ON THE DISTRIBUTION OF CYCLIC NUMBER FIELDS OF PRIME DEGREE

SEOK HYEONG LEE AND GYUJIN OH

ABSTRACT. Let $N_{C_p}(X)$ denote the number of C_p Galois extensions of $\mathbb{Q}$ with absolute discriminant $\leq X$. A well-known theorem of Wright [1] implies that when p is prime, we have $N_{C_p}(X) = c(p)X^{\frac{1}{p-1}} + O(X^{\frac{1}{p}})$ for some positive real $c(p)$. In this paper, we improve this result by reducing the secondary error term to $O(X^{\frac{1}{2(p-1)}})$. Moreover, under GRH, we obtain the following stronger result

$$N_{C_p}(X) = c(p)X^{\frac{1}{p-1}} + X^{\frac{1}{3(p-1)}}R_p(\log X) + O(X^{\frac{1}{4(p-1)}+\varepsilon}).$$

Here $R_p(x) \in \mathbb{R}[x]$ is a polynomial of degree $\lfloor p(p-2)/3 \rfloor - 1$. This confirms a speculation of Cohen, Diaz y Diaz, and Olivier [3] in the case of C_3 extensions.

1. Introduction

Here we investigate the distribution of cyclic C_p Galois extensions of $\mathbb{Q}$ by studying the asymptotic behavior of $N_{C_p}(X)$, the number of C_p Galois extensions of $\mathbb{Q}$ with absolute discriminant $\leq X$. In [1], Wright proves a general theorem, which in the case of C_p says that

$$N_{C_p}(X) = c(p)X^{\frac{1}{p-1}} + O(X^{\frac{1}{p}}),$$

where $c(p)$ is a given non-zero constant. We refine Wright's work, and assuming the Generalized Riemann Hypothesis, we obtain the following theorem.

Theorem 1.1. *Let p be an odd prime. Under the assumption of the Generalized Riemann Hypothesis, we have*

$$N_{C_p}(X) = c(p)X^{\frac{1}{p-1}} + X^{\frac{1}{3(p-1)}}R_p(\log X) + O_\varepsilon(X^{\frac{1}{4(p-1)}+\varepsilon})$$

where $R_p(x) \in \mathbb{R}[x]$ has degree $\lfloor p(p-2)/3 \rfloor - 1$.

Remark. We assume the Generalized Riemann Hypothesis for the Riemann zeta-function and Dirichlet L-functions $L(s, \chi)$ for characters of conductor p.

Unconditionally, we obtain the following weaker result.

The authors are grateful for support from Stanford University and NSF in funding us the Emory REU this year. The authors would also like to thank our advisors Andrew Yang and Ken Ono for their guidance, useful suggestions, comments on the paper, and hosting the REU.

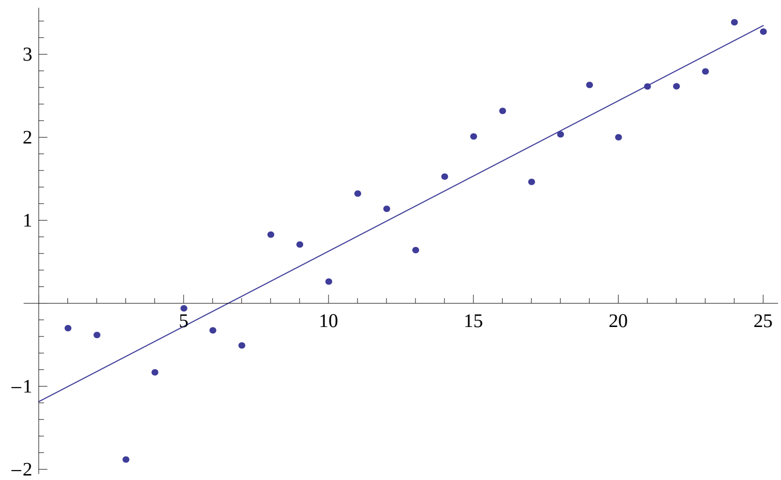
Theorem 1.2. *For any prime p, we have*

$$N_{C_p}(X) = c(p)X^{\frac{1}{p-1}} + O(X^{\frac{1}{2(p-1)}}).$$

Remark. In the case of $p = 3$, Cohen, Diaz y Diaz, and Olivier [3] speculated that

$$N_{C_3}(X) = c(3)X^{1/2} + \tilde{O}(X^{1/6}).$$

They formulated this speculation based on extensive numerical calculations. We note that Theorem 1.1 confirms this speculation. Specifically, based on data from [3] and [4], the best fit linear regression model for the graph $\log_{10} X$ versus $\log_{10}(N_{C_3}(X) - c(3)X^{1/2})$ is $\log_{10}(N_{C_3}(X) - c(3)X^{1/2}) = -0.98962297 + 0.16233864 \log_{10} X$. Note that the slope of the model is very close to $\frac{1}{6}$. The actual data and the best fit model are shown in the following graph.



