On the invariant $M(A_{/K}, n)$ of Chen-Kuan for Galois representations

By Hyunsuk MOON

Department of Mathematics, College of Natural Sciences, Kyungpook National University, Daegu 702-701, Korea

(Communicated by Shigefumi MORI, M.J.A., June 12, 2014)

Abstract: Let X be a finite set with a continuous action of the absolute Galois group of a global field K. We suppose that X is unramified outside a finite set S of places of K. For a place $\mathfrak{p} \notin S$, let $N_{X,\mathfrak{p}}$ be the number of fixed points of X by the Frobenius element $\mathrm{Frob}_{\mathfrak{p}} \subset G_K$. We define the average value $M(X)$ of $N_{X,\mathfrak{p}}$ where $\mathfrak{p}$ runs through the non-archimedean places in K. This generalize the invariant of Chen-Kuan and we apply this for Galois representations. Our results show that there is a certain relationship between $M(X)$ and the size of the image of Galois representations.

Key words: Galois representations; torsion points; distribution.

Let A be an abelian variety over a number field K. For a prime $\mathfrak{p}$ in K, denote the residue field by $\mathbf{F}_{\mathfrak{p}}$. If A has good reduction at $\mathfrak{p}$, let $N_{\mathfrak{p},n}$ be the number of n-torsion $\mathbf{F}_{\mathfrak{p}}$-rational points of the reduction of A modulo $\mathfrak{p}$, where n is a positive integer. When $\dim A = 1$, Chen and Kuan determined the average value $M(A_{/K}, n)$ of $N_{\mathfrak{p},n}$ as the prime $\mathfrak{p}$ varies. In this paper, we generalize their invariant $M(A_{/K}, n)$ for Galois representations.

Let K be a global field (i.e., finite extension of $\mathbf{Q}$ or algebraic function field in one variable over a finite field) and G_K its absolute Galois group. Let X be a finite set with a continuous action of G_K. We call this X a finite G_K-set. For example, the set of n-torsion points of an abelian variety A over K is a finite G_K-set. We suppose that X is unramified outside a finite set S of places of K (including all archimedean places) 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 $\mathfrak{p} \notin S$, the Frobenius element $\mathrm{Frob}_{\mathfrak{p}} \subset G_K$, which is considered as a well-defined conjugacy class, acts on X. Let $N_{X,\mathfrak{p}}$ be the number of fixed points of X by $\mathrm{Frob}_{\mathfrak{p}}$. We are interested in the average value of $N_{X,\mathfrak{p}}$ where $\mathfrak{p}$ runs through the non-archimedean places in K, namely the limit

$$\lim_{x\to\infty} \frac{1}{\pi_K(x)} \sum_{N\mathfrak{p}\le x,\ \mathfrak{p}\notin S} N_{X,\mathfrak{p}}$$

where $\pi_K(x)$ is the number of places $\mathfrak{p}$ with norm $N\mathfrak{p} \le x$. ($N\mathfrak{p}$ means the number of elements of the residue field of $\mathfrak{p}$). We denote this limit by $M(X)$, if it exists. Note that $M(X)$ does not depend on the choice of S. The following theorem is a straightforward generalization of Chen and Kuan's Theorem 1.2 in [1]; here we reproduce their proof for the convenience of the reader.

Theorem 1. *The limit $M(X)$ exists and it is equal to the number of orbits of G_K in X.*

Proof. Let L be a finite Galois extension of K such that the action of G_K on X factors through $G := \mathrm{Gal}(L/K)$. For $1 \le m \le |X|$, let $G(m)$ be the set of elements $g \in G$ which have exactly m fixed points. Then $G(m)$ is a union of conjugacy classes for each m. Observe that, for a prime $\mathfrak{p}$ which is unramified in L, we have $N_{X,\mathfrak{p}} = m$ if and only if the Artin symbol $(\mathfrak{p}, L/K) \subset G(m)$. One derives

$$\begin{aligned} M(X) &= \lim_{x\to\infty} \frac{1}{\pi_K(x)} \sum_{m=1}^{|X|} \sum_{\mathfrak{p}\notin S,\ N\mathfrak{p}\le x,\ (\mathfrak{p},L/K)\subset G(m)} m \\ &= \sum_{m=1}^{|X|} m \lim_{x\to\infty} \frac{1}{\pi_K(x)} \sum_{\mathfrak{p}\notin S,\ N\mathfrak{p}\le x,\ (\mathfrak{p},L/K)\subset G(m)} 1 \\ &= \sum_{m=1}^{|X|} m \frac{|G(m)|}{|G|}, \end{aligned}$$

using the Chebotarev density theorem for the last equality. The proof of the theorem is complete by applying Burnside's lemma ([5]). □

It is well-known ([4]) that if $M(X)$ exists, the Dirichlet version of $M(X)$ exists and is equal to $M(X)$:

2010 Mathematics Subject Classification. Primary 11F80; Secondary 11G05, 11N45.

doi: 10.3792/pjaa.90.98

Corollary 2.

$$M(X) = \lim_{s\to 1+} \frac{\sum_{\mathfrak{p}\notin S} N_{X,\mathfrak{p}} \cdot (N\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} (N\mathfrak{p})^{-s}}.$$

For finite G_K-sets X_1 and X_2, we define that X_1 and X_2 are *independent from each other* if the Galois image over $X_1 \times X_2$ is the direct product of the Galois images over X_1 and X_2, where the Galois image over X means $\mathrm{Im}(G_K \to \mathrm{Aut}(X))$.

