International Journal of Number Theory
Vol. 17, No. 4 (2021) 1029–1045

DOI: 10.1142/S1793042121500226

On the moments of torsion points modulo primes and their applications

Amir Akbary* and Peng-Jie Wong†

Department of Mathematics and Computer Science
University of Lethbridge
Lethbridge, Alberta T1K 3M4, Canada
**amir.akbary@uleth.ca*
†*pengjie.wong@uleth.ca*

Received 7 November 2019
Accepted 17 August 2020
Published 30 September 2020

Let $\mathbb{A}[n]$ be the group of n-torsion points of a commutative algebraic group $\mathbb{A}$ defined over a number field F. For a prime $\mathfrak{p}$ of F, we let $N_{\mathfrak{p}}(\mathbb{A}[n])$ be the number of $\mathbb{F}_{\mathfrak{p}}$-solutions of the system of polynomial equations defining $\mathbb{A}[n]$ when reduced modulo $\mathfrak{p}$. Here, $\mathbb{F}_{\mathfrak{p}}$ is the residue field at $\mathfrak{p}$. Let $\pi_F(x)$ denote the number of primes $\mathfrak{p}$ of F such that $N(\mathfrak{p}) \leq x$. We then, for algebraic groups of dimension one, compute the kth moment limit

$$M_k(\mathbb{A}/F, n) = \lim_{x\to\infty} \frac{1}{\pi_F(x)} \sum_{N(\mathfrak{p})\leq x} N_{\mathfrak{p}}^k(\mathbb{A}[n])$$

by appealing to the Chebotarev density theorem. We further interpret this limit as the number of orbits of the action of the absolute Galois group of F on k copies of $\mathbb{A}[n]$ by an application of Burnside's Lemma. These concrete examples suggest a possible approach for determining the number of orbits of a group acting on k copies of a set.

Keywords: Number of torsion points on reduction mod p; group action; Burnside Lemma; Chebotarev density theorem.

Mathematics Subject Classification 2020: 11N45, 11G05, 11N13, 11R18

1. Introduction

Let $\mathbb{A}$ be a commutative algebraic group defined over a number field F. We let $\mathbb{A}[n]$ be the group of n-torsion points of $\mathbb{A}$ and $F(\mathbb{A}[n])$ be the field generated by adding the coordinates of $\mathbb{A}[n]$ to F. For a prime $\mathfrak{p}$ of F that is unramified in $F(\mathbb{A}[n])/F$, let $\mathbb{F}_{\mathfrak{p}}$ denote the residue field at $\mathfrak{p}$, and let $N_{\mathfrak{p}}(\mathbb{A}[n])$ be the number of $\mathbb{F}_{\mathfrak{p}}$-solutions of the system of polynomial equations defining $\mathbb{A}[n]$ when reduced modulo $\mathfrak{p}$. If $\mathfrak{p}$ ramifies, we set $N_{\mathfrak{p}}(\mathbb{A}[n]) = 0$. In order to investigate the average size of $N_{\mathfrak{p}}(\mathbb{A}[n])$, we set

$$M(\mathbb{A}/F, n) = \lim_{x\to\infty} \frac{1}{\pi_F(x)} \sum_{N(\mathfrak{p})\leq x} N_{\mathfrak{p}}(\mathbb{A}[n]), \tag{1.1}$$

where $\pi_F(x)$ denotes the number of primes $\mathfrak{p}$ of F whose norm $N(\mathfrak{p})$ do not exceed x.

In [2], Chen and Kuan investigated the average size of the arithmetic function $N_{\mathfrak{p}}(\mathbb{A}[n])$ by determining $M(\mathbb{A}/F,n)$ as the number of orbits of the group $\mathrm{Gal}(F(\mathbb{A}[n])/F)$ acting on the n-torsion points $\mathbb{A}[n]$ (see [2, Theorem 1.2]). Moreover, they showed that for commutative algebraic groups of dimension one other than $\mathbb{G}_a$, the value of $M(\mathbb{A}/F,n)$ is given by a divisor function. More precisely, it is known that a commutative algebraic group of dimension one over F is either the additive group $\mathbb{G}_a$, the multiplicative group $\mathbb{G}_m$, an algebraic torus of dimension one, or an elliptic curve. For $\mathbb{G}_a$ we have $M(\mathbb{G}_a/F,n)=1$. For other cases, the following assertions are proved in [2, Corollaries 1.3, 1.5 and Theorems 1.4, 1.6]. Here, ζ_n denotes a primitive nth root of unity and $d(n)$ is the number of positive divisors of n.

Theorem 1.1 (Chen–Kuan). (i) *Assume that* $F\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}$. *Then* $M(\mathbb{G}_m/F,n)=d(n)$.

(ii) *Let* $\mathbb{T}$ *denote a one-dimensional torus over* $\mathbb{Q}$. *Then there is a positive constant* $C:=C(\mathbb{T})$, *depending only on* $\mathbb{T}$, *such that for* n *with* $(n,C)=1$, *one has* $M(\mathbb{T}/\mathbb{Q},n)=d(n)$.

(iii) *Assume that* E *is a non-CM elliptic curve defined over* F. *Then there is a positive constant* $C:=C(E,F)$, *depending only on* E *and* F, *such that for* n *with* $(n,C)=1$, *one has* $M(E/F,n)=d(n)$.

(iv) *Assume that* E *is an elliptic curve defined over* F *which has complex multiplication by an order in an imaginary quadratic field* K. *Assume* $FK\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}$. *Then there is a positive constant* $C:=C(E,F)$, *depending only on* E *and* F, *such that for* n *with* $(n,2C)=1$, *one has*

$$M(E/F,n)=\begin{cases} d_K(n) & \text{if } K\subseteq F,\\ \frac{1}{2}(d_K(n)+d(n)) & \text{if } K\not\subseteq F.\end{cases}$$

Here, $d_K(n)$ *denotes the number of ideal divisors of the ideal* $n\mathcal{O}_K$ *in* $\mathcal{O}_K$, *the ring of integers of* K. *The conditions* $FK\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}$ *and* $(n,2)=1$ *only apply to the case that* $K\not\subseteq F$.

Remark 1.2. (i) In [2], the function $N_{\mathfrak{p}}(\mathbb{A}[n])$ is defined, for a prime $\mathfrak{p}$ of good reduction of $\mathbb{A}$, as the number of n-torsion points in the group of $\mathbb{F}_{\mathfrak{p}}$-rational points of the reduction modulo $\mathfrak{p}$ of $\mathbb{A}$. Our definition of $N_{\mathfrak{p}}(\mathbb{A}[n])$ may differ from that definition only at finitely many prime ideals $\mathfrak{p}$, and thus it will not affect the assertions of Theorem 1.1.

(ii) Parts (iii) and (iv) of Theorem 1.1 are also stated and proved in [6, Corollaries 1, 3, and 4].

(iii) The conditions $FK\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}$ and $(n,2)=1$ in part (iv) of Theorem 1.1 is not clearly stated in [2, Theorem 1.6]; however, these conditions are used in the proof of Theorem 1.6 in [2].

(iv) In [2, Theorem 1.4], it is also proved that the constant C in part (ii) of Theorem 1.1 can be taken as 1 if $m>0$ and as D_m if $m<0$, where m is the square-free integer in the equation $x^2 - my^2 = 1$ defining $\mathbb{T}$, and D_m is the discriminant of the quadratic field $\mathbb{Q}(\sqrt{m})$. Also, it is shown, for $F = \mathbb{Q}$, that in part (iv) of Theorem 1.1 the constant C can be taken as $6\Delta_E$, where Δ_E is the discriminant of E (see [2, Theorem 1.6]). In addition, the extensions of Theorem 1.1 to the case of function fields are given in [3].

