A. Bucur et al. (2016) "The Distribution of $\mathbb{F}_q$-Points on Cyclic ℓ-Covers of Genus g,"
International Mathematics Research Notices, Vol. 2016, No. 14, pp. 4297–4340
Advance Access Publication October 1, 2015
doi:10.1093/imrn/rnv279

The Distribution of $\mathbb{F}_q$-Points on Cyclic ℓ-Covers of Genus g

Alina Bucur[1], Chantal David[2], Brooke Feigon[3], Nathan Kaplan[4], Matilde Lalín[5], Ekin Ozman[6], and Melanie Matchett Wood[7]

[1]Department of Mathematics, University of California at San Diego, 9500 Gilman Drive #0112, La Jolla, CA 92093, USA, [2]Department of Mathematics and Statistics, Concordia University, 1455 de Maisonneuve West, Montreal, QC H3G 1M8, Canada, [3]Department of Mathematics, The City College of New York and CUNY Graduate Center, NAC 8/133, New York, NY 10031, USA, [4]Department of Mathematics, University of California, Irvine, CA 92697, USA, [5]Département de Mathématiques et de Statistique, Université de Montréal, CP 6128, succ. Centre-ville, Montreal, QC H3C 3J7, Canada, [6]Faculty of Arts and Science, Department of Mathematics, Bogazici University, 34342 Bebek-Istanbul, Turkey, and [7]Department of Mathematics, University of Wisconsin-Madison, 480 Lincoln Drive, Madison, WI 53706, USA and American Institute of Mathematics, 360 Portage Avenue, Palo Alto, CA 94306-2244, USA

Correspondence to be sent to: e-mail: bfeigon@ccny.cuny.edu

We study fluctuations in the number of points of ℓ-cyclic covers of the projective line over the finite field $\mathbb{F}_q$ when $q \equiv 1 \bmod \ell$ is fixed and the genus tends to infinity. The distribution is given as a sum of $q+1$ i.i.d. random variables. This was settled for hyperelliptic curves by Kurlberg and Rudnick [7], while statistics were obtained for certain components of the moduli space of ℓ-cyclic covers in [1]. In this paper, we obtain statistics for the distribution of the number of points as the covers vary over the full moduli space of

Received December 12 2014; Revised July 3, 2015; Accepted August 25, 2015

ℓ-cyclic covers of genus g. This is achieved by relating ℓ-covers to cyclic function field extensions, and counting such extensions with prescribed ramification and splitting conditions at a finite number of primes.

1 Introduction and Results

Let q be a prime power and let $\mathbb{F}_q$ be the finite field with q elements. The goal of this paper is to establish statistics for the distribution of the number of $\mathbb{F}_q$-points of ℓ-cyclic covers C of $\mathbb{P}^1$ defined over $\mathbb{F}_q$, as C varies over the moduli space $\mathcal{H}_{g,\ell}$ of such covers of genus g for large g (and fixed q). We always suppose that ℓ is a prime number such that $q \equiv 1 \pmod{\ell}$. For $\ell = 2$ (the case of hyperelliptic curves), this was addressed by Kurlberg and Rudnick [7] who showed that the probability that $\#C(\mathbb{F}_q) = m$ for some integer m is the probability that the sum of $q+1$ independent and identically distributed (i.i.d.) random variables is equal to m. This was generalized to cyclic ℓ-covers of degree d by the first, second, third, and fifth authors in [1] who obtained statistics for each irreducible component $\mathcal{H}^{(d_1,\dots,d_{\ell-1})}$ of the moduli space

$$\mathcal{H}_{g,\ell} = \bigcup_{\substack{d_1+2d_2+\cdots+(\ell-1)d_{\ell-1}\equiv 0 \pmod{\ell}, \\ 2g=(\ell-1)(d_1+\cdots+d_{\ell-1}-2)}} \mathcal{H}^{(d_1,\dots,d_{\ell-1})}, \tag{1}$$

as $\min\{d_1, d_2, \dots, d_\ell\}$ tends to infinity. These components will be defined in Section 5.1. Similarly to the hyperelliptic case, the probability that $\#C(\mathbb{F}_q) = m$ for some integer m, as C varies over $\mathcal{H}^{(d_1,\dots,d_{\ell-1})}$ and $\min\{d_1,\dots,d_{\ell-1}\} \to \infty$, is the probability that the sum of $q+1$ i.i.d. random variables is equal to m. The i.i.d. random variables $X_1,\dots,X_{q+1}$ are given by (for any prime $\ell \geq 2$)

$$X_i = \begin{cases} 0 & \text{with probability } \dfrac{(\ell-1)\,q}{\ell\,(q+\ell-1)}, \\ 1 & \text{with probability } \dfrac{\ell-1}{q+\ell-1}, \\ \ell & \text{with probability } \dfrac{q}{\ell\,(q+\ell-1)}. \end{cases} \tag{2}$$

As the statistics hold for $\min\{d_1,\dots,d_{\ell-1}\} \to \infty$, this result does not give statistics for the distribution of the number of $\mathbb{F}_q$-points on covers as we vary over all of $\mathcal{H}_{g,\ell}$, since $g \to \infty$ does not mean that $\min\{d_1,\dots,d_{\ell-1}\} \to \infty$ on all components $\mathcal{H}^{(d_1,\dots,d_{\ell-1})}$ for a given genus in (1). Other statistics for cyclic ℓ-covers were also obtained by counting the covers in a different way (which does not preserve the genus) by Xiong [16] and Cheong et al. [2], and the distribution of the number of (affine) $\mathbb{F}_q$-points on those covers was also given by a sum of i.i.d. random variables but with different probabilities from the random variables of (2).

We show in this paper that the statistics for the distribution of the number of $\mathbb{F}_q$-points for covers in $\mathcal{H}_{g,\ell}$ are also given by the random variables (2). The strategy is completely different from the work in [1]. There, the counting is done directly by considering affine models for the covers in each separate component $\mathcal{H}^{(d_1,\ldots,d_{\ell-1})}$ of the moduli space. Here, we study the equivalent question of counting the number of extensions of the function field $K=\mathbb{F}_q(X)$ with Galois group $\mathbb{Z}/\ell\mathbb{Z}$, conductor of degree $\mathfrak{n}$, and prescribed splitting/ramification conditions at a finite set of fixed primes of $\mathbb{F}_q(X)$. As a result, we directly obtain the total count in $\mathcal{H}_{g,\ell}$. We explain in Section 5 why these two questions are equivalent, and give general formulas for the number of points on covers in terms of the distribution of the function field extensions that they define.

In order to count the cyclic function field extensions associated to our statistics for point counting on covers, we use a classical approach described by Wright [15] (and first due to Cohn [4] for the case of cubic extensions of the rationals), which is to study the generating series

$$\sum_{\mathrm{Gal}(L/K)\cong G} \mathfrak{D}\,(L/K)^{-s}\,, \tag{3}$$

where $\mathfrak{D}(L/K)$ is the absolute norm of the discriminant $\mathrm{Disc}(L/K)$. The approach uses class field theory to give an explicit expression for the Dirichlet series (3). This is done in generality by Wright in [15] for any global field K and any abelian group G. The count is then obtained by an application of the Tauberian theorem, and the main term is given by the rightmost pole of the Dirichlet series. The order of this pole varies according to the group G and the ground field K, (more precisely with the number of roots of unity in K). This is described in [15, Theorem 1.1].

In this paper, we apply those techniques to the case $K=\mathbb{F}_q(X)$ and $G=\mathbb{Z}/\ell\mathbb{Z}$, and we further restrict to counting extensions with prescribed splitting conditions at the $\mathbb{F}_q$-rational places of K. To find our desired statistics for point counts of curves, we need to obtain explicit constants in our asymptotics, and in particular to understand how those constants change as we change the splitting conditions. For this, we use the last author's further development of Wright's method in [13], which determines probabilities of various splitting types in abelian extensions of number fields. We are also interested in the secondary terms and the power saving that can be obtained after taking them into consideration. Our results can then be used to get the distribution of the number of points on covers as we vary over all of $\mathcal{H}_{g,\ell}$, but also have other applications for statistics on the moduli spaces of curves over finite fields, such as the power of traces and the one-level density. We give more details about these applications in Section 1.1. We also compute the values of the constants for the leading term of the asymptotic formulas, so the counts obtained with those techniques can be compared with the counts of [1] (see Section 5.1).

We now state the main results of our paper. We first define some notation. Let $\mathcal{V}_K$ be the set of places of K. Let $N(\mathbb{Z}/\ell\mathbb{Z},\mathfrak{n})$ be the number of extensions of $K=\mathbb{F}_q(X)$ with Galois group $\mathbb{Z}/\ell\mathbb{Z}$ such that the degree of the conductor is equal to $\mathfrak{n}$. Let $\mathcal{V}_R$, $\mathcal{V}_S$, $\mathcal{V}_I$ denote three finite and disjoint sets of places of $\mathbb{F}_q(X)$, and let $N(\mathbb{Z}/\ell\mathbb{Z},\mathfrak{n};\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I)$ be the number of extensions of $\mathbb{F}_q(X)$ with Galois group $\mathbb{Z}/\ell\mathbb{Z}$, which are ramified at the places of $\mathcal{V}_R$, split at the places of $\mathcal{V}_S$, and inert at the places of $\mathcal{V}_I$, and such that the degree of the conductor is equal to $\mathfrak{n}$.

Theorem 1.1. Let $\ell\geq 2$ be a prime. Let $\mathcal{V}_R$, $\mathcal{V}_S$, $\mathcal{V}_I$, and $N(\mathbb{Z}/\ell\mathbb{Z},\mathfrak{n};\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I)$ be as defined above, and let $\mathcal{V}=\mathcal{V}_R\cup\mathcal{V}_S\cup\mathcal{V}_I$. Then,

$$N\left(\mathbb{Z}/\ell\mathbb{Z},\mathfrak{n}\right)=C_\ell q^{\mathfrak{n}}P\left(\mathfrak{n}\right)+O\left(q^{\left(\frac{1}{2}+\varepsilon\right)\mathfrak{n}}\right),$$

$$N\left(\mathbb{Z}/\ell\mathbb{Z},\mathfrak{n};\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I\right)=C_\ell\left(\prod_{v\in\mathcal{V}}c_v\right)q^{\mathfrak{n}}P_{\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I}\left(\mathfrak{n}\right)+O\left(q^{\left(\frac{1}{2}+\varepsilon\right)\mathfrak{n}}\right),$$

where $P(X)$, $P_{\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I}(X)\in\mathbb{R}[X]$ are monic polynomials of degree $\ell-2$. Furthermore, C_ℓ is the non-zero constant given by

$$C_\ell=\frac{\left(1-q^{-2}\right)^{\ell-1}}{(\ell-2)!}\prod_{j=1}^{\ell-2}\prod_{v\in\mathcal{V}_K}\left(1-\frac{jq^{-2\deg v}}{\left(1+q^{-\deg v}\right)\left(1+jq^{-\deg v}\right)}\right),\tag{4}$$

and, for each place $v\in\mathcal{V}$, we have

$$c_v=\begin{cases}\dfrac{(\ell-1)\,q^{-\deg v}}{1+(\ell-1)\,q^{-\deg v}} & \text{if } v\in\mathcal{V}_R,\\[2ex] \dfrac{1}{\ell\left(1+(\ell-1)\,q^{-\deg v}\right)} & \text{if } v\in\mathcal{V}_S,\\[2ex] \dfrac{\ell-1}{\ell\left(1+(\ell-1)\,q^{-\deg v}\right)} & \text{if } v\in\mathcal{V}_I.\end{cases}$$

Furthermore, for $\ell = 2$ we obtain the exact count

$$N(\mathbb{Z}/2\mathbb{Z}, \mathfrak{n}) = \begin{cases} 2\left(q^{\mathfrak{n}} - q^{\mathfrak{n}-2}\right) & \mathfrak{n} > 2, \mathfrak{n} \text{ even}, \\ 2q^2 & \mathfrak{n} = 2, \\ 0 & \mathfrak{n} \text{ odd}. \end{cases}$$

$$N(\mathbb{Z}/2\mathbb{Z}, \mathfrak{n}, v_0, \text{ramified}) = \frac{\left(1 - q^{-2}\right)}{1 + q^{-\deg v_0}} q^{\mathfrak{n} - \deg v_0} + O_q(1). \qquad \square$$

We prove Theorem 1.1 by using class field theory to show that counting $\mathbb{Z}/\ell\mathbb{Z}$ extensions of $\mathbb{F}_q(X)$ is equivalent to counting continuous homomorphisms of the idèle class group of $\mathbb{F}_q(X)$ to $\mathbb{Z}/\ell\mathbb{Z}$. This is the method implemented by [15] for general abelian extensions over function fields and number fields, and also in some recent work of the last author [13] that finds probabilities of various splitting types in abelian extensions of number fields. The idea of obtaining statistics for the families of curves over finite fields by considering the family of function field extensions attached to those curves was also used by Wood [14] and by Thorne and Xiong [12] for the family of trigonal curves (corresponding to non-Galois cubic extensions of $\mathbb{F}_q(X)$).

We record below a special case of this result which will be needed in the applications described in Section 1.1. The following corollary has a necessary ingredient for proving such results, namely, the explicit dependence of each of the coefficients of the polynomial $P_{\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I}(X)$ with respect to the splitting/ramification conditions to ensure enough cancellation in the relative densities for the split and inert primes. More corollaries of this type can be extracted from the proof of Theorem 1.1 if needed for other applications.

Corollary 1.2. Let $v \in \mathcal{V}_K$ be a place, let $\epsilon \in \{\text{ramified, split, inert}\}$, and let $N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}, v, \epsilon)$ be the number of extensions of $\mathbb{F}_q(X)$ with Galois group $\mathbb{Z}/\ell\mathbb{Z}$ such that the degree of the conductor is equal to $\mathfrak{n}$ and with prescribed behavior ϵ at the place v. Then,

$$N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}, v, \text{ramified}) = \frac{(\ell-1)\, q^{-\deg v}}{1 + (\ell-1)\, q^{-\deg v}} C_\ell q^{\mathfrak{n}} P_R(\mathfrak{n}) + O\left(q^{\left(\frac{1}{2}+\varepsilon\right)\mathfrak{n}}\right),$$

$$N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}, v, \text{split}) = \frac{1}{\ell\left(1 + (\ell-1)\, q^{-\deg v}\right)} C_\ell q^{\mathfrak{n}} P_S(\mathfrak{n}) + O\left(q^{\left(\frac{1}{2}+\varepsilon\right)\mathfrak{n}}\right),$$

$$N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}, v, \text{inert}) = \frac{1}{\ell\left(1 + (\ell-1)\, q^{-\deg v}\right)} C_\ell q^{\mathfrak{n}} P_I(\mathfrak{n}) + O\left(q^{\left(\frac{1}{2}+\varepsilon\right)\mathfrak{n}}\right),$$

where C_ℓ is the non-zero constant defined by (4), $P_R(X)$ and $P_S(X) \in \mathbb{R}[X]$ are monic polynomials of degree $\ell - 2$ and $P_I(X) = (\ell - 1) P_S(X)$.

When $\ell = 2$, we obtain a better error term for the ramified case

$$N(\mathbb{Z}/2\mathbb{Z}, \mathfrak{n}, v, \text{ramified}) = \frac{(1-q^{-2})\, q^{-\deg v}}{1+q^{-\deg v}} q^{\mathfrak{n}} + O_q(1). \qquad \square$$

Finally, we state our main result for the distribution of points on ℓ-cyclic covers of $\mathbb{P}^1$ of fixed genus that can be obtained by a simple application of Theorem 1.1. This distribution is given in terms of the same random variables obtained in [1] for each irreducible component of the moduli space $\mathcal{H}_{g,\ell}$.

Theorem 1.3. Let $\mathcal{H}_{g,\ell}$ be the moduli space of $\mathbb{Z}/\ell\mathbb{Z}$ Galois covers of $\mathbb{P}^1$ of genus g. Then, as $g \to \infty$,

$$\frac{|\{C \in \mathcal{H}_{g,\ell}(\mathbb{F}_q) : \#C(\mathbb{F}_q) = m\}|'}{|\mathcal{H}_{g,\ell}(\mathbb{F}_q)|'} = \text{Prob}\left(X_1 + \ldots X_{q+1} = m\right) + O_\ell\left(\frac{1}{g}\right),$$

where the X_i's are independent identically distributed random variables such that

$$X_i = \begin{cases} 0 & \text{with probability } \dfrac{(\ell-1)\,q}{\ell(q+\ell-1)}, \\ 1 & \text{with probability } \dfrac{\ell-1}{q+\ell-1}, \\ \ell & \text{with probability } \dfrac{q}{\ell(q+\ell-1)}. \end{cases}$$

In the formula, as usual, the $'$ notation means that the covers C on the moduli space are counted with the usual weights $1/|\text{Aut}(C)|$. $\square$

1.1 Relation to previous work and outline of the paper

As we mentioned above, using class field theory to count abelian extensions of global fields was first used in the elegant note of Cohn [4] for the particular case $K = \mathbb{Q}$ and $G = \mathbb{Z}/3\mathbb{Z}$, and was vastly generalized by Wright in his influential paper on the subject [15]. The main idea is to write the generating series (3) as a finite linear combination of Euler products whose factors are relatively simple. In [15], Wright gets an asymptotic for all abelian extensions of a global field. In the present paper, we are interested in a special case of his work, namely $K = \mathbb{F}_q(X)$ and $G = \mathbb{Z}/\ell\mathbb{Z}$, but we need results that are completely explicit because of the applications to statistics of curves over finite fields, which is our main goal. We then need the values of the constants $c(k, G)$ in [15, Theorem I.3], which are not determined by Wright. He manages by an ingenious argument to show that they are non-zero, and that the density exists. In this paper, we compute these constants explicitly and show that they fit the count of [1], ignoring the error terms (see Section 5). For the case of number field extensions, the explicit computation of the constants $c(k, G)$ from [15, Theorem I.3] was addressed by Cohen et al. [5], again for the case of cyclic extensions of prime degree. Their techniques are completely different from the class field theory approach of [4, 15], as they use Kummer theory. The authors of [5] do not compute the relative densities for the splitting conditions with their approach, and to our knowledge, this is not done in the current literature with the Kummer theory approach.