In the graph above, the parameters for the horizontal and vertical axes are $\log_{10} X$ and $\log_{10}(N_{C_3}(X) - c(3)X^{1/2})$, respectively, and the scatterplot is based on the data for $X = 10^i, i = 1, 2, \cdots, 25$.

In Section 2 we recall Wright's work, and in Section 3 we prove Theorems 1.1 and 1.2.

2. Preliminaries

To obtain asymptotics for $N_{C_p}(X)$, it is standard to study the poles of an associated Dirichlet series on the positive real line. For a given abelian Galois group G, this series is defined by

$$D_G(s) = \sum_{\mathrm{Gal}(K/\mathbb{Q}) \cong G} |\mathrm{disc}(K)|^{-s}. \tag{1}$$

In [1], Wright uses class field theory to understand this Dirichlet series in terms of the product of conductors of characters on the idelé class group of the base field. Specifically, let $C(n)$ be the group of characters χ on the idelé class group of $\mathbb{Q}$ satisfying $\chi^n = 1$, and let $G \cong (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_m\mathbb{Z})$ be the invariant factor decomposition of G. (i.e. $n_i \mid n_{i+1}$ for $1 \leq i < m$). Define $C(G) = \prod_j C(n_j)$. For any element $\chi = (\chi_1, \cdots, \chi_m)$ of $C(G)$, define

$$\mathcal{F}_G(\chi) = \prod_{0 \leq i_1 < n_1} \cdots \prod_{0 \leq i_m < n_m} \Phi(\chi_1^{i_1} \cdots \chi_m^{i_m}) \tag{2}$$

where $\Phi(-)$ is the absolute norm of the conductor of the character.

We define the following series.

$$F_G(s) = \sum_{\chi \in C(G)} \mathcal{F}_G(\chi)^{-s}. \tag{3}$$

Wright [1] reformulates $D_G(s)$ as follows.

Proposition 2.1 ([1], eqn I.2)**.** *The Dirichlet series $D_G(s)$ satisfies*

$$D_G(s) = \frac{1}{\phi(G)} \sum_{H \leq G} \mu(G/H) F_H\left(\frac{|G|}{|H|} s\right).$$

In the above expression, $\phi(G)$ is the number of automorphisms of G and $\mu(H)$ is the Möbius function for the lattice of abelian groups.

By using this fact, we can compute the Dirichlet series explicitly for a given abelian Galois group G. In particular, when $G = C_p$, we have the following.

Proposition 2.2. *For an odd prime p, we have*

$$D_{C_p}(s) = \frac{1}{p-1}\left(\left(1 + \frac{p-1}{p^{2(p-1)s}}\right) \prod_{q \equiv 1 (\mathrm{mod}\, p)} \left(1 + \frac{p-1}{q^{(p-1)s}}\right) - 1\right).$$

Proof. It is well known that the idelé class group of $\mathbb{Q}$ is given by the following.

$$\mathbb{R}_{>0} \times \prod_{q \text{ finite prime}} \mathbb{Z}_q.$$

Since the idelé class group of $\mathbb{Q}$ is a cartesian product of the completion at each prime, $F_{C_p}(s)$ is in fact an Euler product. Therefore, $F_{C_p}(s)$ can be determined by investigating the conductor of characters on $\mathbb{Z}_q$ whose p-th power is a trivial character.

First, consider the case $p \nmid (q-1), p \neq q$. Since the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ is the cyclic group of order $q-1$, for any $y \in \mathbb{Z}$ we can find $x \in (\mathbb{Z}/q\mathbb{Z})^\times$ such that $x^p \equiv y (\mathrm{mod}\, q)$. Thus, by Hensel's lemma, every element of $\mathbb{Z}_q$ is a p-th power of some element in $\mathbb{Z}_q$. For any character χ in $C(p)$, the conductor of χ on $\mathbb{Z}_q$ is 1.

On the other hand, if $p \mid (q-1)$, then there are a restricted number of elements in $(\mathbb{Z}/q\mathbb{Z})^\times$ which are p-th powers. Also, by Hensel's lemma, if an element in $\mathbb{Z}_q$ is a p-th power in $(\mathbb{Z}/q\mathbb{Z})^\times$, then it is also a p-th power in $\mathbb{Z}_q$. Therefore, $\mathbb{Z}_q/\mathbb{Z}_q^p \cong C_p$, and from this we can conclude that there are p characters in $C(p)$ when restricted to $\mathbb{Z}_q$, and that every nontrivial character has a conductor q.