The proof of the first three parts of Theorem 1.1 can be unified and simplified considerably if one interprets the limit (1.1) as the number of the orbits of $\mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$, the group of invertible $m \times m$ matrices with entries in $\mathbb{Z}/n\mathbb{Z}$, acting on the product of m copies of $\mathbb{Z}/n\mathbb{Z}$, when $m = 1$ or 2. In this direction, the following can be considered as a generalization of the underlying result in parts (i), (ii), and (iii) of Theorem 1.1.

Theorem 1.3. *Let L be a number field of class number* 1. *Then the number of orbits of $\mathrm{GL}_m(\mathcal{O}_L/n\mathcal{O}_L)$ acting on $(\mathcal{O}_L/n\mathcal{O}_L)^m$ is $d_L(n)$, where $d_L(\cdot)$ is the number field analogue of the divisor function.*

In another direction, as a consequence of the results of this paper, we give a generalization of Theorem 1.1 by considering the kth moment limit

$$M_k(\mathbb{A}/F, n) = \lim_{x\to\infty} \frac{1}{\pi_F(x)} \sum_{N(\mathfrak{p})\leq x} N_{\mathfrak{p}}^k(\mathbb{A}[n]).$$

Note that, for every $k \geq 1$, $M_k(\mathbb{G}_a/F, n) = 1$. In order to state our result for other algebraic groups of dimension one, we need to introduce the following notation. For $k \in \mathbb{Z}^{\geq 0}$ and $n \in \mathbb{N}$, let

$$M_k(n) := \sum_{\substack{d,e \\ de\,|\,n}} \frac{d^k \mu(e)}{\varphi(de)},$$

where μ is the Möbius function, and φ is the Euler function. Observe that for $a, b \in \mathbb{N}$ and integer $k \geq 0$, by letting

$$P_k(a, b) = \frac{a^k - b^k}{a - b},$$

we have

$$M_k(n) = \prod_{\ell^s \| n} \left(\sum_{e=1}^{s} P_k(\ell^e, \ell^{e-1}) + 1 \right).$$

Note that $M_0(n) = 1$ and $M_1(n) = d(n)$. Thus, $M_k(n)$ can be considered as a generalization of the divisor function.

We have the following generalization of Theorem 1.1.

Theorem 1.4. (i) *Assume that $F \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. Then $M_k(\mathbb{G}_m/F, n) = M_k(n)$.*

(ii) *Let $\mathbb{T}$ be a one-dimensional torus defined over $\mathbb{Q}$. Then there is a positive constant $C := C(\mathbb{T})$, depending only on $\mathbb{T}$, such that for n with $(n, C) = 1$, we have $M_k(\mathbb{T}/\mathbb{Q}, n) = M_k(n)$.*

(iii) *Assume that E is a non-CM elliptic curve defined over F. Then there is a positive constant $C := C(E, F)$, depending only on E and F, such that for square-free n with $(n, C) = 1$, we have*

$$M_k(E/F, n) = \prod_{\ell \mid n} \frac{\ell^{2k-1} + \ell^{k-1}(\ell^3 - 2\ell - 1) + \ell^3 - 2\ell^2 - \ell + 3}{(\ell - 1)^2(\ell + 1)}.$$

(iv) *Assume that E is an elliptic curve defined over $\mathbb{Q}$ that has complex multiplication by $\mathcal{O}_K$. Then there is a positive constant $C := C(E)$, depending only on E, such that for prime ℓ with $(\ell, 2C) = 1$, we have*

$$M_k(E/\mathbb{Q}, \ell) = \frac{\ell^{2k} + (d_K(\ell) - 1)(\ell^{k+1} + \ell^k) + 2\ell^2 - (d_K(\ell) - 1)\ell - (d_K(\ell) + 2)}{2(\ell^2 - 1)}.$$

Remark 1.5. For $k \geq 3$, the ℓ-factor in the product expression for $M_k(E/F, n)$ in part (iii) of Theorem 1.4 is a polynomial function of degree $2k - 4$ of ℓ with integral coefficients. For $k = 1$ (respectively, $k = 2$), the ℓ-factor is 2 (respectively, $\ell + 3$). The expression in part (iv) is a polynomial function of degree $2k - 2$ of ℓ with half-integral coefficients.

Theorem 1.4, similarly to Theorem 1.1, is intimately related to a group theory result. In order to describe the connection, we introduce a more general setup.

Let $\overline{F}$ denote the algebraic closure of a number field F. Let Y be an algebraic set (affine or projective), given as the set of $\overline{F}$-solutions of a finite family of polynomial equations E_Y defined over the ring of integers $\mathcal{O}_F$ of F. (If Y is projective, "polynomial equations" means "homogeneous polynomial equations" and "$\mathbb{F}_\mathfrak{p}$-solutions" means "projective $\mathbb{F}_\mathfrak{p}$-solutions"). For an unramified prime ideal $\mathfrak{p}$ in the extension $F(Y)/F$, we let

$$N_\mathfrak{p}(Y) := \#\{\text{solutions of } E_Y \,(\mathrm{mod}\, \mathfrak{p}) \text{ in } \mathbb{F}_\mathfrak{p}\}.$$

If Y is the set of $\overline{F}$-solutions of a single polynomial f, we also denote $N_\mathfrak{p}(Y)$ by $N_\mathfrak{p}(f)$.

Remark 1.6. Theorem 1.2(c) of [15] provides a generalization of Theorem 1.1 and another interpretation for the limit (1.1) for the case $F = \mathbb{Q}$. For an algebraic set Y defined over $\mathbb{Z}$, let $N_p(Y)$ be as defined above. Then if the dimension $\dim Y(\mathbb{C}) \leq d_0$, one has

$$\lim_{x \to \infty} \frac{1}{\pi(x^{d_0+1})} \sum_{p \leq x} N_p(Y) = r_0(Y),$$

where $r_0(Y)$ is the number of $\mathbb{Q}$-irreducible components of dimension d_0 of Y over $\mathbb{Q}$. Here, $\pi(x) := \pi_\mathbb{Q}(x)$. Note that for $d_0 = 0$, the above limit is analogous to the one evaluated in Theorem 1.1. For example, for the algebraic set Y defined by $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$, where $\Phi_d(x)$ is the dth cyclotomic polynomial, we have $r_0(Y) = d(n)$.

We now assume that Y has dimension zero (so it is finite) and let $M_k(G,Y)$ be the number of orbits of $G = \mathrm{Gal}(F(Y)/F)$ acting on k copies of Y. Since there are only finitely many prime ideals that ramify in $F(Y)/F$, for a ramified prime ideal $\mathfrak{p}$ we define $N_{\mathfrak{p}}(Y) = 0$ for convenience. The following main result represents $M_k(G,Y)$ as an asymptotic average of the values $N_{\mathfrak{p}}^k(Y)$ as $\mathfrak{p}$ varies over the set of primes of F.

Theorem 1.7. *Let Y be an algebraic set of dimension zero defined over F, $G = \mathrm{Gal}(F(Y)/F)$, and $M_k(G,Y)$ as defined above. Then, for $k \in \mathbb{N}$, we have*

$$\lim_{x\to\infty} \frac{1}{\pi_F(x)} \sum_{N(\mathfrak{p})\le x} N_{\mathfrak{p}}^k(Y) = M_k(G,Y).$$

The above theorem can be considered as a generalization of a classical result due to Frobenius and Kronecker (see [14, p. 436]).

