Functiones et Approximatio
46.2 (2012), 235–260
doi: 10.7169/facm/2012.46.2.8

DIVISOR FUNCTIONS OVER QUATERNION ALGEBRAS AND A TYPE OF IDENTITIES

Yichao Zhang

Abstract: In order to prove a result on fourth moments of modular L-functions, Duke derived an identity of the divisor function over the rational Hamiltonian quaternion algebra. Recently Kim and the author generalized Duke's divisor function, the identity and other related results from level two to general prime level. In this note, we consider such identities in general.

Keywords: divisor function, quaternion algebra, modular form, L-function, fourth moments.

1. Introduction

In 1988, Duke [1] gave a sharp bound on average for the fourth moments of L-functions attached to newforms of level 2 by extending Sarnak's method [11] on fourth moments of Grössencharakeren zeta functions. In 2009, Kim and the author [4] were able to generalize Duke's result to general prime level. In both of their works, an identity involving zeta functions and divisor functions over some maximal order of a quaternion algebra plays an important role, namely

$$\sum_{\mathfrak{a}}{}'(d(\mathfrak{a}))^2 N(\mathfrak{a})^{-s} = \frac{\zeta_{\mathcal{O}}^4(s)}{\zeta_{\mathcal{O}}(2s)}.$$

This is analogous to the well-known identity for rational numbers

$$\sum_{n=1}^{\infty}(d(n))^2 n^{-s} = \frac{\zeta^4(s)}{\zeta(2s)}.$$

In this note, we will explore more on this type of identities for orders not necessarily maximal in a rational quaternion algebra. In Section 2, we fix a definite rational quaternion algebra which ramifies precisely at p and ∞ and an order of any fixed level; we calculate then the number of ideals with fixed norm. In Section 3,

2010 Mathematics Subject Classification: primary: 11R52; secondary: 11F11

we further assume that the level of our order is square-free and explore the divisor function for it. As a corollary, we may generalize our result in [4] to square-free level. Our main theorem is

Theorem 1. *Let $\mathfrak{A}$ be the rational quaternion algebra which ramifies precisely at p and ∞, $\mathcal{O}$ be any fixed order of level $N = pM$ with N being square-free. Then*

$$\sum_{\mathfrak{a}}(d(\mathfrak{a}))^2 N(\mathfrak{a})^{-s} = \frac{\zeta_{\mathcal{O}}^4(s)}{\zeta_{\mathcal{O}}(2s)} \prod_{q|M} P(q,s),$$

where

$$P(q,s) = \frac{(1+q^{1-2s})}{(1+q^{-s})(1+q^{1-s})^4(1-q^{1-2s})} \times$$

$$(1+q^{-s}+4q^{1-s}-2q^{1-2s}+8q^{2-2s}-2q^{1-3s}-8q^{2-3s}-2q^{3-3s}-4q^{3-4s}-q^{3-4s}-q^{4-5s}).$$

In the last section, we consider the identity above for the maximal orders $\mathcal{O}$ of a quaternion algebra over any algebraic number field F and we get

Theorem 2.

$$\sum_{\mathfrak{a}}{}'(d(\mathfrak{a}))^2 N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s} = \frac{\zeta_{\mathcal{O}}(s)^4}{\zeta_{\mathcal{O}}(2s)},$$

where the sum is over all nonzero integral left $\mathcal{O}$-ideals.

Please see the notations in corresponding sections.

Acknowledgements. We would like to thank my supervisor Kim for all the support during the work of this note. We also thank the referee for carefully reading this note and providing a few comments.

2. Number of integral ideals with fixed norm

Let N be any non-square positive integer and assume $N = p^{2r+1}M$ with p a prime, $(p, M) = 1$ and r a non-negative integer. Note that any non-square positive integer N has such a decomposition(not unique in general).

Let $\mathfrak{A} = \mathfrak{A}(p)$ be the quaternion algebra over $\mathbb{Q}$ which ramifies precisely at p and ∞. Recall that $\mathfrak{A}_p = \mathfrak{A} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and for a lattice L in $\mathfrak{A}$, $L_p = L \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Let $L/\mathbb{Q}_p$ be the unique unramified quadratic extension with R the ring of integers. Denote by σ the generator of $Gal(L/\mathbb{Q}_p)$ and denote by $\mathcal{O}_{2r+1}^{(p)}$ the order in the algebra $\mathfrak{A}_p$ given by

$$\left\{ \begin{pmatrix} \alpha & p^r\beta \\ p^{r+1}\beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha, \beta \in R \right\}$$

Recall that {all ideals with left order of level N}+{all orders of level N} form a groupoid, with the latter set the set of identities. For definitions of orders, levels, ideals and other concepts we might encounter later, see [2],[6] and [10].

Throughout this section and the next, we fix p, N and $\mathfrak{A}$ as above and we also fix any order $\mathcal{O}$ of level N. Moreover, all ideals are assumed to be integral, unless otherwise specified.

Now we may begin the calculation of the number of integral ideals with fixed norm. Since the number of integral ideals with fixed norm, if considered as a function over positive integers, is multiplicative, it is enough to do the local case. For a prime q, let us denote the number of integral ideals with norm q^n by $a(q,n)$.

First comes the case $q=p$, where we have

$$\mathfrak{A}_p \cong \left\{ \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha,\beta \in L \right\} \quad \text{and} \quad \mathcal{O}_p \cong \left\{ \begin{pmatrix} \alpha & p^r\beta \\ p^{r+1}\beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha,\beta \in R \right\}$$

Proposition 3.

$$a(p,n) = \begin{cases} 1 & \text{if } n = 2m \text{ and } m \geqslant r \\ p^n & \text{if } n = 2m \text{ and } 0 \leqslant m < r \\ p^{2r} & \text{if } n = 2m+1 \text{ and } m \geqslant r \\ 0 & \text{if } n = 2m+1 \text{ and } 0 \leqslant m < r. \end{cases}$$

Proof. We know that there exists a unique maximal order in $\mathfrak{A}_p$, namely, $\mathcal{M}_p = \mathcal{O}_1^{(p)}$. We may assume $\mathcal{O}_p = \mathcal{O}_{2r+1}^{(p)}$, since $a(p,n)$ is invariant under isomorphism. Then it is obvious that

$$\mathcal{M}_p^\times = \left\{ \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha \in R^\times, \beta \in R \right\}$$

and

$$\mathcal{O}_p^\times \cong \left\{ \begin{pmatrix} \alpha & p^r\beta \\ p^{r+1}\beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha \in R^\times, \beta \in R \right\}.$$

We know that there exists a unique ideal in $\mathcal{M}_p$ for any fixed norm p^n, namely, the one generated by $(\alpha_0)^n$, where

$$\alpha_0 = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}.$$

Hence the set of elements in $\mathcal{M}_p$ with norm p^n is $\mathcal{M}_p^\times(\alpha_0)^n$. Now it is obvious that

$$a(p,n) = \#((\mathcal{M}_p^\times(\alpha_0)^n \cap \mathcal{O}_p)/\sim),$$

where $\alpha \sim \beta$ if there exists $\gamma \in \mathcal{O}_p^\times$ such that $\alpha = \gamma\beta$.

If $n = 2m$ and $m \geqslant r$, then $\mathcal{M}_p^\times(\alpha_0)^n = p^m\mathcal{M}_p^\times \subset \mathcal{O}_p$ and $(p^m\mathcal{M}_p^\times/\sim) = \{p^m\}$, so $a(p,n)=1$.

If $n = 2m$ but $0 \leqslant m < r$, then

$$\mathcal{M}_p^\times(\alpha_0)^n \cap \mathcal{O}_p = p^m\mathcal{M}_p^\times \cap \mathcal{O}_p = \left\{ p^m \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha \in R^\times, \beta \in p^{r-m}R \right\},$$

and

$$((\mathcal{M}_p^\times(\alpha_0)^n \cap \mathcal{O}_p)/\sim) = \left\{ p^m \begin{pmatrix} 1 & p^{r-m}\beta \\ p^{r-m+1}\beta^\sigma & 1 \end{pmatrix} : \beta \bmod (p^m) \right\},$$

where $\beta \bmod (p^m)$ means that β runs through a complete set of residue classes for $R/(p^m R)$; hence $a(p,n) = p^{2m} = p^n$.

If $n = 2m+1$ and $m \geqslant r$, then $(\alpha_0)^{2m+1} = p\alpha_0$ and

$$\mathcal{M}_p^\times(\alpha_0)^{2m+1} \cap \mathcal{O}_p = p^m \mathcal{M}_p^\times \alpha_0 = \left\{ p^m \begin{pmatrix} p\beta & \alpha \\ p\alpha^\sigma & p\beta^\sigma \end{pmatrix} : \alpha \in R^\times, \beta \in R \right\}.$$

Hence

$$((\mathcal{M}_p^\times(\alpha_0)^{2m+1} \cap \mathcal{O}_p)/\sim) = \left\{ p^m \begin{pmatrix} p\beta & 1 \\ p & p\beta^\sigma \end{pmatrix} : \beta \bmod (p^r) \right\},$$

so $a(p,n) = p^{2r}$.

If, finally, $n = 2m+1$ and $0 \leqslant m < r$, then $\mathcal{M}_p^\times(\alpha_0)^{2m+1} \cap \mathcal{O}_p = \emptyset$ and $a(p,n) = 0$. Done. ■

Corollary 4.

$$\zeta_{\mathcal{O},p} = \frac{1 - p^{2r(1-s)}}{1 - p^{2(1-s)}} + \frac{p^{-2rs}(1 + p^{2r-s})}{1 - p^{-2s}}.$$

Proof. By above result, this is trivial. ■

Now assume $q|M$ with $v_q(M) = f$. We know that $\mathfrak{A}_q = M(2, \mathbb{Q}_q)$ and we may assume

$$\mathcal{O}_q = \begin{pmatrix} \mathbb{Z}_q & \mathbb{Z}_q \\ q^f\mathbb{Z}_q & \mathbb{Z}_q \end{pmatrix}.$$

Define

$$A = \left\{ \begin{pmatrix} q^l & b \\ q^f c & q^{n-l} \end{pmatrix} : b \bmod q^{n-l},\ c \bmod q^l,\ 0 \leqslant l \leqslant n \right\},$$

where $b \bmod m$ denotes the set $\{0, 1, \cdots, m-1\}$.