Finally, if $p = q$, consider $f_y(x) = x^p - y$ for any $y \in \mathbb{Z}_p$. By Hensel's lemma, if we find a p-th root of $y (\bmod p^3)$, we can find a p-th root of y in $\mathbb{Z}_p$. In particular, if $x^p \equiv y (\bmod p^3)$ and $y \equiv 1 (\bmod p)$, then $x \equiv kp + 1 (\bmod p^2)$ for some $k \in \mathbb{Z}$. Note that $(kp+1)^p \equiv kp^2 + 1 (\bmod p^3)$. Therefore, every nontrivial character of $C(p)$ on $\mathbb{Z}_p$ should have conductor p^2. Therefore, we have

$$F_{C_p}(s) = \left(1 + \frac{p-1}{p^{2(p-1)s}}\right) \prod_{q \equiv 1 (\bmod p)} \left(1 + \frac{p-1}{q^{(p-1)s}}\right).$$

Note that $\mu(C_p) = -1$ and $\mu(1) = 1$. Therefore, using Proposition 2.1, the conclusion follows. $\square$

3. Proof of Theorems 1.1 and 1.2

One can, in principle, completely read off the full asymptotic expansion of $N_{C_p}(X)$ if complete information is known about the poles of $D_{C_p}(s)$. Suppose $D_{C_p}(s)$ is given so that it is analytic on the region $\mathrm{Re}(s) > 1$. If it also meromorphically extends to the region $\mathrm{Re}(s) > \rho \geq 0$ with poles $\alpha_1, \alpha_2, \cdots, \alpha_k$ with order $m_1, m_2, \cdots, m_k$ respectively, we have

$$N_{C_p}(X) = \sum_i X^{\alpha_i} P_i(\log X) + O(X^{\rho+\varepsilon}) \tag{4}$$

for real polynomials P_i of degree $m_i - 1$. This can be obtained by Perron's formula

$$N_{C_p}(X) = \int_{c-i\infty}^{c+i\infty} D_{C_p}(s) \frac{X^s}{s} ds,$$

and the Tauberian theorem of Ikehara [5]. Poles contribute to the main asymptotics as

$$\int_{c-i\infty}^{c+i\infty} \frac{1}{(s-\alpha)^k} \frac{X^s}{s} ds = X^\alpha P_{k-1,\alpha}(\log X) + O(1).$$

In the equation above, $P_{k-1,\alpha}(x) \in \mathbb{R}[x]$ has degree $k-1$ and the coefficients depends on α. We shall make use of the straightforward generalization of the strategy to obtain information about secondary error terms. Note that Ikehara's theorem establishes that the remaining integral is $O(X^{\rho+\epsilon})$.

To this end, we first verify several lemmas to prove that $D_{C_p}(s)$ can be meromorphically extended over its original region of convergence. We then argue that the meromorphic continuation implies Theorems 1.1 and 1.2.

3.1. **Meromorphic Continuation of $D_{C_p}(s)$.** It is clear that the poles of $D_{C_p}(s)$ and those of $\prod_{q\equiv 1 (\mathrm{mod}\, p)} \left(1+\frac{p-1}{q^{(p-1)s}}\right)$ are the same. Furthermore, the region of convergence for this product is the region $\mathrm{Re}((p-1)s) > 1$.

We first claim that the product can be meromorphically extended to $\mathrm{Re}((p-1)s) > \frac{1}{4}$.

Proposition 3.1. *The product*

$$\prod_{q\equiv 1 (\mathrm{mod}\, p)} \left(1+\frac{p-1}{q^{(p-1)s}}\right)$$

can be meromorphically continued to the region $\mathrm{Re}((p-1)s) > \frac{1}{4}$. *Also, it has a factorization of form*

$$P_1(s)P_2(s)P_3(s) \cdot \left(\text{analytic and nonvanishing part on}\, \mathrm{Re}((p-1)s) > \frac{1}{4}\right),$$

where

$$\begin{aligned} P_1(s) &= \zeta\left((p-1)s\right) \prod_{\chi\neq\chi_0} L\left((p-1)s,\chi\right), \\ P_2(s) &= \zeta\left(2(p-1)s\right)^{-(p+1)/2} \prod_{\chi\neq\chi_0} L\left(2(p-1)s,\chi\right)^{-(p+1)/2} \\ &\quad \cdot \prod_{\chi(-1)\neq 1} L\left(2(p-1)s,\chi\right), \\ P_3(s) &= \zeta\left(3(p-1)s\right)^{\lfloor p(p-2)/3\rfloor} \prod_{\chi\neq\chi_0} L\left(3(p-1)s,\chi\right)^{\lfloor p(p-2)/3\rfloor} \\ &\quad \cdot \prod_{\chi(\alpha)\neq 1} L\left(3(p-1)s,\chi\right). \end{aligned}$$