Theorem 1.8 (Frobenius–Kronecker). *For an irreducible polynomial $f \in \mathbb{Z}[x]$, we have*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\le x} N_p(f) = 1.$$

Indeed, let $F = \mathbb{Q}$, $Y =$ the set of roots of f in $\overline{\mathbb{Q}}$, $k = 1$, and $G = \mathrm{Gal}(F(Y)/F)$ in Theorem 1.7. Then, observing that the action of the Galois group on the set of roots of f is transitive, we obtain Theorem 1.8 as a corollary of Theorem 1.7. Note that although the action of G on Y in Theorem 1.8 is transitive, the action on $k \ge 2$ copies of Y is not transitive if $|Y| > 1$. Thus, determining $M_k(G,Y)$ appears to be a nontrivial problem for $k \ge 2$, even when Y is defined by an irreducible polynomial.

As a direct consequence of Theorem 1.7, we establish the existence of an asymptotic distribution function for the arithmetic function $N_{\mathfrak{p}}(Y)$.

Corollary 1.9. *Let Y be an algebraic set of dimension zero defined over F. Then the arithmetic function $N_{\mathfrak{p}}(Y)$ possesses an asymptotic distribution function. In other words, the sequence*

$$H_n(z) = \frac{\#\{\mathfrak{p}; N(\mathfrak{p}) \le n \text{ and } N_{\mathfrak{p}}(Y) \le z\}}{\pi_F(n)}$$

converges weakly to a distribution function H, as $n \to \infty$ (i.e. there is a distribution function H where $H_n(z)$ converges point-wise to $H(z)$ at any continuity point z of H). Moreover, for complex t-values with $|t| < 1$,

$$\varphi_H(t) = \lim_{n\to\infty} \frac{1}{\pi_F(n)} \sum_{N(\mathfrak{p})\le n} e^{itN_{\mathfrak{p}}(Y)} = \sum_{k=0}^{\infty} M_k(G,Y) \frac{(it)^k}{k!},$$

where $G = \mathrm{Gal}(F(Y)/Y)$, and $\varphi_H(t)$ is the characteristic function of H.

We next describe that how Theorem 1.7 can be exploited to answer some pure group-theoretic questions. A fundamental question regarding the action of a group

G on a set X is to determine the number of orbits in X under the action of G. Moreover, if the number of orbits in X under the action of G is known, one may further ask whether there exists a formula for $M_k(G,X)$, the number of orbits in k copies of X under the action of G. Indeed, both are deep questions. Here, we show that how Theorem 1.7 can be employed in computing $M_k(G,X)$. The following definition describes our setup.

Definition 1.10. An action of a finite group G on a finite set X is called "arithmetically realizable over a number field F", if there is a set Y of solutions of a finite family of equations defined over $\mathcal{O}_F$, a bijection ψ from X to Y, and a group isomorphism ϕ from G to $\mathrm{Gal}(F(Y)/F)$ such that $\psi(gx) = \phi(g)\psi(x)$.

Inspiring by this definition, we can rewrite Theorem 1.7 as the following.

Theorem 1.7 (Second Version). *Suppose that the finite group G has an action on a finite set X that is arithmetically realizable over F. Let Y be as given in Definition* 1.10*. Then, for any $k \in \mathbb{N}$, we have*

$$M_k(G,X) = \lim_{x\to\infty} \frac{1}{\pi_F(x)} \sum_{N(\mathfrak{p})\le x} N_{\mathfrak{p}}^k(Y).$$

This formulation of Theorem 1.7 provides a line of approach in computing $M_k(G,X)$ for an arithmetically realizable action. Of course, more generally, one can consider the problem of computing $M_k(G,X)$ for an action of a group G on a set X. In this generality, the problem appears to be difficult, and we refer the reader to Cameron's survey [1] for results regarding the computation of $M_k(G,X)$ when the action of a permutation group G (finite or not) on a set X is oligomorphic (i.e. G has only finitely many orbits in X^k for all k).

Our purpose here is to demonstrate by some examples that for arithmetically realizable actions a number-theoretic approach via Theorem 1.7 and the Chebotarev density theorem might help one to compute $M_k(G,X)$. For instance, as a consequence of Propositions 1.12 and 1.13, we have the following explicit values for $M_k(G,X)$. (In all cases below, the actions are considered multiplicatively and in (ii) also componentwise.)

Theorem 1.11. (i) *If $G = (\mathbb{Z}/n\mathbb{Z})^\times$ and $X = \mathbb{Z}/n\mathbb{Z}$, we have $M_k(G,X) = M_k(n)$.*

(ii) *Let*

$$G = \left\{\begin{pmatrix} 1 & 0 \\ b & d\end{pmatrix};\ b \in \mathbb{Z}/n\mathbb{Z} \text{ and } d \in (\mathbb{Z}/n\mathbb{Z})^\times\right\} \simeq (\mathbb{Z}/n\mathbb{Z})^\times \ltimes \mathbb{Z}/n\mathbb{Z}.$$

If $X = (\{1\}\times\mathbb{Z}/n\mathbb{Z}) \times (\{0\}\times\mathbb{Z}/n\mathbb{Z})$, then $M_k(G,X) = M_{2k-1}(n)$.

(iii) *For prime ℓ, if $G = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and $X = \mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}$, then*

$$M_k(G,X) = \frac{\ell^4 - 2\ell^3 - \ell^2 + 3\ell}{(\ell^2-\ell)(\ell^2-1)} + \ell^k \frac{\ell^3 - 2\ell - 1}{(\ell^2-\ell)(\ell^2-1)} + \ell^{2k}\frac{1}{(\ell^2-\ell)(\ell^2-1)}.$$

The proof of Theorem 1.11 relies on explicit computations of the moment limit in Theorem 1.7 for certain algebraic sets Y via the prime number theorem in arithmetic progressions and more generally by the Chebotarev density theorem. We summarize these concrete evaluations in Propositions 1.12 and 1.13. For $n \in \mathbb{N}$ and integer $a \in \mathbb{Z}$, let

$$f_{n,a}(x) := x^n - a.$$

We have the following.

Proposition 1.12. *Let n be a natural number. Let a be a square-free positive integer if n is odd, and let a be a square-free positive integer such that $a \nmid n$ if n is even. Then the following estimates hold:*

(i) *For $k \in \mathbb{Z}^{\geq 0}$, $n \in \mathbb{N}$, we have*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} N_p^k(f_{n,1}) = M_k(n).$$

(ii) *For $k \in \mathbb{N}$, $n \in \mathbb{N}$, we have*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} N_p^k(f_{n,a}) = M_{k-1}(n).$$

(iii) *For any $k_1 \in \mathbb{N}$, $k_2 \in \mathbb{Z}^{\geq 0}$, we have*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} N_p^{k_1}(f_{n,a}) N_p^{k_2}(f_{n,1}) = M_{k_1+k_2-1}(n).$$

We next let E be an elliptic curve defined over $\mathbb{Q}$. For prime ℓ let $E[\ell]$ denote the group of ℓ-torsion points of E. The following assertions hold.

Proposition 1.13. (i) *Assume that* $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. *Then*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} N_p^k(E[\ell]) = \frac{\ell^4 - 2\ell^3 - \ell^2 + 3\ell}{(\ell^2-\ell)(\ell^2-1)} + \ell^k \frac{\ell^3 - 2\ell - 1}{(\ell^2-\ell)(\ell^2-1)} + \ell^{2k} \frac{1}{(\ell^2-\ell)(\ell^2-1)}.$$

(ii) *Let E have complex multiplication by $\mathcal{O}_K$, the ring of integers of an imaginary quadratic field K. For a fixed odd prime ℓ, assume that* $\mathrm{Gal}(K(E[\ell])/K) \simeq \mathrm{GL}_1(\mathcal{O}_K/\ell\mathcal{O}_K)$. *Then*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} N_p^k(E[\ell]) = \frac{2\ell^2 - (d_K(\ell)-1)\ell - (d_K(\ell)+2)}{2(\ell^2-1)} + \ell^k \frac{d_K(\ell)-1}{2(\ell-1)} + \ell^{2k} \frac{1}{2(\ell^2-1)},$$

where $d_K(\ell)$ is the number field analogue of the divisor function. More precisely, $d_K(\ell) = 4, 3, 2$ if ℓ splits, ramifies, or remains inert in K, respectively.