The relative densities for general abelian extensions of number fields were computed explicitly by the last author of the present paper in [13] using the class field theory approach, with an emphasis on characterizing the extensions of $\mathbb{Q}$ where the independence between the various primes in the relative densities is false. In some ways, the present paper is a function field analog of [13], but of course the application for counting points on curves is different. There are also many differences between function fields and number fields, because of the special role of the place at infinity, and the fact that all residue fields have the same characteristic. There are also different analytic issues between number fields and function fields. Some related work on the density of cyclic extensions of prime degree over function fields can also be found in [3].

Among other possible applications of counting function fields extensions and curves over finite fields, one can think of statistics for the distribution of points over finite fields $\mathbb{F}_{q^n}$ as n varies (but the family of covers is still defined over $\mathbb{F}_q$), and the one-level density for the family, as studied by Rudnick [10] for hyperelliptic curves. Those applications are also suitable for an approach using the relative densities of the function field extensions corresponding to the family of curves. For this particular application, one needs all secondary terms which can be obtained by computing the residues of all the poles in the line $\mathrm{Re}(s) = 1/(\ell - 1)$ of the generating series (3), that is, the polynomials $P(\mathfrak{n})$ appearing in Theorem 1.1 and Corollary 1.2, and not only the main term given by the highest order pole. This would provide enough cancellation between the different relative densities appearing in the explicit formulas relating the point counting to the zeroes of the zeta functions of the curves. The quality of the results obtained for statistics for the number of points over $\mathbb{F}_{q^n}$ (namely how large n is with respect to the genus of the family) and the one-level density (namely the support of the Fourier transform) is influenced by the error term, which is obtained from the Tauberian theorem after considering the poles as discussed. One important feature of the error term is its dependence on the degree of the primes with splitting/ramification conditions. This dependence raises delicate and nontrivial issues, as there are cyclic ℓ-covers where the zeroes of the zeta functions are related and their contribution to the error term is large, but they should not influence the average over the family as they are exceptional. These questions are not addressed in this paper, but are being considered in work in progress.

Finally, we say a few words about our restriction to $q \equiv 1 \bmod \ell$. We are interested in counting points on the curves $Y^\ell = F(X)$ defined over $\mathbb{F}_q$. If $q \not\equiv 1 \bmod \ell$, the point counting on the curves is trivial as every element in $\mathbb{F}_q$ is an ℓth power (in a unique way). Also, if $q \not\equiv 1 \bmod \ell$, then the extension corresponding to the curve $Y^\ell = F(X)$ is not a cyclic extension, and the cyclic extensions of $\mathbb{F}_q(X)$ of degree ℓ do not come from those curves in the case where $q \not\equiv 1 \bmod \ell$.

We now outline the organization of the paper. In Section 2, we establish the notation and use class field theory to translate the counting of extensions to the counting of maps of the idèle class group. We also prove a general form of the Tauberian theorem over function fields that we need to analyze the Dirichlet series for cyclic extensions of $\mathbb{F}_q(X)$ that is a slight generalization of a result in [9]. In Section 3, we define Dirichlet characters over $\mathbb{F}_q(X)$, and we prove analytic properties of some Dirichlet series that appear in future sections. In Section 4, we prove our main result, Theorem 1.1. In Section 4.1, we look at the particular case of $\ell = 2$ where we can get the exact result for the total number of quadratic extensions with fixed conductor, and the case with one prescribed ramified place with a better error term without using the Tauberian theorem. Finally, we explain in Section 5 how to obtain statistics for the point counting over the moduli space of cyclic ℓ-covers, and we compare our results with those of [1].

2 Background and Setup

In this section, we set up notation and recall basic facts from Galois theory and class field theory that allow us to rephrase our problem in terms of counting continuous homomorphisms from the idèle class group of a function field to a cyclic group of prime order.

Fix a prime ℓ. Throughout the paper $\mathbb{F}_q$ denotes a finite field with $q \equiv 1 \pmod{\ell}$ elements and $K = \mathbb{F}_q(X)$ is the rational function field over $\mathbb{F}_q$.

2.1 Notation

We will denote by G_K the absolute Galois group of K, that is the Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ of the separable closure of K. Let $\mathcal{D}_K^+$ be the set of effective divisors of K. For each place v of K we will use the standard notations K_v for the completion at v, $\mathcal{O}_v$ for the local ring, κ_v for the residue field, and π_v for a uniformizer at v which we choose to be monic. Recall that the degree of a place v is given by $\deg v = [\kappa_v : \mathbb{F}_q]$ and its norm is $Nv = q^{\deg v}$, the number of elements in the residue field κ_v. Of course, for a place v_f associated to an irreducible polynomial $f \in \mathbb{F}_q[X]$, we have that $\deg v = \deg f$. For the place at infinity associated with the uniformizer $\pi_\infty = 1/X$, we have that $\deg v_\infty = 1$.

2.2 From covers to field extensions

A $\mathbb{Z}/\ell\mathbb{Z}$ cover is a pair (C, π) where $C \xrightarrow{\pi} \mathbb{P}^1$ is an ℓ-degree cover map defined over K. Each $\mathbb{Z}/\ell\mathbb{Z}$ cover (C, π) together with an isomorphism $\mathbb{Z}/\ell\mathbb{Z} \to \mathrm{Aut}(C/\mathbb{P}^1)$ corresponds to a Galois extension L of $K = \mathbb{F}_q(X)$ together with a distinguished isomorphism $\mathrm{Gal}(L/K) \xrightarrow{\tau} \mathbb{Z}/\ell\mathbb{Z}$. We refer to such extensions as ℓ-cyclic extensions. The genus of the curve C is related to the discriminant $\mathrm{Disc}(L/K)$ via the Riemann–Hurwitz formula (see, for instance [9, Theorem 7.16]),

$$2g_C - 2 = \ell\,(2g_{\mathbb{P}^1} - 2) + \deg \mathrm{Disc}\,(L/K)\,.$$

Since $q \equiv 1 \pmod{\ell}$, there is no wild ramification and each place v of K either ramifies completely, splits completely, or is inert. Thus

$$\mathrm{Disc}\,(L/K) = \sum_{v \text{ ramified in } L} (\ell - 1)\, v \tag{5}$$

and

$$2g_C = (\ell - 1)\left[-2 + \sum_{v \text{ ramified in } L} \deg v\right],$$

where the sum is taken over the places v of K that ramify in L.

2.3 From field extensions to maps

Our translation from counting extensions to counting maps has two steps. First, by Galois theory, ℓ-cyclic extensions L/K with a distinguished isomorphism $\mathrm{Gal}(L/K) \xrightarrow{\tau} \mathbb{Z}/\ell\mathbb{Z}$ are in one-to-one correspondence with the surjective continuous homomorphisms $G_K \to \mathbb{Z}/\ell\mathbb{Z}$ from the absolute Galois group of K to $\mathbb{Z}/\ell\mathbb{Z}$. By class field theory, the maps $G_K \to \mathbb{Z}/\ell\mathbb{Z}$ are in one-to-one correspondence with the maps $\mathbf{J}_K/K^\times \to \mathbb{Z}/\ell\mathbb{Z}$ from the idèle class group of K to $\mathbb{Z}/\ell\mathbb{Z}$.

Since K contains all ℓth roots of unity and $(\ell, q) = 1$, by Kummer theory, each unramified ℓ-cyclic Galois cover is of the form $K(\sqrt[\ell]{\beta}), \ldots, K(\sqrt[\ell]{\beta^{\ell-1}})$ for any $\beta \in \mathbb{F}_q^\times$ not an ℓth power. These correspond to $\ell - 1$ unramified surjective continuous homomorphisms $\mathbf{J}_K/K^\times \to \mathbb{Z}/\ell\mathbb{Z}$, one for each generator of $\mathbb{Z}/\ell\mathbb{Z}$. There is also the trivial map, which is also unramified everywhere. In terms of extensions, this corresponds to the

K-algebra K^ℓ. In terms of covers of $\mathbb{P}^1$, this corresponds to the split cover that consists of ℓ disjoint copies of $\mathbb{P}^1$.

Thus an ℓ-cyclic extension L/K of given discriminant corresponds to a nontrivial continuous homomorphism $\varphi : \mathbf{J}_K/K^\times \to \mathbb{Z}/\ell\mathbb{Z}$.

Let ϕ be a map

$$\phi : \pi_\infty^{\mathbb{Z}} \times \prod_v \mathcal{O}_v^\times \to \mathbb{Z}/\ell\mathbb{Z} \tag{6}$$

which is trivial on the embedding of $\mathbb{F}_q^\times$ in $\prod_v \mathcal{O}_v^\times$. Here $\pi_\infty^{\mathbb{Z}}$ is the free abelian group generated by π_∞ and the product is taken over all the places v including the place at infinity (unless otherwise specified, we will continue using the convention that the sums and products over v denote all places including the place at infinity).

Remark 2.1. We remark that ϕ and φ are two different maps. □

The maps ϕ and φ are closely related via the following proposition whose proof can be found in [6, Section 7, p. 90].

Proposition 2.2. Let

$$\phi = \psi_\infty \otimes_v \phi_v : \pi_\infty^{\mathbb{Z}} \times \prod_v \mathcal{O}_v^\times \to \mathbb{Z}/\ell\mathbb{Z}.$$

Then the following conditions are satisfied:

(1) If ϕ is trivial on the embedding of $\mathbb{F}_q^\times$ in $\prod_v \mathcal{O}_v^\times$ it has a unique extension to a map

$$\varphi : \mathbf{J}_K/K^\times \to \mathbb{Z}/\ell\mathbb{Z}.$$

(2) A place v of K ramifies in an ℓ-cyclic extension L corresponding to ϕ if and only if the map ϕ_v is non-trivial on $\mathcal{O}_v^\times$. □

Thus the conductor of the map ϕ is

$$\mathrm{Cond}\,(\phi) = \sum_{v \text{ ramified in } L} v,$$

which is also the conductor of the extension L/K. As there is no wild ramification, the discriminant-conductor formula (see, for instance [11, Section 12.6]) yields

$$\mathrm{Disc}\,(L/K) = (\ell - 1)\,\mathrm{Cond}\,(L/K) = (\ell - 1)\,\mathrm{Cond}\,(\phi)\,. \tag{7}$$

In Section 4, we prove our main results by working with ϕ. For the remainder of this section, we explicate the relationship between ϕ and the corresponding L/K.

First, we address the global compatibility condition needed for ϕ to extend to a function φ defined over $\mathbf{J}_K/K^\times$ and hence correspond to an extension L. Namely, that ϕ must be trivial on the embedding of $\mathbb{F}_q^\times$ in $\prod_v \mathcal{O}_v^\times$. Fix $\mu \in \mathbb{F}_q$, a generator of the multiplicative group $\mathbb{F}_q^\times$. Clearly, ϕ is trivial on $\mathbb{F}_q^\times$ if and only if $\phi(1, \mu, \mu, \dots) = 0$ where the first component in the infinite vector corresponds to the identity element in the free abelian group $\pi_\infty^{\mathbb{Z}}$.

For each place v of K, we note that the map $\phi_v : \mathcal{O}_v^\times \to \mathbb{Z}/\ell\mathbb{Z}$ factors through $\mathcal{O}_v^\times/(1+\pi_v\mathcal{O}_v) \cong (\mathcal{O}_v/(\pi_v))^\times$. Recall that $\deg v = [\mathcal{O}_v/(\pi_v) : \mathbb{F}_q]$ and thus

$$\mathcal{O}_v/\,(\pi_v) \cong \mathbb{F}_{q^{\deg v}}.$$

For each v, fix a choice of $g_v \in \mathcal{O}_v$ whose image generates $\mathcal{O}_v^\times/(1+\pi_v\mathcal{O}_v) \cong (\mathbb{F}_{q^{\deg v}})^\times$ and such that

$$\mu = g_v^{\frac{q^{\deg v}-1}{q-1}}.$$

Then

$$\begin{aligned}
\phi\,(1, \mu, \mu, \dots) &= \phi\,((1, \mu, 1, 1, \dots)\,(1, 1, \mu, 1, \dots)\cdots) \\
&= \phi\,(1, \mu, 1, 1, \dots) + \phi\,(1, 1, \mu, 1, \dots) + \cdots \\
&= \sum_v \phi_v\,(\mu) = \sum_v \phi_v \left(g_v^{\frac{q^{\deg v}-1}{q-1}}\right) = \sum_v \left(\frac{q^{\deg v}-1}{q-1}\right)\phi_v\,(g_v)\,.
\end{aligned}$$

We note that $\frac{q^{\deg v}-1}{q-1} = q^{\deg v-1} + q^{\deg v-2} + \cdots + q + 1 \equiv \deg v \pmod{\ell}$ since $q \equiv 1 \pmod{\ell}$. We have now proved the following proposition.

Proposition 2.3. For each v let $g_v \in \mathcal{O}_v$ as defined above. A map $\phi : \pi_\infty^{\mathbb{Z}} \times \prod_v \mathcal{O}_v^\times \to \mathbb{Z}/\ell\mathbb{Z}$ is trivial on the embedding of $\mathbb{F}_q^\times$ in $\prod_v \mathcal{O}_v^\times$ if and only if

$$\sum_{v\in\mathrm{Cond}(\phi)} \phi_v\,(g_v)\,\deg v \equiv 0 \pmod{\ell}. \tag{8}$$

□

Thus, in order to count the extensions L/K with prescribed splitting/ramification conditions at places v of $K = \mathbb{F}_q(X)$, it is necessary and sufficient to count the maps ϕ as in (6) satisfying the global compatibility condition (8) with corresponding conditions at places v of K, which we describe below. By Proposition 2.2, a place v is ramified if and only if ϕ_v is nontrivial on $\mathcal{O}_v^\times$. Now, we deal with the remaining two cases, inert and completely split.

Proposition 2.4. Let

$$\phi = \psi_\infty \otimes_v \phi_v : \pi_\infty^{\mathbb{Z}} \times \prod_v \mathcal{O}_v^\times \to \mathbb{Z}/\ell\mathbb{Z}$$

be trivial on the embedding of $\mathbb{F}_q^\times$ in $\prod_v \mathcal{O}_v^\times$. Let

$$\varphi : \mathbf{J}_K/K^\times \to \mathbb{Z}/\ell\mathbb{Z}$$

be the unique extension of ϕ to the idèle class group of K and let L be the ℓ-cyclic extension of K corresponding to φ. Let v_0 be a place of K different from v_∞. Then we have the following:

(1) $v = v_0$ or v_∞ ramifies in L if and only if the map ϕ_v is nontrivial on $\mathcal{O}_v^\times$,

(2) v_0 splits completely in L if and only if $\phi_{v_0}(\mathcal{O}_{v_0}^\times) = 0$ and

$$\psi_\infty\left(\pi_\infty^{-\deg v_0}\right) + \sum_{v \neq v_0, v_\infty} \phi_v\left(\pi_{v_0}\right) = 0, \tag{9}$$

(3) v_0 is inert in L if and only if $\phi_{v_0}(\mathcal{O}_{v_0}^\times) = 0$ and

$$\psi_\infty\left(\pi_\infty^{-\deg v_0}\right) + \sum_{v \neq v_0, v_\infty} \phi_v\left(\pi_{v_0}\right) \neq 0,$$

(4) v_∞ splits completely in L if and only if $\phi_{v_\infty}(\mathcal{O}_{v_\infty}^\times) = 0$ and $\psi_\infty(\pi_\infty) = 0$,

(5) v_∞ is inert in L if and only if $\phi_{v_\infty}(\mathcal{O}_{v_\infty}^\times) = 0$ and $\psi_\infty(\pi_\infty) \neq 0$. □

Proof. Let φ_v be the composition of φ with the canonical map $K_v^\times \to \mathbf{J}_K \to \mathbf{J}_K/K^\times$. In the case where v is unramified, the map φ_v is trivial on $\mathcal{O}_v^\times$ and therefore its image is dictated by $\varphi_v(\pi_v^{\mathbb{Z}}) \in \mathbb{Z}/\ell\mathbb{Z}$. Thus, the image is a subgroup of a simple abelian group and we have only two possibilities: either φ_v is surjective or φ_v is trivial. Since Frob_v corresponds to the vector with π_v in the v place and 1 elsewhere under the correspondence from class field theory, v splits if and only if $\varphi_v(\pi_v) = 0$.