In the expression above, χ *(*χ_0*, resp.) denotes any Dirichlet character (the trivial character, resp.)* $\mathrm{mod}\, p$. *The product* $\prod_{\chi(\alpha)\neq 1} L\left(3(p-1)s,\chi\right)$ *in* $P_3(s)$ *only appears when* $p\equiv 1 (\mathrm{mod}\, 3)$ *and* α *is an order 3 element in* $(\mathbb{Z}/p\mathbb{Z})^\times$.

The general strategy for the proof follows from earlier work of Cohn [2]. We begin by establishing several propositions and lemmas which will be used to prove Proposition 3.1.

Let q_i be any prime congruent to $i \pmod p$, and let $\prod_{q_i}$ be the product over all such primes. For $1 \le i \le p-1$, let $Q_i(s)$ be defined as follows.

$$Q_i(s) := \prod_{q_i} \left(1 - \frac{1}{{q_i}^s}\right)^{-1} = \prod_{q \equiv i (\operatorname{mod} p)} \left(1 - \frac{1}{q^s}\right)^{-1}.$$

The following proposition suggests a factorization of the Euler product in $D_{C_p}(s)$, which enables a meromorphic continuation over its region of convergence.

Proposition 3.2. *For an odd prime p, the product*

$$\prod_{q \equiv 1 (\operatorname{mod} p)} \left(1 + \frac{p-1}{q^{(p-1)s}}\right)$$

can be factored as

$$Q_1((p-1)s)^{p-1} Q_1(2(p-1)s)^{-p(p-1)/2} Q_1(3(p-1)s)^{p(p-1)(p-2)/3}$$
$$\cdot \left(\text{analytic and nonvanishing on} \operatorname{Re}(s) > \frac{1}{4(p-1)}\right).$$

Proposition 3.2 is a consequence of the following lemma, after plugging $q^{-(p-1)s}$ into x.

Lemma 3.1. *For sufficiently small x, we have*

$$(1 + (p-1)x)(1-x)^{p-1}(1-x^2)^{-p(p-1)/2}(1-x^3)^{p(p-1)(p-2)/3} = 1 + O(x^4).$$

Proof. The lemma immediately follows from the polynomial expansion

$$(1 + (p-1)x)(1-x)^{p-1}(1+x^2)^{p(p-1)/2}(1-x^3)^{p(p-1)(p-2)/3} = 1 + O(x^4)$$

and the expression

$$(1-x^2)^{-p(p-1)/2}(1+x^2)^{-p(p-1)/2} = 1 + O(x^4).$$

$\square$

Before proving the next lemma, we recall a general fact for Dirichlet characters with a prime conductor. Dirichlet characters with conductor p correspond to homomorphisms $(\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}$, and we know $(\mathbb{Z}/p\mathbb{Z})^\times \simeq C_{p-1}$. Therefore, there is a bijective correspondence between the Dirichlet characters with conductor p and primitive $(p-1)$-th roots of unity. Given a primitive root $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ and a primitive $(p-1)$-th root of unity ω_{p-1}, the Dirichlet characters mod p can be labeled $\chi_0, \chi_1, \cdots, \chi_{p-2}$, where $\chi_i(g) = \omega_{p-1}^i$.

Lemma 3.2. *Let* $\operatorname{ord}_p(i)$ *be the multiplicative order of* i *in* $(\mathbb{Z}/p\mathbb{Z})^\times$. *The product* $Q_1(s)$ *has the following factorization.*

$$\begin{aligned} Q_1(s)^{p-1} &= \prod_{\chi} L(s,\chi) \prod_{i\neq 1} Q_i(\operatorname{ord}_p(i)s)^{-(p-1)/\operatorname{ord}_p(i)} \\ &= \zeta(s)(1-p^{-s}) \prod_{\chi\neq\chi_0} L(s,\chi) \prod_{i\neq 1} Q_i(\operatorname{ord}_p(i)s)^{-(p-1)/\operatorname{ord}_p(i)}, \end{aligned}$$

where the product $\prod_{\chi\neq\chi_0}$ *is over all nontrivial Dirichlet characters* χ *with conductor* p.