In the rest of this paper, we prove our results. The structure of this paper is as follows. In Sec. 2, we give a proof of Theorem 1.3. Section 3 provides a proof of our general result, Theorem 1.7, and Corollary 1.9. In Sec. 4, we compute some concrete examples of the kth moment in Theorem 1.7 by appealing to the prime number theorem in arithmetic progressions and the Chebotarev density theorem (Propositions 1.12 and 1.13). Combining the results proved in Secs. 3 and 4, in Sec. 5, by proving Theorem 1.11, we compute the number of orbits of certain finite groups acting on the product of k copies of certain finite sets. Finally, in Sec. 6, by applying the group-theoretic results proved in Sec. 5 and also Proposition 1.13(ii), we prove Theorem 1.4.

2. Proof of Theorem 1.3

Proof. We first give a proof for $L = \mathbb{Q}$ and then we show how the proof can be adjusted to the case of a number field L of class number one. We let $\mathrm{M}_{m\times 1}(\mathbb{Z}/n\mathbb{Z})$ be the collection of $m \times 1$ column vectors with entries in $\mathbb{Z}/n\mathbb{Z}$.

For $r \mid n$, a positive divisor r of n, the orbit of $\mathbf{r} = (r\ 0\ \cdots\ 0)^T \in \mathrm{M}_{m\times 1}(\mathbb{Z}/n\mathbb{Z})$ is $\langle \mathbf{r}\rangle = \{A\mathbf{r}; A \in \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})\}$. (By abuse of notation here we used r both as an integer and also as an element of $\mathbb{Z}/n\mathbb{Z}$.) Note that if $A\mathbf{r} = \mathbf{s}$, where $\mathbf{s} = (s_1\ s_2\ \cdots\ s_m)^T$, then $(r, n) \mid (s_1, \ldots, s_m, n)$. Also since $A^{-1}\mathbf{s} = \mathbf{r}$, we have $(s_1, \ldots, s_m, n) \mid (r, n)$. So, $A\mathbf{r} = \mathbf{s}$ implies that $(r, n) = (s_1, \ldots, s_m, n)$.

The above observation shows that for two distinct positive divisors of n like r_1 and r_2 the orbits $\langle \mathbf{r}_1\rangle$ and $\langle \mathbf{r}_2\rangle$ are disjoint. Indeed, if the two orbits intersect, for instance $A\mathbf{r}_1 = B\mathbf{r}_2 = \mathbf{s}$ for some $A, B \in \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$, then $(r_1, n) = (r_2, n) = (s_1, \ldots, s_m, n)$, and thus $r_1 = r_2$.

Next, we note that the two elements $A\mathbf{r}$ and $B\mathbf{r}$ in $\langle \mathbf{r}\rangle$ are equal if and only if $(n/r) \mid a_{i1} - b_{i1}$ for $1 \le i \le m$. Since the map sending $A \in \mathrm{GL}_m(\mathbb{Z}/n\mathbb{Z})$ to $A \in \mathrm{GL}_m(\mathbb{Z}/(n/r)\mathbb{Z})$ is onto, then for $r \neq n$ with $r \mid n$ the cardinality of $\langle \mathbf{r}\rangle$ is

$$\Psi(n/r) := \#\left\{\begin{pmatrix} a_{11} \\ \vdots \\ a_{m1}\end{pmatrix} \in \mathrm{M}_{m\times 1}(\mathbb{Z}/(n/r)\mathbb{Z}); \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm}\end{pmatrix} \in \mathrm{GL}_m(\mathbb{Z}/(n/r)\mathbb{Z})\right\}.$$

For $r = n$, we have $\langle \mathbf{r}\rangle = 1$, and so we define $\Psi(1) = 1$. Observe that, for a prime p, since the $p^m - 1$ possibilities for the first column of matrices in $\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$ lift to $(p^\alpha)^m - (p^{\alpha-1})^m$ possibilities for the first column of matrices in $\mathrm{GL}_m(\mathbb{Z}/p^\alpha\mathbb{Z})$, we have $\Psi(p^\alpha) = (p^\alpha)^m - (p^{\alpha-1})^m$.

We claim that $\sum_{r \mid n} \Psi(n/r) = n^m$. Since Ψ is multiplicative, in order to show this, it would suffice to show it for $n = p^\alpha$, a prime power. We have

$$\sum_{r \mid p^\alpha} \Psi(p^\alpha/r) = ((p^\alpha)^m - (p^{\alpha-1})^m) + \cdots + (p^m - 1) + 1 = (p^\alpha)^m.$$

Now, since $\sum_{r\,|\,n} \Psi(n/r) = n^m$, we conclude that the sets $\langle \mathbf{r} \rangle$ as r varies over distinct divisors of n form a partition of $(\mathbb{Z}/n\mathbb{Z})^m$, and thus the number of orbits is equal to $d(n)$.

Next, for a number field L of class number one, we note that for any integral ideal $\mathfrak{r}\,|\,(n)$ of $\mathcal{O}_L$, we may choose a representative r so that $\mathfrak{r} = (r)$. To process the argument as the case $L = \mathbb{Q}$, it suffices to note that if $r' = ur$ for some unit $u \in \mathcal{O}_L$, there is a matrix $A \in \mathrm{GL}_m(\mathcal{O}_L/n\mathcal{O}_L)$ whose $(1,1)$-entry is u such that $A\mathbf{r} = \mathbf{r}'$, where $\mathbf{r} = (r\ 0\ \cdots\ 0)^T$ and $\mathbf{r}' = (r'\ 0\ \cdots\ 0)^T$. This, in particular, implies that

$$\{A\mathbf{r}; A \in \mathrm{GL}_m(\mathcal{O}_L/n\mathcal{O}_L)\} = \{A\mathbf{r}'; A \in \mathrm{GL}_m(\mathcal{O}_L/n\mathcal{O}_L)\}. \qquad \square$$

Remark 2.1. For $L = \mathbb{Q}$ and $k = 1$, a short proof of Theorem 1.3 can be obtained by noticing that the group action can be realized as the action of the Galois group of $x^n - 1$ on the nth roots of unity. Now, the result follows since the roots of the dth cyclotomic polynomial $\Phi_d(x)$ are those roots of unity that have exactly order d, the cyclotomic polynomials $\Phi_d(x)$ are irreducible over $\mathbb{Q}$, and $x^n - 1 = \prod_{d\,|\,n} \Phi_d(x)$.

3. Proofs of Theorem 1.7 and Corollary 1.9

To prove Theorem 1.7, we require "Burnside's Lemma" stated as follows.

Lemma 3.1 (Burnside's Lemma). *Let G be a finite group acting on a finite set X, and let $\chi(g)$ be the number of fixed points of g on X. Then the number of orbits of G in X is equal to*

$$\frac{1}{|G|} \sum_{g \in G} \chi(g).$$

Proof. See [16, Proposition 1.1]. $\square$

Now, we are in a position to prove Theorem 1.7.

