



ELSEVIER

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



General Section

Root numbers for the Jacobian varieties of Fermat curves

Jie Shu¹

School of Mathematical Sciences, Tongji University, Shanghai, 200092, China

ARTICLE INFO

Article history:

Received 16 December 2020

Received in revised form 25 March 2021

Accepted 30 March 2021

Available online 19 April 2021

Communicated by L. Smajlovic

Keywords:

Fermat curves

Root numbers

L-functions

ABSTRACT

Let p be an odd prime number. Let K be the p -th cyclotomic field. We give general formulae for the root numbers of the Jacobian varieties of the Fermat curves $X^p + Y^p = \delta$ where δ is an integer. As an application of these general formulae, we derive the equidistribution of the root numbers for the families of Jacobian varieties of the Fermat curves.

© 2021 Elsevier Inc. All rights reserved.

Contents

1.	Introduction	244
2.	The Jacobian varieties of Fermat curves	247
2.1.	Jacobi sums and algebraic Hecke characters	247
2.2.	The automorphic representations and L-functions	248
3.	Root numbers	249
3.1.	Local root numbers	250
3.2.	Kummer extensions	251
3.3.	Local root numbers outside p	257
3.4.	Local root number at p	261
3.5.	Global root numbers	265
3.6.	Equidistribution of root numbers	267

E-mail address: shujie@tongji.edu.cn.¹ The author is supported by the National Natural Science Foundation of China (Grant No. 11701092).<https://doi.org/10.1016/j.jnt.2021.03.012>

0022-314X/© 2021 Elsevier Inc. All rights reserved.

Acknowledgments	269
References	269

1. Introduction

The parity of the Mordell-Weil rank of an abelian variety is given by its root number by the Birch and Swinnerton-Dyer conjecture. For elliptic curves over $\mathbb{Q}$, the root-number equidistribution conjecture states that 50% of elliptic curves over $\mathbb{Q}$ have root number $+1$ and the other 50% have root number -1 . Another interesting problem is to analyse the distribution of the root number in various families of elliptic curves. For example, it is well known that in the family of quadratic twists of a given elliptic curve over $\mathbb{Q}$, the root number is equidistributed; L. Mai [12] proved the root number in the cubic twists family $x^3 + y^3 = \delta$ is equidistributed. From these equidistributions of root numbers, the BSD conjecture predicts that half of the elliptic curves should have even ranks and the other half should have odd ranks in the corresponding families. Moreover, the Goldfeld conjecture [6, Conjecture B] states that in the family of quadratic twists of an elliptic curves over $\mathbb{Q}$, the elliptic curves have rank 0, 1 with probability $1/2$ respectively.

In this article, we establish general formulae for the root numbers of Jacobian varieties of Fermat curves and prove the equidistribution of root numbers in the family of p -th twists of these Jacobian varieties.

Let p be an odd prime number and μ_p the group of p -th root of unity with a generator ω . Let $K = \mathbb{Q}(\omega)$ be the p -th cyclotomic field. Let δ be a p -th power-free rational number and let F_δ be the Fermat curve over $\mathbb{Q}$ defined by

$$X^p + Y^p = \delta.$$

For integers $r, s, t > 0$ satisfying $r + s + t = p$, let $C_{r,s,t;\delta}$ be the smooth projective curve over $\mathbb{Q}$ of genus $g = (p-1)/2$, which is defined by the affine equation

$$y^p = x^r(\delta - x)^s.$$

Let $J_{r,s,t;\delta}$ be the Jacobian variety of the curve $C_{r,s,t;\delta}$. The curves $C_{r,s,t;\delta}$ are natural quotient curves of the Fermat curve F_δ and the quotient maps induce an isogenous decomposition of the Jacobian $\text{Jac}(F_\delta)$ by the various Jacobian varieties $J_{r,s,t;\delta}$ over $\mathbb{Q}$ [13]. Therefore, the Jacobian varieties $J_{r,s,t;\delta}$ are referred as the Jacobian varieties of the Fermat curves.

The curve

$$C_{r,s,t;\delta} : y^p = x^r(\delta - x)^s$$

is defined over $\mathbb{Q}$. Let $\Lambda(s, J_{r,s,t;\delta}/\mathbb{Q})$ be the complete Hasse-Weil L -function of the Jacobian variety $J_{r,s,t;\delta}/\mathbb{Q}$. Weil [22] proved this L -function is modular and can be identified

with the L -function of a Hecke character over K . Therefore $\Lambda(s, J_{r,s,t;\delta}/\mathbb{Q})$ is entire and satisfies Hecke's functional equation

$$\Lambda(s, J_{r,s,t;\delta}/\mathbb{Q}) = \epsilon_{r,s,t;\delta} \Lambda(2-s, J_{r,s,t;\delta}/\mathbb{Q})$$

where $\epsilon_{r,s,t;\delta} = \pm 1$ is the root number.

For $p = 3$, we must have $r = s = t = 1$, and $C_{1,1,1;\delta}$ are elliptic curves. In this case, the root numbers have been computed by Birch, Stephens and Liverance [1,18,11]. For the classical Fermat-curve case i.e. $\delta = 1$, the root numbers $\epsilon_{r,s,t;1}$ have been computed by Gross and Rorlich [7,14]. We will establish the general formulae for the root numbers $\epsilon_{r,s,t;\delta}$ of the Jacobian varieties $J_{r,s,t;\delta}/\mathbb{Q}$ for all $\delta \in \mathbb{Q}^\times$. In what follows, without loss of generality, we always assume $\delta \in \mathbb{Q}^\times$ is a p -th power-free integer.

For a p -th power-free integer $n \in \mathbb{Q}^\times$, we write, in $\mathbb{Q}_p^\times$, that $n = \epsilon p^a(1-p)^b$ with $\epsilon \in \mathbb{F}_p^\times \hookrightarrow \mathbb{Q}_p^\times$, $a \in \{0, 1, \dots, p-1\}$, and $b \in \mathbb{Z}_p$. Set

$$u(n) = \min(\text{ord}_p(a), \text{ord}_p(b) + 1).$$

Note that $u(n) = \text{ord}_p(b) + 1$ if $a = 0$, and $u(n) = 0$ otherwise. Let $d \in (\mathbb{Z}/p\mathbb{Z})^\times$ be the residue class given by

$$d = \begin{cases} \frac{(r^r s^s (t-p)^t \delta^{r+s})^{p-1} - 1}{p} \bmod p, & \text{if } u(r^r s^s (t-p)^t \delta^{r+s}) = 1; \\ (r+s)\text{ord}_p(\delta) \bmod p, & \text{if } u(r^r s^s (t-p)^t \delta^{r+s}) = 0. \end{cases}$$

We have the following general formulae for the root numbers.

Theorem 1.1. *Let $r, s, t > 0$ be integers satisfying $r + s + t = p$, and let $J_{r,s,t;\delta}$ be the corresponding Fermat Jacobian over $\mathbb{Q}$. The root number $\epsilon_{r,s,t;\delta}$ for the Hasse-Weil L -function of $J_{r,s,t;\delta}/\mathbb{Q}$ is explicitly given as follows:*

$$\epsilon_{r,s,t;\delta} = \prod_{\ell} \epsilon_{r,s,t;\delta,\ell},$$

where

$$\epsilon_{r,s,t;\delta,\ell} = \begin{cases} \left(\frac{-1}{p}\right), & \text{if } \ell = \infty; \\ \left(\frac{\ell}{p}\right), & \text{if } \ell \neq p \text{ and } \ell \mid \delta; \\ +1, & \text{if } \ell \nmid p\delta; \end{cases}$$

and

$$\epsilon_{r,s,t;\delta,p} = \begin{cases} -\left(\frac{-rst\delta}{p}\right), & \text{if } u(r^r s^s (t-p)^t \delta^{r+s}) = 0; \\ -\left(\frac{rst\delta}{p}\right), & \text{if } u(r^r s^s (t-p)^t \delta^{r+s}) = 1; \\ \left(\frac{-2}{p}\right), & \text{if } u(r^r s^s (t-p)^t \delta^{r+s}) \geq 2. \end{cases}$$

The above formulae are compatible with those given in [1,18,11] for $p = 3$ and those in [7,14] for $\delta = 1$. The formulae in [7] involves a quantity m related to the CM type of the Jacobian variety $J_{r,s,t;1}$. Perhaps, it is this quantity m that makes trouble when the authors in [7] verified the parity conjectures for the abelian varieties $J_{r,s,t;1}$, and they gave a full treatment only in the case $r = s = 1$. On the other hand, since the above formulae depend on r, s, t and δ in a direct way, they are easily accessible and more convenient in applications. Indeed, they are successfully applied in [17] to verify the parity conjectures for the Jacobian varieties $J_{r,s,t;\delta}$. As another application we will prove the equidistribution of the root numbers.

Theorem 1.2. *Let $\mathbb{N}^{(p)}$ be the set of p -th power-free positive integers. We have the following equidistribution*

$$\lim_{X \rightarrow +\infty} \frac{\#\{\delta \in \mathbb{N}^{(p)} : \delta \leq X \text{ and } \epsilon_{r,s,t;\delta} = +1\}}{\#\{\delta \in \mathbb{N}^{(p)} : \delta \leq X\}} = \frac{1}{2}.$$

When $p = 3$ ($r = s = t = 1$), this is proved by L. Mai [12]. For a general odd prime p , the curves $C_{1,1;p-2;\delta}$, $C_{1,(p-1)/2,(p-1)/2;\delta}$ and $C_{1,p-2,1;\delta}$ are hyperelliptic curves and the root numbers of these curves can be obtained by [19] (with constrain $p \nmid \delta$). T. Jedrzejak [10] generalized the result of L. Mai for these hyperelliptic families $J_{1,1;p-2;\delta}$, $J_{1,(p-1)/2,(p-1)/2;\delta}$ and $J_{1,p-2,1;\delta}$ with $p \nmid \delta$.