Proof. The above equation can be rewritten as

$$\begin{aligned} \prod_{\chi} L(s,\chi) &= \prod_{1\leq i\leq p-1} Q_i(\operatorname{ord}_p(i)s)^{(p-1)/\operatorname{ord}_p(i)} \\ &= \prod_{1\leq i\leq p-1} \left(\prod_{q_i} \left(1 - \frac{1}{q_i^{\operatorname{ord}_p(i)s}}\right)^{-(p-1)/\operatorname{ord}_p(i)} \right). \end{aligned}$$

Note that, for any Dirichlet character χ with conductor p, $L(s,\chi)$ can be expressed as the following Euler product:

$$L(s,\chi) = \prod_{1\leq i\leq p-1} \prod_{q_i} \left(1 - \frac{\chi(i)}{q_i^s}\right)^{-1}. \tag{5}$$

Therefore, we have

$$\prod_{\chi} L(s,\chi) = \prod_{1\leq i\leq p-1} \prod_{q_i} \prod_{\chi} \left(1 - \frac{\chi(i)}{q_i^s}\right)^{-1}.$$

To prove the lemma, it is enough to show that

$$\prod_{\chi} (1-\chi(i)X) = \left(1 - X^{\operatorname{ord}_p(i)s}\right)^{(p-1)/\operatorname{ord}_p(i)} \tag{6}$$

for $1 \leq i \leq p-1$. Let $0 \leq l \leq p-2$ be an integer satisfying $i \equiv g^l (\operatorname{mod} p)$. Then, for any $0 \leq j \leq p-2$, we have $\chi_j(i) = \chi_j(g^l) = \omega_{p-1}^{jl}$, so the left side of (6) can be written as follows:

$$\prod_{\chi} (1-\chi(i)X) = \prod_{j=0}^{p-2} (1-\chi_j(i)X) = \prod_{j=0}^{p-2} \left(1 - \left(\omega_{p-1}^l\right)^j X\right).$$

Note that ω_{p-1}^l is a primitive e-th root of unity, with $e = (p-1)/\gcd(l, p-1)$. Therefore, we have

$$\prod_{j=0}^{e-1} (1 - (\omega_{p-1}^l)^j X) = 1 - X^e,$$

and we have

$$\prod_{j=0}^{p-2}(1-({\omega_{p-1}}^{l})^{j}X)=\left(\prod_{j=0}^{e-1}\left(1-\left(\omega_{p-1}^{l}\right)^{j}X\right)\right)^{\frac{p-1}{e}}=(1-X^{e})^{\frac{p-1}{e}}.$$

Since e is equal to the order of g^l in $(\mathbb{Z}/p\mathbb{Z})^\times$, it follows that

$$\prod_{\chi}(1-\chi(i)X)=(1-X^{e})^{\frac{p-1}{e}}=\left(1-X^{\operatorname{ord}_p(i)}\right)^{(p-1)/\operatorname{ord}_p(i)}.$$

This is (6). ∎

Proposition 3.3. *For an odd prime p, the product*

$$Q_1(s)^{(p-1)/2}Q_{p-1}(s)^{-(p-1)/2}=\prod_{q_1}\left(1-\frac{1}{q_1^s}\right)^{-(p-1)/2}\prod_{q_{p-1}}\left(1-\frac{1}{q_{p-1}^s}\right)^{(p-1)/2}$$

can be factored as

$$\prod_{\chi(-1)=-1}L(s,\chi)\cdot\left(\text{analytic and nonvanishing on }\operatorname{Re}(s)>\frac{1}{2}\right).$$

Proof. Formula (5) gives the following equation.

$$\prod_{\chi(-1)=-1}L(s,\chi)=\prod_{1\le i\le p-1}\prod_{q_i}\prod_{\chi(-1)=-1}\left(1-\frac{\chi(i)}{q_i^s}\right)^{-1}. \tag{7}$$

For $i=1$ and $i=p-1$, the corresponding products in (7) are $\prod_{q_1}\left(1-{q_1}^{-s}\right)^{-(p-1)/2}$ and $\prod_{q_{p-1}}\left(1+q_{p-1}^{-s}\right)^{-(p-1)/2}$, respectively. Note that the product of the cases $i=1$ and $i=p-1$ can be rewritten as

$$\begin{aligned}&\prod_{q_1}\left(1-\frac{1}{q_1^s}\right)^{-(p-1)/2}\prod_{q_{p-1}}\left(1+\frac{1}{q_{p-1}^s}\right)^{-(p-1)/2}\\&=\prod_{q_1}\left(1-\frac{1}{q_1^s}\right)^{-(p-1)/2}\prod_{q_{p-1}}\left(1-\frac{1}{q_{p-1}^s}\right)^{(p-1)/2}\prod_{q_{p-1}}\left(1-\frac{1}{q_{p-1}^{2s}}\right)^{-(p-1)/2}.\end{aligned}$$