Proof of Theorem 1.7. Write $L = F(Y)$. Let $\mathfrak{p}$ denote an unramified prime in L/F, and let $\mathfrak{P}$ be a prime above $\mathfrak{p}$. Let E_Y be the family of polynomial equations defining Y. For any prime $\mathfrak{p}$ (respectively, $\mathfrak{P}$) of F (respectively, L), we let $S_{Y,\mathfrak{p}}$ (respectively, $S_{Y,\mathfrak{P}}$) denote the set of solutions of $E_Y \pmod{\mathfrak{p}}$ (respectively, $E_Y \pmod{\mathfrak{P}}$) in the residue field $\mathcal{O}_F/\mathfrak{p}$ (respectively, $\mathcal{O}_L/\mathfrak{P}$).

For any prime $\mathfrak{P}\,|\,\mathfrak{p}$, we write $\mathrm{Frob}_{\mathfrak{P}}$ for the generator of $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_F/\mathfrak{p}))$. Then we have

$$N_{\mathfrak{p}}(Y) = |S_{Y,\mathfrak{p}}| = \#\{y \in S_{Y,\mathfrak{P}}; y \text{ is fixed by } \mathrm{Frob}_{\mathfrak{P}}\},$$

where the last quantity is independent of the choice of $\mathfrak{P}$.

Now, let $\sigma_{\mathfrak{P}}$ be the lift of $\mathrm{Frob}_{\mathfrak{P}}$ to $\mathrm{Gal}(F(Y)/F)$ and $\sigma_{\mathfrak{p}} = \{\sigma_{\mathfrak{P}};\ \mathfrak{P}\,|\,\mathfrak{p}\}$ be the Artin symbol at $\mathfrak{p}$. For each m, let $G(m)$ stand for the set of elements in

$G = \mathrm{Gal}(F(Y)/F)$ that fixes exactly m points in Y. Then for any unramified $\mathfrak{p}$, we have that $N_{\mathfrak{p}}(Y) = m$ if and only if $\sigma_{\mathfrak{p}} \subseteq G(m)$. As one has

$$\sum_{N(\mathfrak{p})\le x} N_{\mathfrak{p}}^k(Y) = \sum_{m=0}^{|Y|} \sum_{\substack{N(\mathfrak{p})\le x \\ \sigma_{\mathfrak{p}}\subseteq G(m)}} m^k = \sum_{m=1}^{|Y|} m^k \sum_{\substack{N(\mathfrak{p})\le x \\ \sigma_{\mathfrak{p}}\subseteq G(m)}} 1,$$

the Chebotarev density theorem yields that

$$\lim_{x\to\infty} \frac{1}{\pi_F(x)} \sum_{N(\mathfrak{p})\le x} N_{\mathfrak{p}}^k(Y) = \sum_{m=1}^{|Y|} m^k \frac{|G(m)|}{|G|}. \tag{3.1}$$

We note that $\chi^k(g)$ is the number of points in $Y \times \cdots \times Y$, the k copies of Y, fixed by g. Thus, we can rewrite the sum on the right of (3.1) as

$$\sum_{m=1}^{|Y|} m^k \frac{|G(m)|}{|G|} = \frac{1}{|G|} \sum_{g\in G} \chi^k(g).$$

Now, we conclude the proof by applying Burnside's Lemma that asserts that the above average is the number of orbits of G in the k copies of Y. □

Proof of Corollary 1.9. The proof follows the method of moments as described on [5, pp. 59–61]. We observe that by Theorem 1.7 we have

$$\alpha_k := \lim_{n\to\infty} \int_{-\infty}^{\infty} z^k dH_n(z) = \lim_{n\to\infty} \frac{1}{\pi_F(n)} \sum_{N(\mathfrak{p})\le n} N_{\mathfrak{p}}^k(Y) = M_k(G, Y).$$

Note that

$$\alpha_k \ll |Y|^k.$$

Thus, for complex t-values with $|t| < 1$, the series

$$\sum_{k=0}^{\infty} \alpha_k \frac{(it)^k}{k!}$$

converges absolutely. Hence, from [5, Lemmata 1.43 and 1.44], it follows that the α_k determine a unique distribution function H that satisfies the conditions given in Corollary 1.9. □

4. Proofs of Propositions 1.12 and 1.13

Proof of Proposition 1.12. (i) As there are only finitely many primes p with $(p, n) > 1$, we may assume that $(p, n) = 1$. In particular, all summations below are over primes p with $(p, n) = 1$.

Since $\mathbb{F}_p^\times$ is a cyclic group of order $p - 1$, we have

$$N_p(f_{n,1}) = (p - 1, n).$$

Thus,

$$\sum_{p\le x} N_p^k(f_{n,1}) = \sum_{\substack{p\le x\\ d=(p-1,n)}} d^k = \sum_{d\,|\,n} d^k \sum_{\substack{p\le x\\ d=(p-1,n)}} 1 = \sum_{d\,|\,n} d^k \sum_{\substack{p\le x\\ d\,|\,p-1\\ \left(\frac{p-1}{d},\frac{n}{d}\right)=1}} 1,$$

which, by the Möbius inversion, is

$$\sum_{d\,|\,n} d^k \sum_{\substack{p\le x\\ d\,|\,p-1}} \sum_{e\,|\,\left(\frac{p-1}{d},\frac{n}{d}\right)} \mu(e) = \sum_{\substack{d,e\\ de\,|\,n}} d^k\mu(e) \sum_{\substack{p\le x\\ de\,|\,p-1}} 1.$$

Now, by the prime number theorem for arithmetic progressions, the last inner sum is asymptotic to

$$\frac{1}{\varphi(de)}\pi(x),$$

as $x\to\infty$, which completes the proof.

(ii) We may assume that $(p,na)=1$. In particular, all summations below (and also in (iii)) are over primes p with $(p,na)=1$.

It is known that $N_p(f_{n,a})\ne 0$ if and only if

$$a^{\frac{p-1}{d}} \equiv 1 \pmod p,$$

where $d=(p-1,n)$. Moreover, if $N_p(f_{n,a})\ne 0$, then $N_p(f_{n,a})=(p-1,n)$ (see [7, Proposition 4.2.1]). Thus, we have

$$\begin{aligned}\sum_{p\le x} N_p^k(f_{n,a})\\ &= \sum_{\substack{p\le x\\ d=(p-1,n)\\ a^{\frac{p-1}{d}}\equiv 1 \pmod p}} d^k = \sum_{d\,|\,n} d^k \sum_{\substack{p\le x\\ d=(p-1,n)\\ a^{\frac{p-1}{d}}\equiv 1 \pmod p}} 1 = \sum_{d\,|\,n} d^k \sum_{\substack{p\le x\\ d\,|\,p-1\\ \left(\frac{p-1}{d},\frac{n}{d}\right)=1\\ a^{\frac{p-1}{d}}\equiv 1 \pmod p}} 1.\end{aligned}$$

Again, the Möbius inversion yields

$$\sum_{p\le x} N_p^k(f_{n,a}) = \sum_{d\,|\,n} \sum_{\substack{p\le x\\ d\,|\,p-1\\ a^{\frac{p-1}{d}}\equiv 1 \pmod p}} \sum_{e\,|\,\left(\frac{p-1}{d},\frac{n}{d}\right)} \mu(e) = \sum_{\substack{d,e\\ de\,|\,n}} d^k\mu(e) \sum_{\substack{p\le x\\ de\,|\,p-1\\ a^{\frac{p-1}{d}}\equiv 1 \pmod p}} 1. \tag{4.1}$$

Now, we analyze the last inner sum in (4.1). For $d=1$, the sum is equal to

$$\sum_{\substack{p\le x\\ de\,|\,p-1}} 1$$

since the condition $a^{p-1}\equiv 1 \pmod p$ is always valid by Fermat's little theorem. This contributes

$$\frac{1}{\varphi(de)}\pi(x), \tag{4.2}$$

as $x \to \infty$. For $d \geq 2$, on the one hand, $de \mid p-1$ implies that $d \mid p-1$, which together with the condition