Notations. Let $F = \mathbb{Q}(\omega + \omega^{-1})$ be the maximal real subfield of K . Let $\mathcal{O}_K$ resp. $\mathcal{O}$ be the ring of integers of the field K resp. F . Let $\mathbb{A}$ be the adèle ring of F . Let $|\cdot|_{\mathbb{A}} : \mathbb{A}^{\times} \rightarrow \mathbb{R}_+^{\times}$ denote the standard adélic absolute value so that $d(ab) = |a|_{\mathbb{A}} db$ for any Haar measure db on $\mathbb{A}$. Let $|\cdot|_v$ denote the absolute value on $F_v^{\times}$ for each place v of F such that $|x|_{\mathbb{A}} = \prod_v |x_v|_v$ for any $x = (x_v) \in \mathbb{A}^{\times}$. For a finite place v , sometimes we also denote by v its corresponding prime ideal and $q_v = \#\mathcal{O}/v$. For $x \in F^{\times}$, denote by $\text{ord}_v(x)$ the additive valuation of x at v so that $\text{ord}_v(v) = 1$. We denote by ∞ the set of infinite places of F . Let $\mathbb{A}_K = K \otimes_F \mathbb{A}$ be the adèle ring of K . The notations $|\cdot|_{\mathbb{A}_K}, |\cdot|_V, q_V$, and $\text{ord}_V(\cdot)$ are similarly defined for K where V is a finite place of K .

2. The Jacobian varieties of Fermat curves

2.1. Jacobi sums and algebraic Hecke characters

The readers can refer to [22,3] for the basics of the Jacobi sums. Let $r, s, t > 0$ be integers satisfying $r + s + t = p$. Let V be any finite place of K not dividing p . The p -th power residue character $\chi_V : (\mathcal{O}_K/V)^\times \rightarrow \mu_p$ modulo V is given by

$$\chi_V(x) \equiv x^{\frac{q_V-1}{p}} \pmod{V}.$$

The Jacobi sum

$$j_{r,s,t}(V) = - \sum_{\substack{x \in \mathcal{O}_K/V \\ x \neq 0,1}} \chi_V(x)^r \chi_V(1-x)^s$$

is an integer in $\mathcal{O}_K$. The set

$$\Phi_{r,s,t} = \left\{ h \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \left\langle \frac{hr}{p} \right\rangle + \left\langle \frac{hs}{p} \right\rangle + \left\langle \frac{ht}{p} \right\rangle = 1 \right\}$$

can be identified with the CM-type of $J_{r,s,t;1}$ through the Artin isomorphism

$$\sigma : (\mathbb{Z}/p\mathbb{Z})^\times \simeq \text{Gal}(K/\mathbb{Q}), \quad \sigma_h(\omega) = \omega^h.$$

Here $\langle \cdot \rangle$ denotes the fractional part of a rational number. If we put

$$\Phi_{r,s,t}^{-1} = \{h^{-1} \in (\mathbb{Z}/p\mathbb{Z})^\times \mid h \in \Phi_{r,s,t}\},$$

then the CM type $(K, \Phi_{r,s,t}^{-1})$ is the reflex of the CM type $(K, \Phi_{r,s,t})$. The Stickelberger relation holds

$$(j_{r,s,t}(V)) = \prod_{h \in \Phi_{r,s,t}} V^{\sigma_h^{-1}}, \quad (2.1)$$

and it follows that $j_{r,s,t}(V)$ has absolute value $q_V^{1/2}$ for any complex embedding of K in $\mathbb{C}$.

We extend the definition of $j_{r,s,t}(V)$ to all ideals prime to p in K by the condition

$$j_{r,s,t}(\mathfrak{ab}) = j_{r,s,t}(\mathfrak{a})j_{r,s,t}(\mathfrak{b}).$$

Weil proved in [22] that the resulting function $j_{r,s,t}(\mathfrak{a})$ is indeed an algebraic Hecke character on K with values in K of conductor dividing Π^2 and infinity type $\Phi_{r,s,t}^{-1}$, i.e. for any $x \in K^\times$ such that $x \equiv 1 \pmod{\Pi^2}$,

$$j_{r,s,t}((x)) = x^{\Phi_{r,s,t}^{-1}} = \prod_{\sigma \in \Phi_{r,s,t}^{-1}} x^{\sigma}.$$

Here $\Pi = \omega - \bar{\omega}$ is a primitive element of K at the place above p . The infinity type

$$\Phi_{r,s,t}^{-1} : K^{\times} \longrightarrow K^{\times}, \quad x \mapsto \prod_{\sigma \in \Phi_{r,s,t}^{-1}} x^{\sigma},$$

induces a homomorphism, by linearity, on idèles:

$$\Phi_{r,s,t}^{-1} : \mathbb{A}_K^{\times} \longrightarrow \mathbb{A}_K^{\times}.$$

Let $\tau_0 \in \text{Hom}(K, \mathbb{C})$ be a fixed element and we identify K as a subfield of $\mathbb{C}$ via τ_0 . Let

$$\Phi_{r,s,t;\tau_0}^{-1} : \mathbb{A}_K^{\times} \longrightarrow \mathbb{A}_K^{\times} \xrightarrow{\tau_0} \mathbb{C}$$

be the composition of $\Phi_{r,s,t}^{-1}$ with the projection through τ_0 . It is well known [22] that

$$\phi_{r,s,t} = j_{r,s,t} \cdot (\Phi_{r,s,t;\tau_0}^{-1})^{-1} : K^{\times} \backslash \mathbb{A}_K^{\times} \rightarrow \mathbb{C}^{\times}$$

is the Hecke character associated to the CM abelian variety $J_{r,s,t;1/K}$ in the sense of [16, Proposition 19.9]. Generally, if $\delta \in K^{\times}/K^{\times p}$, then according to Weil [22] the abelian variety $J_{r,s,t;\delta/K}$ also has CM type $(K, \Phi_{r,s,t})$ and the associated Hecke character is $\phi_{r,s,t;\delta} = \chi_{\delta}^{r+s} \cdot j_{r,s,t} \cdot (\Phi_{r,s,t;\tau_0}^{-1})^{-1}$ where χ_{δ} is the character on ideals prime to δ such that $\chi_{\delta}(V) = \chi_V(\delta)$. It follows from the Stickelberger relation (2.1) that the Hecke characters

$$\phi_{r,s,t;\delta} = (\chi_{\delta}^{r+s} j_{r,s,t} \cdot (-\Phi_{r,s,t}^{-1}))_{\tau_0} | \cdot |_{\mathbb{A}_K}^{1/2} : K^{\times} \backslash \mathbb{A}_K^{\times} \longrightarrow \mathbb{C}^{\times}$$

are all unitary.

2.2. The automorphic representations and L -functions

Suppose δ is a p -th power-free integer. Fix the triple (r, s, t) with $r, s, t > 0$ and $r + s + t = p$. Both $C_{r,s,t;\delta}$ and $J_{r,s,t;\delta}$ are rational over F . Let $\pi_{r,s,t;\delta}$ be the cuspidal automorphic representation on $\text{GL}_2(\mathbb{A})$ associated to $J_{r,s,t;\delta/F}$. Explicitly $\pi_{r,s,t;\delta}$ is the representation on $\text{GL}_2(\mathbb{A})$ locally constructed from $\phi_{r,s,t;\delta}$ using Weil representation. The L -function $L(s, \pi_{r,s,t;\delta})$ is entire and satisfies a functional equation

$$L(s, \pi_{r,s,t;\delta}) = \epsilon_{r,s,t;\delta} L(1-s, \pi_{r,s,t;\delta}),$$

where the epsilon factor $\epsilon_{r,s,t;\delta} = \pm 1$. By [9, Theorem 4.7], we know

$$L(s, \pi_{r,s,t;\delta}) = L(s, \phi_{r,s,t;\delta}).$$

Furthermore, the curve

$$C_{r,s,t;\delta} : y^p = x^r(\delta - x)^s$$

is defined over $\mathbb{Q}$ and has good reduction at all rational primes $\ell \nmid p\delta$. Let

$$Z(C_{r,s,t;\delta}/\mathbb{F}_\ell, T) = \frac{P_\ell(T)}{(1-T)(1-\ell T)}$$

be the Zeta function of the reduced curve $C_{r,s,t;\delta}/\mathbb{F}_\ell$. Then $P_\ell(T)$ is a polynomial with integral coefficients of degree $2g = p - 1$.