Since the product $\displaystyle\prod_{q_{p-1}}\left(1-\frac{1}{q_{p-1}^{2s}}\right)^{-(p-1)/2}$ is analytic and nonvanishing on the region $\operatorname{Re}(s)>\frac{1}{2}$, we only need to prove that the right side of (7) with $i\neq 1,p-1$ is analytic and nonvanishing on the same region. To prove this, it is sufficient to show that, for any $i \neq 1, p-1$ and for any q_i, the following holds.

$$\prod_{\chi(-1)=-1} (1-\chi(i){q_i}^{-s})^{-1} = 1 + O({q_i}^{-2s}). \tag{8}$$

By expanding the left side of (8), we know that

$$\prod_{\chi(-1)=-1} (1-\chi(i)X)^{-1} = 1 + \sum_{\chi(-1)=-1} \chi(i)X + O(X^2).$$

Therefore, it is enough to show that the sum $\sum_{\chi(-1)=-1} \chi(i)$ vanishes when $i \neq 1, p-1$. This comes from the orthogonality of Dirichlet characters, which gives

$$\sum_{\chi} \chi(i) = \sum_{\chi(-1)=1} \chi(i) + \sum_{\chi(-1)=-1} \chi(i) = 0,$$

and

$$\begin{aligned}\sum_{\chi} \chi(-i) &= \sum_{\chi(-1)=1} \chi(-i) + \sum_{\chi(-1)=-1} \chi(-i)\\ &= \sum_{\chi(-1)=1} \chi(i) - \sum_{\chi(-1)=-1} \chi(i) = 0.\end{aligned}$$

□

Proposition 3.4. *Let p be a prime $\equiv 1 (\mathrm{mod}\, 3)$, and $1 \leq a, b \leq p-1$ be the two distinct integers of order 3 mod p. Then the product*

$$\begin{aligned}&Q_1(s)^{2(p-1)/3} Q_a(s)^{-(p-1)/3} Q_b(s)^{-(p-1)/3}\\ =&\prod_{q_1}\left(1-\frac{1}{q_1^s}\right)^{-2(p-1)/3} \prod_{q_a}\left(1-\frac{1}{q_a^s}\right)^{(p-1)/3} \prod_{q_b}\left(1-\frac{1}{q_b^s}\right)^{(p-1)/3}\end{aligned}$$

can be factored as

$$\prod_{\chi(a)\neq 1} L(s,\chi) \cdot \left(\text{analytic and nonvanishing on } \operatorname{Re}(s) > \frac{1}{2}\right).$$

Proof. The proof is similar to that of Proposition 3.3. First, the following equation is true.

$$\prod_{\chi(a)\neq 1} L(s,\chi) = \prod_{1\leq i\leq p-1} \prod_{q_i} \prod_{\chi(a)\neq 1} \left(1-\frac{\chi(i)}{{q_i}^s}\right)^{-1}. \tag{9}$$

For $i=1$, the product on the right side of the above equation is $\prod_{q_1}(1-{q_1}^{-s})^{-2(p-1)/3}$. On the other hand, for $i=a$, $\chi(a)$ is equal to either ω_3 or ω_3^2, i.e. the two primitive third roots of unity. Since the Dirichlet characters exist in conjugates, these two cases occur with the same frequency. Therefore, there are $(p-1)/3$ copies of both $(1-\omega_3 q_a^{-s})^{-1}$ and $(1-\omega_3^2 q_a^{-s})^{-1}$ in the product on the right side of (9). Thus the desired product for the case $i=a$ is

$$\prod_{q_a}(1+q_a^{-s}+q_a^{-2s})^{-(p-1)/3}=\prod_{q_a}(1-q_a^{s})^{(p-1)/3}(1-q_a^{3s})^{-(p-1)/3}.$$

The same argument can be applied to the case $i=b$.

We claim that all the other products on the right side of (9) are analytic and do not vanish on the region $\mathrm{Re}(s)>\frac{1}{2}$. If we prove

$$\prod_{\chi(a)\neq 1}(1-\chi(i){q_i}^{-s})^{-1}=1+O({q_i}^{-2s})$$

holds for any $i\neq 1,a,b$, then the right side of (9) with $i\neq 1,a,b$ is well-defined and does not vanish on the desired region, proving the proposition. By expanding the product, we know that

$$\prod_{\chi(a)\neq 1}(1-\chi(i)X)^{-1}=1+\sum_{\chi(a)\neq 1}\chi(i)X+O(X^2).$$