Proposition 5. *If $n < f$, elements of A generate distinct integral ideals of norm q^n and they generate all of them, so $a(q,n) = (n+1)q^n$.*

Proof. It is trivial that all elements in A are of norm q^n. Suppose

$$\alpha_1 = \begin{pmatrix} q^{l_1} & b_1 \\ q^f c_1 & q^{n-l_1} \end{pmatrix} \qquad \text{and} \qquad \alpha_2 = \begin{pmatrix} q^{l_2} & b_2 \\ q^f c_2 & q^{n-l_2} \end{pmatrix} \in A$$

generate the same ideal, so there exists $\alpha \in \mathcal{O}_q^\times$ such that $\alpha\alpha_1 = \alpha_2$. It is obvious that α is of the form

$$\begin{pmatrix} a' & b' \\ q^f c' & d' \end{pmatrix}$$

where $a', d' \in \mathbb{Z}_q^\times$ and $b', c' \in \mathbb{Z}_q$. Now we have

$$q^{l_1}a' + q^f b' c_1 = q^{l_2} \tag{1}$$
$$a'b_1 + q^{n-l_1}b' = b_2 \tag{2}$$
$$q^{f+l_1}c' + q^f d' c_1 = q^f c_2 \tag{3}$$
$$q^f c' b_1 + q^{n-l_1}d' = q^{n-l_2}. \tag{4}$$

From (1), by comparing the valuations, we have $l_1 = l_2$, since $f > n \geqslant \max\{l_1, l_2\}$, so $a' = 1 - q^{f-l_1}b'c_1$. Plugging this expression for a' in (2), we get

$$b_1 - b_1 q^{f-l_1}b'c_1 + q^{n-l_1}b' = b_2,$$

which gives $b_1 \equiv b_2 \bmod q^{n-l_1}$, hence $b_1 = b_2$. Similarly, from (3) we have $d' = 1 - q^{f+l_1-n}c'b_1$; plugging this into (4), we get

$$q^{l_1}c' + c_1 - c_1 q^{f+l_1-n}b_1 c' = c_2,$$

so $c_1 \equiv c_2 \bmod q^{l_1}$, hence $c_1 = c_2$.

Now we are left to show that any integral ideal $\mathfrak{a}$ of norm q^n is one of those generated by elements of A. Assume

$$\mathfrak{a} = \mathcal{O}_q \alpha = \mathcal{O}_q \begin{pmatrix} a & b \\ q^f & d \end{pmatrix},$$

where $N(\alpha) = q^n$. Since $f > n$, this implies $v_q(ad) = n$. Denote $l = v_q(a)$, hence $v_q(d) = n - l$ and assume $a = q^l \epsilon_1$, $d = q^{n-l}\epsilon_2$ with $\epsilon_{1,2} \in \mathbb{Z}_q^\times$. Let $\gamma \in \mathcal{O}_q^\times$ be of the form

$$\begin{pmatrix} a' & b' \\ q^f c' & d' \end{pmatrix}, \qquad \text{where } a', d' \in \mathbb{Z}_q^\times,\ b', c' \in \mathbb{Z}_q.$$

Then

$$\gamma\alpha = \begin{pmatrix} q^l\epsilon_1 a' + q^f b' & a'b + q^{n-l}\epsilon_2 b' \\ q^{f+l}\epsilon_1 c' + q^f d' & q^f bc' + q^{n-l}\epsilon_2 d' \end{pmatrix} := \begin{pmatrix} a_1 & b_1 \\ q^f c_1 & d_1 \end{pmatrix}.$$

Since $f > n \geqslant l$, $v_q(a_1) = l$ and if we let $a' = \epsilon_1^{-1}(1 - q^{f-l}b')$(with $b' \in \mathbb{Z}_q$ to be determined latter), then $a' \in \mathbb{Z}_q$ and $a_1 = q^l$. We have

$$b_1 = \epsilon_1^{-1}b + q^{n-l}(\epsilon_2 - q^{f-n}\epsilon_1 b)b'.$$

Since $f > n$, the coefficient of b' has valuation $n - l$, we can choose b' to make b_1 and integer between 0 and $q^{n-l} - 1$; indeed, we may consider the q-adic expression of $\epsilon_1^{-1}b$ and choose b' to get rid of the tail series starting from the power q^{n-l}.

Similarly, we may first choose d' to make $d_1 = q^{n-l}$ and then choose c' to make c_1 an integer between 0 and $q^l - 1$. So $\gamma\alpha \in A$ and we are done. ■

Now let us assume $f \leqslant n$. Denote

$$B_1 = \left\{ \begin{pmatrix} 0 & q^{n-f-t} \\ q^{f+t} & d \end{pmatrix} : d \bmod q^{n-t},\ 0 \leqslant t \leqslant n-f \right\},$$

$$B_2 = \left\{ \begin{pmatrix} q^l & b \\ 0 & q^{n-l} \end{pmatrix} : b \bmod q^{n-l},\ 0 \leqslant l \leqslant n \right\},$$

$$B_3 = \left\{ \begin{pmatrix} q^l & b \\ q^{f+t} & q^{n-l}d \end{pmatrix} : b \bmod q^{n-l},\ d \bmod q^{l-t},\ q \nmid d,\ 0 \leqslant t < l \leqslant n < f+t \right\}$$

and

$$B_4 = \left\{ \begin{pmatrix} q^l & e + q^{n-f-t}b \\ q^{f+t} & q^{f+t-l}(e + q^{n-f-t}d) \end{pmatrix} : e \bmod q^{n-f-t}, \right.$$
$$\left. b \bmod q^{f+t-l},\ d \bmod q^{l-t},\ q \nmid (b,d),\ 0 \leqslant t < l < f+t \leqslant n \right\},$$

Let $B = \cup_{i=1}^{4} B_i$.

Lemma 6. *Elements of B generates distinct integral ideals of norm q^n.*

Proof. Let $\alpha \in \mathcal{O}_q^\times$ and $\beta, \gamma \in B$. It is obvious that all elements in B have norm q^n, so it suffices to show that if $\alpha\beta = \gamma$ for some α, then $\beta = \gamma$. Let α be the following matrix

$$\begin{pmatrix} a' & b' \\ q^f c' & d' \end{pmatrix} \qquad \text{with } a', d' \in \mathbb{Z}_q^\times,\ b', c' \in \mathbb{Z}_q.$$

We will prove the cases that $\beta, \gamma \in B_3$ or $\beta, \gamma \in B_4$. All the other cases are similar but easier.

Assume $\beta, \gamma \in B_3$ and they have the forms

$$\beta = \begin{pmatrix} q^{l_1} & b_1 \\ q^{f+t_1} & q^{n-l_1}d_1 \end{pmatrix} \qquad \text{and} \qquad \gamma = \begin{pmatrix} q^{l_2} & b_2 \\ q^{f+t_2} & q^{n-l_2}d_2 \end{pmatrix},$$

so $\alpha\beta = \gamma$ implies

$$q^{l_1}a' + q^{f+t_1}b' = q^{l_2} \tag{5}$$
$$a'b_1 + q^{n-l_1}b'd_1 = b_2 \tag{6}$$
$$q^{f+l_1}c' + q^{f+t_1}d' = q^{f+t_2} \tag{7}$$
$$q^f c'b_1 + q^{n-l_1}d'd_1 = q^{n-l_2}d_2. \tag{8}$$

Since $l_1 < f + t_1$ and $a' \in \mathbb{Z}_q^\times$, by comparing valuations in (5), we get $l_1 = l_2$ and $a' = 1 - b'q^{f+t_1-l_1}$. Similarly, since $l_1 > t_1$, from (7), we know $t_1 = t_2$ and $d' = 1 - q^{l_1-t_1}c'$. Plug the expression of a' into (6) and we get

$$b_1 - q^{n-l_1}b'(q^{f+t_1-n}b_1 - d_1) = b_2,$$

so $b_1 \equiv b_2 \bmod q^{n-l_1}$, hence $b_1 = b_2$. Similarly $d_1 = d_2$.

Assume $\beta, \gamma \in B_4$ and they have the forms

$$\beta = \begin{pmatrix} q^{l_1} & e_1 + q^{n-f-t_1} b_1 \\ q^{f+t_1} & q^{f+t_1-l_1}(e_1 + q^{n-f-t_1} d_1) \end{pmatrix}$$

and

$$\gamma = \begin{pmatrix} q^{l_2} & e_2 + q^{n-f-t_2} b_2 \\ q^{f+t_2} & q^{f+t_2-l_2}(e_2 + q^{n-f-t_2} d_2) \end{pmatrix}$$

so $\alpha\beta = \gamma$ implies

$$q^{l_1} a' + q^{f+t_1} b' = q^{l_2} \tag{9}$$

$$a' e_1 + q^{n-f-t_1} a' b_1 + q^{f+t_1-l_1} e_1 b' + q^{n-l_1} b' d_1 = e_2 + q^{n-f-t_2} b_2 \tag{10}$$

$$q^{f+l_1} c' + q^{f+t_1} d' = q^{f+t_2} \tag{11}$$

$$q^f e_1 c' + q^{n-t_1} c' b_1 + e_1 q^{f+t_1-l_1} d' + q^{n-l_1} d' d_1 = q^{f+t_2-l_2} e_2 + q^{n-l_2} d_2. \tag{12}$$

Since $l_1 < f + t_1$ and $a' \in \mathbb{Z}_q^\times$, by comparing valuations in (9), we get $l_1 = l_2$ and $a' = 1 - b' q^{f+t_1-l_1}$. Similarly, since $l_1 > t_1$, from (11), we know $t_1 = t_2$ and $d' = 1 - q^{l_1-t_1} c'$. Plug the expression of a' into (10) and we get

$$e_1 - q^{n-l_1}(b_1 - d_1) b' + q^{n-f-t_1} b_1 = e_2 + q^{n-f-t_1} b_2,$$

so $e_1 \equiv e_2 \bmod q^{n-f-t_1}$ and $e_1 = e_2$. Get rid of e_1, e_2, and we see that $b_1 \equiv b_2 \bmod q^{f+t_1-l_1}$, hence $b_1 = b_2$. Similarly $d_1 = d_2$. Done. ■

Lemma 7. *The ideals generated by elements of B give us all the integral ideals of norm q^n, where $n \geqslant f$.*

Proof. For any $\beta \in \mathcal{O}_q$ with norm q^n, we need to show that there exists $\alpha \in \mathcal{O}_q^\times$ such that $\alpha\beta \in B$.