The Jacobian variety $J_{r,s,t;\delta}/\mathbb{Q}$ has a global L -function

$$L(s, J_{r,s,t;\delta}/\mathbb{Q}) = \prod_{\ell \nmid p\delta} P_\ell(\ell^{-s})^{-1}.$$

This Euler product converges for $\text{Re}(s) > 3/2$. Weil [22] proved in this region

$$L(s, J_{r,s,t;\delta}/\mathbb{Q}) = L^{(\infty)}(s - 1/2, \phi_{r,s,t;\delta}),$$

where $\phi_{r,s,t;\delta} = \chi_\delta^{r+s} \phi_{r,s,t}$ is the Hecke character associated to the CM abelian variety $J_{r,s,t;\delta}/K$ in the sense of [16, Proposition 19.9] (see §1.1) and $L^{(\infty)}$ means the L -function with the infinite factors removed. Therefore

$$L\left(s, J_{r,s,t;\delta}/\mathbb{Q}\right) = L^{(\infty)}(s - 1/2, \phi_{r,s,t;\delta}) = L^{(\infty)}(s - 1/2, \pi_{r,s,t;\delta}).$$

Set the complete L -function as

$$\Lambda\left(s, J_{r,s,t;\delta}/\mathbb{Q}\right) = N_{r,s,t;\delta}^{s/2} ((2\pi)^{-s} \Gamma(s))^{(p-1)/2} L\left(s, J_{r,s,t;\delta}/\mathbb{Q}\right),$$

where $N_{r,s,t;\delta}$ is the conductor of the curve $C_{r,s,t;\delta}/\mathbb{Q}$. Then $\Lambda\left(s, J_{r,s,t;\delta}/\mathbb{Q}\right)$ satisfies Hecke's functional equation

$$\Lambda\left(s, J_{r,s,t;\delta}/\mathbb{Q}\right) = \epsilon_{r,s,t;\delta} \Lambda\left(2 - s, J_{r,s,t;\delta}/\mathbb{Q}\right).$$

Therefore, we see the Jacobian variety $J_{r,s,t;\delta}/\mathbb{Q}$ and the cuspidal automorphic representations $\pi_{r,s,t;\delta}$ share the same root number $\epsilon_{r,s,t;\delta}$, and hence, in order to compute $\epsilon_{r,s,t;\delta}$, we will compute the root number of the Hecke character $\phi_{r,s,t;\delta}$.

3. Root numbers

Suppose δ is a p -th power-free integer. Fix the triple (r, s, t) of positive integers satisfying $r + s + t = p$. Simply denote $J_\delta = J_{r,s,t;\delta}$, and denote $\phi = \phi_{r,s,t}$ and $\phi_\delta = \phi_{r,s,t;\delta} = \phi \chi_\delta^{r+s}$ the Hecke characters associated to J and J_δ respectively. We shall compute the local root number of the Hecke character ϕ_δ .

3.1. Local root numbers

We shall recall several formulae for the local root numbers. The basic references to this subject are [20,9,4,21]. Let L be a nonarchimedean local field. Fix a nontrivial additive character ψ of L , and denote by dx the self-dual Haar measure on L with respect to ψ . Let χ be a unitary character of $F^\times$. The local epsilon factor $\epsilon(\chi, \psi) = \epsilon(\chi, \psi, dx)$ associated to χ with respect to ψ is given by [4, (3.3.1)], and define

$$\epsilon(s, \chi, \psi) = \epsilon(\chi| \cdot |^s, \psi).$$

The local root number associated to χ with respect to ψ is

$$\frac{\epsilon(\chi, \psi)}{|\epsilon(\chi, \psi)|} = \epsilon(1/2, \chi, \psi).$$

If L is archimedean, the formulae for the local epsilon factors can be found in [4, (3.4.1)-(3.4.2)] or [9, p. 97]. Now suppose L is nonarchimedean with ring of integers $\mathcal{O}$, and a uniformizer ϖ . Define the conductors:

- $n(\psi)$ = the largest integer n such that $\psi|_{\varpi^{-n}\mathcal{O}} = 1$;
- $c(\chi)$ = the smallest positive integer m such that $\chi|_{(1+\varpi^m\mathcal{O})} = 1$ if χ is ramified, and 0 if χ is unramified.

We may also refer to $\varpi^{-n}\mathcal{O}$ resp. $\varpi^m\mathcal{O}$ as the conductor of ψ resp. χ .

If χ is unramified, then

$$\epsilon(s, \chi, \psi) = \chi(\varpi^{n(\psi)})|\varpi|^{n(\psi)(s-\frac{1}{2})}. \quad (3.1)$$

So if $n(\psi) = 0$, then the root number

$$\epsilon(1/2, \chi, \psi) = 1.$$

If χ is ramified, then from [4, (3.4.3.2)] we have

$$\epsilon(s, \chi, \psi) = \int_{\varpi^{-(n(\psi)+c(\chi))}\mathcal{O}^\times} \chi^{-1}(x)|x|^{-s}\psi(x)dx. \quad (3.2)$$

We introduce another useful result on local epsilon factors. Suppose M is a finite extension of $\mathbb{Q}_\ell$, and let L be a separable quadratic extension of M . This determines uniquely an element Δ in $L^\times$ modulo $M^\times$ such that

$$L = M[\Delta], \quad \Delta^2 \in M^\times. \quad (3.3)$$

Let $\psi_\ell : \mathbb{Q}_p \rightarrow \mathbb{C}^\times$ be the additive character given by

$$\psi_\ell(x) = e^{2\pi i \iota(x)} \quad (3.4)$$

where $\iota : \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathbb{Q}/\mathbb{Z}$ is the natural embedding. Then define $\psi_L : L \rightarrow \mathbb{C}^\times$ by

$$\psi_L(x) = \psi_\ell(\mathrm{Tr}_{L/\mathbb{Q}_\ell}(x)).$$

Proposition 3.1 (Frölich-Queyruat [5, Theorem 3]). *Let L be a separable quadratic extension of M , with Δ satisfying (3.3), and let χ be a character of $L^\times$ so that $\chi|_{M^\times} = 1$. Then*

$$\epsilon(1/2, \chi, \psi_L) = \chi(\Delta).$$

3.2. Kummer extensions

The field extension $K/\mathbb{Q}$ is totally ramified at p . Put

$$\Pi = \omega - \bar{\omega} \text{ and } \pi = \Pi^2 = \omega^2 + \bar{\omega}^2 - 2.$$

Then the ideal $\mathfrak{P} = (\Pi)$ resp. $\mathfrak{p} = (\pi)$ is the unique prime ideal of K resp. F above p .

Note under the class field theory, the character χ_δ can be viewed as a character on the Galois group $\chi_\delta : G_K \rightarrow \mathcal{O}_K^\times$ which is characterized by $\chi_\delta(\sigma) = (\sqrt[p]{\delta})^{\sigma-1}$.

Lemma 3.2. *Let $\mathfrak{D}_0$ be the product of all distinct prime factors of (δ) in K not dividing p . Then*

$$\chi_\delta|_{\mathbb{A}^\times} = 1,$$

and the conductor $c(\chi_\delta)$ divides $\mathfrak{P}^{p+1}\mathfrak{D}_0$.

Proof. Denote $L = K(\sqrt[p]{\delta})$. We first note that the extension L/K is unramified outside the places dividing $p\delta$. Under the Artin reciprocity map, we have the isomorphism

$$\sigma : K^\times \mathrm{N}_{L/K}(\mathbb{A}_L^\times) \backslash \mathbb{A}_K^\times \simeq \mathrm{Gal}(L/K).$$

Denote by σ_t the image of $t \in K^\times \mathrm{N}_{L/K}(\mathbb{A}_L^\times) \backslash \mathbb{A}_K^\times$ under the Artin reciprocity map. Let $c \in \mathrm{Gal}(K/F)$ be the non-trivial element and c extends to an involution on $\mathbb{A}_K$ through its action on K . Then for any $t \in K^\times \mathrm{N}_{L/K}(\mathbb{A}_L^\times) \backslash \mathbb{A}_K^\times$, we have

$$\sigma_t^{-1} = c\sigma_t c = \sigma_{t^c}.$$

The first identity is clear from the effect of $c\sigma_t c$ on $\sqrt[p]{\delta}$, and the second identity follows from [21, §1].

Denote by N the norm map from K to F . For a finite place v of F , let $K_v = K \otimes_F F_v$ and we embed $K_v^\times$ naturally into $\mathbb{A}_K^\times$. Then for any $t \in K_v^\times$, $\sigma_{N(t)} = \sigma_t \sigma_{t^c} = 1$. In

particular, $\chi_\delta|_{N(K_v^\times)} = 1$. If v is split in K , then $N(K_v^\times) = F_v^\times$. If v is inert in K , then $N(K_v^\times)$ is a subgroup of $F_v^\times$ of index 2. Since χ_δ is a character of order p , in both cases, χ_δ is trivial when restricted on $F_v^\times$. Since χ_δ has trivial local factors at infinite places, we have $\chi_\delta|_{\mathbb{A}^\times} = 1$.

For any $V \neq \Pi$ dividing δ and $t \in (1 + \mathfrak{D}_0 \mathcal{O}_{K,v})$,

$$\chi_\delta(t) = \left(\frac{t, \delta}{K_V; p} \right) \equiv t^{-\frac{\text{ord}_V(\delta)(q_V-1)}{p}} \equiv 1 \pmod{\mathfrak{D}_0 \mathcal{O}_{K,V}},$$

where $\left(\frac{\cdot, \cdot}{K_V; p} \right)$ denotes the p -th Hilbert symbol over K_V .

