i}$ reduction of $g$. Hence it is sufficient to calculate the number of orbits of $G_m$ (:= the inverse image of $G_1$ in $\mathrm{GL}_d(R/\pi^m)$) in each $U_{m,0}$ for $1 \leq m \leq n$. Now we show that the numbers of orbits of $G_m$ on $U_{m,0}$ are the same for each $1 \leq m \leq n$.

Let $v_1$, $v_2 \in U_{1,0} = V_1 \smallsetminus \{0\}$ be in the same orbit of $G_1$, i. e. , $v_2 = g_1 v_1$ for some $g_1 \in G_1$. Let $\hat{v}_i$ be a lift of $v_i$ in $U_{m,0}$, and let $\hat{g}_1$ be a lift of $g_1$ in $G_m$. Then for each $2 \leq m \leq n$, there exists an $x_m \in \mathrm{M}_d(R/\pi^m)$ satisfying $1 + \pi x_m \in G_m$ and

$$\hat{v}_2 + \pi V_m = \hat{g}_1(1 + \pi x_m)(\hat{v}_1 + \pi V_m)$$

by the assumption. Also, we can make $\hat{v}_2 = \hat{g}_1(1 + \pi x_m)\hat{v}_1$ by choosing a $x_m \in \mathrm{M}_d(R/\pi^m)$. Thus the inverse image in $U_{m,0}$ of a $G_1$-orbit in $U_{1,0}$ forms one $G_m$-orbit. □

**Theorem 3.2.** *Let $B$ be a Borel subgroup in $\mathrm{GL}_d(k)$. If $G = \rho(G_K)$ is the inverse image of $B$ by mod $\pi$ reduction map, then $M(\rho) = nd + 1$.*

*Proof.* By Lemma 3.1, it is enough to calculate the number of orbits of $B$ in $k^{\oplus d}$. If we let

$$U_0 = k^{\oplus d} \supset U_1 = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_{d-1} \\ 0 \end{pmatrix} \mid x_i \in k \right\} \supset U_2 = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_{d-2} \\ 0 \\ 0 \end{pmatrix} \right\}$$

$$\supset \cdots \supset U_{d-1} = \left\{ \begin{pmatrix} x_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right\} \supset U_d = \{0\},$$

then $B = \left\{ \begin{pmatrix} * & \cdots & * \\ & \ddots & \vdots \\ & & * \end{pmatrix} \right\}$ acts on $U_i \setminus U_{i+1}$ transitively for $0 \le i \le d$. Hence $M(\bar{\rho}) = d + 1$ and $M(\rho) = nd + 1$. □

**Theorem 3.3.** *Let $C_\mathrm{s}$ be a split Cartan subgroup in $\mathrm{GL}_d(k)$. If $G = \rho(G_K)$ is the inverse image of $C_\mathrm{s}$ by mod $\pi$ reduction map, then $M(\rho) = n(2^d - 1) + 1$.*

*Proof.* Since $C_\mathrm{s}$ is a subgroup conjugate to the group of the diagonal matrices in $\mathrm{GL}_d(k)$, each $i$th coordinate space is stable under the action of $C_\mathrm{s}$ and the number of orbits of $C_\mathrm{s}$ in $k^{\oplus d}$ is equal to the number of permutations choosing $d$ from 2 different types, i. e. , $2^d$. Hence $M(\rho) = n(2^d - 1) + 1$. □

**Theorem 3.4.** *Let $N_+$ be the normalizer of a split Cartan subgroup in $\mathrm{GL}_d(k)$. If $G = \rho(G_K)$ is the inverse image of $N_+$ by mod $\pi$ reduction map, then*

$$M(\rho) = nd + 1$$

*Proof.* We know that $N_+$ is generated by diagonal matrices $\begin{pmatrix} * & & \\ & \ddots & \\ & & * \end{pmatrix}$ and the Weyl group (which consists of the permutation matrices). Thus the orbits in $k^{\oplus d}$ are

$$U_i := \{(x_1, \cdots, x_d) | \text{ just } i \text{ of } x_1, \cdots, x_d \text{ are non-zero and the rest are } 0\ \},$$

for $i = 0, \cdots, d$. Hence $M(\bar{\rho}) = d + 1$, and $M(\rho) = nd + 1$. □

**Acknowledgements.** The author would like to thank the referee for useful comments and suggestions.

## References

[1] K. Arai, *On uniform lower bound of the Galois image associated to elliptic curves*, J. Théor. Nombres Bordeaux, **20**(2008), 23–43.

[2] A. Cadoret and A. Tamagawa, *A uniform open image theorem for $\ell$-adic representations II*, Duke Math. J. **162**(2013), 2301–2344.

[3] Y. J. Chen and Y. Kuan, *On the distribution of torsion points modulo primes*, Bull. Aust. Math. Soc. **86**(2012), 339–347.

[4] H. Huang, *The average number of torsion points on elliptic curves*, J. Number Theory **135**(2014), 374–389.

[5] B. Mazur, *Rational points on modular curves*, Modular functions of one variable V, Lecture Notes in Math., Vol. 601, Springer, Berlin (1977), 107–148.

[6] H. Moon, *On the invariant $M(A_{/K}, n)$ of Chen-Kuan for Galois representations*, Proc. Japan Acad. **90**(2014), 98–100.

[7] H. Moon, *On the invariant of Chen-Kuan for abelian varieties*, Kyungpook Math. J., **56(3)**(2016), 755–761.

[8] J.-P. Serre, *Abelian $\ell$-adic representations and elliptic curves*, Lecture at McGill University., W. A. Benjamin Inc., New York Amsterdam, 1968.