Assume

$$\beta = \begin{pmatrix} a & b \\ q^f c & d \end{pmatrix} = \begin{pmatrix} q^l \epsilon_1 & b \\ q^{f+t} \epsilon_2 & d \end{pmatrix} \quad \text{and} \quad \alpha = \begin{pmatrix} a' & b' \\ q^f c' & d' \end{pmatrix},$$

where $v_q(ad - q^f bc) = n$, $v_q(a) = l$, $v_q(c) = t$ and $a', d' \in \mathbb{Z}_q^\times$. Then

$$\alpha\beta = \begin{pmatrix} q^l \epsilon_1 a' + q^{f+t} \epsilon_2 b' & a' b + b' d \\ q^{f+l} \epsilon_1 c' + q^{f+t} \epsilon_2 d' & q^f b c' + d d' \end{pmatrix} := \begin{pmatrix} a_1 & b_1 \\ q^f c_1 & d_1 \end{pmatrix}.$$

Let us consider several cases.

Case 1: $l \leqslant t$. It is easy to see that $v_q(a_1) = l$; choose $a' = \epsilon_1^{-1}(1 - q^{f+t-l} \epsilon_2 b')$ to make $a_1 = q^l$. Substitute this expression of a' to that of b_1, and we have

$$b_1 = \epsilon_1^{-1} b - q^{-l} \epsilon_1^{-1}(q^f bc - ad) b',$$

so the coefficient of b' has valuation $n - l$. Hence we can choose b' to make b_1 an integer between 0 and $q^{n-l} - 1$. Since $l \leqslant t$, we may fix $c' = -\epsilon_1^{-1} \epsilon_2 q^{l-t} d'$ to make $c_1 = 0$; plugging this expression of c' into d_1, we have

$$d_1 = \epsilon_1^{-1} q^{-l}(ad - q^f bc) d',$$

so we may choose d' to make $d_1 = q^{n-l}$. With this choice of α, $\alpha\beta \in B_2$.

Case 2: $l \geqslant f+t$. First choose $b' = -\epsilon_2^{-1}\epsilon_1 q^{l-f-t}a'$ to make $a_1 = 0$. Then

$$b_1 = q^{-(f+t)}\epsilon_2^{-1}(q^f bc - ad)a',$$

and we can fix a' to make $b_1 = q^{n-f-t}$. Next choose $d' = \epsilon_2^{-1}(1 - q^{l-t}\epsilon_1 c')$ to make $c_1 = q^{f+t}$; then

$$d_1 = \epsilon_2^{-1}d + \epsilon_2^{-1}q^{-t}(q^f bc - ad)c',$$

so we may choose c' to make d_1 an integer between 0 and $q^{n-t}-1$. Hence $\alpha\beta \in B_1$.

Case 3: $t < l < f+t$. Fix $a' = \epsilon_1^{-1}(1 - q^{f+t-l}\epsilon_1 b')$ to make $a_1 = q^l$; then

$$b_1 = \epsilon_1^{-1}b + \epsilon_1^{-1}q^{-l}(ad - q^f bc)b',$$

so we may choose b' to make b_1 an integer between 0 and $q^{n-l}-1$. Let $d' = \epsilon_2^{-1}(1 - q^{l-t}\epsilon_1 c')$ and then $c_1 = q^{f+t}$; so

$$d_1 = d\epsilon_2^{-1} + \epsilon_2^{-1}q^{-t}(q^f bc - ad)c',$$

hence we may choose c' to make d_1 an integer between 0 and $q^{n-t}-1$.

Subcase 3.1: $f+t > n$. Since $v_q(a_1d_1 - q^f b_1 c_1) = n$, this implies $v_q(a_1 d_1) = n$, hence $v_q(d_1) = n - l$. So $d_1 = q^{n-l}d_1'$ where $(q, d_1') = 1$ and d_1' is an integer between 0 and $q^{l-t}-1$. So $\alpha\beta \in B_4$.

Subcase 3.2: $f+t \leqslant n$. Since $v_q(a_1d_1 - q^f b_1 c_1) = n$, we have $v_q(b_1 q^{f+t-l} - d_1) = n - l$, so $d_1 = q^{f+t-l}d_2$ and d_2 is an integer between 0 and $q^{n+l-f-2t}-1$. We have $v_q(b_1 - d_2) = n - f - t$. Let $b_1 = b_1' + q^{n-f-t}b_1''$ be any integer mod q^{n-l}, with b_1' mod q^{n-f-t} and b_1'' mod ${}^{f+t-l}$ and $d_2 = d_2' + q^{n-f-t}d_2''$ be any integer mod q^{n-t} with d_2' mod q^{n-f-t} and d_2'' mod q^f. Then we must have $b_1' = d_2'$ and $q \nmid (b_1'', d_2'')$; hence $\alpha\beta \in B_3$.

So we are done. ∎

Proposition 8. *If* $n \geqslant f$,

$$a(q,n) = \frac{(f+1)q^{n+1} - (f-1)q^{n-1}}{q-1} + \frac{(f-1)q^{f-2} + f}{q-1} - \frac{q^f(q+1) - 2}{(q-1)^2}.$$

The local factor of our zeta function is

$$\zeta_{\mathcal{O},q}(s) = \frac{1 - 2q^{1-s} + q^{f(1-s)}}{(1-q^{1-s})^2} - \frac{fq^{f(1-s)}}{1-q^{1-s}} + A_1\frac{q^{f(1-s)}}{1-q^{1-s}} + A_2\frac{q^{-fs}}{1-q^{-s}},$$

where

$$A_1 = \frac{q^2(f+1) - (f-1)}{q(q-1)}, A_2 = \frac{(f-1)q^{f-2} + f}{q-1} - \frac{q^f(q+1) - 2}{(q-1)^2}.$$

Proof. From above two lemmas,

$$a(q,n)=\sum_{t=0}^{n-f}q^{n-t}+\sum_{l=0}^{n}q^{n-l}+\sum_{l=n-f+2}^{n}\sum_{t=n-f+1}^{l-1}q^{n-l}(q^{l-t}-1)$$
$$+\sum_{t=0}^{n-f}\sum_{l=t+1}^{f+t-1}q^{n-f-t}(q^f-q^{f-2}),$$

and the formula for $a(q,n)$ follows by elementary calculations. With what we have in Proposition 5, the local zeta factor at q also follows easily. Done. ■

Theorem 9.
$$\zeta_{\mathcal{O}}(s)=\zeta(s)\zeta(s-1)\prod_{q|N}Q_q(s),$$
where if $q=p$,
$$Q_p(s)=\frac{(1-p^{2r(1-s)})(1-p^{-s})}{1+p^{1-s}}+\frac{p^{-2rs}(1+p^{2r-s})(1-p^{1-s})}{1+p^{-s}},$$
and if $q|M$ with $v_q(M)=f$,
$$Q_q(s)=\frac{(1-q^{-s})(1-q^{f(1-s)})}{1-q^{1-s}}-fq^{f(1-s)}(1-q^{-s})$$
$$+A_1(1-q^{-s})q^{f(1-s)}+A_2q^{-fs}(1-q^{1-s}),$$
where A_1,A_2 are the two constants in Proposition 8.

Proof. We know that if $q\nmid N$, $\zeta_{\mathcal{O},q}=(1-q^{-s})^{-1}(1-q^{1-s})^{-1}$. We then just put all local factors together. The calculations are easy and we skip them here. Done. ■

Corollary 10. *If N is square free, that is $r=0$ and $v_q(M)\leqslant 1$ for any prime q, then $Q_p(s)=1-p^{1-s}$ and for $q\mid M$, $Q_q(s)=1+q^{1-s}$. Consequently, $\zeta_{\mathcal{O}}(s)$ is holomorphic on the half plane $re(s)>1$ except a simple at $s=1$.*

Proof. It follows trivially from Theorem 9 and properties of $\zeta(s)$. ■

3. Divisor function

As in Section 2, we fix $\mathcal{O}$ as an order of level $N=p^{2r+1}M$.

Lemma 11. *Given any integral left $\mathcal{O}$ ideal $\mathfrak{a}$ with $N(\mathfrak{a})=\prod_i^k q_i^{l_i}$ where q_i's are mutually distinct, there exists a unique (proper) factorization $\mathfrak{a}=\mathfrak{a}_1\cdots\mathfrak{a}_k$ such that $N(\mathfrak{a}_i)=q_i^{l_i}$.*

Proof. For the existence, assume $\mathfrak{a} = \mathfrak{A} \cap \cap_{q<\infty} \mathcal{O}_q \mu_q$. Since $N(\mathfrak{a}) = \prod_q n(\mu_q)$, $n(\mu_{q_i}) = q_i^{l_i}$ and $\mu_q = 1$ if $q \neq q_i$. Define

$$\mathfrak{a}_1 = \mathfrak{A} \cap \mathcal{O}_{q_1} \mu_{q_1} \cap (\cap_{q \neq q_1} \mathcal{O}_q),$$

and for $1 < i \leqslant k$,

$$\mathfrak{a}_i = \mathfrak{A} \cap (\cap_{t=1}^{i-1} \mu_{q_t}^{-1} \mathcal{O}_{q_t} \mu_{q_t}) \cap \mathcal{O}_{q_i} \mu_{q_i} \cap (\cap_{q \neq q_1, \cdots, q_i} \mathcal{O}_q).$$

For $1 \leqslant i \leqslant k$, let

$$\mathcal{O}_i = \mathfrak{A} \cap (\cap_{t=1}^{i-1} \mu_{q_t}^{-1} \mathcal{O}_{q_t} \mu_{q_t}) \cap (\cap_{q \neq q_1, \cdots, q_{i-1}} \mathcal{O}_q).$$

It is obvious that $\mathcal{O}_i$'s have the same level as $\mathcal{O}$, $\mathfrak{a}_i$ has left order $\mathcal{O}_i$ and right order $\mathcal{O}_{i+1}$, and $N(\mathfrak{a}_i) = n(\mu_{q_i}) = q_i^{l_i}$. This gives us the existence.