For any $t = 1 + x \in K_\Pi^\times$ with $\text{ord}_\Pi(x) > p$, it is easy to see that the binomial expansion

$$(1+x)^{\frac{1}{p}} = \sum_{i=0}^{\infty} \binom{1/p}{i} x^i$$

converges, and hence t is a p -th power in $K_\Pi^\times$. Then

$$\chi_\delta(t) = \left(\frac{t, \delta}{K_\Pi; p} \right) = \left(\frac{\delta, t}{K_\Pi; p} \right)^{-1} = 1. \quad \square$$

Lemma 3.3. *Let $\ell \neq p$ be a rational prime number. Let $V \mid \ell$ be a place of K . Then V is fixed by the complex conjugation, or equivalently, V is inert in the extension K/F , if and only if ℓ has even order in $\mathbb{F}_p^\times$. In particular, the places of F above ℓ have the same inertia degree in the quadratic extension K/F .*

Proof. We identify the Galois group $\text{Gal}(K/\mathbb{Q})$ with $(\mathbb{Z}/p\mathbb{Z})^\times$ by the Artin reciprocity map, via which the complex conjugation is identified with -1 . Let D_V be the decomposition group of V with respect to the extension $K/\mathbb{Q}$. Since V is unramified,

$$D_V \simeq \text{Gal}(\mathbb{F}_{q_V}/\mathbb{F}_\ell).$$

Then V is fixed by the complex conjugation if and only if D_V contains -1 . This is equivalent to that the inertia degree $[q_V : \ell]$ is even. It is well-known that the inertia degree $[q_V : \ell]$ is the order of ℓ in $\mathbb{F}_p^\times$. Since $K/\mathbb{Q}$ is abelian, if any D_V contains -1 , so do the others, and the last assertion follows. $\square$

We write, in $\mathbb{Q}_p^\times$, that

$$\delta = \epsilon p^a (1-p)^b$$

with $\epsilon \in \mathbb{F}_p^\times \subset \mathbb{Q}_p^\times$, $a \in \{0, 1, \dots, p-1\}$, and $b \in \mathbb{Z}_p$. Note such a and b are uniquely determined by

$$a = \text{ord}_p(\delta), \quad b = \frac{\log(\delta)}{\log(1-p)},$$

where $\log$ denotes the p -adic Iwasawa logarithm (i.e. $\log(p) = 0$). If $a = 0$, we also have

$$\text{ord}_p(b) = \text{ord}_p\left(\frac{\delta^{p-1} - 1}{p}\right).$$

Put

$$u(\delta) = \min(\text{ord}_p(a), \text{ord}_p(b) + 1). \quad (3.5)$$

We note that $u(\delta) = \text{ord}_p(b) + 1$ if $a = 0$, and $u(\delta) = 0$ otherwise.

Proposition 3.4. *The conductor of the Hecke character χ_δ is given as*

$$c(\chi_\delta) = \begin{cases} \mathfrak{P}^{p+1}\mathfrak{D}_0, & \text{if } u(\delta) = 0; \\ \mathfrak{P}^2\mathfrak{D}_0, & \text{if } u(\delta) = 1; \\ \mathfrak{D}_0, & \text{if } u(\delta) \geq 2; \end{cases}$$

Proof. This follows from Lemma 3.2 and [3, Theorem 6.1] or [15, Theorem 8]. $\square$

Put

$$\Pi' = 1 - \omega.$$

We have

$$\Pi = -2\Pi' + \Pi'\overline{\Pi'}, \quad \omega = 1 - \Pi',$$

and note

$$K = F[\Pi], \quad \Pi^2 \in F^\times. \quad (3.6)$$

For any place V of K , denote by $\chi_{\delta,V}$ the V -adic component of χ_δ . By Proposition 3.4, if $u(\delta) \geq 2$, then the local character $\chi_{\delta,\Pi}$ is unramified.

Proposition 3.5.

1. Suppose $u(\delta) = 1$. The local character $\chi_{\delta,\Pi}$ has conductor (Π^2) , and

$$\chi_{\delta,\Pi}(1 + \Pi) = \omega^{2\left(\frac{\delta^{p-1}-1}{p}\right)}.$$

2. Suppose $u(\delta) = 0$. The local character $\chi_{\delta, \Pi}$ has conductor (Π^{p+1}) , and

$$\chi_{\delta, \Pi}(1 + \Pi^p) = \omega^{2\text{ord}_p(\delta)}.$$

Proof. First suppose $u(\delta) = 1$. In this case, $a = 0$ and $\chi_{\delta, \Pi}$ has conductor (Π^2) by Proposition 3.4. Since ϵ is a p -th power in $K_{\Pi}^{\times}$, we have

$$\chi_{\delta, \Pi}(1 + \Pi) = \left(\frac{1 + \Pi, \delta}{K_{\Pi}; p} \right) = \left(\frac{1 + \Pi, (1 - p)^b}{K_{\Pi}; p} \right).$$

By an explicit reciprocity formula of Artin-Hasse-Iwasawa [8], we have

$$\left(\frac{1 + \Pi, (1 - p)^b}{K_{\Pi}; p} \right) = \omega^{[1 + \Pi, (1 - p)^b]}$$

where

$$[1 + \Pi, (1 - p)^b] = -\frac{1}{p} \text{Tr}_{K_{\Pi}/\mathbb{Q}_p} \left(\frac{\omega}{1 + \Pi} \frac{d(1 + \Pi)}{d\Pi'} \log(1 - p)^b \right).$$

Note

$$\log(1 - p)^b = -bp \left(1 + \frac{p}{2} + \frac{p^2}{3} + \cdots \right).$$

And

$$\begin{aligned} \frac{\omega}{1 + \Pi} \frac{d(1 + \Pi)}{d\Pi'} &= \frac{1 - \Pi'}{1 - 2\Pi' + \Pi'\overline{\Pi'}} \cdot \frac{d(1 - 2\Pi' + \Pi'\overline{\Pi'})}{d\Pi'} \\ &\equiv -2 \pmod{\Pi'}. \end{aligned}$$

Hence

$$-\frac{1}{p} \text{Tr}_{K_{\Pi}/\mathbb{Q}_p} \left(\frac{\omega}{1 + \Pi} \frac{d(1 + \Pi)}{d\Pi'} \log(1 - p)^b \right) \equiv -\text{Tr}_{K_{\Pi}/\mathbb{Q}_p}(2b) \equiv 2b \pmod{p}.$$

On the other hand,

$$\delta^{p-1} = (\epsilon(1 - p)^b)^{p-1} \equiv 1 + bp \pmod{p^2}.$$

So

$$-\frac{1}{p} \text{Tr}_{K_{\Pi}/\mathbb{Q}_p} \left(\frac{\omega}{1 + \Pi} \frac{d(1 + \Pi)}{d\Pi'} \log(1 - p)^b \right) \equiv 2 \left(\frac{\delta^{p-1} - 1}{p} \right) \pmod{p}.$$

The first assertion follows.

Next suppose $u(\delta) = 0$. In this case, $a \neq 0$, and the local character $\chi_{\delta, \Pi}$ has conductor (Π^{p+1}) . We have

$$\chi_{\delta, \Pi}(1 + \Pi^p) = \left(\frac{1 + \Pi^p, p^a(1-p)^b}{K_{\Pi}; p} \right).$$

By Proposition 3.4, the local character $\chi_{(1-p)^b, \Pi}$ has conductor dividing (Π^2) . Hence

$$\chi_{\delta, \Pi}(1 + \Pi^p) = \left(\frac{1 + \Pi^p, p^a}{K_{\Pi}; p} \right).$$

Since

$$1 + \Pi^p = 1 + (-2\Pi' + \Pi\overline{\Pi'})^p \equiv 1 + (-2)^p \Pi'^p \equiv (1 + \Pi'^p)^{-2} \pmod{\Pi^{p+1}},$$

$$\chi_{\delta, \Pi}(1 + \Pi^p) = \left(\frac{1 + \Pi'^p, p}{K_{\Pi}; p} \right)^{-2a}.$$

It suffices to compute

$$\left(\frac{1 + \Pi'^p, p}{K_{\Pi}; p} \right),$$

and we will apply Coleman's explicit reciprocity law [2, Theorem 1] and [3, p. 89] to do this calculation. Let $g_1(T) \in \mathbb{Z}_p[[T]]$ be as in p. 90 of [3]:

$$g_1(T) = \prod_{a=1}^{p-1} [a](T),$$

where $[a](T) = 1 - (1-T)^a$ is the a -th power homomorphism of the multiplicative formal group $\widehat{\mathbb{G}}_m$ with group law $\widehat{\mathbb{G}}_m(X, Y) = X + Y - XY$. Then

$$g_1(\Pi') = p.$$

Define

$$\Lambda : 1 + T\mathbb{Z}_p[[T]] \longrightarrow T\mathbb{Z}_p[[T]], \quad \Lambda(f) = \log(f) - \frac{1}{p} \log(f([p])).$$

By Coleman's explicit reciprocity law

$$\left(\frac{1 + \Pi'^p, p}{K_{\Pi}; p} \right) = \omega^{-n},$$

where

$$n = \int_1 \Lambda(1 + T^p) \frac{Dg_1}{g_1},$$

and we note the Hilbert symbol is the inverse of that in Coleman's paper [3, p. 43]. It is straight-forward to verify

$$\Lambda(1 + T^p) \equiv (1 - p^{p-1})T^p \pmod{T^{p+1}\mathbb{Z}_p[[T]]}.$$

Since $\frac{Dg_1}{g_1}$ has at most a single pole at $T = 0$, we obtain

$$n = \frac{1}{p} \text{Tr}_{K_\Pi/\mathbb{Q}_p} \left(\left(\Lambda(1 + T^p) \frac{Dg_1}{g_1} \right) \Big|_{T=\Pi'} \right).$$