Now, let $v_0 \neq v_\infty$ be unramified. For the purpose of this particular discussion we denote elements in the idèles by vectors with the infinite component first and the v_0 component second. Under this notation v_0 splits if and only if $\varphi(1, \pi_{v_0}, 1, 1, \ldots) = 0$. Since φ is trivial on $K^\times$, we know that

$$\begin{aligned} 0 &= \varphi\left(\pi_{v_0}, \pi_{v_0}, \ldots\right) = \varphi\left(\pi_{v_0}, 1, \ldots\right) + \varphi\left(1, \pi_{v_0}, 1, \ldots\right) + \varphi\left(1, 1, \pi_{v_0}, 1, \ldots\right) + \cdots \\ &= \varphi\left(\pi_\infty^{-\deg v_0}, 1, \ldots\right) + \varphi\left(\pi_{v_0}\pi_\infty^{\deg v_0}, 1, \ldots\right) + \varphi\left(1, \pi_{v_0}, 1, \ldots\right) \\ &\quad + \varphi\left(1, 1, \pi_{v_0}, 1, \ldots\right) + \varphi\left(1, 1, 1, \pi_{v_0}, 1, \ldots\right) + \cdots . \end{aligned}$$

Since we chose π_{v_0} to be monic and $\mathrm{val}_\infty(\pi_{v_0}\pi_\infty^{\deg v_0})=0$, we have that $\varphi(\pi_{v_0}\pi_\infty^{\deg v_0},1,\ldots)=0$. Denoting by $\varphi_{v_0}(\pi_{v_0})$ the term $\varphi(1,\pi_{v_0},1,\ldots,1)$ where we recall the convention that the second place corresponds to v_0, we obtain

$$\psi_\infty\left(\pi_\infty^{-\deg v_0}\right)+\varphi_{v_0}\left(\pi_{v_0}\right)+\sum_{v\neq v_0,v_\infty}\phi_v\left(\pi_{v_0}\right)=0.$$

Since v_0 splits if and only if $\varphi_{v_0}(\pi_{v_0})=0$, we see that

- v_0 splits if and only if $\phi_{v_0}(\mathcal{O}_{v_0}^\times)=0$ and

$$\psi_\infty\left(\pi_\infty^{-\deg v_0}\right)+\sum_{v\neq v_0,v_\infty}\phi_v\left(\pi_{v_0}\right)=0. \tag{10}$$

- v_0 is inert if and only if $\phi_{v_0}(\mathcal{O}_{v_0}^\times)=0$ and

$$\psi_\infty\left(\pi_\infty^{-\deg v_0}\right)+\sum_{v\neq v_0,v_\infty}\phi_v\left(\pi_{v_0}\right)\neq 0.$$

If $v=v_\infty$, we can read the splitting behavior from $\phi(\pi_\infty,1,1,\ldots)$. Namely, we have that $v_\infty\notin\mathrm{Cond}(\phi)$ if and only if $\phi_{v_\infty}(\mathcal{O}_{v_\infty}^\times)=0$. Therefore,

- v_∞ splits completely in L when $\phi_{v_\infty}(\mathcal{O}_{v_\infty}^\times)=0$ and $\psi_\infty(\pi_\infty)=0$,
- v_∞ is inert when $\phi_{v_\infty}(\mathcal{O}_{v_\infty}^\times)=0$ and $\psi_\infty(\pi_\infty)\neq 0$. ■

2.4 Generating series and the Tauberian Theorem

As in previous work, our strategy is to make use of the Tauberian theorem to deduce an asymptotic formula for the number of field extensions L/K with discriminant of degree $\mathfrak{n}$ from the analytic properties of the generating series

$$\sum_{\mathrm{Gal}(L/K)\cong\mathbb{Z}/\ell\mathbb{Z}}\mathfrak{D}\left(L/K\right)^{-s},$$

where $\mathfrak{D}(L/K)$ is the norm of the discriminant $\mathrm{Disc}(L/K)$. As mentioned above, since we are dealing with cyclic extension of prime degree ℓ, the conductor–discriminant relation gives

$$\mathrm{Disc}\left(L/K\right)=\left(\ell-1\right)\mathrm{Cond}\left(L/K\right)\iff\mathfrak{D}\left(L/K\right)=N\left(\mathrm{Cond}\left(L/K\right)\right)^{\ell-1},$$

and it is more natural to write the generating series as

$$\sum_{\mathrm{Gal}(L/K)\cong\mathbb{Z}/\ell\mathbb{Z}}\mathfrak{D}\left(L/K\right)^{-s}:=\sum_{f\in\mathcal{D}_K^+}\frac{a_\ell\left(f\right)}{Nf^{(\ell-1)s}},$$

where $a_\ell(f)$ is the number of cyclic extensions of degree ℓ of $K=\mathbb{F}_q(X)$ with conductor f. We will then extend this analysis to study the extensions L that are counted by $N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}; \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_I)$ as defined in Section 1 by understanding the generating series

$$\sum_{\substack{\mathrm{Gal}(L/K)\cong\mathbb{Z}/\ell\mathbb{Z} \\ \mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I}} \mathfrak{D}\left(L/K\right)^{-s},$$

where the sum now runs over the cyclic extensions of degree ℓ that satisfy all of prescribed splitting/ramification conditions at the places of $\mathcal{V}_R\cup\mathcal{V}_S\cup\mathcal{V}_I$. Again, we will write this Dirichlet series as

$$\sum_{\substack{\mathrm{Gal}(L/K)\cong\mathbb{Z}/\ell\mathbb{Z} \\ \mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I}} \mathfrak{D}\left(L/K\right)^{-s} := \sum_{f\in\mathcal{D}_K^+} \frac{a_\ell\left(f, \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_I\right)}{Nf^{(\ell-1)s}},$$

where $a_\ell(f, \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_I)$ is the number of cyclic extensions of degree ℓ of $K=\mathbb{F}_q(X)$ with conductor f that satisfy all of the prescribed splitting/ramification conditions.

We now state and prove the version of the Tauberian theorem needed to analyze the Dirichlet series above. More generally, let k be a positive integer, let $a:\mathcal{D}_K^+\to\mathbb{C}$, and $\mathcal{F}(s)$ be the Dirichlet series

$$\mathcal{F}\left(s\right)=\sum_{f\in\mathcal{D}_K^+}\frac{a\left(f\right)}{Nf^{ks}}.$$

We need a Tauberian theorem that will allow us to evaluate $\sum_{\deg f=\mathfrak{n}} a(f)$ in the situation when the half-plane of absolute convergence is $\mathrm{Re}(s)>1/k$ for some positive integer k, and the function $\mathcal{F}(s)$ has a finite number of poles (of arbitrary multiplicities) on the line $\mathrm{Re}(s)=1/k$. This is a slight generalization of [9, Theorem 17.1].

Since the function q^{-ks}, and therefore $\mathcal{F}(s)$, are periodic with period $2\pi\mathrm{i}/(k\log q)$, nothing is lost by confining our attention to the region

$$B_k=\left\{s\in\mathbb{C}:-\frac{\pi\mathrm{i}}{k\log q}\leq\mathrm{Im}\left(s\right)<\frac{\pi\mathrm{i}}{k\log q}\right\}. \tag{11}$$

We will always suppose that s is confined to the region B_k.

Theorem 2.5. Let k be a positive integer and let $0<\delta<1/k$. Let $a:\mathcal{D}_K^+\to\mathbb{C}$, and suppose that the Dirichlet series

$$\mathcal{F}\left(s\right)=\sum_{f\in\mathcal{D}_K^+}\frac{a\left(f\right)}{Nf^{ks}}$$

converges absolutely for $\mathrm{Re}(s)>1/k$, and is holomorphic on $\{s\in B_k:\mathrm{Re}(s)\geq\delta\}$ except for a finite number of poles on the line $\mathrm{Re}(s)=1/k$. Let $u=q^{-ks}$ and define

$F(u) = \mathcal{F}(s)$. Then

$$\sum_{\deg f = n} a(f) = -\sum_{|u|=q^{-1}} \mathrm{Res}_u \frac{F(u)}{u^{n+1}} + O\left(q^{\delta k n} M\right),$$

where

$$M = \max_{|u|=q^{-k\delta}} |F(u)| = \max_{\mathrm{Re}(s)=\delta} |\mathcal{F}(s)|. \qquad \square$$

Proof. With the change of variable $u = q^{-ks}$, we have that

$$F(u) = \sum_{n=0}^{\infty} \left(\sum_{\deg f = n} a(f) \right) u^n,$$

and by hypothesis, $F(u)$ is a meromorphic function on the disk $\{u \in \mathbb{C} : |u| \le q^{-k\delta}\}$, except for finitely many poles with $|u| = 1/q$. Let $C_\delta = \{u \in \mathbb{C} : |u| = q^{-k\delta}\}$, oriented counterclockwise. Choose any $\eta > 1$ and let $C_\eta = \{u \in \mathbb{C} : |u| = q^{-\eta}\}$, oriented clockwise. Note that $\frac{F(u)}{u^{n+1}}$ is a meromorphic function between the two circles C_η and C_δ with finitely many poles at $|u| = 1/q$. Thus, by the Cauchy's integral formula,

$$\frac{1}{2\pi i} \oint_{C_\delta + C_\eta} \frac{F(u)}{u^{n+1}}\, du = \sum_{|u|=q^{-1}} \mathrm{Res}_u \frac{F(u)}{u^{n+1}}.$$

Since $q^{-\eta} < q^{-1}$, using the power series expansion of $F(u)$ around $u = 0$, we have that

$$\frac{1}{2\pi i} \oint_{C_\eta} \frac{F(u)}{u^{n+1}}\, du = -\sum_{\deg f = n} a(f).$$

Therefore, we obtain

$$\sum_{\deg f = n} a(f) = -\sum_{|u|=q^{-1}} \mathrm{Res}_u \frac{F(u)}{u^{n+1}} + \frac{1}{2\pi i} \oint_{C_\delta} \frac{F(u)}{u^{n+1}}\, du.$$

Let M be the maximum of $|F(u)|$ over C_δ. Then

$$\left| \frac{1}{2\pi i} \oint_{C_\delta} \frac{F(u)}{u^{n+1}}\, du \right| \le M q^{\delta k n},$$

which proves the result. ∎

3 Dirichlet Characters and L-Functions

In this section, we define ℓth-power residue symbols over $\mathbb{F}_q[X]$. We refer the reader to [8, 9] for details. We then study the convergence properties of some auxiliary functions built out of the ℓth-power residue symbols that will be used in the proofs of our main results.

Recall that ℓ is a prime such that $q \equiv 1 \pmod{\ell}$. Thus $\mathbb{F}_q^\times$ contains the ℓth roots of unity. In particular, $b_\ell = \mu^{\frac{q-1}{\ell}}$ is one of these roots where μ is a fixed generator of $\mathbb{F}_q^\times$. For a place $v \neq v_\infty$ of K, we also let $v = v(X) \in \mathbb{F}_q[X]$ represent the monic irreducible polynomial in $K^\times$ corresponding to v. We define the ℓth power residue symbol as follows. Let

$$\left(\frac{\cdot}{v}\right)_\ell : \left(\mathbb{F}_q[X]/v\,(X)\right)^\times \to \mathbb{F}_q^\times$$

be defined by

$$\left(\frac{f}{v}\right)_\ell \equiv f^{\frac{Nv-1}{\ell}} \pmod{v}.$$

In other words, the ℓth power residue symbol is given by an ℓth root of unity.

Recall that the choice of μ made in Section 2.3 determined for each place v a generator g_v of

$$\left(\mathcal{O}_v/\left(\pi_v\right)\right)^\times \cong \left(\mathbb{F}_q[X]/\left(v\,(X)\right)\right)^\times \cong \left(\mathbb{F}_{q^{\deg v}}\right)^\times$$

such that $\mu = g_v^{\frac{q^{\deg v}-1}{q-1}}$. We have

$$g_v^{\frac{q^{\deg v}-1}{\ell}} = \left(g_v^{\frac{q^{\deg v}-1}{q-1}}\right)^{\frac{q-1}{\ell}} = \mu^{\frac{q-1}{\ell}} = b_\ell.$$

By the definition of the ℓth power symbol,

$$\left(\frac{g_v}{v}\right)_\ell \equiv b_\ell \pmod{v}.$$

We let σ be an ℓ-order character from $\mathbb{F}_q^\times \to \mathbb{C}^\times$. Then,

$$\chi_{v,\ell} := \sigma \circ \left(\frac{\cdot}{v}\right)_\ell$$

is a Dirichlet character $\chi : \mathbb{F}_q[X] \to \mathbb{C}^\times$ of modulus v, where we define $\chi_{v,\ell}(f(x)) = 0$ if $v(x)$ divides $f(x)$.

For the infinite place v_∞, we further define

$$\chi_{v,\ell}\left(v_\infty\right) = \begin{cases} 1 & \deg v \equiv 0 \pmod{\ell}, \\ 0 & \deg v \not\equiv 0 \pmod{\ell}. \end{cases} \tag{12}$$

For χ a nontrivial Dirichlet character, we denote by $L(s,\chi)$ the Dirichlet L-function

$$L\left(s,\chi\right) = \sum_{F \in \mathbb{F}_q[X] F \text{ monic}} \frac{\chi\left(F\right)}{|F|^s}$$

where F varies over the monic polynomials of $\mathbb{F}_q[X]$, and by $L^*(s,\chi)$ the completed L-function that includes the place at infinity. For a Dirichlet character modulo a monic polynomial v, we have that

$$L^*(s,\chi) = \left(1-q^{-s}\right)^{-\lambda_v} L(s,\chi),$$

where λ_v is 1 if $\deg v \equiv 0 \pmod{\ell}$, and 0 otherwise.

Then, for χ nontrivial, we remark that both $L(s,\chi)$ and $L^*(s,\chi)$ are analytic and non-zero for $\mathrm{Re}(s) > 1/2$.

By ℓ-power reciprocity, we can write this character as

$$\chi_{v,\ell}(v_0) = \sigma \circ \left(\frac{v_0}{v}\right)_\ell = \sigma\left(\left((-1)^{(q-1)/\ell}\right)^{\deg v_0 \deg v}\left(\frac{v}{v_0}\right)_\ell\right) = \Psi_{v_0,\ell}(v)\,\chi_{v_0,\ell}(v), \tag{13}$$

where $\chi_{v_0,\ell}(v)$ is the Dirichlet character modulo v_0 defined above, and $\Psi_{v_0,\ell}(v)$ depends only on the degree of v.

If $v = v_\infty$, let a_n be the principal coefficient of f. Then we define

$$\chi_{v_\infty,\ell}(f) := \begin{cases} \sigma(a_n) & \deg f \equiv 0 \pmod{\ell}, \\ 0 & \deg f \not\equiv 0 \pmod{\ell}. \end{cases}$$

We note that the above definition together with (12) agree with ℓ-power reciprocity in the following way:

$$\chi_{v,\ell}(v_\infty) = \left((-1)^{(q-1)/\ell}\right)^{\deg v} \chi_{v_\infty,\ell}(v) = \begin{cases} 1 & \deg v \equiv 0 \pmod{\ell}, \\ 0 & \deg v \not\equiv 0 \pmod{\ell}. \end{cases} \tag{14}$$

We have used that v is a monic polynomial, which implies that $\chi_{v_\infty,\ell}(v) = 1$ when $\ell \mid \deg v$, that $\deg v_\infty = 1$, and that $((-1)^{(q-1)/\ell})^{\deg v} = 1$ when $\ell \mid \deg v$ and q is odd, and is trivially 1 when q is even since then we have characteristic 2 and $1 = -1$ in this case.

Finally, we remark that by the above, the Kronecker symbol codifies ramification in extensions in the usual way. Let $f \in \mathbb{F}_q[X]$ (not necessarily monic). Then,

$$\chi_{v,\ell}(f) = \begin{cases} 1 & v \text{ splits in } K\left(\sqrt[\ell]{f}\right), \\ \xi_\ell^k, \text{ for some } 1 \le k \le \ell-1 & v \text{ is inert in } K\left(\sqrt[\ell]{f}\right), \\ 0 & v \text{ ramifies in } K\left(\sqrt[\ell]{f}\right), \end{cases}$$

where $\xi_\ell \in \mathbb{C}$ is a primitive ℓth root of 1.

We now proceed to prove convergence results for Dirichlet series and similar functions.

Lemma 3.1. Let χ be a nontrivial Dirichlet character and let Ψ be a function on $\mathbb{F}_q[X]$ such that $\Psi(F) = \Psi(G)$ when $\deg F = \deg G$. Then

$$L(s, \Psi\chi) = \sum_{\substack{F \in \mathbb{F}_q[X] \\ F \text{ monic}}} \frac{\Psi(F)\chi(F)}{|F|^s}$$

is an analytic function on $\mathbb{C}$. □

Proof. Let

$$A(n, \Psi, \chi) = \sum_{\substack{F \in \mathbb{F}_q[X], \\ F \text{ monic}, \\ \deg F = n}} \Psi(F)\chi(F).$$

Then $L(s, \Psi\chi)$ equals

$$\sum_{n=0}^{\infty} \frac{A(n, \Psi, \chi)}{q^{ns}}. \tag{15}$$

We note that

$$A(n, \Psi, \chi) = \Psi(G) \sum_{\substack{F \in \mathbb{F}_q[X], \\ F \text{ monic}, \\ \deg F = n}} \chi(F)$$

for any polynomial G of degree n, and thus $A(n, \Psi, \chi) = 0$ if n is greater than or equal to the degree of the modulus of χ by the orthogonality relations of characters. This implies that the sum in (15) is finite and therefore $L(s, \Psi\chi)$ is analytic. ■

Lemma 3.2. Let ξ_ℓ be a primitive ℓth root of 1. Let $\mathcal{V}_R$, $\mathcal{V}_S$, and $\mathcal{V}_U$ be finite subsets of places of $\mathcal{V}_K$ such that $\mathcal{V}_S = \{v_1, \ldots, v_n\} \subset \mathcal{V}_U$, and $\mathcal{V}_U \cap \mathcal{V}_R = \varnothing$. For each $0 \le j \le \ell - 1$, and each tuple $(k_1, \ldots, k_n) \ne (0, \ldots, 0)$ with $0 \le k_i \le \ell - 1$, let

$$\begin{aligned} &\mathcal{M}_{j,k_1,\ldots,k_n}(s; \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_U) \\ &:= \prod_{v \notin \mathcal{V}_R \cup \mathcal{V}_U} \left(1 + \left(\xi_\ell^{j \deg v} \prod_{h=1}^{n} \chi_{v,\ell}(v_h)^{k_h} + \cdots + \xi_\ell^{(\ell-1) j \deg v} \prod_{h=1}^{n} \chi_{v,\ell}(v_h)^{(\ell-1)k_h}\right) Nv^{-(\ell-1)s}\right). \end{aligned}$$

Then, each $\mathcal{M}_{j,k_1,\ldots,k_n}(s; \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_U)$ converges absolutely for $\mathrm{Re}(s) > \frac{1}{\ell-1}$ and has analytic continuation to the region $\mathrm{Re}(s) > \frac{1}{2(\ell-1)}$. □

In the case where we have only one place $v_0 \in \mathcal{V}_K$ with prescribed ramification $\epsilon_0 \in \{\text{ramified, split, inert}\}$, we will denote the above function by

$$\mathcal{M}_{j,k}(s; v_0, \epsilon_0) := \mathcal{M}_{j,k_1}(s; \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_U). \tag{16}$$

Proof. For the absolute convergence, we have that the convergence of $\prod_v (1 + (\ell - 1)|Nv^{-s(\ell-1)}|)$ is equivalent to that of $\sum_v \frac{1}{Nv^{s(\ell-1)}}$ and this convergence follows in the same way as the absolute convergence for the zeta function $\zeta_K(s)$ in $\mathrm{Re}(s) > 1$.