For the uniqueness, suppose we have two decompositions $\mathfrak{a} = \mathfrak{b}_1 \mathfrak{c}_1 = \mathfrak{b}_2 \mathfrak{c}_2$ where

$$N(\mathfrak{b}_1) = N(\mathfrak{b}_2) = n, \qquad N(\mathfrak{c}_1) = N(\mathfrak{c}_2) = m \qquad \text{and} \qquad (n, m) = 1.$$

Then we have $(m)\overline{\mathfrak{b}}_2 \mathfrak{b}_1 = (n)\mathfrak{c}_1 \overline{\mathfrak{c}}_2$ where all factors are integral ideals. So $(m)(n^{-1})\overline{\mathfrak{b}}_2 \mathfrak{b}_1$ is integral left $\mathcal{O}$-ideal where $\mathcal{O}$ is the right order of $\mathfrak{b}_2$. Assume $\mathcal{O} = \mathbb{Z}\{v_1, v_2, v_3, v_4\}$, and for any $w \in \overline{\mathfrak{b}}_2 \mathfrak{b}_1$, assume $w = \sum_i a_i v_i$. Since $(m)(n^{-1})\overline{\mathfrak{b}}_2 \mathfrak{b}_1$ is integral, $m a_i / n$ is integral for all i. That $(m, n) = 1$ implies a_i/n is integral, hence $w/n \in \mathcal{O}$ and $\mathfrak{d} = (n^{-1})\overline{\mathfrak{b}}_2 \mathfrak{b}_1$ is integral. But $N(\mathfrak{d}) = 1$ implies that $\mathfrak{d} = \mathcal{O}$ and hence $\overline{\mathfrak{b}}_2 \mathfrak{b}_1 = (n)$ and $\mathfrak{b}_1 = \mathfrak{b}_2$. Apply this to all prime power factors and we know that $\mathfrak{a}_i$'s are unique. Done. ■

As in [4], we define the divisor function, for any integral ideal $\mathfrak{a}$, as follows

$$d(\mathfrak{a}) = \#\{(\mathfrak{b}, \mathfrak{c}) : \mathfrak{a} = \mathfrak{b}\mathfrak{c}, \text{ with } \mathfrak{b}, \mathfrak{c} \text{ integral}\}.$$

Proposition 12. *The divisor function is multiplicative; that is, if $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ and $N(\mathfrak{b})$, $N(\mathfrak{c})$ are relatively prime, then $d(\mathfrak{a}) = d(\mathfrak{b})d(\mathfrak{c})$.*

Proof. Note that the proof of Proposition 6 in [4] only relies on Lemma 4 there; so the same proof goes through here. Done. ■

From this proposition, we know that to completely understand the divisor function it also suffices to work locally.

From now on, let us assume N is square-free, that is, a case of Eichler orders.

We have $r = 0$ and $f = 1$ for any $q \mid M$. The cases when $q = p$ and $q \nmid N$ are done in [4]. Let us focus on the case $q \mid M$.

Let us fix any $q \mid M$ and assume $\mathfrak{A}_q = M(2, \mathbb{Q}_q)$, the two-by-two matrix algebra over $\mathbb{Q}_q$. We will reserve $\mathcal{O}_q$ to denote a general order of level q and let

$$\mathcal{O}_{q,0} = \begin{pmatrix} \mathbb{Z}_q & \mathbb{Z}_q \\ q\mathbb{Z}_q & \mathbb{Z}_q \end{pmatrix}.$$

For convenience, let us denote

$$q_1(n,t,d) = \begin{pmatrix} 0 & q^{n-t-1} \\ q^{t+1} & d \end{pmatrix} \qquad \text{and} \qquad q_2(n,l,b) = \begin{pmatrix} q^l & b \\ 0 & q^{n-l} \end{pmatrix}.$$

Lemma 13.

(1) *All integral left $\mathcal{O}_{q,0}$ ideals of fixed norm q^n are*

$$\{\mathcal{O}_{q,0}q_1(n,t,d) : d \bmod q^{n-t},\ 0 \leqslant t \leqslant n-1\}$$

and

$$\{\mathcal{O}_{q,0}q_2(n,l,b) : b \bmod q^{n-l},\ 0 \leqslant l \leqslant n\};$$

(2) *An integral ideal is maximal if and only if it has norm q;*

(3) *The unique double-sided maximal ideal is*

$$\mathfrak{p} = \mathcal{O}_{q,0}q_1(1,0,0) = \mathcal{O}_{q,0} \begin{pmatrix} 0 & 1 \\ q & 0 \end{pmatrix},$$

and $\mathfrak{p}^2 = (q) = q\mathcal{O}_{q,0}$.

Proof. (1) This is a special case of Lemma 7.

(2) An ideal having norm q is necessarily maximal. Now assume $n \geqslant 2$ and $N(\mathfrak{a}) = q^n$. It is enough to show that $\mathfrak{a}$ is left divisible by some integral ideal $\mathfrak{b}$ with $1 < N(b) < q^n$.

If $\mathfrak{a} = \mathcal{O}_{q,0}q_1(n,t,d)$ and $0 \leqslant t \leqslant n-2$, then direct calculations imply $\mathcal{O}_{q,0}q_1(t+1,t,d_1)$ left divides $\mathfrak{a}$, where $d_1 \bmod q = d \bmod q$. If on the other hand $t = n-1$, then we have $\mathcal{O}_{q,0}q_2(1,1,0)$ left divides $\mathfrak{a}$.

Similarly, if $\mathfrak{a} = \mathcal{O}_{q,0}q_2(n,l,b)$ and $l \geqslant 1$, $\mathcal{O}_{q,0}q_2(1,1,0)$ left divides $\mathfrak{a}$; while if $l = 0$, then $\mathcal{O}_{q,0}q_2(1,0,b_1)$ left divides $\mathfrak{a}$, where $b_1 \bmod q = b \bmod q$.

(3) By (2), there are $2q+1$ maximal ideals. It is not hard to check that only $\mathfrak{p}$ gives a double-sided ideal. See also Eichler's notes [3]. Done. ■

Definition 14. *For any integral left $\mathcal{O}_{q,0}$-ideal $\mathfrak{a}$, we say that $\mathfrak{a}$ is primitive if it is not left divisible by $\mathfrak{p}$.*

More generally, for any order $\mathcal{O}_q$ of level q, let $\mathfrak{q}$ be the unique double-sided maximal ideal. We say an integral left $\mathcal{O}_q$-ideal $\mathfrak{a}$ is primitive if it is not left divisible by $\mathfrak{q}$.

Remark 15. If $\mathcal{O}_q$ is another order of level q, then $\mathcal{O}_q = \gamma\mathcal{O}_{q,0}\gamma^{-1}$ for some $\gamma \in \mathfrak{A}_q^\times$. Hence there is also a unique double-sided maximal ideal for $\mathcal{O}_q$, namely $\mathfrak{q} = \gamma\mathfrak{p}\gamma^{-1}$; actually, the normalizer of $\mathcal{O}_{q,0}$ inside $\mathfrak{A}_q^\times$ is (see Pizer's paper, [7] page 104)

$$N_{\mathfrak{A}_q^\times}(\mathcal{O}_{q,0}) = \mathcal{O}_{q,0}^\times\mathbb{Q}_q^\times \cup \begin{pmatrix} 0 & 1 \\ q & 0 \end{pmatrix} \mathcal{O}_{q,0}^\times\mathbb{Q}_q^\times,$$

so different choice of γ give rise to the same $\mathfrak{q}$.

Lemma 16. *All the primitive integral left $\mathcal{O}_{q,0}$ of fixed norm q^n are generated by quaternions in*

$$\{q_1(n,t,d) : d \bmod q^{n-t},\ q \nmid d,\ 0 \leqslant t \leqslant n-1\} \cup \{q_2(n,n,0)\}$$

and

$$\{q_2(n,0,b) : b \bmod q^n\}.$$

Proof. We know that $\mathfrak{p} \mid_l \mathcal{O}_{q,0} q_1(n,t,d)$ if and only if

$$\begin{pmatrix} 0 & q^{n-t-1} \\ q^{t+1} & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ q & 0 \end{pmatrix}^{-1} = \begin{pmatrix} q^{n-t-1} & 0 \\ d & q^t \end{pmatrix} \in \mathcal{O}_{q,0},$$

hence if and only if $q \mid d$.

Similarly, $\mathfrak{p} \mid_l \mathcal{O}_{q,0} q_2(n,l,b)$ if and only if

$$\begin{pmatrix} q^l & b \\ 0 & q^{n-l} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ q & 0 \end{pmatrix}^{-1} = \begin{pmatrix} b & q^{l-1} \\ q^{n-l} & 0 \end{pmatrix} \in \mathcal{O}_{q,0},$$

hence if and only if $1 \leqslant l \leqslant n-1$. Done. ■

Let us denote $P_1 = \{q_1(1,0,d) : d \bmod q, q \nmid d\} \cup \{q_2 1,1,0\}$, $P_2 = \{q_2(1,0,b) : b \bmod q\}$ and $P = P_1 \cup P_2 \cup \{\alpha_0 = q_1(1,0,0)\}$. Hence $\mathcal{O}_{q,0}P$ are all maximal left $\mathcal{O}_{q,0}$-ideals, among which $\mathcal{O}_{q,0}(P_1 \cup P_2)$ are the primitive ones.

Definition 17.