Since $\chi_{p,\Pi}$ has conductor $p + 1$, by [3, Theorem 6.3], we have

$$n \equiv \frac{1}{p} \text{Tr}_{K_\Pi/\mathbb{Q}_p} \left(\left((1 - p^{p-1})T^p \frac{Dg_1}{g_1} \right) \Big|_{T=\Pi'} \right) \equiv \frac{1}{p} \text{Tr}_{K_\Pi/\mathbb{Q}_p} \left(\left(T^p \frac{Dg_1}{g_1} \right) \Big|_{T=\Pi'} \right) \pmod{p}.$$

It follows from [3, Lemma 6.5] that (There is a sign error in this lemma: indeed, the expression for $D[a]/[a]$ in [3, p. 91] has a sign error.)

$$n \equiv \frac{1}{p} \text{Tr}_{K_\Pi/\mathbb{Q}_p} (\Pi'^{p-1}) \pmod{p}.$$

On the other hand,

$$\begin{aligned} \text{Tr}_{K_\Pi/\mathbb{Q}_p} (\Pi'^{p-1}) &= \sum_{j=1}^{p-1} (1 - \omega^j)^{p-1} \\ &= p - 1 + \sum_{i=1}^{p-1} \binom{p-1}{i} (-1)^i (\omega^i + \omega^{2i} + \cdots + \omega^{(p-1)i}) \\ &= p - 1 + \sum_{i=1}^{p-1} \binom{p-1}{i} (-1)^{i+1} \\ &= p - \sum_{i=0}^{p-1} \binom{p-1}{i} (-1)^i = p. \end{aligned}$$

So

$$n \equiv 1 \pmod{p},$$

and hence

$$\chi_{\delta,\Pi}(1 + \Pi^p) = \omega^{2a}. \quad \square$$

For any prime ℓ , denote

$$\chi_{\delta,\ell} = \prod_{V|\ell} \chi_{\delta,V}$$

where V runs through the places of K above ℓ .

Proposition 3.6. *For any prime ℓ , we have $\chi_{\delta,\ell}(\Pi) = 1$.*

Proof. If $\ell = \infty$, this is clear because the infinite factor $\chi_{\delta,\infty} = 1$. Next we assume ℓ is finite. By our choice of Π , we have $\Pi^2 \in F$. By Lemma 3.2,

$$\chi_{\delta,\ell}(\Pi^2) = 1, \text{ i.e. } \chi_{\delta,\ell}(\Pi) = \pm 1.$$

On the other hand, by definition, we know $\chi_{\delta,\ell}(\Pi)$ is a p -th root of unity, and we conclude $\chi_{\delta,\ell}(\Pi) = 1$. $\square$

3.3. Local root numbers outside p

For any finite place v resp. V of F resp. K outside p , denote by ϖ_v resp. Π_V the corresponding uniformizers of F_v resp. K_V .

We fix an additive character ψ_{K_V} of K_V for each place V of K as follows: If V is archimedean, then

$$\psi_{K_V}(x) = e^{-2\pi i \text{Tr}_{K_V/\mathbb{R}}(x)};$$

If V is non-archimedean and dividing ℓ , then

$$\psi_{K_V}(x) = \psi_\ell(\text{Tr}_{K_V/\mathbb{Q}_\ell}(x)),$$

where ψ_ℓ is as in (3.4). Then the product $\psi = \prod_V \psi_{K_V}$ is an additive character on $K \backslash \mathbb{A}_K$. The L-function $L(s, \phi_\delta)$ satisfies a functional equation

$$L(s, \phi_\delta) = \epsilon(s, \phi_\delta) L(1-s, \phi_\delta^{-1}).$$

The epsilon-factor admits a local product

$$\epsilon(s, \phi_\delta) = \prod_V \epsilon(s, \phi_{\delta,V}, \psi_{K_V}),$$

and the epsilon-factor $\epsilon(s, \phi_\delta)$ is independent of the choices of ψ_{K_V} .

Let V be an infinite place of K . Then

$$K_V \simeq \mathbb{C}, \quad \phi_{\delta,V}(z) = z^{-1} |z|_{\mathbb{C}}^{1/2},$$

and, from [4, (3.3.3), (3.4.2)] or [9, p. 97], we have

$$\epsilon(1/2, \phi_{\delta,V}, \psi_{K_V}) = i^{-1}. \quad (3.7)$$

For a place $V \nmid p\delta$ of K , $\phi_{\delta,V}$ is unramified, and we have by (3.1) that

$$\epsilon(1/2, \phi_{\delta,V}, \psi_{K_V}) = 1. \quad (3.8)$$

Let V be a place where $\phi_{\delta,V}$ is ramified. Simply denote $c_V = c(\phi_{\delta,V})$ and $n_V = n(\psi_{K_V})$. It follows from (3.2) that

$$\begin{aligned} \epsilon(1/2, \phi_{\delta,V}, \psi_{K_V}) &= \phi_{\delta,V}(\Pi_V)^{n_V+c_V} q_V^{\frac{n_V-c_V}{2}} \\ &\quad \times \int_{\mathcal{O}_{K,V}} dx \sum_{a \in \mathcal{O}_{K,V}^\times / (1+\Pi_V^{c_V} \mathcal{O}_{K,V})} \phi_{\delta,V}^{-1}(a) \psi_{K_V} \left(\frac{a}{\Pi_V^{n_V+c_V}} \right). \end{aligned} \quad (3.9)$$

Since ϕ is unramified outside p , it follows immediately from the above formula that

Lemma 3.7. *For any place $V \nmid p$, we have*

$$\epsilon(1/2, \phi_{\delta,V}, \psi_{K_V}) = \epsilon(1/2, \chi_{\delta,V}, \psi_{K_V}) \phi_V(\Pi_V)^{n_V+c_V}.$$

Proof. This lemma follows from (3.9) by noting that $\phi_\delta = \phi \chi_\delta^{r+s}$ and that ϕ is unramified at the place V . $\square$

In order to compute the local root numbers for $\phi_{\delta,V}$ for $V \nmid p$ and $V \mid \delta$, it suffices to compute $\phi_V(\Pi_V)$ and $\epsilon(1/2, \chi_{\delta,V}, \psi_{K_V})$ for these places. Since our choice of Π satisfies (3.3), by Proposition 3.1, for any finite place V of K ,

$$\epsilon(1/2, \chi_{\delta,V}, \psi_{K_V}) = \chi_{\delta,V}(\Pi) = 1, \quad (3.10)$$

which is given by Proposition 3.6. So it remains to compute the values of $\phi_V(\Pi_V)$ for $V \neq \Pi$.

Proposition 3.8. *Let $v \neq \pi$ be a finite place of F . If v is inert in K , let V be the unique place above v . Then*

$$\phi_V(\Pi_V) = -1.$$

If v is split in K , let V and $\overline{V}$ be two distinct places above v . Then

$$\phi_V(\Pi_V) \phi_{\overline{V}}(\Pi_{\overline{V}}) = +1.$$

Proof. First suppose v is inert in K . The prime ideal V of K is fixed by the complex conjugation. By the Stickelberger relation (2.1) and the fact that $\Phi_{r,s,t}$ is a CM-type, i.e. a set of coset representatives of $(\mathbb{Z}/p\mathbb{Z})^\times$ modulo $\{\pm 1\}$, $j_{r,s,t}(V)$ generates the same ideal as $q_v = q_V^{1/2}$. Hence

$$j_{r,s,t}(V) = uq_v$$

for some unit $u \in \mathcal{O}_K^\times$. Since u has absolute value 1 for any complex embedding, it must be a root of unity. Note $q_v \equiv -1 \pmod{p}$. Then the congruence

$$j_{r,s,t}(V) \equiv 1 \pmod{\Pi^2}$$

forces $u = -1$. Then

$$\phi_V(\Pi_V) = j_{r,s,t}(V) \cdot q_V^{-1/2} = -1.$$

Next, we suppose v is split in K . Then by definition we have

$$\phi_V(\Pi_V) \equiv - \sum_{\substack{x \in \mathcal{O}_K/V \\ x \neq 0,1}} (x^r(1-x)^s)^{\frac{q_V-1}{p}} \pmod{V},$$

and

$$\phi_{\overline{V}}(\Pi_{\overline{V}}) \equiv - \sum_{\substack{x \in \mathcal{O}_K/\overline{V} \\ x \neq 0,1}} (x^r(1-x)^s)^{\frac{q_{\overline{V}}-1}{p}} \pmod{\overline{V}}.$$

Since v is split in K , we have natural identities

$$\mathcal{O}/v = \mathcal{O}_K/V = \mathcal{O}_K/\overline{V},$$

and we may take the representatives in $\mathcal{O}$ for each x . Taking complex conjugation, we have then

$$\overline{\phi_{\overline{V}}(\Pi_{\overline{V}})} \equiv - \sum_{\substack{x \in \mathcal{O}_K/\overline{V} \\ x \neq 0,1}} (x^r(1-x)^s)^{\frac{q_v-1}{p}} \pmod{V}.$$

So we have

$$\overline{\phi_{\overline{V}}(\Pi_{\overline{V}})} = \phi_V(\Pi_V),$$

and hence

$$\phi_V(\Pi_V)\phi_{\overline{V}}(\Pi_{\overline{V}}) = +1 \quad \square$$

Corollary 3.9. *Denote*

$$\phi_\ell = \prod_{V|\ell} \phi_V(\Pi_V)$$

for each prime $\ell \neq p$. Then

$$\phi_\ell = \left(\frac{\ell}{p}\right).$$

Proof. Let f be the order of ℓ in $\mathbb{F}_p^\times$. Then f is the inertia degree of the places of K above ℓ . If $\left(\frac{\ell}{p}\right) = +1$, then $(p-1)/f$ is even, i.e. there are even places of K above ℓ . Then it follows from Lemma 3.3 and Proposition 3.8 that if all the places of F above ℓ are split in K ,

$$\phi_\ell = (+1)^{(p-1)/2f} = +1,$$

and if all the places of F above ℓ are inert in K ,

$$\phi_\ell = (-1)^{(p-1)/f} = +1.$$

If $\left(\frac{\ell}{p}\right) = -1$, then $(p-1)/f$ is odd. By Lemma 3.3, the places of K above ℓ must be inert in the quadratic extension K/F . Then in this case we have

$$\phi_\ell = (-1)^{(p-1)/f} = -1. \quad \square$$

Recall we simply denote $c_V = c(\phi_{\delta,V})$ and $n_V = n(\psi_{K_V})$ for any place V of K .