For the analytic continuation, we write

$$\begin{aligned}
&\mathcal{M}_{j,k_1,\dots,k_n}(s; \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_U) \\
&\quad = \mathcal{C}^1_{j,k_1,\dots,k_n}(s) \prod_{i=1}^{\ell-1} \prod_{v \notin \mathcal{V}_R \cup \mathcal{V}_U} \left(1 + \xi_\ell^{ij \deg v} \prod_{h=1}^{n} \chi_{v,\ell}(v_h)^{ik_h} Nv^{-(\ell-1)s}\right) \\
&\quad = \mathcal{C}^2_{j,k_1,\dots,k_n}(s) \prod_{i=1}^{\ell-1} \prod_{v \notin \mathcal{V}_R \cup \mathcal{V}_U} \left(1 - \xi_\ell^{ij \deg v} \prod_{h=1}^{n} \Psi_{v_h,\ell}(v)^{ik_h} \chi_{v_h,\ell}(v)^{ik_h} Nv^{-(\ell-1)s}\right)^{-1},
\end{aligned}$$

where we have used ℓ-power reciprocity (13), and where $\mathcal{C}^1_{j,k_1,\dots,k_n}(s)$ and $\mathcal{C}^2_{j,k_1,\dots,k_n}(s)$ are analytic functions for $\mathrm{Re}(s) > 1/2(\ell - 1)$ as the Euler products converge absolutely in that region. For each $1 \le i \le \ell - 1$, each $0 \le j \le \ell - 1$ and each tuple $(k_1, \dots, k_n)$ as above, we have that the functions

$$\begin{aligned}
L_{i,j,k_1,\dots k_n}(s) &= \prod_{v \notin \mathcal{V}_R \cup \mathcal{V}_U} \left(1 - \xi_\ell^{ij \deg v} \prod_{h=1}^{n} \Psi_{v_h,\ell}(v)^{ik_h} \chi_{v_h,\ell}(v)^{ik_h} Nv^{-(\ell-1)s}\right)^{-1} \\
&= L\left(s_1, \Psi_{i,j,k_1,\dots,k_h} \chi_{i,j,k_1,\dots,k_h}\right)
\end{aligned}$$

are twisted Dirichlet functions as in Lemma 3.1, where $s_1 = (\ell - 1)s$,

$$\Psi_{i,j,k_1,\dots,k_h}(v) = \xi_\ell^{ij \deg v} \prod_{h=1}^{n} \Psi_{v_h,\ell}(v)^{ik_h},$$

$$\chi_{i,j,k_1,\dots,k_h}(v) = \prod_{h=1}^{n} \chi_{v_h,\ell}(v)^{ik_h}.$$

Then, $\Psi_{i,j,k_1,\dots,k_h}(v)$ depends only on the degree of v, and $\chi_{i,j,k_1,\dots,k_h}(v)$ is a nontrivial Dirichlet character since $1 \le i \le \ell - 1$, $(k_1, \dots, k_n) \ne 0$ and the product is taken over different places so that there is no possibility of cancellation. Applying Lemma 3.1, this completes the proof of the analytic continuation. ∎

Let ξ_ℓ be a primitive ℓth root of 1. We now prove a result bounding the meromorphic continuation of the functions

$$\mathcal{A}(s) := \prod_v \left(1 + (\ell - 1)\, Nv^{-(\ell-1)s}\right) \tag{17}$$

$$\mathcal{B}(s) := \prod_v \left(1 + \left(\xi_\ell^{\deg v} + \cdots + \xi_\ell^{(\ell-1)\deg v}\right) Nv^{-(\ell-1)s}\right) \tag{18}$$

on the line $\mathrm{Re}(s) = \frac{1}{2(\ell-1)} + \varepsilon$ for any $\varepsilon > 0$. We remark that the Euler products converge (absolutely and uniformly) for $\mathrm{Re}(s) > \frac{1}{\ell-1}$.

Unless otherwise specified, we continue to use the convention that all the sums and products over v include all places, including the place at infinity.

Lemma 3.3. Let $0 < \varepsilon < \frac{1}{2(\ell-1)}$. The functions $\mathcal{A}(s)$ and $\mathcal{B}(s)$ have meromorphic continuation to the region $\mathrm{Re}(s) > \frac{1}{2(\ell-1)} + \varepsilon$, and their only singularities in this region are poles on the line $\mathrm{Re}(s) = \frac{1}{\ell-1}$. Furthermore, both functions are absolutely bounded on the region $\frac{1}{2(\ell-1)} < \mathrm{Re}(s) < \frac{1}{\ell-1} - \varepsilon$. □

Proof. For $\mathrm{Re}(s) > \frac{1}{\ell-1}$, we have

$$\begin{aligned}
\mathcal{A}(s) &= \prod_v \left(1 + (\ell-1)\, Nv^{-(\ell-1)s}\right) \\
&= \zeta_K((\ell-1)s)^{\ell-1} \prod_v \left(1 + (\ell-1)\, Nv^{-(\ell-1)s}\right)\left(1 - Nv^{-(\ell-1)s}\right)^{\ell-1} \\
&= \zeta_K((\ell-1)s)^{\ell-1} \prod_v \left(1 + (\ell-1)\, Nv^{-(\ell-1)s}\right)\left(1 - (\ell-1)\, Nv^{-(\ell-1)s}\right. \\
&\quad \left. + Nv^{-2(\ell-1)s} + Nv^{-3(\ell-1)s} O_\ell(1)\right) \\
&= \zeta_K((\ell-1)s)^{\ell-1} \prod_v \left(1 - Nv^{-2(\ell-1)s} + Nv^{-3(\ell-1)s} O_\ell(1)\right) \\
&= \mathcal{C}(s)\, \zeta_K((\ell-1)s)^{\ell-1} \prod_v \left(1 - Nv^{-2(\ell-1)s}\right)^{\frac{\ell(\ell-1)}{2}} \\
&= \mathcal{C}(s)\, \frac{\zeta_K((\ell-1)s)^{\ell-1}}{\zeta_K(2(\ell-1)s)^{\frac{\ell(\ell-1)}{2}}},
\end{aligned}$$

where $\mathcal{C}(s)$ is analytic for $\mathrm{Re}(s) > \frac{1}{3(\ell-1)} + \varepsilon$. Thus, for $s = \frac{1}{2(\ell-1)} + \varepsilon$, as ε goes to zero, the function $\mathcal{A}(s)$ converges to zero, and the result follows. The poles are given by those of $\zeta_K((\ell-1)s)$, namely $s = 1/(\ell-1)$, with multiplicity $\ell-1$.

Similarly, for $\mathrm{Re}(s) > \frac{1}{\ell-1}$, we have

$$\mathcal{B}(s) = \prod_v \left(1 + \left(\xi_\ell^{\deg v} + \cdots + \xi_\ell^{(\ell-1)\deg v}\right) Nv^{-(\ell-1)s}\right)$$
$$= \prod_{j=1}^{\ell-1} Z_K\left(\xi_\ell^j u\right) \prod_v \left(1 + \left(\xi_\ell^{\deg v} + \cdots + \xi_\ell^{(\ell-1)\deg v}\right) Nv^{-(\ell-1)s}\right) \prod_{j=1}^{\ell-1} \left(1 - \xi_\ell^{j\deg v} Nv^{-(\ell-1)s}\right),$$

where $u = q^{-(\ell-1)s}$ and $Z_K(u) := \frac{1}{(1-qu)(1-u)}$ is the zeta function of K.

Thus, we have

$$\mathcal{B}(s) = \prod_{j=1}^{\ell-1} Z_K\left(\xi_\ell^j u\right) \prod_v \left(1 + \left(\xi_\ell^{\deg v} + \cdots + \xi_\ell^{(\ell-1)\deg v}\right) Nv^{-(\ell-1)s}\right)$$
$$\times \prod_v \left(1 - \left(\xi_\ell^{\deg v} + \cdots + \xi_\ell^{(\ell-1)\deg v}\right) Nv^{-(\ell-1)s}\right.$$
$$\left. + \left(\sum_{1\le i<j\le \ell-1} \xi_\ell^{i\deg v}\xi_\ell^{j\deg v}\right) Nv^{-2(\ell-1)s} + Nv^{-3(\ell-1)s} O_\ell(1)\right)$$
$$= \mathcal{C}(s) \prod_{j=1}^{\ell-1} Z_K\left(\xi_\ell^j u\right) \prod_v \left(1 + c(\ell)\, Nv^{-2(\ell-1)s}\right),$$

where

$$c(\ell) = -\left(\xi_\ell^{\deg v} + \cdots + \xi_\ell^{(\ell-1)\deg v}\right)^2 + \sum_{1\le i<j\le \ell-1} \xi_\ell^{i\deg v}\xi_\ell^{j\deg v}$$
$$= -\sum_{1\le i\le j\le \ell-1} \xi_\ell^{i\deg v}\xi_\ell^{j\deg v}$$
$$= \begin{cases} -\dfrac{\ell(\ell-1)}{2} & \ell \mid \deg v,\ \ell > 2, \\ 0 & \ell \nmid \deg v,\ \ell > 2, \\ -1 & \ell = 2, \end{cases}$$

and $\mathcal{C}(s)$ is analytic for $\mathrm{Re}(s) > \frac{1}{3(\ell-1)} + \varepsilon$. Thus, for $s = \frac{1}{2(\ell-1)} + \varepsilon$, as $\varepsilon \to 0$, the function $\mathcal{B}(s)$ converges to 0, and the result follows.

The poles are those of $Z_K(\xi_\ell^j u)$, namely, poles of order one at $s = \frac{1}{\ell-1} + \frac{2j\pi i}{(\ell-1)\ell\log q}$. ■

4 ℓ-Cyclic Extensions

In this section, we give the proofs of the main results of this paper. We will continue with the notation introduced in the earlier sections. Recall that, for a fixed prime ℓ, $N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n})$ denotes the number of extensions of K with Galois group $\mathbb{Z}/\ell\mathbb{Z}$ such that the degree of the conductor is $\mathfrak{n}$. As before, $\xi_\ell \in \mathbb{C}$ stands for a primitive ℓth root of 1.

We start by proving the first part of Theorem 1.1.

Theorem 4.1. Let $\ell \in \mathbb{Z}$ be a prime. We have

$$N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}) = C_\ell q^{\mathfrak{n}} P_\ell(\mathfrak{n}) + O\left(q^{\left(\frac{1}{2}+\varepsilon\right)\mathfrak{n}}\right), \tag{19}$$

where $P_\ell(X) \in \mathbb{R}[X]$ is a monic polynomial of degree $\ell - 2$, and where C_ℓ is the non-zero constant given by

$$C_\ell = \frac{\left(1-q^{-2}\right)^{\ell-1}}{(\ell-2)!} \prod_{j=1}^{\ell-2} \prod_v \left(1 - \frac{jq^{-2\deg v}}{\left(1+q^{-\deg v}\right)\left(1+jq^{-\deg v}\right)}\right). \qquad \square$$

Proof. To compute $N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n})$, we consider the Dirichlet series $\mathcal{F}(s)$, which is the generating function with an added constant, namely,

$$\mathcal{F}(s) := \ell + \sum_{\mathrm{Gal}(L/K)\cong\mathbb{Z}/\ell\mathbb{Z}} \mathfrak{D}(L/K)^{-s}.$$

We claim that

$$\begin{aligned}\mathcal{F}(s) &= \sum_{j=0}^{\ell-1} \prod_v \left(1 + \left(\xi_\ell^{j\deg v} + \cdots + \xi_\ell^{(\ell-1)j\deg v}\right) Nv^{-(\ell-1)s}\right) \\ &= \prod_v \left(1 + (\ell-1) Nv^{-(\ell-1)s}\right) + (\ell-1) \prod_v \left(1 + \left(\xi_\ell^{\deg v} + \cdots + \xi_\ell^{(\ell-1)\deg v}\right) Nv^{-(\ell-1)s}\right) \\ &= \mathcal{A}(s) + (\ell-1)\mathcal{B}(s).\end{aligned}$$

Indeed, by Propositions 2.2 and 2.3 the extensions L/K are in one-to-one correspondence with the maps $\phi : \pi_\infty^{\mathbb{Z}} \times \prod_v \mathcal{O}_v^\times \to \mathbb{Z}/\ell\mathbb{Z}$ satisfying (8). Let $\mathrm{Cond}(\phi)$ be the conductor of such a map ϕ, and v be a place of the conductor. In the first line above, the ith term $\xi_\ell^{ij\deg v} Nv^{-(\ell-1)s}$ in each Euler product corresponds to the map where $\phi_v(g_v) = i$ for $1 \le i \le \ell - 1$. Therefore, considering all the places v of $\mathrm{Cond}(\phi)$, the term in the jth Dirichlet series above corresponding to the global map ϕ equals

$$\left(\xi_\ell^{\sum_v j\phi_v(g_v)\deg v}\right) \times N\left(\mathrm{Cond}\left(\phi\right)\right)^{-(\ell-1)s}$$

for $0 \le j \le \ell-1$. Thus, the sum of those terms over the index j yields $\ell N(\mathrm{Cond}(\phi))^{-(\ell-1)s}$ if $\sum_v \phi_v(g_v)\deg v \equiv 0 \pmod{\ell}$ and 0 otherwise, and we recover (8). Note that the ℓ factor multiplying $N(\mathrm{Cond}(\phi))^{-(\ell-1)s}$ is accounting for the different extensions with the same conductor $K(\sqrt[\ell]{f}), K(\sqrt[\ell]{\beta f}), \dots, K(\sqrt[\ell]{\beta^{\ell-1} f})$ for $\beta \in \mathbb{F}_q^\times$ not an ℓth power. Similarly, the constant ℓ in the definition of $\mathcal{F}(s)$ accounts for the extensions $K(\sqrt[\ell]{\beta}), \dots, K(\sqrt[\ell]{\beta^{\ell-1}})$ for $\beta \in \mathbb{F}_q^\times$ not an ℓth power, as well as the K-algebra given by the completely split cover.

Using the identity

$$\frac{1+(\ell-1)\,u}{(1+u)^{\ell-1}} = \prod_{j=1}^{\ell-2}\left(1 - \frac{ju^2}{(1+u)\,(1+ju)}\right),$$

we write

$$\begin{aligned}\mathcal{A}\left(s\right) &= \prod_v \left(1+(\ell-1)\,Nv^{-(\ell-1)s}\right)\\ &= \left(\frac{\zeta_K\left((\ell-1)\,s\right)}{\zeta_K\left(2\,(\ell-1)\,s\right)}\right)^{\ell-1} \prod_{j=1}^{\ell-2}\prod_v \left(1 - \frac{jNv^{-2(\ell-1)s}}{\left(1+Nv^{-(\ell-1)s}\right)\left(1+jNv^{-(\ell-1)s}\right)}\right),\end{aligned}$$

where the absolute convergence of the infinite products for $\mathrm{Re}(s) > \frac{1}{2(\ell-1)}$ follows from that of $\sum_v \frac{1}{Nv^{2(\ell-1)s}}$.

We also write

$$\begin{aligned}\mathcal{B}\left(s\right) &= \prod_v \left(1+\left(\xi_\ell^{\deg v}+\dots+\xi_\ell^{(\ell-1)\deg v}\right)Nv^{-(\ell-1)s}\right)\\ &= \prod_v \prod_{j=1}^{\ell-1}\left(1+\xi_\ell^{j\deg v}Nv^{-(\ell-1)s}\right)\prod_v \frac{\left(1+\left(\xi_\ell^{\deg v}+\dots+\xi_\ell^{(\ell-1)\deg v}\right)Nv^{-(\ell-1)s}\right)}{\prod_{j=1}^{\ell-1}\left(1+\xi_\ell^{j\deg v}Nv^{-(\ell-1)s}\right)},\end{aligned}$$

where the absolute convergence of the infinite products follows in the same way as the products appearing in $\mathcal{A}(s)$.