(1) *Ideals in $\mathcal{O}_{q,0}P_1$ are called maximal ideals of class one and those in $\mathcal{O}_{q,0}P_2$ are called maximal ideals of class two. As before, $\mathfrak{p}$ is called double-sided;*
(2) *Let $\alpha \in \mathcal{O}_{q,0}$ be of norm q. Then we say α is double-sided(of class one, of class two, resp.), if $\mathcal{O}_{q,0}\alpha$ equals $\mathfrak{p}$(belongs to $\mathcal{O}_{q,0}P_1$, belongs to $\mathcal{O}_{q,0}P_2$, resp.);*
(3) *More generally, given any order $\mathcal{O}_q$ of level q, fix a conjugator for $\mathcal{O}_q$, namely $\gamma \in \mathfrak{A}_q^\times$ such that $\mathcal{O}_q = \gamma^{-1}\mathcal{O}_{q,0}\gamma$. For any maximal left $\mathcal{O}_q$-ideal $\mathfrak{a}$, there exists a unique $\alpha \in P$ such that $\mathfrak{a} = \gamma^{-1}\mathcal{O}_{q,0}\alpha\gamma$. Then we say $\mathfrak{a}$ is double-sided(of class one, of class two, resp.), if $\alpha = \alpha_0$($\alpha \in P_1$, $\alpha \in P_2$, resp.);*
(4) *Let $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_k$ be a proper product of maximal ideals. Fix any conjugator γ for $\mathcal{O}_l(\mathfrak{a}_1)$, and there exists a unique $\alpha_1 \in P$ for $\mathfrak{a}_1$ as in (3). Use $\alpha_1\gamma$ as the conjugator for $\mathcal{O}_l(\mathfrak{a}_2)$, we get α_2 for $\mathfrak{a}_2$. Keep this way and we get $\alpha_i \in P$ for each $\mathfrak{a}_i$. We say $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_k$ is a product of the same class if $\mathfrak{a}_i$ is primitive for any $1 \leqslant i \leqslant k$ and all of α_i's are of the same class.*

Remark 18. This definition is well defined by the same reason in Remark 15. But we caution here that it is not possible to fix a class for a primitive maximal ideal without fixing a conjugator; for example,

$$\mathfrak{a} = \mathcal{O}_{q,0}\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$$

gives us class one, but

$$\mathfrak{a} = \alpha_0^{-1}\mathcal{O}_{q,0}\begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}\alpha_0,$$

gives us class two. This is because the second part of the normalizer $N_{\mathfrak{A}_q^\times}(\mathcal{O}_{q,0})$ (see [7]) actually permutes the two classes; we will make this clear in the following couple of lemmas.

Lemma 19. *Let $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_k$ be a proper product of maximal ideals. Then $\mathfrak{a}$ is primitive if and only if $\mathfrak{a}_1 \cdots \mathfrak{a}_k$ is a product of the same class. If this is the case, the factorization into maximal ideals is unique.*

Proof. Fix a conjugator γ for $\mathcal{O}_l(\mathfrak{a})$. Then we get $\alpha_i \in P$ for $\mathfrak{a}_i$ as in Definition 19, hence $\mathfrak{a} = \gamma^{-1}\mathcal{O}_{q,0}\alpha_k \cdots \alpha_1\gamma$. Assume first that $\mathfrak{a}$ is primitive and we denote

$$\begin{aligned} M = &\{\mathcal{O}_{q,0}q_1(n,t,d) : d \bmod q^{n-t},\ q \nmid d,\ 0 \leqslant t \leqslant n,\ n \geqslant 1\} \\ &\cup \{\mathcal{O}_{q,0}q_2(n,n,0) : n \geqslant 1\} \end{aligned}$$

and

$$N = \{\mathcal{O}_{q,0}q_2(n,l,b) : b \bmod q^{n-l},\ 0 \leqslant t \leqslant n,\ n \geqslant 1\}.$$

Assume $\mathfrak{a}' = \mathcal{O}_{q,0}\alpha_k \cdots \alpha_1 \in M$ and equals $\mathcal{O}_{q,0}q_1(k,t,d) \in M$ for some $d \bmod q^{k-t}$, $q \nmid d$ and $0 \leqslant t \leqslant k$. If $t = 0$, then it is easy to verify that α_1 has to be $q_1(1,0,d_1)$ where $d_1 \equiv d \bmod q$ and $\mathcal{O}_{q,0}\alpha_k \cdots \alpha_2 \in M$. If $t \geqslant 1$, $\alpha_1 = q_2(1,1,0)$ and also $\mathcal{O}_{q,0}\alpha_k \cdots \alpha_2 \in M$. If $\mathfrak{a}' = q_2(k,k,0)$, $\alpha_1 = q_2(1,1,0)$ and $\mathcal{O}_{q,0}\alpha_k \cdots \alpha_2 \in M$. So in any case, α_1 is of class one and $\mathcal{O}_{q,0}\alpha_k \cdots \alpha_2 \in M$. By induction on k, we know that all α_i's are of class one. Similarly, if $\mathfrak{a}' \in N$, we can show that all α_i's are of class two. At the same time, we proved that if $\mathfrak{a}$ is primitive such a factorization is unique.

Assume on the other hand that all α_i's are of the same class. It is easy to verify that if two elements generate two ideals in M(N, resp.), their product also generate an ideal in M(N, resp.), hence a primitive ideal. This is enough for our purpose. We skip the calculations here. Done. ■

(3) If $\mathfrak{a}_i\mathfrak{a}_{i+1}$ is not of the same class for some i, then for some $\gamma \in \mathfrak{A}_q^\times$ and some α, $\beta \in P$, $\mathfrak{a}_i = \gamma^{-1}\mathcal{O}_{q,0}\alpha\gamma$ and $\mathfrak{a}_{i+1} = \gamma^{-1}\alpha^{-1}\mathcal{O}_{q,0}\beta\alpha\gamma$. By assumption, α, β are not in the same class, hence $\mathfrak{a}_i\mathfrak{a}_{i+1} = \gamma^{-1}\mathcal{O}_{q,0}\beta\alpha\gamma$ is not primitive by part (1). It follows that $\mathfrak{a}$ is not primitive by shifting the resulting double-sided maximal ideal to the front and we have a contradiction.

Assume $\mathfrak{a}_i\mathfrak{a}_{i+1}$ is a product of the same class, for any $1 \leqslant i \leqslant k-1$. Then we can write the product down explicitly, say for some $\gamma \in \mathfrak{A}_q^\times$ and $\alpha_i \in P(1 \leqslant i \leqslant k)$,

$$\mathfrak{a}_1 = \gamma^{-1}\mathcal{O}_{q,0}\alpha_1\gamma, \mathfrak{a}_i = \gamma^{-1}\alpha_1^{-1}\cdots\alpha_{i-1}^{-1}\mathcal{O}_{q,0}\alpha_i\alpha_{i-1}\cdots\alpha_1\gamma.$$

By assumption, all α_i's belong to the same class and then $\mathfrak{a} = \gamma^{-1}\mathcal{O}_{q,0}\alpha_k \cdots \alpha_1\gamma$ is primitive by part (1). Done.

Lemma 20.

(1) *Assume* α, $\beta \in P_1 \cup P_2$ *and they are of different class. Then either* $\mathcal{O}_{q,0}\beta\alpha = (q)$ *or* $\mathcal{O}_{q,0}\beta\alpha = \mathfrak{p}\mathcal{O}_{q,0}\gamma$ *and* γ *belongs to the same class as* β*;*

(2) *Conjugation by* α_0 *switches the two class; more precisely, if* α *is of class one(class two,resp.), then* $\alpha_0^{-1}\alpha\alpha_0$ *is of class two(class one,resp.);*

(3) *Let* $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_i \mathfrak{p}_{i+1} \mathfrak{a}_{i+1} \cdots \mathfrak{a}_k$ *be a proper product into maximal ideals, where* $\mathfrak{p}_j$ *is the double-sided maximal ideal in* $\mathcal{O}_l(\mathfrak{a}_j)$*. Fix a conjugator for* $\mathcal{O}_l(\mathfrak{a})$*. Then if we write* $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1 \cdots \mathfrak{a}_i\mathfrak{a}_{i+1} \cdots \mathfrak{a}_k$*, we change the classes of* $\mathfrak{a}_j$ *if* $1 \leqslant j \leqslant i$ *and keep the classes of* $\mathfrak{a}_j$ *if* $i+1 \leqslant j \leqslant k$*, whenever* $\mathfrak{a}_j$ *is primitive.*

Proof. (1) This is done by easy verification. For example,

$$q_1(1,0,d)q_2(1,0,b)\alpha_0^{-1} \sim \begin{cases} q_2(1,1,0) & \text{if } q \mid (b+d), \\ q_1(1,0,d_1) & \text{if } q \nmid (b+d), \end{cases}$$

where $d_1 \equiv (b+d)^{-1} \bmod q$. Other cases are similar.

(2) Since

$$\begin{aligned} &\alpha_0^{-1}q_2(1,1,0)\alpha_0 \sim q_2(1,0,0), \\ &\alpha_0^{-1}q_1(1,0,d)\alpha_0 \sim q_2(1,0,b), \qquad b \equiv d^{-1} \bmod q, \\ &\alpha_0^{-1}q_2(1,0,0)\alpha_0 \sim q_2(1,1,0), \qquad \text{and} \\ &\alpha_0^{-1}q_2(1,0,b)\alpha_0 \sim q_1(1,0,d), \qquad d \equiv b^{-1} \bmod q, \qquad \text{if } b \neq 0, \end{aligned}$$

this part follows trivially.