Lemma 3.10.

1. The conductors $n_\Pi = 1$ and $n_V = 0$ for all $V \neq \Pi$.
2. The conductors $c_V = 0$ if $V \nmid p\delta$, $c_V = 1$ if $V \mid \delta$ but $V \neq \Pi$, and

$$c_\Pi = \begin{cases} \leq 2, & \text{if } p \nmid \delta; \\ p+1, & \text{if } p \mid \delta. \end{cases}$$

Proof. Recall the relative different $\partial_{K/F}$ is defined to be the integral ideal of K such that

$$\partial_{K/F}^{-1} = \{x \in K \mid \text{tr}_{K/F}(xy) \in \mathcal{O}_F \text{ for all } y \in \mathcal{O}_F\}.$$

It follows from the discriminant formula

$$d_K = d_F^2 \cdot N_{K/\mathbb{Q}}(\partial_{K/F})$$

that $N_{K/\mathbb{Q}}(\partial_{K/F}) = (p)$, and hence $\partial_{K/F} = (\Pi)$. By the definition of ψ_{K_V} , n_V is the exponent of $\partial_{K/F}$ at V . Then the values for n_V follow. The second assertion follows from Proposition 3.4 and the conductors of ϕ . $\square$

Let ℓ be a prime number, including the infinity place ∞ . Denote

$$\epsilon_\ell(\phi_{r,s,t;\delta}) = \prod_{V|\ell} \epsilon(1/2, \phi_{r,s,t;\delta,V}, \psi_{K_V})$$

where V runs through the places of K above ℓ .

Proposition 3.11. *Let $\ell \neq p$ be a prime number.*

1. *If $\ell = \infty$ is archimedean, then*

$$\epsilon_\infty(\phi_{r,s,t;\delta}) = i^{-\frac{p-1}{2}};$$

If ℓ is a finite prime with $\ell \nmid p\delta$, then

$$\epsilon_\ell(\phi_{r,s,t;\delta}) = 1;$$

2. *If $\ell \neq p$ and $\ell \mid \delta$, then*

$$\epsilon_\ell(\phi_{r,s,t;\delta}) = \left(\frac{\ell}{p}\right).$$

Proof. The first assertion is just (3.7) and (3.8). By Lemma 3.7 and Lemma 3.10,

$$\epsilon(1/2, \phi_{\delta,V}, \psi_{K_V}) = \epsilon(1/2, \chi_{\delta,V}, \psi_{K_V}) \phi_V(\Pi_V)$$

for any finite place $V \neq \Pi$ and $V \mid \delta$. Then the remaining follows from (3.10) and Corollary 3.9. $\square$

3.4. Local root number at p

Let η be the quadratic character of $F^\times \backslash \mathbb{A}^\times$ determined by the quadratic extension K/F through class-field theory. Then η is unramified outside p . For any finite place v of F not dividing p , we have

$$\epsilon(1/2, \eta_v) = +1. \quad (3.11)$$

For each archimedean place $\tau : F \hookrightarrow \mathbb{R}$, we have

$$F_\tau \simeq \mathbb{R}, \text{ and } \eta_\tau(x) = \frac{|x|}{x}, x \neq 0.$$

Then we have by [9, p. 97] that

$$\epsilon(1/2, \eta_\tau, \psi_{\mathbb{R}}) = i^{-1}. \quad (3.12)$$

Finally, for the place π , we have

$$\epsilon(1/2, \eta_\pi, \psi_{F_\pi}) = i^{\frac{p-1}{2}}. \quad (3.13)$$

The character ϕ is equivariant with respect to the complex conjugation. In particular, we have

$$\phi|_{\mathbb{A}^\times} = \eta.$$

Since

$$\chi_\delta|_{\mathbb{A}^\times} = 1,$$

we have

$$\phi_\delta = \phi\chi_\delta^{r+s}|_{\mathbb{A}^\times} = \eta.$$

Recall for any $\delta \in \mathbb{Q}^\times \cap \mathbb{Z}_p$, we have the following decomposition in $\mathbb{Q}_p^\times$:

$$\delta = \epsilon p^a (1-p)^b$$

with $\epsilon \in \mathbb{F}_p^\times \subset \mathbb{Q}_p^\times$, $a \in \{0, 1, \dots, p-1\}$, and $b \in \mathbb{Z}_p$. We have defined in (3.5) that

$$u(\delta) = \min(\text{ord}_p(a), \text{ord}_p(b) + 1).$$

Proposition 3.12.

1. If

$$u(r^r s^s (t-p)^t \delta^{r+s}) \geq 2,$$

then $c(\phi_{\delta, \Pi}) = 1$, and

$$\epsilon(1/2, \phi_{\delta, \Pi}, \psi_{K_\Pi}) = \left(\frac{2}{p}\right) i^{\frac{p-1}{2}}.$$

2. If

$$u(r^r s^s (t-p)^t \delta^{r+s}) = 1,$$

then $c(\phi_{\delta, \Pi}) = 2$, and

$$\epsilon(1/2, \phi_{\delta, \Pi}, \psi_{K_{\Pi}}) = - \left(\frac{-rstd}{p} \right) i^{\frac{p-1}{2}},$$

where

$$d \equiv \frac{(r^r s^s (t-p)^t \delta^{r+s})^{p-1} - 1}{p} \pmod{p}.$$

3. If

$$u(r^r s^s (t-p)^t \delta^{r+s}) = u(\delta^{r+s}) = 0,$$

then $c(\phi_{\delta, \Pi}) = p + 1$, and

$$\epsilon(1/2, \phi_{\delta, \Pi}, \psi_{K_{\Pi}}) = - \left(\frac{rstd}{p} \right) i^{\frac{p-1}{2}},$$

where

$$d \equiv (r+s) \text{ord}_p(\delta) \pmod{p}.$$

Proof. First we clarify the conditions for the conductors of $\phi_{\delta, \Pi}$. By [3, Theorem 5.3], for any $x \in \mathcal{O}_{K, \Pi}^{\times}$,

$$\phi_{\delta, \Pi}(x) = \left(\frac{x, r^r s^s (t-p)^t \delta^{r+s}}{K_{\Pi}; p} \right) \left(\frac{x, \Pi}{K_{\Pi}; 2} \right). \quad (3.14)$$

Then the statement on the conductors $c(\phi_{\delta, \Pi})$ follows from Proposition 3.4 by noting that the character

$$x \mapsto \left(\frac{x, \Pi}{K_{\Pi}; 2} \right)$$

has conductor 1.

If $c(\phi_{\delta, \Pi}) = 1$, then by [14, Proposition 2]

$$\frac{\epsilon(1/2, \phi_{\delta, \Pi}, \psi_{K_{\Pi}})}{\epsilon(1/2, \eta_{\pi}, \psi_{F_{\pi}})} = \left(\frac{2}{p} \right),$$

and the first assertion follows by (3.13).