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$$

asserts that p splits completely in $\mathbb{Q}(\zeta_d, a^{1/d})/\mathbb{Q}$. On the other hand, the condition $de \mid p-1$ tells us that the prime p ($\neq 2$) splits completely in $\mathbb{Q}(\zeta_{de})/\mathbb{Q}$. Thus, for $d \geq 2$, the last inner sum in (4.1) is

$$\#\{p \leq x; p \text{ splits completely in } \mathbb{Q}(\zeta_{de}, a^{1/d})/\mathbb{Q}\} \sim \frac{1}{d\varphi(de)}\pi(x), \tag{4.3}$$

as $x \to \infty$, where the asymptotic behavior is assured by the Chebotarev density theorem for the Galois extension $\mathbb{Q}(\zeta_{de}, a^{1/d})/\mathbb{Q}$, and the fact that under given conditions on a, $[\mathbb{Q}(\zeta_{de}, a^{1/d}) : \mathbb{Q}] = d\varphi(de)$ (see [10, Lemma 1]). Applying (4.2) and (4.3) in (4.1) and observing that $d^{k-1} = 1$ if $d = 1$, we conclude the proof.

(iii) It suffices to note that the sum is, in fact, equal to

$$\sum_{\substack{p \leq x \\ d=(p-1,n) \\ a^{\frac{p-1}{d}} \equiv 1 \pmod{p}}} d^{k_1} d^{k_2}.$$

Now, the result follows from part (ii). □

Proof of Proposition 1.13. During the proof, we assume that $p \geq 5$ is a prime such that $p \nmid \ell N_E$, where N_E is the conductor of E.

(i) Let $E_p(\mathbb{F}_p)$ be the set of $\mathbb{F}_p$-points of E_p (the reduction modulo p of E). Observe that $N_p(E[\ell]) = |E_p(\mathbb{F}_p)[\ell]|$, where $E_p(\mathbb{F}_p)[\ell]$ is the set of ℓ-torsion points of $E_p(\mathbb{F}_p)$. Note that since $E_p(\mathbb{F}_p)[\ell] \subseteq E_p[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, $E_p(\mathbb{F}_p)[\ell]$ has either 1, ℓ, or ℓ^2 elements. Moreover, it is known that $N_p(E[\ell]) = |E_p(\mathbb{F}_p)[\ell]| = \ell^2$ if and only if p splits completely in the ℓ-division field $L = \mathbb{Q}(E[\ell])$ of E (see [11, Lemma 2]).

If $N_p(E[\ell]) = \ell$, then for a prime $\mathfrak{P} \mid p$ we can conclude that $\sigma_{\mathfrak{P}}$ (the lift of $\mathrm{Frob}_{\mathfrak{P}}$ to $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$) can have a representation in the form

$$\begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_\ell) \Big\backslash \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \tag{4.4}$$

for some $b \in \mathbb{F}_\ell$ and $c \in \mathbb{F}_\ell^\times$. Thus, $N_p(E[\ell]) = \ell$ if and only if the Artin symbol σ_p considered as a conjugacy class of $\mathrm{GL}_2(\mathbb{F}_\ell)$ has an element of the form (4.4). By the Jordan canonical form, a matrix of the form (4.4) is conjugate to either

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} \tag{4.5}$$

for some $c \in \mathbb{F}_\ell^\times \backslash \{1\}$. Now, from the classification of conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_\ell)$ (see [9, Table 12.4, p. 714]), it may be computed that the number of elements of such forms in $\mathrm{GL}_2(\mathbb{F}_\ell)$ is $\ell^3 - 2\ell - 1$. (Indeed, the "unipotent" instance in (4.5) contributes ℓ^2-1 conjugate elements, and the "rational not central" instances in (4.5) contribute $(\ell-2)(\ell^2+\ell)$ elements.)

Let $\pi_E(x;\ell,i)$ for $0\le i\le 2$ be defined as

$$\pi_E(x;\ell,i)=\#\{p\le x; N_p(E[\ell])=\ell^i\}. \tag{4.6}$$

The above discussion, together with the Chebotarev density theorem and the fact that by our assumption $[\mathbb{Q}(E[\ell]):\mathbb{Q}]=(\ell^2-\ell)(\ell^2-1)$, yields that, as $x\to\infty$,

$$\pi_E(x;\ell,1)\sim\frac{\ell^3-2\ell-1}{(\ell^2-\ell)(\ell^2-1)}\pi(x)\quad\text{and}\quad \pi_E(x;\ell,2)\sim\frac{1}{(\ell^2-\ell)(\ell^2-1)}\pi(x).$$

Hence, as $x\to\infty$,

$$\pi_E(x;\ell,0)\sim\frac{\ell^4-2\ell^3-\ell^2+3\ell}{(\ell^2-\ell)(\ell^2-1)}\pi(x).$$

Clearly, it follows from (4.6) that

$$\sum_{p\le x}N_p^k(E[\ell])=1^k\cdot\pi_E(x;\ell,0)+\ell^k\cdot\pi_E(x;\ell,1)+\ell^{2k}\cdot\pi_E(x;\ell,2).$$

Therefore, $\lim_{x\to\infty}\frac{1}{\pi(x)}\sum_{p\le x}N_p^k(E[\ell])$ equals to

$$\frac{\ell^4-2\ell^3-\ell^2+3\ell}{(\ell^2-\ell)(\ell^2-1)}+\ell^k\frac{\ell^3-2\ell-1}{(\ell^2-\ell)(\ell^2-1)}+\ell^{2k}\frac{1}{(\ell^2-\ell)(\ell^2-1)}.$$

(ii) We have

$$\sum_{p\le x}N_p^k(E[\ell])=\sum_{\substack{p\le x\\ p\text{ splits in }K}}N_p^k(E[\ell])+\sum_{\substack{p\le x\\ p\text{ is inert or ramifies in }K}}N_p^k(E[\ell]). \tag{4.7}$$

It is known that if p is inert or ramifies in K, then p is supersingular [8, Theorem 12, p. 182], which implies that (for $p\ge 5$) $|E_p(\mathbb{F}_p)|=p+1$ [17, Exercise 5.10(b), p. 145] and the odd part of $E_p(\mathbb{F}_p)$ is cyclic [12, Theorem 1]. So, for odd ℓ, we have $N_p(E[\ell])=(\ell,p+1)$. Following the proof of Proposition 1.12(i), we conclude that

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\sum_{\substack{p\le x\\ p\text{ is inert or ramifies in }K}}N_p^k(E[\ell])=\frac{1}{2}M_k(\ell)=\frac{\ell-2}{2(\ell-1)}+\ell^k\frac{1}{2(\ell-1)}. \tag{4.8}$$

For $0\le i\le 2$, we let

$$\pi_E^s(x;\ell,i)=\#\{p\le x;\ p\text{ splits in }K\text{ and }N_p(E[\ell])=\ell^i\}.$$

It follows from the definition that

$$\sum_{\substack{p\le x\\ p\text{ splits in }K}}N_p^k(E[\ell])=1^k\cdot\pi_E^s(x;\ell,0)+\ell^k\cdot\pi_E^s(x;\ell,1)+\ell^{2k}\cdot\pi_E^s(x;\ell,2). \tag{4.9}$$