(3) Fix a conjugator for $\mathcal{O}_l(\mathfrak{a})$ and assume $\alpha_j \in P$ is the associated element for $\mathfrak{a}_j$. After shifting the double-sided maximal ideal to the front, we can see easily that the associated element for $\mathfrak{a}_j$ is $\alpha_0^{-1}\alpha_i\alpha_0$ if $1 \leqslant j \leqslant i$ and α_i if $i+1 \leqslant j \leqslant k$. Hence this part follows easily from part (2). Done. ∎

Lemma 21. *Let* $\mathfrak{b} = \mathfrak{b}_k \cdots \mathfrak{b}_1$ *and* $\mathfrak{c} = \mathfrak{c}_1 \cdots \mathfrak{c}_l$ *be the unique factorizations into maximal ideals for two primitive ideals* $\mathfrak{b}$ *and* $\mathfrak{c}$*, respectively. Assume* $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ *is proper and let* $\mathfrak{p}$ *be the double-sided maximal ideal in the left order of* $\mathfrak{a}$*. Then*

(1) $\mathfrak{p} \mid_l \mathfrak{a}$ *if and only if* $\mathfrak{b}_1\mathfrak{c}_1$ *is not of the same class;*

(2) $(q) \mid_l \mathfrak{a}$ *if and only if* $\mathfrak{b}_1 = \bar{\mathfrak{c}}_1$*.*

Proof. (1) This is trivial by Lemma 19.

(2) One direction is trivial. For the other direction, one sees that $\mathfrak{b}_1\mathfrak{c}_1 = \mathfrak{p}_1\mathfrak{d}$ where $\mathfrak{p}_1$ is the double-sided maximal ideal in the left order of $\mathfrak{b}_1$. If $\mathfrak{b}_1 \neq \bar{\mathfrak{c}}_1$, then $\mathfrak{d}$ is primitive. By Lemma 20 (1), $\mathfrak{b}_1$ and $\mathfrak{d}$ are in different class. In the process of shifting $\mathfrak{p}_1$ to the front and get $\mathfrak{p}$, we change the classes of $\mathfrak{b}_i$'s by Lemma 20. As a consequence, $\mathfrak{b}_k \cdots \mathfrak{b}_2\mathfrak{d}\mathfrak{c}_2 \cdots \mathfrak{c}_l$ is product of the same class, hence primitive. We get a contradiction. ∎

Now we can start to explore the divisor function.

Definition 22. *Given an integral left $\mathcal{O}_q$-ideal $\mathfrak{a}$, we say $\mathfrak{a}$ has signature (n,m) if $N(\mathfrak{a}) = q^{n+m}$ and $\mathfrak{p}^n \mid \mathfrak{a}$ with n maximal, where $\mathfrak{p}$ is the maximal double-sided ideal in $\mathcal{O}_q$. Hence $\mathfrak{a}$ is primitive if and only if $n=0$.*

Definition 23. *Let $\mathfrak{a}$ be a integral ideal of signature (n,m), define $d(n,m) = d(\mathfrak{a})$ and*

$$c(n,m) = \{(\mathfrak{b},\mathfrak{c}) : \mathfrak{a} = \mathfrak{b}\mathfrak{c}, \mathfrak{b}, \mathfrak{c} \text{ are primitive } \}.$$

Later we will see that these quantities do not depend on the ideal and the notations make sense.

Lemma 24. *We fix an integral ideal $\mathfrak{a}$ of signature (n,m). Then*

$$c(n,m) = \begin{cases} m+1, & n=0, \\ m(q-1), & n=1, \\ 2q, & n=2. \end{cases}$$

Proof. We may assume $\mathcal{O}_l(\mathfrak{a}) = \mathcal{O}_{q,0}$.

The case when $n=0$ is trivial because of Lemma 19.

Consider the case $n=1$. First, $c(1,0)=0$ is obvious, since $\mathfrak{a} = \mathfrak{p}$ is maximal. Second, $c(1,1) = q-1$. Actually, this is done by direct computations; $\mathfrak{a}$ can only be $\mathcal{O}_{q,0}q_1(2,1,0)$, $\mathcal{O}_{q,0}q_1(2,0,bq)(b \bmod q)$ or $\mathcal{O}_{q,0}q_2(2,1,d)(d \bmod q \neq 0 \bmod q)$ and in each case we have precisely $(q-1)$ primitive decompositions. To finish this, we only need to show that for $m \geqslant 2$,

$$c(1,m) = c(1,m-1) + q - 1.$$

Assume $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$ and $\mathfrak{b}$ is primitive, so we have a unique decomposition $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2$ with $N(\mathfrak{b}_2) = q$. Let $\mathfrak{c} = \mathfrak{p}\mathfrak{b}_1$ and hence $\mathfrak{a} = \mathfrak{c}\mathfrak{b}_2$. Define

$$\begin{aligned} A_1 &= \{(\mathfrak{a}_1,\mathfrak{a}_2) : \mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2, \mathfrak{a}_1, \mathfrak{a}_2 \text{ primitive, } N(\mathfrak{a}_2) \geqslant q^2\}, \\ A_2 &= \{(\mathfrak{a}_1,\mathfrak{a}_2) : \mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2, \mathfrak{a}_1, \mathfrak{a}_2 \text{ primitive, } N(\mathfrak{a}_2) = q\}, \\ C &= \{(\mathfrak{c}_1,\mathfrak{c}_2) : \mathfrak{c} = \mathfrak{c}_1\mathfrak{c}_2, \mathfrak{c}_1, \mathfrak{c}_2 \text{ primitive}\}, \end{aligned}$$

and a map $\phi : A_1 \to C$ by $\phi(\mathfrak{a}_1,\mathfrak{a}_2) = (\mathfrak{a}_1, \mathfrak{a}_2\mathfrak{b}_2^{-1})$. Assume $\mathfrak{a}_1 = \mathfrak{a}_{1,k}\cdots\mathfrak{a}_{1,1}$ and $\mathfrak{a}_2 = \mathfrak{a}_{2,1}\cdots\mathfrak{a}_{2,l}$ with $l \geqslant 2$ and $\mathfrak{a}_{i,j}$ maximal. Now Lemma 21 says $\mathfrak{a}_{1,1}\mathfrak{a}_{2,1} = \mathfrak{p}\mathfrak{d}$ where $\mathfrak{d}$ is maximal and $\mathfrak{p}$ is the maximal double-sided ideal in the left order of $\mathfrak{a}_{1,1}$. So $\mathfrak{a}_{1,k}\cdots\mathfrak{a}_{1,2}\mathfrak{d}\mathfrak{a}_{2,2}\cdots\mathfrak{a}_{2,l}$ is a primitive factorization of $\mathfrak{b}$; by uniqueness, this gives us $\mathfrak{a}_{2,l} = \mathfrak{b}_2$, hence ϕ is well-defined. It is trivial that ϕ is injective. Moreover, for any $(\mathfrak{c}_1,\mathfrak{c}_2) \in C$, $\mathfrak{c}_2\mathfrak{b}_2$ must be a product of the same class, because otherwise we would get $(q) \mid \mathfrak{a}$. So $(\mathfrak{c}_1, \mathfrak{c}_2\mathfrak{b}_2) \in A_1$ and has image $(\mathfrak{c}_1,\mathfrak{c}_2)$ under ϕ. So ϕ is bijective and it suffices to show $\#A_2 = q-1$. Actually, this is done similarly by constructing a bijective map from A_2 to the set of primitive decompositions of

$\mathfrak{p}\mathfrak{b}_2$ where $\mathfrak{p}$ is the maximal double-sided ideal in the left order of $\mathfrak{b}_2$. The map is $(\mathfrak{a}_1, \mathfrak{a}_2) \to (\mathfrak{a}_{1,1}, \mathfrak{a}_2)$ and we skip the details here. So $\#A_2 = c(1,1) = q-1$ and we get the second formula.

Finally, $n = 2$. First, $c(2,0) = 2q$; indeed, any primitive maximal ideal $\mathfrak{a}_1$ gives a decomposition $(\mathfrak{a}_1, \overline{\mathfrak{a}}_1)$ and those are all of them. Now it is enough to show $c(2,m) = c(2,0)$ for any $m \geqslant 1$. Given any decomposition $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ with $\mathfrak{a}_1 = \mathfrak{a}_{1,k} \cdots \mathfrak{a}_{1,1}$ and $\mathfrak{a}_2 = \mathfrak{a}_{2,1} \cdots \mathfrak{a}_{2,l}$(into maximal ideals). Since $(q) \mid \mathfrak{a}$, $\mathfrak{a}_{1,1}\mathfrak{a}_{2,1} = (q)$ by Lemma 21. But if $k, l \geqslant 2$, then $\mathfrak{a}_{1,2}\mathfrak{a}_{2,2}$ would be a product of different class, hence $\mathfrak{p}^3 \mid \mathfrak{a}$ which is not possible. So we must have $k = 1$ or $l = 1$. Assume $\mathfrak{a} = q\mathfrak{b}$. In each case, only half of the $2q$ primitive decompositions of $(q) = \mathfrak{a}_1\overline{\mathfrak{a}}_1$ give us primitive decompositions of $\mathfrak{a}$, namely precisely one of $(\mathfrak{a}_1, \overline{\mathfrak{a}}_1\mathfrak{b})$ and $(\mathfrak{b}\mathfrak{a}_1, \overline{\mathfrak{a}}_1)$, because we need to match the classes to give primitive ideals. So we have $c(2,m) = 2q$. Done. ■

Lemma 25. *We fix any integral ideal $\mathfrak{a}$ of signature (n,m). Then*

(1) *for $n \geqslant 3$, $c(n,m) = qc(n-2,m)$;*

(2)

$$c(n,m) = \begin{cases} m+1, & n = 0, \\ mq^k(q-1), & n = 2k+1,\ k \geqslant 0, \\ 2q^k, & n = 2k,\ k > 0. \end{cases}$$

Proof. Part (2) follows easily from part (1), taking into account Lemma 24. So it is enough to show part (1).