Recall from Lemma 3.3 that $\mathcal{A}(s)$ is a meromorphic function on $\mathrm{Re}(s) > \frac{1}{2(\ell-1)}$ with a pole of order $\ell-1$ at $s = \frac{1}{\ell-1}$ in the region $B_{\ell-1}$ as defined in (11). The function $\mathcal{B}(s)$ is also meromorphic in $\mathrm{Re}(s) > \frac{1}{2(\ell-1)}$, with simple poles at $s_j = \frac{1}{\ell-1} + \frac{2j\pi i}{(\ell-1)\ell\log q}$ for $|2j| < \ell$ in the region $B_{\ell-1}$.

We set $u = q^{-(\ell-1)s}$, and write $A(u) := \mathcal{A}(s)$ and $B(u) := \mathcal{B}(s)$. Thus,

$$A(u) = \left(\frac{(1-qu^2)(1+u)}{(1-qu)}\right)^{\ell-1} \prod_{j=1}^{\ell-2} \prod_v \left(1 - \frac{ju^{2\deg v}}{\left(1+u^{\deg v}\right)\left(1+ju^{\deg v}\right)}\right),$$

$$B(u) = \prod_v \prod_{j=1}^{\ell-1} \left(1 + \left(\xi_\ell^j u\right)^{\deg v}\right) \prod_v \frac{\left(1 + \left(\xi_\ell^{\deg v} + \cdots + \xi_\ell^{(\ell-1)\deg v}\right) u^{\deg v}\right)}{\prod_{j=1}^{\ell-1}\left(1 + \left(\xi_\ell^j u\right)^{\deg v}\right)}$$

$$= \prod_{j=1}^{\ell-1} \frac{Z_K\left(\xi_\ell^j u\right)}{Z_K\left(\xi_\ell^{2j} u^2\right)} \prod_v \frac{\left(1 + b(v) u^{\deg v}\right)}{\prod_{j=1}^{\ell-1}\left(1 + \left(\xi_\ell^j u\right)^{\deg v}\right)},$$

where $Z_K(u) = \frac{1}{(1-qu)(1-u)}$ and $b(v) = \xi_\ell^{\deg v} + \cdots + \xi_\ell^{(\ell-1)\deg v}$.

Fix any δ with $\frac{1}{2(\ell-1)} < \delta < \frac{1}{\ell-1}$. Then $A(u)$ and $B(u)$ are meromorphic functions on the disk $\{u : |u| \le q^{-\delta}\}$. We see that $A(u)$ has a pole of order $\ell - 1$ at $u = 1/q$ and $B(u)$ has $(\ell-1)$ simple poles at $u = (q\xi_\ell^j)^{-1}$ for $j = 1, \ldots, \ell-1$. Then, applying Theorem 2.5 and Lemma 3.3 to $\mathcal{F}(s) = \mathcal{A}(s) + (\ell-1)\mathcal{B}(s)$ with $\delta = \frac{1}{2(\ell-1)} + \varepsilon$ for $\varepsilon > 0$, we have that

$$N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}) = -\mathrm{Res}_{u=q^{-1}} \frac{A(u)}{u^{\mathfrak{n}+1}} - \sum_{j=1}^{\ell-1} \mathrm{Res}_{u=\left(q\xi_\ell^j\right)^{-1}} \frac{B(u)}{u^{\mathfrak{n}+1}} + O\left(q^{(1/2+\varepsilon)\mathfrak{n}}\right). \tag{20}$$

We compute

$$\mathrm{Res}_{u=q^{-1}} \frac{A(u)}{u^{\mathfrak{n}+1}} = \lim_{u \to q^{-1}} \frac{1}{(\ell-2)!} \frac{d^{\ell-2}}{du^{\ell-2}} \left(u - q^{-1}\right)^{\ell-1} \frac{1}{u^{\mathfrak{n}+1}} \left(\frac{(1-qu^2)(1+u)}{(1-qu)}\right)^{\ell-1}$$
$$\times \prod_{j=1}^{\ell-2} \prod_v \left(1 - \frac{ju^{2\deg v}}{\left(1+u^{\deg v}\right)\left(1+ju^{\deg v}\right)}\right)$$
$$= \lim_{u \to q^{-1}} \frac{1}{(\ell-2)!} \frac{d^{\ell-2}}{du^{\ell-2}} \left(\frac{\left(-\left(1-qu^2\right)(1+u)\right)^{\ell-1}}{q^{\ell-1}u^{\mathfrak{n}+1}}\right)$$
$$\times \prod_{j=1}^{\ell-2} \prod_v \left(1 - \frac{ju^{2\deg v}}{\left(1+u^{\deg v}\right)\left(1+ju^{\deg v}\right)}\right).$$

Let

$$H_\ell(u) := \frac{1}{(\ell-2)!} \left(\frac{\left(-\left(1-qu^2\right)(1+u)\right)^{\ell-1}}{q^{\ell-1}}\right) \prod_{j=1}^{\ell-2} \prod_v \left(1 - \frac{ju^{2\deg v}}{\left(1+u^{\deg v}\right)\left(1+ju^{\deg v}\right)}\right). \tag{21}$$

Then, using the product rule for derivatives, we get

$$\begin{aligned}\mathrm{Res}_{u=q^{-1}}\frac{A(u)}{u^{\mathfrak{n}+1}} &= \lim_{u\to q^{-1}}\sum_{i=0}^{\ell-2}\frac{d^i}{du^i}\left(\frac{1}{u^{\mathfrak{n}+1}}\right)\frac{d^{\ell-2-i}}{du^{\ell-2-i}}H_\ell(u)\\ &= \lim_{u\to q^{-1}}\sum_{i=0}^{\ell-2}\frac{(-1)^i(\mathfrak{n}+1)\cdots(\mathfrak{n}+i)}{u^{\mathfrak{n}+i+1}}\frac{d^{\ell-2-i}}{du^{\ell-2-i}}H_\ell(u)\\ &= \sum_{i=0}^{\ell-2}(-1)^i(\mathfrak{n}+1)\cdots(\mathfrak{n}+i)\,q^{\mathfrak{n}+i+1}\left.\frac{d^{\ell-2-i}}{du^{\ell-2-i}}H_\ell(u)\right|_{u=q^{-1}},\end{aligned}$$

which proves that this residue is given by a polynomial in $\mathfrak{n}$.

We take a closer look at the main term of this polynomial, which is the dominating term when $\mathfrak{n}\to\infty$. We obtain

$$\begin{aligned}\mathrm{Res}_{u=q^{-1}}\frac{A(u)}{u^{\mathfrak{n}+1}} &= \lim_{u\to q^{-1}}\frac{1}{(\ell-2)!}\frac{(-1)^{\ell-2}(\mathfrak{n}+1)\cdots(\mathfrak{n}+\ell-2)}{u^{\mathfrak{n}+\ell-1}}\left(\frac{\left(-\left(1-qu^2\right)(1+u)\right)^{\ell-1}}{q^{\ell-1}}\right)\\ &\quad\times\prod_{j=1}^{\ell-2}\prod_{v}\left(1-\frac{ju^{2\deg v}}{\left(1+u^{\deg v}\right)\left(1+ju^{\deg v}\right)}\right)(1+O(1/\mathfrak{n}))\\ &= -\frac{\mathfrak{n}^{\ell-2}}{(\ell-2)!}\left(1-q^{-2}\right)^{\ell-1}q^{\mathfrak{n}}\prod_{j=1}^{\ell-2}\prod_{v}\left(1-\frac{jq^{-2\deg v}}{\left(1+q^{-\deg v}\right)\left(1+jq^{-\deg v}\right)}\right)\\ &\quad\times(1+O(1/\mathfrak{n})).\end{aligned}$$

For the other residues, coming from simple poles,

$$\begin{aligned}\mathrm{Res}_{u=\left(q\xi_\ell^{j_0}\right)^{-1}}\frac{B(u)}{u^{\mathfrak{n}+1}} &= \lim_{u\to q^{-1}\xi_\ell^{-j_0}}\frac{\left(u-q^{-1}\xi_\ell^{-j_0}\right)}{u^{\mathfrak{n}+1}}\prod_{j=1}^{\ell-1}\frac{\left(1-q\xi_\ell^{2j}u^2\right)\left(1+\xi_\ell^ju\right)}{\left(1-q\xi_\ell^ju\right)}\\ &\quad\times\prod_v\frac{\left(1+b(v)\,u^{\deg v}\right)}{\prod_{j=1}^{\ell-1}\left(1+\left(\xi_\ell^ju\right)^{\deg v}\right)}\\ &= \lim_{u\to q^{-1}\xi_\ell^{-j_0}}\frac{-\left(1-q\xi_\ell^{2j_0}u^2\right)\left(1+\xi_\ell^{j_0}u\right)}{u^{\mathfrak{n}+1}q\xi_\ell^{j_0}}\prod_{j=1,\,j\neq j_0}^{\ell-1}\frac{\left(1-q\xi_\ell^{2j}u^2\right)\left(1+\xi_\ell^ju\right)}{\left(1-q\xi_\ell^ju\right)}\\ &\quad\times\prod_v\frac{\left(1+b(v)\,u^{\deg v}\right)}{\prod_{j=1}^{\ell-1}\left(1+\left(\xi_\ell^ju\right)^{\deg v}\right)}\end{aligned}$$

$$= -\left(q\xi_\ell^{j_0}\right)^{\mathfrak{n}}\left(1-q^{-2}\right)\prod_{j=1,\, j\neq j_0}^{\ell-1}\frac{\left(1-q^{-1}\xi_\ell^{2j-2j_0}\right)\left(1+q^{-1}\xi_\ell^{j-j_0}\right)}{\left(1-\xi_\ell^{j-j_0}\right)}$$

$$\times\prod_{v}\frac{\left(1+b(v)\left(q^{-1}\xi_\ell^{-j_0}\right)^{\deg v}\right)}{\prod_{j=1}^{\ell-1}\left(1+\left(q^{-1}\xi_\ell^{j-j_0}\right)^{\deg v}\right)}.$$

We note that the line above is $O(q^{\mathfrak{n}})$ and it contributes to the constant coefficient of $P_\ell(\mathfrak{n})$.

Replacing the residues in (20) with the equations above completes the proof. ■

In spite of the fact that Corollary 1.2 can be deduced from the statement of Theorem 1.1, we will prove it first and independently of Theorem 1.1 as a way of introducing the key ideas in the proof of Theorem 1.1. The case of v ramified and $\ell=2$ will be discussed later, in Section 4.1.

Recall that

$$C_\ell = \frac{\left(1-q^{-2}\right)^{\ell-1}}{(\ell-2)!}\prod_{j=1}^{\ell-2}\prod_{v\in\mathcal{V}_K}\left(1-\frac{jq^{-2\deg v}}{\left(1+q^{-\deg v}\right)\left(1+jq^{-\deg v}\right)}\right). \tag{22}$$

Proof of Corollary 1.2. Since v_0 is ramified at a cover L/K if and only if v_0 divides $\mathrm{Disc}(L/K)$, the generating function for the number of extensions counted by $N(\mathbb{Z}/\ell\mathbb{Z},\mathfrak{n})$ that are ramified at v_0 is

$$\begin{aligned}
\mathcal{F}_R(s) &= \sum_{\substack{\mathrm{Gal}(L/K)\cong\mathbb{Z}/\ell\mathbb{Z}\\ v_0\ \text{ramified}}}\mathfrak{D}(L/K)^{-s}\\
&= (\ell-1)\,Nv_0^{-(\ell-1)s}\prod_{v\neq v_0}\left(1+(\ell-1)\,Nv^{-(\ell-1)s}\right)\\
&\quad+(\ell-1)\,b(v_0)\,Nv_0^{-(\ell-1)s}\prod_{v\neq v_0}\left(1+b(v)\,Nv^{-(\ell-1)s}\right)\\
&= \frac{(\ell-1)\,Nv_0^{-(\ell-1)s}}{1+(\ell-1)\,Nv_0^{-(\ell-1)s}}\mathcal{A}(s)+(\ell-1)\,\frac{b(v_0)\,Nv_0^{-(\ell-1)s}}{1+b(v_0)\,Nv_0^{-(\ell-1)s}}\mathcal{B}(s)
\end{aligned}$$

where we have excluded the case $\phi_{v_0}(g_{v_0})=0$ to account for v_0 ramified as stated in Proposition 2.4.

With the change of variable $u=q^{-(\ell-1)s}$, we obtain

$$F_R(u)=\frac{(\ell-1)\,u^{\deg v_0}}{1+(\ell-1)\,u^{\deg v_0}}A(u)+(\ell-1)\,\frac{b(v_0)\,u^{\deg v_0}}{1+b(v_0)\,u^{\deg v_0}}B(u).$$

Then, applying Theorem 2.5 and Lemma 3.3 with $\delta = \frac{1}{2(\ell-1)} + \varepsilon$ for any $\varepsilon > 0$, we get

$$N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}, v_0, \text{ramified}) = -\text{Res}_{u=q^{-1}} \frac{(\ell-1)\, u^{\deg v_0}}{1+(\ell-1)\, u^{\deg v_0}} \frac{A(u)}{u^{\mathfrak{n}+1}} - (\ell-1) \sum_{j=1}^{\ell-1} \text{Res}_{u=\left(q\xi_\ell^j\right)^{-1}} \frac{b(v_0)\, u^{\deg v_0}}{1+b(v_0)\, u^{\deg v_0}} \frac{B(u)}{u^{\mathfrak{n}+1}} + O\left(q^{\left(\frac{1}{2}+\varepsilon\right)\mathfrak{n}}\right).$$

For the residue involving the function $A(u)$, we have

$$\text{Res}_{u=q^{-1}} \frac{(\ell-1)\, u^{\deg v_0}}{1+(\ell-1)\, u^{\deg v_0}} \frac{A(u)}{u^{\mathfrak{n}+1}} = \lim_{u\to q^{-1}} \frac{d^{\ell-2}}{du^{\ell-2}} \frac{(\ell-1)\, u^{\deg v_0}}{1+(\ell-1)\, u^{\deg v_0}} \frac{H_\ell(u)}{u^{\mathfrak{n}+1}},$$

where $H_\ell(u)$ is given by (21). This yields

$$\text{Res}_{u=q^{-1}} \frac{(\ell-1)\, u^{\deg v_0}}{1+(\ell-1)\, u^{\deg v_0}} \frac{A(u)}{u^{\mathfrak{n}+1}} = \sum_{i=0}^{\ell-2} (-1)^i (\mathfrak{n}+1)\cdots(\mathfrak{n}+i) q^{\mathfrak{n}+i+1} \frac{d^{\ell-2-i}}{du^{\ell-2-i}} \frac{(\ell-1)\, u^{\deg v_0}}{1+(\ell-1)\, u^{\deg v_0}} H_\ell(u)\Big|_{u=q^{-1}},$$

and we obtain the polynomial in $\mathfrak{n}$ as in the case of the proof of Theorem 4.1. As before, we record the main coefficient as the dominating term when $\mathfrak{n}\to\infty$ to be

$$\begin{aligned}\text{Res}_{u=q^{-1}} &\frac{(\ell-1)\, u^{\deg v_0}}{1+(\ell-1)\, u^{\deg v_0}} \frac{A(u)}{u^{\mathfrak{n}+1}} \\ &= -\frac{\mathfrak{n}^{\ell-2}}{(\ell-2)!} \left(1-q^{-2}\right)^{\ell-1} q^{\mathfrak{n}} \frac{(\ell-1)\, q^{-\deg v_0}}{1+(\ell-1)\, q^{-\deg v_0}} \\ &\quad \times \prod_{j=1}^{\ell-2} \prod_{v} \left(1 - \frac{jq^{-2\deg v}}{\left(1+q^{-\deg v}\right)\left(1+jq^{-\deg v}\right)}\right) (1+O(1/\mathfrak{n})) \\ &= -C_\ell \frac{(\ell-1)\, q^{-\deg v_0}}{1+(\ell-1)\, q^{-\deg v_q}} q^{\mathfrak{n}} \mathfrak{n}^{\ell-2} (1+O(1/\mathfrak{n})).\end{aligned}$$

For the residues involving the function $B(u)$, we note that, since the poles are of order one,

$$\text{Res}_{u=\left(q\xi_\ell^j\right)^{-1}} \frac{b(v_0)\, u^{\deg v_0}}{1+b(v_0)\, u^{\deg v_0}} \frac{B(u)}{u^{\mathfrak{n}+1}} = \frac{b(v_0)\left(q\xi_\ell^j\right)^{-\deg v_0}}{1+b(v_0)\left(q\xi_\ell^j\right)^{-\deg v_0}} \text{Res}_{u=\left(q\xi_\ell^j\right)^{-1}} \frac{B(u)}{u^{\mathfrak{n}+1}}.$$

The number above is equal to $O(q^{\mathfrak{n}})$ and it will contribute to the constant coefficient of the polynomial $P_R(\mathfrak{n})$. This proves the result for the number of extensions ramifying at v_0. We now consider the case of extensions splitting at v_0. First, we write the generating function for the number of extensions of K unramified at v_0 as

$$\begin{aligned}
\mathcal{F}_U(s) &= \ell + \sum_{\substack{\mathrm{Gal}(L/K)\cong\mathbb{Z}/\ell\mathbb{Z} \\ v_0 \text{ unramified}}} \mathfrak{D}(L/K)^{-s} \\
&= \sum_{j=0}^{\ell-1} \prod_{v\neq v_0} \left(1 + \left(\xi_\ell^{j\deg v} + \cdots + \xi_\ell^{(\ell-1)j\deg v}\right) Nv^{-(\ell-1)s}\right) \\
&= \prod_{v\neq v_0} \left(1 + (\ell-1)\, Nv^{-(\ell-1)s}\right) + (\ell-1) \prod_{v\neq v_0} \left(1 + b(v)\, Nv^{-(\ell-1)s}\right) \\
&= \frac{1}{1+(\ell-1)\, Nv_0^{-(\ell-1)s}} \mathcal{A}(s) + \frac{(\ell-1)}{1+b(v_0)\, Nv_0^{-(\ell-1)s}} \mathcal{B}(s).
\end{aligned}$$