Recall that $N_p(E[\ell]) = \ell^2$ if and only if p splits completely in $L = \mathbb{Q}(E[\ell])$ [11, Lemma 2]. Now, let $p\mathcal{O}_K = (\pi_p\mathcal{O}_K)(\bar{\pi}_p\mathcal{O}_K)$, then $p\mathcal{O}_L$ splits completely in L if and only if $p\mathcal{O}_K$ splits completely in L. Also since, for odd ℓ, $L = \mathbb{Q}(E[\ell]) = K(E[\ell])$ [11, Lemma 6] and $[K(E[\ell]) : K] = \ell^2 - 1$ (according to the assumption), by an application of the Chebotarev density theorem for the extension $K(E[\ell])/K$, we have

$$\begin{aligned}\pi_E^s(x;\ell,2) &= \#\{p \le x;\ p\mathcal{O}_K \text{ splits in } K \text{ and } p\mathcal{O}_L \text{ splits in } \mathbb{Q}(E[\ell])\}\\ &= \frac{1}{2}\#\{\mathfrak{p} \subset \mathcal{O}_K;\ N(\mathfrak{p}) \le x \text{ and } \mathfrak{p} \text{ splits in } K(E[\ell])\} + O\left(\frac{x^{1/2}}{\log x}\right)\\ &= \frac{\pi_K(x)}{2(\ell^2-1)}(1+o(1)) + O\left(\frac{x^{1/2}}{\log x}\right).\end{aligned}$$

The above asymptotic formula together with applications of the Chebotarev density theorem and the fact that $\pi_K(x) \sim \pi(x)$, as $x \to \infty$, result in

$$\begin{aligned}&\pi_E^s(x;\ell,0) \sim \delta_0^s(\ell)\pi(x), \quad \pi_E^s(x;\ell,1) \sim \delta_1^s(\ell)\pi(x), \quad \text{and}\\ &\pi_E^s(x;\ell,2) \sim \frac{1}{2(\ell^2-1)}\pi(x),\end{aligned} \tag{4.10}$$

as $x \to \infty$, where the densities $\delta_0^s(\ell)$ and $\delta_1^s(\ell)$ exist following the discussion at the beginning of (i). Hence, from (4.9) with $k = 0$, we have

$$\delta_0^s(\ell) + \delta_1^s(\ell) + \frac{1}{2(\ell^2-1)} = \frac{1}{2}. \tag{4.11}$$

Also, from (4.9) with $k = 1$, we have

$$\delta_0^s(\ell) + \ell\delta_1^s(\ell) + \frac{\ell^2}{2(\ell^2-1)} = \lim_{x\to\infty}\frac{1}{\pi(x)}\sum_{\substack{p\le x\\ p \text{ splits in } K}} N_p(E[\ell]). \tag{4.12}$$

For a splitting prime p, writing $p\mathcal{O}_K = (\pi_p\mathcal{O}_K)(\bar{\pi}_p\mathcal{O}_K)$ and denoting the reduction (mod $\pi_p\mathcal{O}_K$) of E by $E_{\pi_p}(\mathcal{O}_K/\pi_p\mathcal{O}_K)$, we have

$$N_p(E[\ell]) = |E_p(\mathbb{F}_p)[\ell]| = |E_{\pi_p}(\mathcal{O}_K/\pi_p\mathcal{O}_K)[\ell]| = N_{\pi_p\mathcal{O}_K}(E[\ell]).$$

A similar identity holds by replacing π_p with $\bar{\pi}_p$. Thus,

$$\sum_{\substack{p\le x\\ p \text{ splits in } K}} N_p(E[\ell]) = \frac{1}{2}\sum_{\substack{\mathfrak{p}\subset\mathcal{O}_K\\ N(\mathfrak{p})\le x}} N_{\mathfrak{p}}(E[\ell]) + O\left(\frac{x^{1/2}}{\log x}\right).$$

From this and the fact that $\pi(x) \sim \pi_K(x)$, as $x \to \infty$, we obtain

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\sum_{\substack{p\le x\\ p \text{ splits in } K}} N_p(E[\ell]) = \lim_{x\to\infty}\frac{1}{2\pi_K(x)}\sum_{\substack{\mathfrak{p}\subset\mathcal{O}_K\\ N(\mathfrak{p})\le x}} N_{\mathfrak{p}}(E[\ell]).$$

Now, Theorem 1.7 yields that

$$\lim_{x\to\infty}\frac{1}{2\pi_K(x)}\sum_{\substack{\mathfrak{p}\subset\mathcal{O}_K\\ N(\mathfrak{p})\le x}} N_{\mathfrak{p}}(E[\ell]) = \frac{1}{2}M_1(\mathrm{GL}_1(\mathcal{O}_K/\ell\mathcal{O}_K),\mathcal{O}_K/\ell\mathcal{O}_K).$$

We know that K has class number 1 (see [17, Appendix C, Example 11.3.1]). Therefore, by Theorem 1.3, we have

$$M_1(\mathrm{GL}_1(\mathcal{O}_K/\ell\mathcal{O}_K),\mathcal{O}_K/\ell\mathcal{O}_K) = d_K(\ell),$$

where $d_K(\ell)$ is the divisor function for the number field K. Applying this value in (4.12) yields

$$\delta_0^s(\ell)+\ell\delta_1^s(\ell)+\frac{\ell^2}{2(\ell^2-1)} = \frac{1}{2}d_K(\ell). \tag{4.13}$$

Solving the system of Eqs. (4.11) and (4.13) yields

$$\delta_0^s(\ell) = \frac{\ell^2-(d_K(\ell)-2)\ell-d_K(\ell)}{2(\ell^2-1)} \quad \text{and} \quad \delta_1^s(\ell) = \frac{d_K(\ell)-2}{2(\ell-1)}.$$

Employing these values in (4.10) together with (4.9), (4.8), and (4.7) yield the result. □

5. Proof of Theorem 1.11

(i) Let $F=\mathbb{Q}$ and $Y=\{\zeta_n^i;\ i=1,\ldots,n\}$ be the set of zeros of the polynomial $f_{n,1}(x)=x^n-1$ in $\overline{\mathbb{Q}}$, where ζ_n denotes a primitive nth root of unity. Consider the bijection $\psi: X=\mathbb{Z}/n\mathbb{Z}\to Y$, where $\psi(i)=\zeta_n^i$ and note that $\phi: G=(\mathbb{Z}/n\mathbb{Z})^\times\to \mathrm{Gal}(F(Y)/F)$ defined by $\phi(d)=\phi_d$, where $\phi_d(\zeta_n^j)=\zeta_n^{jd}$, is a group isomorphism. Thus, from Theorem 1.7 and Proposition 1.12(i) we have

$$M_k(G,X) = \lim_{x\to\infty}\frac{1}{\pi(x)}\sum_{p\le x}N_p^k(f_{n,1}) = M_k(n).$$

(ii) Let a be a square-free positive integer if n is odd, and let a be a square-free positive integer such that $a\nmid n$ if n is even. Let the number $a^{1/n}$ be a real solution of the equation $x^n-a=0$. Let $F=\mathbb{Q}$ and $Y=\{(a^{1/n}\zeta_n^i,\zeta_n^j);\ 1\le i,j\le n\}$ be the set of zeros of the system of polynomials $f_{n,a}(x)=x^n-a$ and $f_{n,1}(y)=y^n-1$ in $\overline{\mathbb{Q}}\times\overline{\mathbb{Q}}$. Consider the bijection $\psi: X=(\{1\}\times\mathbb{Z}/n\mathbb{Z})\times(\{0\}\times\mathbb{Z}/n\mathbb{Z})\to Y$, where $\psi(((1,i),(0,j)))=(a^{1/n}\zeta_n^i,\zeta_n^j)$ and note that $\phi: G\to\mathrm{Gal}(F(Y)/F)$ defined by $\phi\left(\left(\begin{smallmatrix}1&0\\ b&d\end{smallmatrix}\right)\right)=\phi_{b,d}$ is an isomorphism, where $\phi_{b,d}((a^{1/n}\zeta_n^i,\zeta_n^j))=(a^{1/n}\zeta_n^{b+id},\zeta_n^{jd})$.