Therefore, it is enough to show that the sum $\sum_{\chi(a)\neq 1}\chi(i)$ vanishes when $i\neq 1,a,b$. This comes from the orthogonality of Dirichlet characters, which gives

$$\sum_{\chi}\chi(i)=\sum_{\chi(a)=1}\chi(i)+\sum_{\chi(a)=\omega_3}\chi(i)+\sum_{\chi(a)=\omega_3^2}\chi(i)=0,$$

$$\sum_{\chi}\chi(ai)=\sum_{\chi(a)=1}\chi(i)+\omega_3\sum_{\chi(a)=\omega_3}\chi(i)+\omega_3^2\sum_{\chi(a)=\omega_3^2}\chi(i)=0,$$

and

$$\sum_{\chi}\chi(a^2i)=\sum_{\chi(a)=1}\chi(i)+\omega_3^2\sum_{\chi(a)=\omega_3}\chi(i)+\omega_3\sum_{\chi(a)=\omega_3^2}\chi(i)=0.$$

□

3.2. **Proof of Proposition 3.1.**

Proof. Define t as $(p-1)s$, for the sake of brevity. Proposition 3.2 implies that the following factorization holds.

$$\begin{aligned}\prod_{q_1}\left(1+\frac{p-1}{{q_1}^t}\right)^{-1} &= Q_1(t)^{p-1}Q_1(2t)^{-p(p-1)/2}Q_1(3t)^{p(p-1)(p-2)/3}\\ &\quad\cdot\left(\text{analytic and nonvanishing on }\ \mathrm{Re}(t)>\frac{1}{4}\right).\end{aligned}$$

We divide the problem into two cases.

3.2.1. *Case 1: $p = 3$ or $p \equiv 2 (\mathrm{mod}\, 3)$.* Lemma 3.2 implies that

$$\begin{aligned} &Q_1(t)^{p-1} \\ &= \zeta(t)(1-p^{-t}) \prod_{\chi \neq \chi_0} L(t,\chi) \prod_{i \neq 1} Q_i(\mathrm{ord}_p(i)t)^{-(p-1)/\mathrm{ord}_p(i)} \\ &= \zeta(t) \prod_{\chi \neq \chi_0} L(t,\chi) Q_{p-1}(2t)^{-(p-1)/2} \cdot \left(\text{analytic and nonvanishing on } \mathrm{Re}(t) > \frac{1}{4}\right). \end{aligned} \tag{10}$$

The equation (10) holds, since the products $Q_i(\mathrm{ord}_p(i)t)$ with $\mathrm{ord}_p(i) \geq 4$ are convergent on the region $\mathrm{Re}(t) > \frac{1}{4}$. By plugging $2t$ and $3t$ into s, Lemma 3.2 implies the following equations.

$$\begin{aligned} &Q_1(2t)^{-\frac{p+1}{2}\cdot(p-1)} \\ &= \zeta(2t)^{-\frac{p+1}{2}} \prod_{\chi \neq \chi_0} L(2t,\chi)^{-\frac{p+1}{2}} \cdot \left(\text{analytic and nonvanishing on } \mathrm{Re}(t) > \frac{1}{4}\right) \end{aligned} \tag{11}$$

$$\begin{aligned} &Q_1(3t)^{\frac{p(p-2)}{3}\cdot(p-1)} \\ &= \zeta(3t)^{\frac{p(p-2)}{3}} \prod_{\chi \neq \chi_0} L(3t,\chi)^{\frac{p(p-2)}{3}} \cdot \left(\text{analytic and nonvanishing on } \mathrm{Re}(t) > \frac{1}{4}\right). \end{aligned} \tag{12}$$

On the other hand, from Proposition 3.3, we obtain

$$\begin{aligned} &Q_1(2t)^{(p-1)/2} Q_{p-1}(2t)^{-(p-1)/2} \\ &= \prod_{\chi(-1)=-1} L(2t,\chi) \cdot \left(\text{analytic and nonvanishing on } \mathrm{Re}(t) > \frac{1}{4}\right). \end{aligned} \tag{13}$$

Proposition 3.1 follows by multiplying all the equations (10), (11), (12), (13). Specifically, $P_1(s)$ appears at (10), $P_2(s)$ appears at (11) and (13), and $P_3(s)$ appears at (12).