Assume $\mathfrak{a} = q\mathfrak{b}$ and let

$$\begin{aligned} A &= \{(\mathfrak{a}_1, \mathfrak{a}_2) : \mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2, \mathfrak{a}_1, \mathfrak{a}_2 \text{ primitive}\}, \\ B &= \{(\mathfrak{b}_1, \mathfrak{b}_2) : \mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2, \mathfrak{b}_1, \mathfrak{b}_2 \text{ primitive}\}. \end{aligned}$$

Define a map $\phi : A \to B$ by $(\mathfrak{a}_1, \mathfrak{a}_2) \mapsto (\mathfrak{b}_1, \mathfrak{b}_2)$, where if $\mathfrak{a}_1 = \mathfrak{a}_{1,k} \cdots \mathfrak{a}_{1,1}$ and $\mathfrak{a}_2 = \mathfrak{a}_{2,1 \cdots \mathfrak{a}_{2,l}}$(into maximal ideals), $\mathfrak{b}_1 = \mathfrak{a}_{1,k} \cdots \mathfrak{a}_{1,2}$ and $\mathfrak{b}_2 = \mathfrak{a}_{2,2} \cdots \mathfrak{a}_{2,l}$. By Lemma 21, $\mathfrak{a}_{1,1}\mathfrak{a}_{2,1} = (q)$ and ϕ is well-defined. It is enough to show that any element $(\mathfrak{b}_1, \mathfrak{b}_2)$ in B has precisely q preimages in A. This is fairly easy to see, since exactly half of the $2q$ primitive decompositions $\mathfrak{a}_1\overline{\mathfrak{a}}_1$ of (q) give us primitive decomposition of $\mathfrak{a}$, namely $(\mathfrak{b}_1\mathfrak{a}_1, \overline{\mathfrak{a}}_1\mathfrak{b}_2)$. Done. ■

Proposition 26. *We fix any integral ideal $\mathfrak{a}$ of signature (n,m). Then*

(1) *if $n = 2k+1 (k \geqslant 0)$,*

$$\begin{aligned} d(2k+1,m) = {} & m(q-1)(2k+1) + (m+1)(2k+2) \\ & + (mq-m+4)\frac{q^{k+1}-q}{q-1} \\ & + 2(mq-m+2)\left(\frac{q^{k+1}-q^2}{(q-1)^2} - \frac{(k-1)q}{q-1}\right); \end{aligned}$$

(2) *if* $n = 2k (k \geqslant 0)$,

$$d(2k, m) = (m+1)(2k+1) + 2(mq - m + q)\frac{q^k - 1}{q-1} + 2(mq - m + 2q)\left(\frac{q^k - q}{(q-1)^2} - \frac{(k-1)}{q-1}\right).$$

Proof. Note that

$$d(\mathfrak{a}) = \sum_{l=0}^{n} (l+1) c(n-l, m).$$

This is not hard to see since any decomposition of $\mathfrak{a} = \mathfrak{p}^n \mathfrak{a}_1$ can be written uniquely as $\mathfrak{a} = (\mathfrak{p}^r \mathfrak{b})(\mathfrak{p}_1^t \mathfrak{c})$ with $\mathfrak{b}$ and $\mathfrak{c}$ primitive where $\mathfrak{p}$ and $\mathfrak{p}_1$ are the maximal double-sided ideals for corresponding orders. So it is produced by primitively decomposing $\mathfrak{p}_1^{n-r-t}\mathfrak{a}_1$, followed by assigning the $r+t$ double-sided maximal ideal factors.

The formulas then follow easily from those for $c(n, m)$. Done. ■

Proposition 27. *The number of integral ideals of fixed left order and fixed signature* (n, m)*, denoted by* $a(q; n, m)$*, is* 1 *if* $m = 0$ *and* $2q^m$ *if* $m \geqslant 0$.

Proof. Again let us fix the left order $\mathcal{O}_{q,0}$. Note that there is a bijective map from the set of integral ideals of signature (n, m) to the set of integral ideals of signature $(0, m)$, namely $\mathfrak{a} \mapsto \mathfrak{p}^{-n}\mathfrak{a}$. So we only need to do the primitive case.

If $m = 0$, $a(q; 0, 0) = 1$, namely the trivial one. If $m \geqslant 1$, by Lemma 14, there are $2q^m$ of them, that is $a(q; 0, m) = 2q^m$. Done. ■

Proof of Theorem 1. Since both sides have Euler products, it suffices to work locally. The cases that $q = p$ and $q \nmid N$ are treated in [4]; let us assume $q \mid M$.

$$\begin{aligned}
&\sum_{\mathfrak{a}} (d(\mathfrak{a}))^2 N(\mathfrak{a})^{-s} \quad (\mathfrak{a} \text{ are over integral ideals with norm } q\text{-powers}) \\
&= \sum_{n,m=0}^{\infty} d(n,m)^2 a(q; n, m) q^{-(n+m)s} \\
&= \sum_{k=0}^{\infty}\sum_{m=1}^{\infty} d(2k+1, m)^2 2q^m q^{-(2k+1+m)s} + \sum_{k=0}^{\infty}\sum_{m=1}^{\infty} d(2k, m)^2 2q^m q^{-(2k+m)s} \\
&\quad + \sum_{k=0}^{\infty} d(2k+1, 0)^2 q^{-(2k+1)s} + \sum_{k=0}^{\infty} d(2k, 0)^2 q^{-2ks}. \\
&= \frac{\zeta^4_{\mathcal{O},q}(s)}{\zeta_{\mathcal{O},q}(2s)} P(q, s).
\end{aligned}$$

where the calculation in the last equality is done using Mathematica. ■

Corollary 28. *For any fixed order* $\mathcal{O}$ *of level* N *(square-free) and some positive* A,

$$\sum_{N(\mathfrak{a}) \leqslant x} (d(\mathfrak{a}))^2 \sim A x^2 \log^3(x).$$

Proof. By the above proposition, taking into account the cases $q = p$ and $q \nmid N$ in [4], we have

$$\sum_{\mathfrak{a}}{}' (d(\mathfrak{a}))^2 N(\mathfrak{a})^{-s} = \frac{\zeta_{\mathcal{O}}^4(s)}{\zeta_{\mathcal{O}}(2s)} \prod_{q|M} P(q,s).$$

It is obvious that $P(q,s)$ is holomorphic on the half plane $Re(s) > 1$ and $P(q,2) \neq 0$; hence this is a holomorphic function on the half plane $Re(s) > 1$, except that at $s = 2$, there is a pole of order 4. By Perron's formula, the corollary is clear. ∎

Corollary 29. *Let notations be the same as those in Theorem 1. Then as* $T \to \infty$*,*

$$\sum_{2<k\leqslant T, k \text{ even}} \sum_{f\in S_k} \int_{-T}^{T} \left| L\left(\frac{k}{2} + it, f\right)\right|^4 dt \ll T^3 \log^4 T,$$

where

$$S_k = \bigcup_{a|M} \bigcup_{d|\frac{M}{a}} S_k^{\text{new}}(pa)^d.$$

Proof. Since the proof here is roughly the one in [4], we only sketch it; for details please refer to that paper.

Let H be the class number of $\mathcal{O}$ and $I_1, ..., I_H$ be a complete set of representatives of all distinct left $\mathcal{O}$-ideal classes. Let $\mathcal{O}_j = \mathcal{O}_r(I_j)$, the right order of I_j. Then $I_j^{-1}I_1, ..., I_j^{-1}I_H$, is a complete set of representatives of all distinct left $\mathcal{O}_j$-ideal classes. Let e_j be the number of units in $\mathcal{O}_j$ and $u_{ij} = N(I_i^{-1}I_j)$. Define the Brandt matrices $B_m(n)$, theta series $\Theta_m(\tau) = (\theta_{ij}^m(\tau))$ and shifted L-functions $\Psi_m(s) = (\psi_{ij}^m(s))$ using Definition 25 in [4].

Let $\Phi_m(s) = (\phi_{ij}^m(s)) = (\frac{N}{4})^s(\Psi_m(s))^2$; as in Lemma 24 in [4], we can show that

$$\phi_{ij}(s) := \phi_{ij}^0(s) = \sum_{\beta\in\Lambda_{ij}} a_{ij}(\beta)|\beta|^{-2s},$$

where Λ_{ij} is the lattice $2\sqrt{u_{ij}N^{-1}}I_j^{-1}I_i$ and $a_{ij}(\beta) = e_j^{-1}d(I_i^{-1}I_j\beta/(2\sqrt{u_{ij}N^{-1}}))$. Moreover,

$$\sum_{j=1}^{H} \sum_{\beta\in\Lambda_{ij}, |\beta|\leqslant x} a_{ij}(\beta)^2 \asymp x^4 \log^3 x.$$

Let C be the same constant $H^2 \times H^2$ matrix used in [4]. Since N is not a prime in general, the matrix representation of the canonical involution $Ef = f|_{w_N}$ may not be given by $B_m(N)$. However, according to Corollary 9.23 in [8], $\tilde{E} = -E$ where the matrix $\tilde{E} = \tilde{W}_p \prod_{q|M} \tilde{W}_q$. Now by Proposition 9.2 and 9.6 and Remark 9.25 in [8], we know that $\tilde{E}$ commutes with all Brandt matrices and $\tilde{E}^2 = I$. Using this matrix and proceeding the same way as in the proof of Proposition 27 in [4], we can prove that the system of the Dirichlet series $(\phi_{11}(s), \cdots, \phi_{ij}(s), \cdots, \phi_{HH}(s))$ is of signature $\langle\Lambda_{11}, \cdots, \Lambda_{ij}, \cdots, \Lambda_{HH}, 4, 0, C\rangle$.

(For reference on Maass Correspondence, please see Maass' original treatment in [5] and the generalization to a system of Dirichlet series in [4].)

Hence by Theorem 20 in [4], the corollary follows in the same way as we did for Theorem 2 and Corollary 3 in [4]. There is only one thing that we need to mention; namely, the Brandt matrices(including $B_m(n)$ where $p \mid n$) might not be simultaneously diagonalizable. But for the inequality in this corollary, we may just get rid of the off-diagonal entries on the left to give the same upper bound. Done. ■

Remark 30. It might be possible to avoid this long calculation for the divisor function by considering the quaternion algebra that ramifies exactly at all $p \mid N$ and ∞. In this case, the orders we need are still maximal, which makes the divisor function much simpler; for example, Ponomarev considered in [9] weight two forms using this type of quaternion algebras. However, we expect that the above argument should work in the case of $N = pM$ and then the above calculation would be necessary.