Corollary 3. *$M(X)$ is multiplicative in X, that is, if X_1 and X_2 are finite G_K-sets independent from each other, then $M(X_1 \times X_2) = M(X_1)M(X_2)$.*

Proof. If X_1 and X_2 are finite G_K-sets, then $X_1 \times X_2$ is also a finite G_K-set. By the independentness, the number of Galois orbits in $X_1 \times X_2$ is the product of the numbers of Galois orbits in X_1 and X_2. □

Next we apply Theorem 1 to Galois representations. Let R be a discrete valuation ring with maximal ideal $\mathfrak{m} = (\pi)$ and finite residue field of order $q := |R/(\pi)|$. Set $R_e := R/\mathfrak{m}^e$ for each $e \geq 1$. Let X be a free R_e-module of finite rank d. Let $\rho_X : G_K \to \mathrm{GL}_{R_e}(X)$ be a continuous Galois representation unramified outside a finite set S of places of K. First we consider two extreme cases. One is the case where the image of ρ_X is trivial. Then we have $M(X) = |X|$, the cardinal number of X. The other is the following case:

Theorem 4. *If ρ_X is surjective, then $M(X) = e + 1$.*

Proof. For each $0 \leq i \leq e$, let $X_i = \pi^i X$. Then $X = X_0 \supset X_1 \supset \cdots \supset X_e = 0$ and X_i's are stable under the Galois action. If we let $U_i = X_i \setminus X_{i+1}$, then each U_i is also stable under the Galois action and by assumption G_K acts transitively on U_i for each i. So the number of orbits of G_K in X is equal to $e + 1$. □

Following the ideas of Chen-Kuan ([1], p. 341), we can combine Corollary 3 and Theorem 4 to show:

Corollary 5 ([1], Cor. 1.5)**.** *Let E be an elliptic curve defined over a number field K without complex multiplication. Then there exists an integer constant $C_{E/K}$ (depending on E and K) such that for all n prime to $C_{E/K}$, we have*

$$M(E[n]) = d(n),$$

where $d(n)$ is the number of positive divisors of n.

Proof. Let $n = \prod p^{e_p}$ be the prime factorization of n and

$$\begin{aligned}\rho : G_K \to \mathrm{Aut}(E[n]) &\simeq \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}) \\ &\simeq \prod \mathrm{GL}_2(\mathbf{Z}/p^{e_p}\mathbf{Z})\end{aligned}$$

be the Galois representation on $E[n]$. By a theorem of Serre ([3], Section 4.2, Theorem 2) together with Appendix of [2], there exists an integer constant $C_{E/K}$ such that ρ is surjective if n is prime to $C_{E/K}$. By Theorem 4, we have $M(E[p^{e_p}]) = e_p + 1$ for each p. By Corollary 3, we have

$$\begin{aligned}M(E[n]) &= \prod M(E[p^{e_p}]) \\ &= \prod (e_p + 1) \\ &= d(n).\end{aligned}$$

□

Now we consider a more general image case.

Theorem 6. *Let c be a positive integer such that $\rho_X(G_K) \supset 1 + \pi^c \mathrm{M}_d(R_e)$. Then we have*

$$M(X) \leq (e - c)(q^{cd} - q^{(c-1)d}) + q^{cd},$$

and the equality holds if and only if $\rho_X(G_K) = 1 + \pi^c \mathrm{M}_d(R_e)$.

Proof. Let $G := \rho_X(G_K) \subset \mathrm{GL}_d(R_e)$. We suppose that $G = 1 + \pi^c \mathrm{M}_d(R_e)$, $1 \leq c \leq e$. We denote $\mathrm{M}_d(R_e)$ by M. For each $0 \leq i < e$, $U_i = X_i \setminus X_{i+1}$ is stable under the action of G; we calculate the number of orbits of G in each U_i. For $u \in U_i$, we have $Gu = (1 + \pi^c \mathrm{M})u = u + \pi^c \mathrm{M}u = u + X_{i+c}$. So,

$$|Gu| = |X_{i+c}| = \begin{cases} q^{(e-i-c)d}, & i \leq e - c, \\ 1, & i \geq e - c. \end{cases}$$

Hence

$$\begin{aligned}|U_i/G| &= \frac{q^{(e-i)d} - q^{(e-i-1)d}}{|Gu|} \\ &= \begin{cases} q^{cd} - q^{(c-1)d}, & i \leq e - c, \\ q^{(e-i)d} - q^{(e-i-1)d}, & i \geq e - c. \end{cases}\end{aligned}$$

Therefore the number of orbits of G is

$$\begin{aligned}|X/G| &= \sum_{i=0}^{e} |U_i/G| \\ &= (e - c)(q^{cd} - q^{(c-1)d}) + q^{cd}.\end{aligned}$$

Moreover if $G \supsetneq 1 + \pi^c \mathrm{M}$, then we have $Gu \supsetneq u + X_{i+c}$ and hence

$$|X/G| \lneq (e - c)(q^{cd} - q^{(c-1)d}) + q^{cd}.$$

□

Acknowledgements. The author was supported by Kyungpook National University Research Fund, 2012 and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2009-0066564).

References

[1] Y.-M. J. Chen and Y.-L. Kuan, On the distribution of torsion points modulo primes, Bull. Aust. Math. Soc. **86** (2012), no. 2, 339–347.

[2] A. C. Cojocaru, On the surjectivity of the Galois representations associated to non-CM elliptic curves, Canad. Math. Bull. **48** (2005), no. 1, 16–31.

[3] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), no. 4, 259–331.

[4] J.-P. Serre, *A course in arithmetic*, translated from the French, Springer, New York, 1973.

[5] J.-P. Serre, On a theorem of Jordan, Bull. Amer. Math. Soc. (N.S.) **40** (2003), no. 4, 429–440 (electronic).