We note that $N_p(Y)$ is the number of solutions (x,y) of $x^n\equiv a \pmod p$ and $y^n\equiv 1 \pmod p$, which is equal to $N_p(f_{n,a})N_p(f_{n,1})$. Thus, from Theorem 1.7, we have

$$M_k(G,X) = \lim_{x\to\infty}\frac{1}{\pi(x)}\sum_{p\le x}N_p^k(Y) = \lim_{x\to\infty}\frac{1}{\pi(x)}\sum_{p\le x}(N_p(f_{n,a})N_p(f_{n,1}))^k,$$

where the limit on the right can be computed by Proposition 1.12(iii).

(iii) For $\ell \neq 2$, let $E[\ell]$ be the ℓ-torsion subgroup of the elliptic curve E_{17a3} (with Cremona label $17a3$), and, for $\ell = 2$, let $E[\ell]$ be corresponded to E_{11a2} (with Cremona label $11a2$). Then $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ (see [18] for details).

For such E, let $F = \mathbb{Q}$ and $Y = E[\ell]$. Consider the bijection $\psi : X = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \to E[\ell]$ and note that $G = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \simeq_\phi \mathrm{Gal}(F(Y)/F)$. Thus, from Theorem 1.7 and Proposition 1.13(i), we have

$$\begin{aligned} M_k(G,X) &= \lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\le x} N_p^k(E[\ell]) \\ &= \frac{\ell^4 - 2\ell^3 - \ell^2 + 3\ell}{(\ell^2-\ell)(\ell^2-1)} + \ell^k \frac{\ell^3 - 2\ell - 1}{(\ell^2-\ell)(\ell^2-1)} + \ell^{2k} \frac{1}{(\ell^2-\ell)(\ell^2-1)}. \end{aligned}$$

6. Proof of Theorem 1.4

(i) Since the corresponding action of $\mathrm{Gal}(F(\mathbb{G}_m[n])/F)$ on $\mathbb{G}_m[n]$ is a realization of the canonical action of $G = (\mathbb{Z}/n\mathbb{Z})^\times$ on $X = \mathbb{Z}/n\mathbb{Z}$, the assertion follows from Theorem 1.11(i) immediately.

(ii) Let $\mathbb{T}$ over $\mathbb{Q}$ be defined by the equation $x^2 - my^2 = 1$, where m is a square-free integer. Then

$$\mathbb{T}[n] = \left\{ \left(\frac{\zeta_n^i + \zeta_n^{-i}}{2}, \frac{\zeta_n^i - \zeta_n^{-i}}{2\sqrt{m}} \right); 1 \le i \le n \right\}$$

is the set of n-torsion points of $\mathbb{T}$. By [2, Lemma 2.1], we know that there is a constant C such that for $(n, C) = 1$, we have $\mathbb{Q}(\mathbb{T}[n]) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}, (\zeta_n - \zeta_n^{-1})/\sqrt{m})$ and $[\mathbb{Q}(\mathbb{T}[n]) : \mathbb{Q}] = \varphi(n)$. Thus, for $1 \le d \le n$ with $(d, n) = 1$, the maps

$$\sigma_d \left(\frac{\zeta_n + \zeta_n^{-1}}{2}, \frac{\zeta_n - \zeta_n^{-1}}{2\sqrt{m}} \right) = \left(\frac{\zeta_n^d + \zeta_n^{-d}}{2}, \frac{\zeta_n^d - \zeta_n^{-d}}{2\sqrt{m}} \right)$$

give the $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\mathbb{T}[n])$, and therefore the action of $\mathrm{Gal}(\mathbb{Q}(\mathbb{T}[n])/\mathbb{Q})$ on $\mathbb{T}[n]$ is a realization of the action of $G = (\mathbb{Z}/n\mathbb{Z})^\times$ on $X = \mathbb{Z}/n\mathbb{Z}$. Now, the result follows from Theorem 1.11(i).

(iii) Let E be a non-CM elliptic curve defined over F, and let $n = \prod_\ell \ell$ be square-free. By Serre's open image theorem [13], there exists a constant C such that for $(\ell, C) = 1$, we have $\mathrm{Gal}(F(E[\ell])/F) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. We note that

$$\mathrm{Gal}(F(E[n])/F) \simeq \prod_{\ell \mid n} \mathrm{Gal}(F(E[\ell])/F)$$

acts on $\prod_{\ell \mid n} (\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z})^k$ componentwise (i.e. the action is the product of the actions of $\mathrm{Gal}(F(E[\ell])/F)$ on $(\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z})^k$). Thus, we have

$$M_k(E/F, n) = \prod_{\ell \mid n} M_k(E/F, \ell). \tag{6.1}$$

Now, applying (6.1) together with Theorem 1.11(iv) completes the proof.

(iv) The proof follows along the same lines as (iii) via employing Deuring's theorem [4] on the image of $\mathrm{Gal}(K(E[\ell])/K)$ and Proposition 1.13(ii).

Acknowledgments

Research of the first author is partially supported by NSERC. Research of the second author is partially supported by a PIMS postdoctoral fellowship. The authors would like to thank the referee for the valuable comments and suggestions.

References

[1] P. J. Cameron, Some counting problems related to permutation groups, *Discrete Math.* **225** (2000) 77–92.
[2] Y.-M. J. Chen and Y.-L. Kuan, On the distribution of torsion points modulo primes, *Bull. Austral. Math. Soc.* **86** (2012) 339–347.
[3] Y.-M. J. Chen and Y.-L. Kuan, On the distribution of torsion points modulo primes: The case of function fields, *Manuscripta Math.* **148** (2015) 435–445.
[4] M. Deuring, Die typen multiplikatorenringe elliptischer funktionenkörper, *Abh. Math. Sem. Univ. Hamburg* **14** (1941) 197–272.
[5] P. D. T. A. Elliott, *Probabilistic Number Theory I*, Grundlehren der Mathematischen Wissenschaften, Vol. 239 (Springer-Verlag, New York–Berlin, 1979).
[6] H.-L. Huang, The average number of torsion points on elliptic curves, *J. Number Theory* **135** (2014) 374–389.
[7] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edition, Graduate Texts in Mathematics, Vol. 84 (Springer-Verlag, New York, 1990).
[8] S. Lang, *Elliptic Functions*, 2nd edition (Springer-Verlag, New York, 1987).
[9] S. Lang, *Algebra*, 3rd edition (Addison-Wesley Publishing, 1993).
[10] P. Moree, On the distribution of the order and index of $g \pmod p$ over residue classes–I, *J. Number Theory* **114** (2005) 238–271.
[11] M. R. Murty, On Artin's conjecture, *J. Number Theory* **16** (1983) 147–168.
[12] M. R. Murty, On the supersingular reduction of elliptic curves, *Proc. Indian Acad. Sci. Math. Sci.* **97** (1987) 247–250.
[13] J.-P. Serre, Propriétés galoisiennes de points d'order fini des courbes elliptiques, *Invent. Math.* **15** (1972) 259–331.
[14] J.-P. Serre, On a theorem of Jordan, *Bull. Amer. Math. Soc.* **40**(4) (2003) 429–440.
[15] J.-P. Serre, *Lectures on $N_X(p)$*, Research Notes in Mathematics, Vol. 11 (CRC Press, 2012).
[16] J.-P. Serre, *Finite Groups: An Introduction* (International Press, Higher Education Press, 2016).
[17] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Vol. 151 (Springer, New York, 1986).
[18] The LMFDB Collab., The L-functions and modular forms database (2013), http://www.lmfdb.org.