3.2.2. *Case 2: $p \equiv 1 (\mathrm{mod}\, 3)$.* Let a, b be the two distinct elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ whose orders are 3. The differences from the previous case are that Q_a, Q_b terms appear in (10) and the following new equation should be deduced from Proposion 3.4.

$$\begin{aligned} &Q_1(3t)^{(p-1)/2} Q_a(3t)^{-(p-1)/2} Q_b(3t)^{-(p-1)/2} \\ &= \prod_{\chi(a) \neq 1} L(3t,\chi) \cdot \left(\text{analytic and nonvanishing on } \mathrm{Re}(t) > \frac{1}{4}\right). \end{aligned} \tag{14}$$

Multiplying all the equations would imply Proposition 3.1 as well. In this case, $P_3(s)$ also appears at (14). $\square$

3.3. **Proof of Theorems 1.1 and 1.2.**

Proof. Recall that the poles of $D_{C_p}(s)$ and those of $\prod_{q_1}\left(1+(p-1){q_1}^{-(p-1)s}\right)$ are the same. Proposition 3.1 implies that

$$\prod_{q_1}\left(1+\frac{p-1}{{q_1}^{(p-1)s}}\right)=P_1(s)P_2(s)P_3(s)\cdot\Big(\text{nonvanishing and analytic}\Big)$$

where

$$\begin{aligned}
P_1(s) &= \zeta((p-1)s)\prod_{\chi\neq\chi_0}L((p-1)s,\chi),\\
P_2(s) &= \zeta(2(p-1)s)^{-(p+1)/2}\prod_{\chi\neq\chi_0}L(2(p-1)s,\chi)^{-(p+1)/2}\\
&\quad\cdot\prod_{\chi(-1)\neq1}L(2(p-1)s,\chi),\\
P_3(s) &= \zeta(3(p-1)s)^{\lfloor p(p-2)/3\rfloor}\prod_{\chi\neq\chi_0}L(3(p-1)s,\chi)^{\lfloor p(p-2)/3\rfloor}\\
&\quad\cdot\prod_{\chi(\alpha)\neq1}L(3(p-1)s,\chi).
\end{aligned}$$

Note that the factors $P_2(s)$ and $P_3(s)$ are analytic and nonvanishing on the region $\mathrm{Re}(s)>\frac{1}{2(p-1)}+\varepsilon$. Therefore, the only pole of $D_{C_p}(s)$ on the region $\mathrm{Re}(s)>\frac{1}{2(p-1)}+\varepsilon$ is a single pole at $s=\frac{1}{p-1}$. This will suffice to prove Theorem 1.2.

Assuming GRH, both $\zeta(2(p-1)s)^{-1}$ and $L(2(p-1)s,\chi)^{-1}$ have (nontrivial) poles only on the line $\mathrm{Re}(s)=\frac{1}{4(p-1)}$. Therefore, both are analytic on the region $\mathrm{Re}(s)>\frac{1}{4(p-1)}+\varepsilon$, which implies that the factor $P_2(s)$ does not contribute to any poles in the region $\mathrm{Re}(s)>\frac{1}{4(p-1)}+\varepsilon$. On the other hand, in the case of $P_3(s)$, $\zeta(3(p-1)s)^{\lfloor p(p-2)/3\rfloor}$ contributes to a pole at $s=\frac{1}{3(p-1)}$ of order $\lfloor p(p-2)/3\rfloor$ and is analytic elsewhere on the region $\mathrm{Re}(s)>\frac{1}{4(p-1)}+\varepsilon$. Note that $L(3(p-1)s,\chi)$ is analytic on the same region, implying that $P_3(s)$ itself has a pole at $s=\frac{1}{3(p-1)}$ and nowhere other in the same region. Moreover, the pole is not cancelled out by any other factors under the Generalized Riemann Hypothesis. That is, neither $\zeta((p-1)s)$ nor $L((p-1)s,\chi)$ can have a zero on the line $\mathrm{Re}(s)=\frac{1}{3(p-1)}$. This proves Theorem 1.1. $\square$

References

[1] David J. Wright, Density of discriminants of abelian extensions. *Proceedings of the London Mathematical Society* **58** (1989) 17-50.

[2] Harvey Cohn, The density of abelian cubic fields. *Proceedings of the American Mathematical Society* **5** (1954) 476-477.
[3] Henri Cohen, Francisco Diaz y Diaz, Michel Olivier, Counting discriminants of number fields. *Journal de Théorie des Nombres de Bordeaux* **18** (2006) 573-593.
[4] Henri Cohen, Comptage exact de discriminants d'extensions abéliennes *Journal de Théorie des Nombres de Bordeaux* **12** (2000) 379-397.
[5] Gérald Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Studies in Advanced Mathematics **46**, Cambridge University Press, Cambridge, 1995.
[6] Serge Lang, *Algebraic Number Theory*, 2nd. edition, Graduate Texts in Mathematics **110**, Springer, 1994.

Department of Mathematics, Stanford University, Stanford, CA 94305
E-mail address: lshyeong@stanford.edu

Department of Mathematics, Stanford University, Stanford, CA 94305
E-mail address: gyujinoh@stanford.edu