Using the notation of Section 3, recall that $b_\ell = \mu^{\frac{q-1}{\ell}}$ where μ is a generator of $\mathbb{F}_q^\times$ (hence b_ℓ is an ℓth root of unity in $\mathbb{F}_q^\times$), and $\sigma : \mathbb{F}_q^\times \to \mathbb{C}$ is a character of order ℓ. Let $\rho_\ell = \sigma(b_\ell)$, which is then a primitive ℓth root of unity in $\mathbb{C}$. For each $v \neq v_0, v_\infty$, denote by n_v a positive integer such that the image of v_0 in $(\mathcal{O}_v/(\pi_v))^\times$ is $g_v^{n_v}$. Then $\phi_v(v_0) = n_v\phi_v(g_v)$. Hence, by Proposition 2.4, v_0 is unramified and split if and only if $\phi_{v_0}(\mathcal{O}_{v_0}^\times) = 0$ and

$$-(\deg v_0)\, \psi_\infty(\pi_\infty) + \sum_{v\neq v_0, v_\infty} n_v\phi_v(g_v) \equiv 0 \pmod{\ell},$$

which is equivalent to

$$\rho_\ell^{-(\deg v_0)\psi_\infty(\pi_\infty)} \prod_{v\neq v_0, v_\infty} \rho_\ell^{n_v\phi_v(g_v)} = 1.$$

By the definition of ρ_ℓ and n_v above and the construction of $\chi_{v,\ell}(v_0)$ from Section 3, we see that $\chi_{v,\ell}(v_0) = \sigma(\frac{g_v^{n_v}}{v})_\ell = \sigma(b_\ell)^{n_v} = \rho_\ell^{n_v}$ and, hence, the above equality can be written as

$$D(v_0) := \rho_\ell^{-(\deg v_0)\psi_\infty(\pi_\infty)} \prod_{v\neq v_0, v_\infty} \chi_{v,\ell}(v_0)^{\phi_v(g_v)} = 1.$$

Thus, $v_0 \neq v_\infty$ is unramified and split if and only if $\phi_{v_0}(\mathcal{O}_{v_0}^\times) = 0$ and

$$D(v_0) = 1. \tag{23}$$

Since $D(v_0)$ is a ℓth root of unity, we can rewrite (23) as

$$\frac{1}{\ell}\sum_{j=0}^{\ell-1} D\left(v_0\right)^j = \begin{cases} 1 & \text{if } v_0 \text{ is unramified and split,} \\ 0 & \text{otherwise,} \end{cases} \tag{24}$$

and this is the criterion that we will use in the generating series.

Analogously, we also have that v_∞ is unramified and split if and only if $\phi_{v_\infty}(\mathcal{O}_{v_\infty}^\times)=0$ and

$$\rho_\ell^{-(\deg v_\infty)\psi_\infty(\pi_\infty)}=1,$$

since $\deg v_\infty = 1$.

We claim that the Dirichlet series for cyclic extensions splitting at a fixed place $v_0 \neq v_\infty$ is

$$\begin{aligned}\mathcal{F}_S\left(s\right) = \frac{1}{\ell^2}\sum_{j=0}^{\ell-1}\sum_{k=0}^{\ell-1}\sum_{r=0}^{\ell-1}\rho_\ell^{-rk\deg v_0} \\ \times \prod_{v\neq v_0, v_\infty}\left(1+\left(\xi_\ell^{j\deg v}\chi_{v,\ell}\left(v_0\right)^k+\cdots+\xi_\ell^{(\ell-1)j\deg v}\chi_{v,\ell}\left(v_0\right)^{(\ell-1)k}\right)Nv^{-(\ell-1)s}\right) \\ \times\left(1+\left(\xi_\ell^{j\deg v_\infty}+\cdots+\xi_\ell^{(\ell-1)j\deg v_\infty}\right)Nv_\infty^{-(\ell-1)s}\right).\end{aligned}$$

Recall by Propositions 2.2–2.4 the cyclic extensions splitting at a fixed place $v_0\neq v_\infty$ are in one-to-one correspondence with the maps $\phi:\pi_\infty^{\mathbb{Z}}\times\prod_v \mathcal{O}_v^\times \to \mathbb{Z}/\ell\mathbb{Z}$ satisfying (8), together with the splitting conditions (23) and $\phi_{v_0}(\mathcal{O}_{v_0}^\times)=0$. Let Cond$(\phi)$ be the conductor of such a map ϕ, and v be a place of the conductor. For each fixed j,k,r in the first line above, the ith term $\rho_\ell^{-rk\deg v_0}\xi_\ell^{ij\deg v}\chi_{v,\ell}(v_0)^{ik}Nv^{-(\ell-1)s}$ in the Euler product corresponds to the map where $\phi_v(g_v)=i$ and $\psi_\infty(\pi_\infty)=r$ for $1\leq i\leq \ell-1$. Considering all the places v of Cond(ϕ) (including v_∞, which is accounted for in the last line of the equation), the term in the j,k,rth Dirichlet series above corresponding to the global map ϕ equals

$$\left(\xi_\ell^{\sum_v j\phi_v(g_v)\deg v}\right)\times\rho_\ell^{-rk\deg v_0}\prod_{v\neq v_0,v_\infty}\chi_{v,\ell}\left(v_0\right)^{k\phi_v(g_v)}\times N\left(\mathrm{Cond}\left(\phi\right)\right)^{-(\ell-1)s}.$$

Summing over j, we obtain zero unless condition (8) is satisfied. Summing over r covers all the possible values of $\psi_\infty(\pi_\infty)$. Finally, summing over k yields zero unless condition (23) is satisfied. Thus the sum of those terms over k, j, together with the correcting factor $\frac{1}{\ell^2}$ will yield $N(\mathrm{Cond}(\phi))^{-(\ell-1)s}$ if both conditions (8) and (23) are satisfied, and zero otherwise.

We also remark that the constant term of $\mathcal{F}_S(s)$ is ℓ if $\ell \mid \deg v_0$, and 1 otherwise. When $v_0 = v_\infty$, we have

$$\mathcal{F}_S(s) = \frac{1}{\ell^2} \sum_{j=0}^{\ell-1} \sum_{k=0}^{\ell-1} \sum_{r=0}^{\ell-1} \rho_\ell^{-rk \deg v_\infty} \prod_{v \neq v_\infty} \left(1 + \left(\xi_\ell^{j \deg v} + \cdots + \xi_\ell^{(\ell-1) j \deg v}\right) N v^{-(\ell-1)s}\right)$$

$$= \frac{1}{\ell} \sum_{j=0}^{\ell-1} \prod_{v \neq v_\infty} \left(1 + \left(\xi_\ell^{j \deg v} + \cdots + \xi_\ell^{(\ell-1) j \deg v}\right) N v^{-(\ell-1)s}\right) = \frac{1}{\ell} \mathcal{F}_U(s).$$

By considering the definitions of $\chi_{v_\infty}(v)$ and $\chi_v(v_\infty)$, the previous two formulas can both be written as

$$\mathcal{F}_S(s) = \frac{1}{\ell^2} \sum_{j=0}^{\ell-1} \sum_{k=0}^{\ell-1} \sum_{r=0}^{\ell-1} \rho_\ell^{-rk \deg v_0}$$

$$\times \prod_{v \neq v_0} \left(1 + \left(\xi_\ell^{j \deg v} \chi_{v,\ell}(v_0)^k + \cdots + \xi_\ell^{(\ell-1) j \deg v} \chi_{v,\ell}(v_0)^{(\ell-1)k}\right) N v^{-(\ell-1)s}\right),$$

which is valid for any place v_0.

Separating the term with $k = 0$ from the terms with $k \neq 0$, we obtain

$$\mathcal{F}_S(s) = \frac{1}{\ell} \mathcal{F}_U(s) + \frac{1}{\ell^2} \sum_{j=0}^{\ell-1} \sum_{k=1}^{\ell-1} \left(\sum_{r=0}^{\ell-1} \rho_\ell^{-rk \deg v_0}\right) \mathcal{M}_{j,k}(s, v_0, \text{split}), \tag{25}$$

where $\mathcal{M}_{j,k}(s, v_0, \text{split})$ is given by (16).

Applying Theorem 2.5 and Lemmas 3.2 and 3.3 to the generating function $\mathcal{F}_S(s)$, we get

$$N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}, v_0, \text{split}) = -\frac{1}{\ell} \operatorname{Res}_{u=q^{-1}} \frac{1}{1 + (\ell-1) u^{\deg v_0}} \frac{A(u)}{u^{\mathfrak{n}+1}} - \frac{\ell-1}{\ell} \sum_{j=1}^{\ell-1} \operatorname{Res}_{u=\left(\xi_\ell^j q\right)^{-1}}$$

$$\frac{1}{\ell\left(1 + b(v_0) u^{\deg v_0}\right)} \frac{B(u)}{u^{\mathfrak{n}+1}} + O\left(q^{(1/2+\varepsilon)\mathfrak{n}}\right). \tag{26}$$

The residue computation is similar to the residue computation leading to the count of $N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}, v_0, \text{ramified})$ above, but we repeat it for completeness. For the residue involving the function $A(u)$, we have

$$\operatorname{Res}_{u=q^{-1}} \frac{1}{1 + (\ell-1) u^{\deg v_0}} \frac{A(u)}{u^{\mathfrak{n}+1}} = \lim_{u \to q^{-1}} \frac{d^{\ell-2}}{du^{\ell-2}} \frac{1}{1 + (\ell-1) u^{\deg v_0}} \frac{H_\ell(u)}{u^{\mathfrak{n}+1}},$$

where $H_\ell(u)$ is given by (21). This yields

$$\begin{aligned}&\mathrm{Res}_{u=q^{-1}} \frac{1}{1+(\ell-1)\,u^{\deg v_0}} \frac{A(u)}{u^{\mathfrak{n}+1}}\\ &\quad= \sum_{i=0}^{\ell-2} (-1)^i\,(\mathfrak{n}+1)\cdots(\mathfrak{n}+i) q^{\mathfrak{n}+i+1}\; \frac{d^{\ell-2-i}}{du^{\ell-2-i}} \frac{1}{1+(\ell-1)\,u^{\deg v_0}} H_\ell\,(u)\Big|_{u=q^{-1}},\end{aligned}$$

which gives $q^{\mathfrak{n}}P(\mathfrak{n})$, where P is a polynomial of degree $\ell-2$ as before. Using the definition of $H_\ell(u)$, the leading term of the polynomial $P(\mathfrak{n})$ is

$$\begin{aligned}&-\frac{\mathfrak{n}^{\ell-2}}{(\ell-2)!}\left(1-q^{-2}\right)^{\ell-1} q^{\mathfrak{n}} \frac{1}{1+(\ell-1)\,q^{-\deg v_0}} \prod_{j=1}^{\ell-2}\prod_{v}\left(1-\frac{jq^{-2\deg v}}{\left(1+q^{-\deg v}\right)\left(1+jq^{-\deg v}\right)}\right)\\ &= -C_\ell \frac{1}{1+(\ell-1)\,q^{-\deg v_0}} q^{\mathfrak{n}}\mathfrak{n}^{\ell-2}.\end{aligned}$$

For the residues involving the function $B(u)$, we note as before that since the poles are of order one, their contribution is of order $O(q^{\mathfrak{n}})$, and they will contribute to the constant coefficient of the polynomial $P_S(\mathfrak{n})$.

Then, replacing in (26), we obtain that

$$N\,(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}, v_0, \text{split}) = \frac{1}{\ell\left(1+(\ell-1)\,q^{-\deg v_0}\right)} C_\ell\, q^{\mathfrak{n}} P_S\,(\mathfrak{n}) + O\left(q^{(1/2+\varepsilon)\mathfrak{n}}\right)$$

as claimed.

Finally, we now consider the Dirichlet series for cyclic extensions for which a fixed place v_0 is inert. It is given by

$$\mathcal{F}_I\,(s) = \mathcal{F}_U\,(s) - \mathcal{F}_S\,(s)\,.$$

Using (25), and applying Theorem 2.5 and Lemmas 3.2 and 3.3 to the generating function $\mathcal{F}_I(s)$, we get

$$\begin{aligned}N\,(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}, v_0, \text{inert}) = (\ell-1)&\left(-\frac{1}{\ell}\mathrm{Res}_{u=q^{-1}} \frac{1}{1+(\ell-1)\,u^{\deg v_0}} \frac{A(u)}{u^{\mathfrak{n}+1}}\right.\\ &\left.-\frac{\ell-1}{\ell}\sum_{j=1}^{\ell-1} \mathrm{Res}_{u=\left(\xi_\ell^j q\right)^{-1}} \frac{1}{\ell\left(1+b\,(v_0)\,u^{\deg v_0}\right)} \frac{B(u)}{u^{\mathfrak{n}+1}}\right) + O\left(q^{(1/2+\varepsilon)\mathfrak{n}}\right),\end{aligned}$$

which proves that

$$N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}, v_0, \text{inert}) = (\ell-1)\, N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}, v_0, \text{split}) + O\left(q^{(1/2+\varepsilon)\mathfrak{n}}\right).$$

This concludes the proof of Corollary 1.2. ■

We are now ready to prove the main result.

Theorem 4.2. Let $\mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_I$ be three finite and disjoint sets of places of K. Let

$$N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}; \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_I)$$

be the number of extensions of $\mathbb{F}_q(X)$ with Galois group $\mathbb{Z}/\ell\mathbb{Z}$ such that the degree of the conductor is $\mathfrak{n}$, and that are ramified at the places of $\mathcal{V}_R$ (completely) split at the places of $\mathcal{V}_S$, and inert at the places of $\mathcal{V}_I$. Let $\mathcal{V} = \mathcal{V}_R \cup \mathcal{V}_S \cup \mathcal{V}_I$. Then,

$$N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}; \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_I) = C_\ell \left(\prod_{v\in\mathcal{V}} c_v\right) q^{\mathfrak{n}} P_{\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I}(\mathfrak{n}) + O\left(q^{\left(\frac{1}{2}+\varepsilon\right)\mathfrak{n}}\right),$$

and

$$\frac{N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n}; \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_I)}{N(\mathbb{Z}/\ell\mathbb{Z}, \mathfrak{n})} = \left(\prod_{v\in\mathcal{V}} c_v\right)\left(1 + O\left(\frac{1}{\mathfrak{n}}\right)\right),$$

where $P_{\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I}(X) \in \mathbb{R}[X]$ is a monic polynomial of degree $\ell-2$ and C_ℓ is given by

$$C_\ell = \frac{\left(1-q^{-2}\right)^{\ell-1}}{(\ell-2)!} \prod_{j=1}^{\ell-2} \prod_{v\in\mathcal{V}_K} \left(1 - \frac{jq^{-2\deg v}}{\left(1+q^{-\deg v}\right)\left(1+jq^{-\deg v}\right)}\right).$$

In addition,

$$c_v = \begin{cases} \dfrac{(\ell-1)\, q^{-\deg v}}{1+(\ell-1)\, q^{-\deg v}} & \text{if } v \in \mathcal{V}_R, \\ \dfrac{1}{\ell\left(1+(\ell-1)\, q^{-\deg v}\right)} & \text{if } v \in \mathcal{V}_S, \\ \dfrac{\ell-1}{\ell\left(1+(\ell-1)\, q^{-\deg v}\right)} & \text{if } v \in \mathcal{V}_I. \end{cases}$$ □

Proof. Let $\mathcal{V}_U = \mathcal{V}_S \cup \mathcal{V}_I$.

We first construct the Dirichlet generating series with prescribed conditions for $\mathcal{V}_R$, $\mathcal{V}_U$, and $\mathcal{V}_S = \{v_1, \ldots, v_n\} \subset \mathcal{V}_U$. In other words, for the elements $v \in \mathcal{V}_I$ we will only prescribe that they are in $\mathcal{V}_U$ and we will ignore the inert condition for the moment.