Again by [14, Proposition 2], if $c(\phi_{\delta, \Pi}) = c > 1$, then

$$\frac{\epsilon(1/2, \phi_{\delta, \Pi}, \psi_{K_{\Pi}})}{\epsilon(1/2, \eta_{\pi}, \psi_{F_{\pi}})} = \left(\frac{-2l}{p} \right) \phi_{\delta, \Pi}(\Pi)^{c-1} i^u, \quad (3.15)$$

where u is given by

$$u = \begin{cases} 0, & \text{if } p \equiv 1 \pmod{4}; \\ 1, & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

and l is given by

$$\phi_{\delta, \Pi}(1 + \Pi^{c-1}) = \omega^l.$$

We compute the values of $\phi_{\delta, \Pi}(\Pi) = \phi_{\Pi}(\Pi)\chi_{\delta, \Pi}^{r+s}(\Pi)$. By Proposition 3.6, it suffices to compute $\phi_{\Pi}(\Pi)$. Since ϕ is a Hecke character unramified outside Π and infinity, we have

$$\phi_{\Pi}(\Pi) = \prod_{V|\infty} \phi_V(\Pi)^{-1} = \prod_{h \in \Phi^{-1}} \frac{\Pi^{\sigma_h}}{|\Pi^{\sigma_h}|_{\mathbb{C}}^{1/2}} = \prod_{h \in \Phi^{-1}} i \cdot \operatorname{sgn}(\sin(2\pi h/p)) = i^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}-k},$$

where k denotes the number of $h \in \Phi^{-1}$ satisfying $1 \leq h \leq (p-1)/2$. By [14, Proposition 4],

$$(-1)^k = -\left(\frac{-2rst}{p}\right).$$

Next we determine the value of l . Suppose $c(\phi_{\delta, \Pi}) = 2$, or equivalently, $u(r^r s^s(t-p)^t \delta^{r+s}) = 1$. By (3.14),

$$\phi_{\delta, \Pi}(1 + \Pi) = \left(\frac{1 + \Pi, r^r s^s(t-p)^t \delta^{r+s}}{K_{\Pi}; p} \right).$$

Then by Proposition 3.5,

$$\phi_{\delta, \Pi}(1 + \Pi) = \omega^{2 \left(\frac{(r^r s^s(t-p)^t \delta^{r+s})^{p-1} - 1}{p} \right)}.$$

In this case, we have

$$l \equiv 2 \frac{(r^r s^s(t-p)^t \delta^{r+s})^{p-1} - 1}{p} \pmod{p}.$$

Then the formula in the second assertion follows by noting

$$i^{\frac{p-1}{2}+u} = \left(\frac{2}{p}\right) \text{ and } \epsilon(1/2, \eta_{\pi}, \psi_{F_{\pi}}) = i^{\frac{p-1}{2}}.$$

Finally, suppose $c(\phi_{\delta, \Pi}) = p+1 \geq 4$. Since ϕ_{Π} has conductor 1 or 2,

$$\phi_{\delta, \Pi}(1 + \Pi^{c-1}) = \chi_{\delta, \Pi}^{r+s}(1 + \Pi^p).$$

Then by Proposition 3.5,

$$\phi_{\delta, \Pi}(1 + \Pi^{c-1}) = \omega^{2(r+s)\text{ord}_p(\delta)},$$

and in this case,

$$l \equiv 2(r+s)\text{ord}_p(\delta) \pmod{p}.$$

Then the formula in the third assertion follows by noting

$$i^{\frac{p(p-1)}{2}+u} = \left(\frac{-2}{p}\right) \text{ and } \epsilon(1/2, \eta_\pi, \psi_{F_\pi}) = i^{\frac{p-1}{2}}. \quad \square$$

3.5. Global root numbers

Fix the triple (r, s, t) of integers with $r, s, t > 0$ and $r + s + t = p$. For any prime ℓ of $\mathbb{Q}$, denote

$$\begin{aligned} \epsilon_\ell(\phi_{r,s,t;\delta}) &= \prod_{V|\ell} \epsilon(1/2, \phi_{r,s,t;\delta,V}, \psi_{K_V}), \\ \epsilon_\ell(\pi_{r,s,t;\delta}) &= \prod_{v|\ell} \epsilon(1/2, \pi_{r,s,t;\delta,v}, \psi_{F_v}), \end{aligned}$$

where V resp. v runs through all places of K resp. F above ℓ . Then by [9, Lemma 1.2, Theorem 4.7], we have

$$\epsilon_\ell(\pi_{r,s,t;\delta}) = \epsilon_\ell(\phi_{r,s,t;\delta}) \epsilon_\ell(\eta). \quad (3.16)$$

Let $d \in (\mathbb{Z}/p\mathbb{Z})^\times$ be residue class given by

$$d = \begin{cases} \frac{(r^r s^s (t-p)^t \delta^{r+s})^{p-1} - 1}{p} \pmod{p}, & \text{if } u(r^r s^s (t-p)^t \delta^{r+s}) = 1; \\ (r+s)\text{ord}_p(\delta) \pmod{p}, & \text{if } u(r^r s^s (t-p)^t \delta^{r+s}) = 0. \end{cases}$$

Theorem 3.13. *The global root number of the automorphic representation $\pi_{r,s,t;\delta}$ is given as follows:*

$$\epsilon_{r,s,t;\delta} = \prod_{\ell} \epsilon_\ell(\pi_{r,s,t;\delta}),$$

where

$$\epsilon_\ell(\pi_{r,s,t;\delta}) = \begin{cases} \left(\frac{-1}{p}\right), & \text{if } \ell = \infty; \\ \left(\frac{\ell}{p}\right), & \text{if } \ell \neq p \text{ and } \ell \mid \delta; \\ +1, & \text{if } \ell \nmid p\delta; \end{cases}$$

and

$$\epsilon_p(\pi_{r,s,t;\delta}) = \begin{cases} -\left(\frac{-rstd}{p}\right), & \text{if } u(r^r s^s (t-p)^t \delta^{r+s}) = 0; \\ -\left(\frac{rstd}{p}\right), & \text{if } u(r^r s^s (t-p)^t \delta^{r+s}) = 1; \\ \left(\frac{-2}{p}\right), & \text{if } u(r^r s^s (t-p)^t \delta^{r+s}) \geq 2. \end{cases}$$

Proof. Taking the relation (3.16) into account, this is the combination of Propositions 3.11 and 3.12 and the formulae ((3.11)-(3.13)). $\square$

In the special case $\delta = 1$, these formulae are compatible with those in [7,14]. Next suppose $p = 3$, $r = s = t = 1$ and $\delta \in \mathbb{Q}^\times / \mathbb{Q}^{\times 3}$. The Fermat curve

$$F_\delta : X^3 + Y^3 = \delta$$

and the quotient curve $C_{1,1,1;\delta}$ are both elliptic curves over $\mathbb{Q}$ and $\varphi_{1,1,1} : F_\delta \rightarrow C_{1,1,1;\delta}$ is an isogeny over $\mathbb{Q}$ of degree 3. The elliptic curve F_δ has Weierstrass equation

$$y^2 = x^3 - 2^4 3^3 \delta^2.$$

Corollary 3.14. *Let δ be a cube-free integer. The global root number of the elliptic curve F_δ is given by*

$$\epsilon = \prod_{\ell | \infty 3 \delta} \epsilon_\ell$$

where

$$\epsilon_\infty = -1;$$

and if $\ell \neq 3$ and $\ell \mid \delta$, then

$$\epsilon_\ell = \left(\frac{\ell}{3}\right);$$

and

$$\epsilon_3 = \begin{cases} -1, & \text{if } \delta \equiv \pm 1 \pmod{9}, \text{ or } \text{ord}_3(\delta) = 1; \\ +1, & \text{otherwise.} \end{cases}$$

Proof. It suffices to translate the expressions of ϵ_3 from Theorem 3.13, since the expressions for ϵ_ℓ are clear for $\ell \neq 3$. In this case, we have $r = s = t = 1$. First suppose $u(r^r s^s (t-p)^t \delta^{r+s}) = 0$ i.e. $a = \text{ord}_3(\delta) > 0$. Then

$$\epsilon_3 = -\left(\frac{-2a}{3}\right),$$

and $\epsilon_3 = -1$ if and only if $a = 1$. Next suppose $u(r^r s^s (t-p)^t \delta^{r+s}) = 1$. Then

$$\epsilon_3 = -\left(\frac{d}{3}\right),$$

and it is straight-forward to verify that $\epsilon_3 = -1$ if and only if $\delta \equiv \pm 1 \pmod{9}$. Finally, if $u(r^r s^s (t-p)^t \delta^{r+s}) = 2$, then

$$\epsilon_3 = \left(\frac{-2}{3}\right) = +1.$$

Combining all these, the corollary follows. $\square$

This is compatible with the results of Birch-Stephens [1,18] and Liverance [11] which gives the formulae for root numbers of the elliptic curves with Weierstrass equation

$$y^2 = x^3 + D$$

for $D \in \mathbb{Q}^\times / \mathbb{Q}^{\times 6}$.

3.6. Equidistribution of root numbers

When $p = 3$ ($r = s = t = 1$), L. Mai [12] proved that the set $\{\delta \text{ cube-free} : \epsilon_{1,1,1;\delta} = +1\}$ has density $1/2$ in the set of cube-free integers. For a general odd prime p , the curves $C_{1,1;p-2;\delta}$, $C_{1,(p-1)/2,(p-1)/2;\delta}$ and $C_{1,p-2,1;\delta}$ are hyperelliptic curves and the sign of the functional equation of L-functions of these curves can be obtained by [19]. Following the strategy of L. Mai, T. Jedrzejak [10] generalized the result of L. Mai for the families $J_{1,1;p-2;\delta}$, $J_{1,(p-1)/2,(p-1)/2;\delta}$ and $J_{1,p-2,1;\delta}$ with $p \nmid \delta$. The constrain $p \nmid \delta$ comes from the calculations of root numbers in [19].

As an application of the general formulae for root numbers of $J_{r,s,t;\delta}$ given in Theorem 3.13, following the strategy and results in [12,10], we obtain the following density of root numbers of the families $J_{r,s,t;\delta}$ with δ varying in the set of p -th power-free integers.