We claim that the generating series is then

$$\mathcal{F}_{\mathcal{V}_R,\mathcal{V}_S\subset\mathcal{V}_U}(s)$$
$$= \frac{1}{\ell^{n+1}} \sum_{j=0}^{\ell-1}\sum_{k_1=0}^{\ell-1}\cdots\sum_{k_n=0}^{\ell-1}\sum_{r=0}^{\ell-1} \rho_\ell^{-r\sum_{h=1}^n k_h \deg v_h}$$
$$\times \prod_{v\notin\mathcal{V}_R\cup\mathcal{V}_U}\left(1+\left(\xi_\ell^{j\deg v}\prod_{h=1}^n \chi_{v,\ell}(v_h)^{k_h}+\cdots+\xi_\ell^{(\ell-1)j\deg v}\prod_{h=1}^n\chi_{v,\ell}(v_h)^{(\ell-1)k_h}\right)Nv^{-(\ell-1)s}\right)$$
$$\times \prod_{v\in\mathcal{V}_R}\left(\xi_\ell^{j\deg v}+\cdots+\xi_\ell^{(\ell-1)j\deg v}\right)Nv^{-(\ell-1)s}.$$

Let us prove that the above formula is correct. Recall by Propositions 2.2–2.4 that the cyclic extensions that are ramified at the primes of $\mathcal{V}_R$, unramified at the primes of $\mathcal{V}_U$, and split at the primes of $\mathcal{V}_S$ are in one-to-one correspondence with the maps $\phi:\pi_\infty^{\mathbb{Z}}\times\prod_v\mathcal{O}_v^\times\to\mathbb{Z}/\ell\mathbb{Z}$ satisfying (8), together with the ramification conditions: ϕ_v is nontrivial on $\mathcal{O}_v^\times$ for $v\in\mathcal{V}_R$, $\phi_v(\mathcal{O}_v^\times)=0$ for $v\in\mathcal{V}_U$, and the splitting conditions (23) for $v\in\mathcal{V}_S$. Thus consider all the possible choices of parameters $(\{r_v\},r)$ where ϕ is determined by setting $\phi_v(g_v)=r_v$ and $\psi_\infty(\pi_\infty)=r$ in such a way that ϕ is ramified at the primes of $\mathcal{V}_R$, unramified at the primes of $\mathcal{V}_U$, and split at the primes of $\mathcal{V}_S$. Therefore we have $0<r_v\le\ell-1$ for all $v\in\mathcal{V}_R$, and $r_v=0$ for all primes of $\mathcal{V}_U$. For each fixed $j,k_1,\dots,k_n$, the map ϕ with parameters $(\{r_v\},r)$ corresponds to the component

$$\left(\prod_{v\notin\mathcal{V}_R\cup\mathcal{V}_U}\rho_\ell^{-r\sum_{h=1}^n k_h\deg v_h}\xi_\ell^{jr_v\deg v}\prod_{h=1}^n\chi_{v,\ell}(v_h)^{r_vk_h}\right)\times\left(\prod_{v\in\mathcal{V}_R}\xi_\ell^{r_vj\deg v}\right)\times N(\mathrm{Cond}(\phi))^{-(\ell-1)s}$$

of the Euler product. Summing over all $j,k_1,\dots,k_n$, we obtain that the coefficient of $N(\mathrm{Cond}(\phi))^{-(\ell-1)s}$ is given by

$$\left(\sum_{k_1=0}^{\ell-1}\rho_\ell^{-rk_1\deg v_1}\prod_v\chi_{v,\ell}(v_1)^{r_vk_1}\right)\times\cdots\times\left(\sum_{k_n=0}^{\ell-1}\rho_\ell^{-rk_n\deg v_n}\prod_v\chi_{v,\ell}(v_n)^{r_vk_n}\right)$$
$$\times\left(\sum_{j=0}^{\ell-1}\xi_\ell^{j\sum_{v|\mathrm{Cond}(\phi)}r_v\deg v}\right)$$
$$=\begin{cases}\ell^{n+1} & \text{if } \sum_{v|\mathrm{Cond}(\phi)}r_v\deg v\equiv 0 \pmod{\ell} \text{ and } \phi \text{ is split at } v_1,\dots,v_n,\\ 0 & \text{otherwise.}\end{cases}$$

We now write the generating series as $\mathcal{F}_{\mathcal{V}_R,\mathcal{V}_S\subset\mathcal{V}_U}(s)=\mathcal{F}^1_{\mathcal{V}_R,\mathcal{V}_S\subset\mathcal{V}_U}(s)+\mathcal{F}^2_{\mathcal{V}_R,\mathcal{V}_S\subset\mathcal{V}_U}(s)$, where the first series contributes to the main term and the second to the error term. Taking $(k_1,\ldots,k_n)=(0,\ldots,0)$ in $\mathcal{F}_{\mathcal{V}_R,\mathcal{V}_S\subset\mathcal{V}_U}(s)$, we have

$$\mathcal{F}^1_{\mathcal{V}_R,\mathcal{V}_S\subset\mathcal{V}_U}(s)=\frac{1}{\ell^n}\left(\prod_{v\in\mathcal{V}_R}\frac{(\ell-1)\,Nv^{-(\ell-1)s}}{1+(\ell-1)\,Nv^{-(\ell-1)s}}\prod_{v\in\mathcal{V}_U}\frac{1}{1+(\ell-1)\,Nv^{-(\ell-1)s}}\mathcal{A}(s)\right.$$
$$\left.+(\ell-1)\prod_{v\in\mathcal{V}_R}\frac{b(v)\,Nv^{-(\ell-1)s}}{1+b(v)\,Nv^{-(\ell-1)s}}\prod_{v\in\mathcal{V}_U}\frac{1}{1+b(v)\,Nv^{-(\ell-1)s}}\mathcal{B}(s)\right),$$

where as usual $j=0$ gives the function $\mathcal{A}(s)$ defined by (17) and the other values of j give $\ell-1$ copies of the function $\mathcal{B}(s)$ defined by (18).

Taking $(k_1,\ldots,k_n)\neq(0,\ldots,0)$ in $\mathcal{F}_{\mathcal{V}_R,\mathcal{V}_S\subset\mathcal{V}_U}(s)$, we have

$$\mathcal{F}^2_{\mathcal{V}_R,\mathcal{V}_S\subset\mathcal{V}_U}(s)=\frac{1}{\ell^{n+1}}\sum_{j=0}^{\ell-1}\sum_{\substack{k_1,\ldots,k_n=0\\(k_1,\ldots,k_n)\neq(0,\ldots,0)}}^{\ell-1}G(s)\,M_{j,k_1,\ldots,k_n}(s;\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_U)$$

where

$$G(s)=\sum_{r=0}^{\ell-1}\rho_\ell^{-r\sum_{h=1}^n k_h\deg v_h}\prod_{v\in\mathcal{V}_R}\left(\xi_\ell^{j\deg v}+\cdots+\xi_\ell^{(\ell-1)j\deg v}\right)Nv^{-(\ell-1)s}$$

is analytic for all $s\in\mathbb{C}$, and where for each fixed vector $(k_1,\ldots,k_n)\neq(0,\ldots,0)$, and for each $0\leq j\leq\ell-1$, we have that

$$\mathcal{M}_{j,k_1,\ldots,k_n}(s;\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_U)$$
$$=\prod_{v\notin\mathcal{V}_R\cup\mathcal{V}_U}\left(1+\left(\xi_\ell^{j\deg v}\prod_{h=1}^n\chi_{v,\ell}(v_h)^{k_h}+\cdots+\xi_\ell^{(\ell-1)j\deg v}\prod_{h=1}^n\chi_{v,\ell}(v_h)^{(\ell-1)k_h}\right)Nv^{-(\ell-1)s}\right)$$

as defined in Lemma 3.2.

Let $N'(\mathbb{Z}/\ell\mathbb{Z},\mathfrak{n};\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I)$ be the number of extensions where the degree of the conductor is $\mathfrak{n}$ and with the prescribed ramification conditions at the primes of $\mathcal{V}_R$ and $\mathcal{V}_S$, and unramified at the primes of $\mathcal{V}_I$, that is, the extensions counted by the generating series $\mathcal{F}_{\mathcal{V}_R,\mathcal{V}_S\subset\mathcal{V}_U}(s)$ above. By Theorem 2.5, and Lemmas 3.2 and 3.3,

$$\begin{aligned}
&N'\left(\mathbb{Z}/\ell\mathbb{Z},\mathfrak{n};\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I\right)\\
&-\frac{1}{\ell^n}\left(\mathrm{Res}_{u=q^{-1}}\prod_{v\in\mathcal{V}_R}\frac{(\ell-1)\,u^{\deg v}}{1+(\ell-1)\,u^{\deg v}}\prod_{v\in\mathcal{V}_U}\frac{1}{1+(\ell-1)\,u^{\deg v}}\frac{A(u)}{u^{\mathfrak{n}+1}}\right.\\
&\left.+(\ell-1)\sum_{j=1}^{\ell-1}\mathrm{Res}_{u=\left(\xi_\ell^j q\right)^{-1}}\prod_{v\in\mathcal{V}_R}\frac{b(v)\,u^{\deg v}}{1+b(v)\,u^{\deg v}}\prod_{v\in\mathcal{V}_U}\frac{1}{1+b(v)\,u^{\deg v}}\frac{B(u)}{u^{\mathfrak{n}+1}}\right)\\
&+O\left(q^{(1/2+\varepsilon)\mathfrak{n}}\right).
\end{aligned}$$

As before, the residue involving the function $A(u)$ yields $q^{\mathfrak{n}}$ times a polynomial in $\mathfrak{n}$ of degree $\ell-2$, and the residues of $B(u)$ are $O(q^{\mathfrak{n}})$, so they contribute to the constant coefficient of the polynomial, and not to the main term. The main term when $\mathfrak{n}$ tends to infinity is then given by the leading term of the polynomial which is

$$\begin{aligned}
&-\frac{1}{\ell^n}\left(\mathrm{Res}_{u=q^{-1}}\prod_{v\in\mathcal{V}_R}\frac{(\ell-1)\,u^{\deg v}}{1+(\ell-1)\,u^{\deg v}}\prod_{v\in\mathcal{V}_U}\frac{1}{1+(\ell-1)\,u^{\deg v}}\frac{A(u)}{u^{\mathfrak{n}+1}}\right)\\
&=\frac{1}{\ell^n}\prod_{v\in\mathcal{V}_R}\frac{(\ell-1)\,q^{-\deg v}}{1+(\ell-1)\,q^{-\deg v}}\prod_{v\in\mathcal{V}_U}\frac{1}{1+(\ell-1)\,q^{-\deg v}}C_\ell q^{\mathfrak{n}}\mathfrak{n}^{\ell-2}.
\end{aligned}\tag{27}$$

We now proceed to add the conditions at the primes of $\mathcal{V}_I=\mathcal{V}_U\setminus\mathcal{V}_S$. Using inclusion–exclusion, it is easy to see that

$$N\left(\mathbb{Z}/\ell\mathbb{Z},\mathfrak{n};\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I\right)=\sum_{\tilde{\mathcal{V}}_I\subset\mathcal{V}_I}(-1)^{|\tilde{\mathcal{V}}_I|}N'\left(\mathbb{Z}/\ell\mathbb{Z},\mathfrak{n};\mathcal{V}_R,\mathcal{V}_S\cup\tilde{\mathcal{V}}_I,\mathcal{V}_I\setminus\tilde{\mathcal{V}}_I\right).\tag{28}$$

We can rewrite the above equation in terms of the generating series. Let $\mathcal{F}_{\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I}(s)$ be the generating series for the extensions counted by $N(\mathbb{Z}/\ell\mathbb{Z},\mathfrak{n};\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I)$. Then, it follows from (28) that

$$\begin{aligned}
\mathcal{F}_{\mathcal{V}_R,\mathcal{V}_S,\mathcal{V}_I}(s)&=\sum_{\tilde{\mathcal{V}}_I\subset\mathcal{V}_I}(-1)^{|\tilde{\mathcal{V}}_I|}\mathcal{F}_{\mathcal{V}_R,\mathcal{V}_S\cup\tilde{\mathcal{V}}_I\subset\mathcal{V}_U}(s)\\
&=\sum_{\tilde{\mathcal{V}}_I\subset\mathcal{V}_I}(-1)^{|\tilde{\mathcal{V}}_I|}\left(\mathcal{F}^1_{\mathcal{V}_R,\mathcal{V}_S\cup\tilde{\mathcal{V}}_I\subset\mathcal{V}_U}(s)+\mathcal{F}^2_{\mathcal{V}_R,\mathcal{V}_S\cup\tilde{\mathcal{V}}_I\subset\mathcal{V}_U}(s)\right),
\end{aligned}$$

and the main term will be given by the sum of the poles of the generating series $\mathcal{F}^1_{\mathcal{V}_R,\mathcal{V}_S\cup\tilde{\mathcal{V}}_I\subset\mathcal{V}_U}(s)$. Using (27), this is given by

$$C_\ell q^{\mathrm{n}} \mathfrak{n}^{\ell-2}\left(\sum_{\tilde{\mathcal{V}}_I\subset\mathcal{V}_I}\frac{(-1)^{|\tilde{\mathcal{V}}_I|}}{\ell^{|\mathcal{V}_S|\cup|\tilde{\mathcal{V}}_I|}}\prod_{v\in\mathcal{V}_R}\frac{(\ell-1)\,q^{-\deg v}}{1+(\ell-1)\,q^{-\deg v}}\prod_{v\in\mathcal{V}_U}\frac{1}{1+(\ell-1)\,q^{-\deg v}}\right)$$

$$=C_\ell q^{\mathrm{n}} \mathfrak{n}^{\ell-2}\left(\frac{1}{\ell}\right)^{|\mathcal{V}_S|}\left(\frac{\ell-1}{\ell}\right)^{|\mathcal{V}_I|}\prod_{v\in\mathcal{V}_R}\frac{(\ell-1)\,q^{-\deg v}}{1+(\ell-1)\,q^{-\deg v}}\prod_{v\in\mathcal{V}_U}\frac{1}{1+(\ell-1)\,q^{-\deg v}}$$

$$=C_\ell\left(\prod_{v\in\mathcal{V}_R\cup\mathcal{V}_S\cup\mathcal{V}_I}c_v\right)q^{\mathrm{n}}\mathfrak{n}^{\ell-2},$$

where the c_v are as in Theorem 4.2.

Dividing the last line by (19) completes the proof of the statement. ■

4.1 Quadratic extensions

We now look specifically at the case $\ell=2$ as we obtain the number of quadratic extensions of K with conductor $\mathfrak{n}$ with no error term, and the ramified case with a better error term without using the Tauberian theorem. The generating function $\mathcal{F}$ is

$$\mathcal{F}(s)=2+\sum_{\mathrm{Gal}(L/K)\cong\mathbb{Z}/2\mathbb{Z}}\mathfrak{D}(L/K)^{-s}=\prod_v\left(1+Nv^{-s}\right)+\prod_v\left(1+(-1)^{\deg v}Nv^{-s}\right).$$

In this case,

$$\mathcal{A}(s)=\prod_v\left(1+Nv^{-s}\right)=\prod_v\frac{\left(1-Nv^{-2s}\right)}{\left(1-Nv^{-s}\right)}$$

$$=\frac{\zeta_K(s)}{\zeta_K(2s)}=\frac{\left(1-q^{1-2s}\right)\left(1+q^{-s}\right)}{1-q^{1-s}}.$$

After making the change of variables $u=q^{-s}$, we obtain

$$A(u):=\frac{\left(1-qu^2\right)(1+u)}{1-qu}.$$

Analogously,

$$\mathcal{B}(s)=\prod_v\left(1+(-1)^{\deg v}Nv^{-s}\right)=\frac{\left(1-q^{1-2s}\right)\left(1-q^{-s}\right)}{1+q^{1-s}}$$

which equals $A(-u)$ after the change of variables $u=q^{-s}$. Then,

$$F(u) = A(u) + A(-u)$$
$$= \left(1 - qu^2\right)\left(\frac{1+u}{1-qu} + \frac{1-u}{1+qu}\right).$$

By identifying the coefficients in the power series expansion in u of the above rational function for $\mathfrak{n} > 0$ with the coefficients of

$$2 + \sum_{\mathfrak{n}=1}^{\infty} N(\mathbb{Z}/2\mathbb{Z}, \mathfrak{n})\, u^{\mathfrak{n}},$$

we finally obtain that

$$N(\mathbb{Z}/2\mathbb{Z}, \mathfrak{n}) = \begin{cases} \left(1 + (-1)^{\mathfrak{n}}\right)\left(q^{\mathfrak{n}} - q^{\mathfrak{n}-2}\right) & \mathfrak{n} \geq 3, \\ 2q^2 & \mathfrak{n} = 2, \\ 0 & \mathfrak{n} = 1 \end{cases}$$

$$= \begin{cases} 2\left(q^{\mathfrak{n}} - q^{\mathfrak{n}-2}\right) & \mathfrak{n} > 2, \mathfrak{n} \text{ even}, \\ 2q^2 & \mathfrak{n} = 2, \\ 0 & \mathfrak{n} \text{ odd}. \end{cases} \tag{29}$$

Remark 4.3. Recall that the number of square-free monic polynomials of degree $d > 1$ is $q^d - q^{d-1}$. In this case, we are counting twice the number of square-free monic polynomials. The counting happens twice since every monic square-free polynomial f gives two quadratic extensions corresponding to $K(\sqrt{f})$ and $K(\sqrt{\beta f})$ where β is a non-square in $\mathbb{F}_q^{\times}$. □

We now proceed to the ramified case.

$$F_R(u) = \frac{u^{\deg v_0}}{1 + u^{\deg v_0}} A(u) + \frac{(-u)^{\deg v_0}}{1 + (-u)^{\deg v_0}} A(-u)$$
$$= \left(1 - qu^2\right)\left(\frac{u^{\deg v_0}(1+u)}{\left(1 + u^{\deg v_0}\right)(1 - qu)} + \frac{(-u)^{\deg v_0}(1-u)}{\left(1 + (-u)^{\deg v_0}\right)(1 + qu)}\right).$$

We have

$$A(u) = \left(1 - qu^2\right)\frac{1+u}{1-qu}$$
$$= 1 + (q+1)\,u + q^2u^2 + \sum_{n=3}^{\infty}\left(q^n - q^{n-2}\right)u^n.$$

Thus,

$$\frac{u^{\deg v_0}}{1+u^{\deg v_0}}A(u) = \left(\sum_{k=1}^{\infty}(-1)^{k-1}u^{k\deg v_0}\right)\left(1+(q+1)u+q^2u^2+\sum_{n=3}^{\infty}\left(q^n-q^{n-2}\right)u^n\right)$$

$$= \sum_{k=1}^{\infty}(-1)^{k-1}u^{k\deg v_0} + (q+1)\sum_{k=1}^{\infty}(-1)^{k-1}u^{k\deg v_0+1} + q^2\sum_{k=1}^{\infty}(-1)^{k-1}u^{k\deg v_0+2}$$

$$+ \sum_{k=1}^{\infty}\sum_{n=3}^{\infty}(-1)^{k-1}\left(q^n-q^{n-2}\right)u^{k\deg v_0+n}$$

$$= \sum_{k=1}^{\infty}(-1)^{k-1}u^{k\deg v_0} + (q+1)\sum_{k=1}^{\infty}(-1)^{k-1}u^{k\deg v_0+1} + q^2\sum_{k=1}^{\infty}(-1)^{k-1}u^{k\deg v_0+2}$$

$$+ \sum_{m=3+\deg v_0}^{\infty}\sum_{k=1}^{\left\lfloor\frac{m-3}{\deg v_0}\right\rfloor}(-1)^{k-1}\left(q^{m-k\deg v_0}-q^{m-k\deg v_0-2}\right)u^m$$

$$= \sum_{m=3+\deg v_0}^{\infty}\frac{1-q^{-2}}{1+q^{-\deg v_0}}q^{m-\deg v_0}u^m + O_q(1)\sum_{m=\deg v_0}^{\infty}u^m.$$

By identifying the coefficients of $F_R(u)$ with the power series

$$\sum_{\mathfrak{n}=1}^{\infty}N\left(\mathbb{Z}/2\mathbb{Z},\mathfrak{n},v_0,\text{ramified}\right)u^{\mathfrak{n}},$$

we obtain,

$$N\left(\mathbb{Z}/2\mathbb{Z},\mathfrak{n},v_0,\text{ramified}\right) = \frac{\left(1-q^{-2}\right)}{1+q^{-\deg v_0}}q^{\mathfrak{n}-\deg v_0} + O_q(1).$$

5 Distribution of the Number of Points on Covers

We explain in this section how the results of this paper apply to the distribution for the number of $\mathbb{F}_q$-points on covers C on the moduli space $\mathcal{H}_{g,\ell}$. We prove Theorem 1.3 and make a comparison with the results of [1].