Let $\mathbb{N}^{(p)}$ be the set of p -th power-free positive integers, which has positive density in the set of natural numbers (see for example [10, Lemma 4]). Denote by $\mathbb{N}_0^{(p)} \subset \mathbb{N}^{(p)}$ the subset consisting of integers with p -adic valuation 0. Then

$$\mathbb{N}^{(p)} = \bigcup_{i=0}^{p-1} p^i \mathbb{N}_0^{(p)}.$$

Theorem 3.15.

$$\lim_{X \rightarrow +\infty} \frac{\#\{\delta \in \mathbb{N}^{(p)} : \delta \leq X \text{ and } \epsilon_{r,s,t;\delta} = +1\}}{\#\{\delta \in \mathbb{N}^{(p)} : \delta \leq X\}} = \frac{1}{2}.$$

For $\delta \in \mathbb{N}^{(p)}$, set

$$\tau_p(\delta) = \# \left\{ \ell \mid \delta : \ell \neq p \text{ and } \left(\frac{\ell}{p} \right) = -1 \right\}.$$

If $\delta = p^i \delta_0$ with $(p, \delta_0) = 1$, then it is clear that $\tau_p(\delta)$ is determined by δ_0 . Define $\alpha_p(\delta) = 0, 1$ by the formula

$$\epsilon_{r,s,t;\delta} = (-1)^{\alpha_p(\delta) + \tau_p(\delta)}.$$

Lemma 3.16. Suppose $\delta = p^i \delta_0 \in \mathbb{N}^{(p)}$ is a p -th power-free integer with $(p, \delta_0) = 1$. Then $\alpha_p(\delta)$ depends on $(\text{ord}_p(\delta), \delta_0 \bmod p^2)$.

Proof. By the formulae for the root number $\epsilon_{r,s,t;\delta}$ in Theorem 3.13, if we write

$$\epsilon_{r,s,t;\delta} = (-1)^{\alpha_p(\delta) + \tau_p(\delta)},$$

then

$$(-1)^{\alpha_p(\delta)} = \begin{cases} - \left(\frac{-rs \cdot \text{ord}_p(\delta)}{p} \right), & \text{if } \text{ord}_p(\delta) > 0; \\ - \left(\frac{-rst \left(\frac{(r^r s^s (r+s)^t \delta^{r+s})^{p-1} - 1}{p} \right)}{p} \right), & \text{if } u(r^r s^s (t-p)^t \delta^{r+s}) = 1; \\ \left(\frac{2}{p} \right), & \text{if } u(r^r s^s (t-p)^t \delta^{r+s}) \geq 2. \end{cases}$$

It follows from these formulae that $\alpha_p(\delta)$ depends on $(\text{ord}_p(\delta), \delta_0 \bmod p^2)$. $\square$

Proof of Theorem 3.15. In fact, we will prove for each $i = 0, 1, \dots, p-1$ that

$$\begin{aligned} & \lim_{X \rightarrow +\infty} \frac{\#\{\delta \in p^i \mathbb{N}_0^{(p)} : \delta \leq X \text{ and } \epsilon_{r,s,t;\delta} = +1\}}{\#\{\delta \in p^i \mathbb{N}_0^{(p)} : \delta \leq X\}} \\ &= \lim_{X \rightarrow +\infty} \frac{\#\{\delta \in \mathbb{N}_0^{(p)} : \delta \leq X \text{ and } \epsilon_{r,s,t;p^i \delta} = +1\}}{\#\{\delta \in \mathbb{N}_0^{(p)} : \delta \leq X\}} = \frac{1}{2}. \end{aligned}$$

For fixed i , by Lemma 3.16, we can define S_i^+ resp. S_i^- to be the subset of $(\mathbb{Z}/p^2\mathbb{Z})^\times$ such that $\alpha_p(p^i \delta_0) = 0$, resp. 1 for $\delta_0 \in S_i^+$ resp. S_i^- . Then $S_i^+ \cap S_i^- = \emptyset$ and $S_i^+ \cup S_i^- = (\mathbb{Z}/p^2\mathbb{Z})^\times$. For a sufficiently large integer X , denote

$$\mathbb{N}_{0,X}^{(p)} = \{\delta \in \mathbb{N}_0^{(p)} : \delta \leq X\}.$$

Then we have

$$\sum_{\substack{\delta \in \mathbb{N}_{0,X}^{(p)} \\ \epsilon_{r,s,t;p^i\delta}=1}} 1 = \sum_{\substack{\delta \in \mathbb{N}_{0,X}^{(p)} \\ \tau_p(\delta) \text{ even} \\ \delta \bmod p^2 \in S_i^+}} 1 + \sum_{\substack{\delta \in \mathbb{N}_{0,X}^{(p)} \\ \tau_p(\delta) \text{ odd} \\ \delta \bmod p^2 \in S_i^-}} 1. \quad (3.17)$$

Fix $k \in (\mathbb{Z}/p^2\mathbb{Z})^\times$. As in [10, Proof of Theorem 1], we have

$$\sum_{\substack{\delta \in \mathbb{N}_{0,X}^{(p)} \\ (-1)^{\tau_p(\delta)} = \pm 1 \\ \delta \equiv k \bmod p^2}} 1 = \frac{1}{2} \sum_{\substack{\delta \in \mathbb{N}_{0,X}^{(p)} \\ \delta \equiv k \bmod p^2}} 1 + O(\sqrt{X} \log^{p-2} X).$$

Then by (3.17) and [10, Lemma 5], we obtain

$$\begin{aligned} \sum_{\substack{\delta \in \mathbb{N}_{0,X}^{(p)} \\ \epsilon_{r,s,t;p^i\delta}=1}} 1 &= \frac{1}{2} \sum_{\substack{\delta \in \mathbb{N}_{0,X}^{(p)} \\ \delta \bmod p^2 \in S_i^+}} 1 + \frac{1}{2} \sum_{\substack{\delta \in \mathbb{N}_{0,X}^{(p)} \\ \delta \bmod p^2 \in S_i^-}} 1 + O(\sqrt{X} \log^{p-2} X) \\ &= \frac{1}{2} \sum_{\delta \in \mathbb{N}_{0,X}^{(p)}} 1 + O(\sqrt{X} \log^{p-2} X). \quad \square \end{aligned}$$

Acknowledgments

The author would like to thank Benedict Gross and Ye Tian for helpful communications. The author also thanks the referee for his/her patience and helpful advices.

References

- [1] B.J. Birch, N.M. Stephens, The parity of the Mordell-Weil group, *Topology* 5 (4) (1966) 295–299.
- [2] R. Coleman, The dilogarithm and the norm residue symbol, *Bull. Soc. Math. Fr.* 109 (1981) 373–402.
- [3] R. Coleman, W. McCallum, Stable reduction of Fermat curves and Jacobi sum Hecke characters, *J. Reine Angew. Math.* 385 (1988) 41–101.
- [4] P. Deligne, Les constantes des équations fonctionnelles des fonctions L, in: *Modular Functions of One Variable, II*, in: *Lecture Notes in Mathematics*, vol. 349, 1973, pp. 501–598.
- [5] A. Fröhlich, J. Queyrut, On the functional equation of Artin L-function for characters of real representations, *Invent. Math.* 20 (1973) 125–138.
- [6] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, *Lect. Notes Math.* 751 (1979) 108–118.
- [7] B.H. Gross, D.E. Rohrlich, Some results on the Mordell-Weil group of the Jacobian of the Fermat curve, *Invent. Math.* 44 (1978) 201–224.
- [8] K. Iwasawa, On explicit formulas for the norm residue symbol, *J. Math. Soc. Jpn.* 20 (1–2) (1968) 151–165.
- [9] H. Jacquet, R.P. Langlands, *Automorphic Forms on GL(2): Part 1*, 1st edition, *Lecture Notes in Mathematics*, vol. 2, Springer, 1970.
- [10] T. Jedrzejak, The analytic rank of a family of Jacobians of Fermat curves, *Bull. Pol. Acad. Sci., Math.* 56 (2008) 199–206.
- [11] E. Liverance, A formula for the root number of a family of elliptic curves, *J. Number Theory* 51 (2) (1995) 288–305.
- [12] L. Mai, The analytic rank of a family of elliptic curves, *Can. J. Math.* 45 (4) (1993) 847–862.
- [13] D.E. Rohrlich, The periods of the Fermat curve, Appendix to B. Gross, *Invent. Math.* 45 (1978) 193–211.

- [14] D.E. Rohrlich, Root numbers of Jacobi-sum Hecke characters, *Ill. J. Math.* 36 (1) (1992) 155–176.
- [15] R.T. Sharifi, On norm residue symbols and conductors, *J. Number Theory* 86 (2) (2001) 196–209.
- [16] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, Princeton, NJ, 1996.
- [17] J. Shu, Selmer groups and the parity conjectures for Jacobian varieties of Fermat curves, preprint, 2019.
- [18] N.M. Stephens, The Diophantine equation $X^3 + Y^3 = DZ^3$ and the conjectures of Birch and Swinnerton-Dyer, *J. Reine Angew. Math.* 231 (1968) 121–162.
- [19] M. Stoll, On the arithmetic of the curves $y^2 = x^\ell + A$, II, *J. Number Theory* (1993) 183–206.
- [20] J. Tate, Fourier analysis in number fields and Hecke’s Zeta-functions, in: *Algebraic Number Theory*, Proc. of the Brighton Conference, 1968, pp. 305–347, chapter XV.
- [21] J. Tate, Number theoretic background, in: *Proceedings of Symposia in Pure Mathematics*, vol. 33, II, 1979, pp. 3–26.
- [22] A. Weil, Jacobi sums as “grossencharaktere”, *Trans. Am. Math. Soc.* 73 (1952) 487–495.