Consider an ℓ-cyclic cover $C \to \mathbb{P}^1$ defined over $\mathbb{F}_q$ and let L be the function field of C. As mentioned in Section 2.2, the genus g_C of the cover C is related to the discriminant $\mathrm{Disc}(L/K)$ via

$$2g_C = (\ell-1)\left[-2+\deg\mathrm{Cond}(L/K)\right],$$

which implies

$$\mathfrak{n} = \frac{2g_C}{\ell - 1} + 2, \tag{30}$$

where $\mathfrak{n}$ is the degree of $\mathrm{Cond}(L/K)$.

Recall that the zeta function of a curve C is given by

$$Z_C(u) = \exp\left(\sum_{n=1}^{\infty} \#C\left(\mathbb{F}_{q^n}\right) \frac{u^n}{n}\right). \tag{31}$$

Moreover,

$$Z_L(u) = Z_C(u)$$

with the usual identification $u = q^{-s}$.

We recall that $\mathcal{V}_K$ is the set of places of K. Suppose that L/K is a Galois extension. We can write

$$Z_L(u) = \prod_{v \in \mathcal{V}_K} \left(1 - u^{f(v) \deg v}\right)^{-r(v)}, \tag{32}$$

where, for each place v, we denote by $e(v)$, $f(v)$, and $r(v)$ the ramification degree, the inertia degree and the number of places of L above v, respectively.

Taking the logarithm on both sides of the equality $Z_C(u) = Z_L(u)$ using (31) and (32), we obtain

$$\sum_{n=0}^{\infty} \#C\left(\mathbb{F}_{q^n}\right) \frac{u^n}{n} = \sum_{v \in \mathcal{V}_K} \sum_{m=1}^{\infty} r(v) \frac{u^{mf(v) \deg v}}{m}.$$

Equating the coefficients of u^n on both sides gives

$$\#C\left(\mathbb{F}_{q^n}\right) = \sum_{\substack{v \in \mathcal{V}_K \\ f(v) \deg v | n}} r(v) f(v) \deg v. \tag{33}$$

The above discussion implies that the fiber above an $\mathbb{F}_q$-point of $\mathbb{P}^1$ that corresponds to the place v of degree 1 of K contains

$$\begin{cases} \ell \text{ distinct } \mathbb{F}_q\text{-points} & \text{if } v \text{ splits completely,} \\ 1\ \mathbb{F}_q\text{-point} & \text{if } v \text{ ramifies,} \\ 0\ \mathbb{F}_q\text{-points} & \text{if } v \text{ is inert.} \end{cases}$$

More generally, a place v of K corresponds to a Galois orbit of rational points of the same degree of $\mathbb{P}^1$. The fiber above each point in the orbit contains

$$\begin{cases} \ell \text{ distinct points of degree } \deg v & \text{if } v \text{ splits completely,} \\ 1 \text{ point of degree } \deg v & \text{if } v \text{ ramifies,} \\ 1 \text{ point of degree } \ell \deg v & \text{if } v \text{ is inert.} \end{cases}$$

To get the distribution of $\#C(\mathbb{F}_q)$ over $\mathcal{H}_{g,\ell}$, we use the relative densities

$$\frac{N\left(\mathbb{Z}/\ell\mathbb{Z}, \frac{2g}{\ell-1}+2; \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_I\right)}{N\left(\mathbb{Z}/\ell\mathbb{Z}, \frac{2g}{\ell-1}+2\right)}$$

where we take the sets $\mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_I$ to be mutually disjoint, and such that $\mathcal{V}_R \cup \mathcal{V}_S \cup \mathcal{V}_I$ is a subset of the set of places of degree 1 in $\mathcal{V}_K$.

Then, using (33) with $n=1$ and Theorem 1.1, we get

$$\begin{aligned} &\frac{\left|\left\{C \in \mathcal{H}_{g,\ell}\left(\mathbb{F}_q\right) : \#C\left(\mathbb{F}_q\right) = m\right\}\right|}{\left|\mathcal{H}_{g,\ell}\left(\mathbb{F}_q\right)\right|} \\ &= \sum_{\ell|\mathcal{V}_S|+|\mathcal{V}_R|=m} \frac{N\left(\mathbb{Z}/\ell\mathbb{Z}, \frac{2g}{\ell-1}+2; \mathcal{V}_R, \mathcal{V}_S, \mathcal{V}_I\right)}{N\left(\mathbb{Z}/\ell\mathbb{Z}, \frac{2g}{\ell-1}+2\right)} \\ &\sim \sum_{\ell|\mathcal{V}_S|+|\mathcal{V}_R|=m} \left(\frac{\ell-1}{q+\ell-1}\right)^{|\mathcal{V}_R|} \left(\frac{q}{\ell(q+\ell-1)}\right)^{|\mathcal{V}_S|} \left(\frac{(\ell-1)q}{\ell(q+\ell-1)}\right)^{q+1-|\mathcal{V}_R|} \\ &= \text{Prob}\left(\sum_{i=1}^{q+1} X_i = m\right), \end{aligned}$$

where the X_i are the random variables of Theorem 1.3.

5.1 Affine models

We compare the results of this paper with the results of [1] concerning the irreducible components $\mathcal{H}^{(d_1,\dots,d_\ell)}$ of $\mathcal{H}_{g,\ell}$. To describe these components, we write the covers concretely in terms of affine models. Each such cover has an affine model of the form

$$C : Y^\ell = f(X) = \beta f_1 f_2^2 \cdots f_{\ell-1}^{\ell-1} \tag{34}$$

where the $f_i \in \mathbb{F}_q[X]$ are monic, square-free, pairwise coprime, of degrees $d_1, \ldots, d_{\ell-1}$. The degree of the conductor depends on the degrees $d_1, \ldots, d_{\ell-1}$ and whether there is ramification at the place at infinity. The ramification at the place at infinity is determined by whether the total degree of the polynomial is divisible by ℓ. When $d_1 + \cdots + (\ell-1)d_{\ell-1}$ is a multiple of ℓ, then the cover does not ramify at infinity, otherwise there is ramification at infinity. In the first case, the degree of the conductor is $d_1 + \cdots + d_{\ell-1}$ and in the second case it is $d_1 + \cdots + d_{\ell-1} + 1$.

By the Riemann–Hurwitz formula the genus of this cover is given by

$$g_C = (\ell-1)\,(d_1 + \cdots + d_{\ell-1} - 2)\,/2$$

in the first case, and by

$$g_C = (\ell-1)\,(d_1 + \cdots + d_{\ell-1} - 1)\,/2,$$

in the second. Both equations are compatible with the relation (30) between the genus g_C and the degree of the conductor $\mathfrak{n}$.

For a given conductor, each $\beta \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^\ell$ yields a different cover given by formula (34). That is, there is one such extension for each element of $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^\ell$. Using the notation from [1], we define

$$\mathcal{F}_{(d_1,\ldots,d_{\ell-1})} = \{(f_1, \ldots, f_{\ell-1}) : f_i \text{ monic, square-free, pairwise coprime,}$$
$$\deg f_i = d_i,\ i = 1, \ldots, \ell-1\}.$$

We consider, for $d_1 + \cdots + (\ell-1)d_{\ell-1} \equiv 0 \pmod{\ell}$,

$$\mathcal{F}_{[d_1,\ldots,d_{\ell-1}]} = \mathcal{F}_{(d_1,\ldots,d_{\ell-1})} \cup \bigcup_{j=1}^{\ell-1} \mathcal{F}_{(d_1,\ldots,d_j-1,\ldots,d_{\ell-1})}. \tag{35}$$

The elements in the first term correspond to affine models from Equation (34) in the case in which there is no ramification at infinity. The elements in the other terms correspond to affine models where there is ramification at infinity (of index j in the term $\mathcal{F}_{(d_1,\ldots,d_j-1,\ldots,d_{\ell-1})}$).

Now suppose that we want to count the number of covers of genus g. For a conductor $f_1 f_2^2 \cdots f_{\ell-1}^{\ell-1}$, there are ℓ different covers according to the class of the leading coefficient as an element of $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^\ell$. In addition, we need to consider that isomorphic covers are obtained by taking automorphisms of $\mathbb{P}^1(\mathbb{F}_q)$, namely the $q(q^2-1)$ elements of $\mathrm{PGL}_2(\mathbb{F}_q)$ (see [1, Section 7] for details).

We denote by $\mathcal{H}^{(d_1,\dots,d_\ell)}$ the corresponding component of $\mathcal{H}_g$, indexed by tuples $(d_1,\dots,d_\ell)$ with the properties that $(\ell-1)(d_1+\cdots+d_{\ell-1}-2)=2g$ and $d_1+2d_2+\cdots+(\ell-1)d_{\ell-1}\equiv 0 \pmod{\ell}$. The discussion in the previous paragraphs implies

$$|\mathcal{H}^{(d_1,\dots,d_{\ell-1})}|'=\frac{\ell}{q\left(q^2-1\right)}|\mathcal{F}_{[d_1,\dots,d_{\ell-1}]}|$$

where, as usual, the $'$ notation means that the covers C on the moduli space are counted with the usual weights $1/|\mathrm{Aut}(C)|$.

Thus, we can write

$$|\mathcal{H}_{g,\ell}\left(\mathbb{F}_q\right)|'=\frac{\ell}{q\left(q^2-1\right)}\sum_{\substack{d_1+\cdots+d_{\ell-1}=2(g+2)/(\ell-1)\\ d_1+\cdots+(\ell-1)d_{\ell-1}\equiv 0 \pmod{\ell}}}|\mathcal{F}_{[d_1,\dots,d_{\ell-1}]}|. \tag{36}$$

Formula (3.1) of [1] says that

$$|\mathcal{F}_{(d_1,\dots,d_{\ell-1})}|=\frac{L_{\ell-2}q^{d_1+\cdots+d_{\ell-1}}}{\zeta_q\left(2\right)^{\ell-1}}\left(1+O\left(\sum_{h=2}^{\ell-1}q^{\varepsilon(d_h+\cdots+d_{\ell-1})-d_h}+q^{-d_1/2}\right)\right), \tag{37}$$

where

$$L_{\ell-2}=\prod_{j=1}^{\ell-2}\prod_{v\neq v_\infty}\left(1-\frac{jq^{-2\deg v}}{\left(1+q^{-\deg v}\right)\left(1+jq^{-\deg v}\right)}\right).$$

The formula above may be rewritten as

$$|\mathcal{F}_{(d_1,\dots,d_{\ell-1})}|=\frac{(\ell-2)!C_\ell q^{d_1+\cdots+d_{\ell-1}}}{\left(1+(\ell-1)\,q^{-1}\right)}\left(1+O\left(\sum_{h=2}^{\ell-1}q^{\varepsilon(d_h+\cdots+d_{\ell-1})-d_h}+q^{-d_1/2}\right)\right).$$

By combining Equations (35) and (36) with the line above, we obtain

$$\begin{aligned} q\left(q^2-1\right)|\mathcal{H}_{g,\ell}\left(\mathbb{F}_q\right)|' &= (\ell-2)!C_\ell q^{\mathfrak{n}}\sum_{\substack{d_1+\cdots+d_{\ell-1}=\mathfrak{n}\\ d_1+\cdots+(\ell-1)d_{\ell-1}\equiv 0 \pmod{\ell}}}\ell+ET\\ &= C_\ell\mathfrak{n}^{\ell-2}q^{\mathfrak{n}}+ET, \end{aligned}$$

where ET denotes an error term and, in the last line, we used that the number of solutions of $d_1+\cdots+d_{\ell-1}=\mathfrak{n}$ is given by $\sim\frac{\mathfrak{n}^{\ell-2}}{(\ell-2)!}$.

Thus the result of Theorem 4.1 is compatible with the result of Theorem 3.1 from [1], in the sense that summing the main terms of (37) gives the same number of elements of $\mathcal{H}_{g,\ell}(\mathbb{F}_q)$ computed in this paper, even if the error terms coming from (37) are only valid when $\min\{d_1,\dots,d_{\ell-1}\}\to\infty$.

Acknowledgements

This work was initiated at a workshop at the American Institute for Mathematics (AIM) and a substantial part of this work was completed during a SQuaREs program at AIM. The authors would like to thank AIM for these opportunities. The authors would also like to thank Colin Weir and Simon Rubinstein–Salzedo for useful discussions. Finally, the authors would like to thank the anonymous referees for their many helpful comments, which greatly improved the exposition of this paper.

Funding

This work was supported by the Simons Foundation [#244988 to A.B.], the National Science Foundation [DMS-1201446 to B.F., DMS-1147782 and DMS-1301690 to M.M.W.], PSC-CUNY [to B.F.], the Natural Sciences and Engineering Research Council of Canada [Discovery Grant 155635-2013 to C.D., 355412-2013 to M.L.], the Fonds de recherche du Québec - Nature et technologies [144987 to M.L., 166534 to C.D. and M.L.], the Scientific and Research Council of Turkey [TUBITAK-114C126 to E.O.], and the American Institute for Mathematics [Five Year Fellowship to M.M.W.].

References

[1] Bucur, A., C. David, B. Feigon, and M. Lalín. "Statistics for traces of cyclic trigonal curves over finite fields." *International Mathematics Research Notices* 2010, no. 5 (2010): 932–67.

[2] Cheong, G., M. M. Wood, and A. Zaman. "The distribution of points on superelliptic curves over finite fields." *Proceedings of the American Mathematical Society*: preprint arXiv:1210.0456.

[3] Chuang, C.-Y. and Y.-L. Kuan. "On the density of abelian ℓ-extensions." (2015): preprint arXiv:1509.01345.

[4] Cohn, H. "The density of abelian cubic fields." *Proceedings of American Mathematical Society* 5, no. 3 (1954): 476–7.

[5] Cohen, H., F. Diaz y Diaz, and M. Olivier. "On the density of discriminants of cyclic extensions of prime degree." *Journal für die Reine und Angewandte Mathematik* 2002, no. 550 (2002): 169–209.

[6] Hayes, D. R. "Explicit class field theory for rational function fields." *Transactions of the American Mathematical Society* 189 (1974): 77–91.

[7] Kurlberg, P. and Z. Rudnick. "The fluctuations in the number of points on a hyperelliptic curve over a finite field." *Journal of Number Theory* 129, no. 3 (2009): 580–7.

[8] Moreno, C. *Algebraic Curves Over Finite Fields*. Cambridge Tracts in Mathematics 97. Cambridge: Cambridge University Press, 1991.

[9] Rosen, M. *Number Theory in Function Fields*. Graduate Texts in Mathematics 210. New York: Springer, 2002.

[10] Rudnick, Z. "Traces of high powers of the Frobenius class in the hyperelliptic ensemble." *Acta Arithmetica* 143, no. 1 (2010): 81–99.

[11] Salvador, G. D. V. *Topics in the Theory of Algebraic Function Fields*. Mathematics: Theory & Applications. Boston, MA: Birkhäuser Boston Inc., 2006.

[12] Thorne, F. and M. Xiong. “Distribution of zeta zeroes for cyclic trigonal curves over a finite field.” in preparation.

[13] Wood, M. M. “On the probabilities of local behaviors in abelian field extensions.” *Compositio Mathematica* 146, no. 1 (2010): 102–28.

[14] Wood, M. M. “The distribution of the number of points on trigonal curves over $\mathbb{F}_q$.” *International Mathematics Research Notices*, no. 23 (2012): 5444–56.

[15] Wright, D. J. “Distribution of discriminants of abelian extensions.” *Proceedings of the London Mathematical Society* (3) 58, no. 1 (1989): 17–50.

[16] Xiong, M. “The fluctuations in the number of points on a family of curves over a finite field.” *Journal de Théorie des Nombres de Bordeaux* 22, no. 3 (2010): 755–69.