4. Quaternion algebras over number fields

Throughout this section, let $F/\mathbb{Q}$ be a number field and $\mathfrak{A}$ be a quaternion algebra over F. We use R to denote the ring of integers in F, $\mathfrak{p}$ a prime ideal in R, $F_\mathfrak{p}$ the completion of F at $\mathfrak{p}$ and $R_\mathfrak{p}$ the completion of R in $F_\mathfrak{p}$. By abuse of language, we also use $\mathfrak{p}$ to mean the maximal ideal in $R_\mathfrak{p}$, namely $\mathfrak{p}R_\mathfrak{p}$.

Let $\mathcal{O}$ be any maximal order in $\mathfrak{A}$ and $\mathfrak{a}$ be any integral left $\mathcal{O}$-ideal. All ideals in this section will be integral ideals for some maximal orders and all products of ideals will be proper.

As usual $N(\mathfrak{a})$ is the norm of $\mathfrak{a}$, that is, the ideal in R generated by all the reduced norms $\{N(\alpha) : \alpha \in \mathfrak{a}\}$. Denote by $N_{F/\mathbb{Q}}$ the norm of the field extension $F/\mathbb{Q}$ and $\mathfrak{a}_\mathfrak{p} = \mathfrak{a} \otimes_R R_\mathfrak{p}$. Define similarly

$$d(\mathfrak{a}) = \#\{(\mathfrak{b}, \mathfrak{c}) : \mathfrak{a} = \mathfrak{b}\mathfrak{c}\}$$

and for any integral ideal $\mathfrak{n}$ in R,

$$a(\mathfrak{n}) = \#\{\mathfrak{a} : N(\mathfrak{a}) = \mathfrak{n}\}.$$

Lemma 31. *Assume $N(\mathfrak{a}) = \mathfrak{n}\mathfrak{m}$ with $\mathfrak{n}, \mathfrak{m}$ relatively prime. Then there exists a unique pair $(\mathfrak{b}, \mathfrak{c})$ of integral ideals such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, $N(\mathfrak{b}) = \mathfrak{n}$ and $N(\mathfrak{c}) = \mathfrak{m}$.*

Proof. The existence follows the same way as that of Lemma 11. For the uniqueness, assume $\mathfrak{a} = \mathfrak{b}_1\mathfrak{c}_1 = \mathfrak{b}_2\mathfrak{c}_2$. Then it suffices to show it locally, that is, $\mathfrak{b}_{1,\mathfrak{p}} = \mathfrak{b}_{2,\mathfrak{p}}$ for all $\mathfrak{p}$. This is true, since for $\mathfrak{p} \mid \mathfrak{n}$ both are equal to $\mathfrak{a}_\mathfrak{p}$ and for $\mathfrak{p} \nmid \mathfrak{n}$ both are trivial. Done. ■

Proposition 32. *Both of the functions d and a are multiplicative; that is, if $\mathfrak{n}$, $\mathfrak{m}$ are relatively prime, then $a(\mathfrak{n}\mathfrak{m}) = a(\mathfrak{n})a(\mathfrak{m})$, and if $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ and $N(\mathfrak{b}) = \mathfrak{n}$, $N(\mathfrak{c}) = \mathfrak{m}$, then $d(\mathfrak{a}) = d(\mathfrak{b})d(\mathfrak{c})$.*

Proof. The statement for a is trivial by Lemma 31. For the divisor function, the whole proof of Proposition 12 gets through here without change. Done. ■

Again Proposition 32 tells us that it is enough to work locally. Let us fix a prime ideal $\mathfrak{p}$ of R and assume $\mathfrak{p} \mid (p)$. Denote by $e = e_{\mathfrak{p}}$ the ramification degree and $f = f_{\mathfrak{p}}$ the residue field extension degree.

If $\mathfrak{A}$ ramifies at $\mathfrak{p}$, then $\mathfrak{A}_{\mathfrak{p}}$ is the division algebra over $F_{\mathfrak{p}}$. Let $K/F_{\mathfrak{p}}$ be the unique unramified quadratic extension of $F_{\mathfrak{p}}$, π be a uniformizer of $\mathfrak{p}$ and σ be the generator of $Gal(K/F_{\mathfrak{p}})$. We have

$$\mathfrak{A}_{\mathfrak{p}} \simeq \left\{ \begin{pmatrix} a & b \\ \pi b^{\sigma} & a^{\sigma} \end{pmatrix} : a, b \in K \right\}.$$

As usual, we shall assume the equality in the above isomorphism, so we have

$$\mathcal{O}_{\mathfrak{p}} = \left\{ \begin{pmatrix} a & b \\ \pi b^{\sigma} & a^{\sigma} \end{pmatrix} : a, b \in R_K \right\},$$

where R_K is the ring of integers in K.

Lemma 33. *For any $n \in \mathbb{Z}_{\geqslant 0}$, $a(\mathfrak{p}^n) = 1$, that is, there exists a unique integral ideal of norm $\mathfrak{p}^n$; namely*

$$\mathcal{O}_{\mathfrak{p}} \begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix}^n .$$

Proof. First, we see that

$$\mathcal{O}_{\mathfrak{p}}^{\times} = \left\{ \begin{pmatrix} a & b \\ \pi b^{\sigma} & a^{\sigma} \end{pmatrix} : a \in R_K^{\times}, b \in R_K \right\};$$

indeed, such an element belongs to $\mathcal{O}_{\mathfrak{p}}^{\times}$ if and only if its norm belongs to $R_K^{\times}$ and the claim follows since π is also a uniformizer for K.

Now suppose $\mathfrak{a} = \mathcal{O}_{\mathfrak{p}}\alpha$ is an ideal of norm $\mathfrak{p}$. Assume

$$\alpha = \begin{pmatrix} a & b \\ \pi b^{\sigma} & a^{\sigma} \end{pmatrix}, \qquad a, b \in R_K.$$

Since $N(\mathfrak{a}) = \mathfrak{p}$, $v_{\mathfrak{p}}(N(\alpha)) = 1$ and $a \in \pi R_K$, $b \in R_K^{\times}$. Let $b_1 = -(\pi b^{\sigma})^{-1} a \in R_K$ and

$$\beta = \begin{pmatrix} 1 & b_1 \\ \pi b_1^{\sigma} & 1 \end{pmatrix} \in \mathcal{O}_{\mathfrak{p}}^{\times}.$$

Now $\beta\alpha$ has zeroes on the main diagonal, so we may assume that $a = 0$. Now

$$\gamma = \begin{pmatrix} b^{-1} & 0 \\ 0 & b^{-\sigma} \end{pmatrix} \in \mathcal{O}_{\mathfrak{p}}^{\times}.$$

and

$$\gamma\alpha = \begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix} := \alpha_0.$$

So $a(\mathfrak{p}) = 1$.

Assume $\mathfrak{a} = \mathcal{O}_\mathfrak{p}\alpha$ is any ideal of norm $\mathfrak{p}^n$ for some $n \geqslant 1$. We can see that if

$$\alpha = \begin{pmatrix} a & b \\ \pi b^\sigma & a^\sigma \end{pmatrix},$$

then $a \in \pi R_K$. As we know, $\mathcal{O}_\mathfrak{p}\alpha_0$ left divides $\mathfrak{a}$ if and only if α_0 right divides α. It is trivial to see that this is true. By induction, we see that $\mathfrak{a} = \mathcal{O}_\mathfrak{p}\alpha_0^n$. Hence $a(\mathfrak{p}^n) = 1$. Done. ∎

Proposition 34. *If $\mathfrak{a}$ has norm $\mathfrak{p}^n$, then $d(\mathfrak{a}) = n + 1$.*

Proof. This follows trivially from Lemma 33. ∎

Suppose now $\mathfrak{A}$ splits at $\mathfrak{p}$, so $\mathfrak{A}_\mathfrak{p} \simeq M(2, F_\mathfrak{p})$, the two-by-two matrix algebra over $F_\mathfrak{p}$. We may assume they are equal, since the quantities here are invariant under isomorphism. One of the maximal orders is $M(2, R_\mathfrak{p})$ and all others are conjugate to this one via $\mathfrak{A}_\mathfrak{p}^\times$. Let $S(\mathfrak{p}, n)$ denote a complete set of representatives in $R_\mathfrak{p}$ for $R_\mathfrak{p}/\mathfrak{p}^n$ when $n \geqslant 0$. Moreover let $S(\mathfrak{p}, n)^\times$ be the subset of invertible elements, that is $S(\mathfrak{p}, n) \cap R^\times$. Hence $\#S(\mathfrak{p}, n) = p^{fn}$. An ideal $\mathfrak{a}$ is called primitive if $(\pi) \nmid_l \mathfrak{a}$, where (π) should be considered as the ideal generated by π in the left order of $\mathfrak{a}$.

Lemma 35. *Let $\mathcal{O}_\mathfrak{p} = M(2, R_\mathfrak{p})$.*

(1) *All integral left $\mathcal{O}_\mathfrak{p}$-ideals of norm $\mathfrak{p}^n$ are*

$$\left\{ \mathcal{O}_\mathfrak{p} \begin{pmatrix} \pi^l & b \\ 0 & \pi^{n-l} \end{pmatrix} : b \in S(\mathfrak{p}, n-l), 0 \leqslant l \leqslant n \right\};$$

hence $a(\mathfrak{p}^n) = \frac{p^{f(n+1)}-1}{p^f-1}$;

(2) *All primitive left $\mathcal{O}_\mathfrak{p}$-ideals of norm $\mathfrak{p}^n$ are*

$$\left\{ \mathcal{O}_\mathfrak{p} \begin{pmatrix} 1 & b \\ 0 & \pi^n \end{pmatrix} : b \in S(\mathfrak{p}, n) \right\} \bigcup \left\{ \mathcal{O}_\mathfrak{p} \begin{pmatrix} \pi^n & 0 \\ 0 & 1 \end{pmatrix} \right\}$$
$$\bigcup \left\{ \mathcal{O}_\mathfrak{p} \begin{pmatrix} \pi^l & b \\ 0 & \pi^{n-l} \end{pmatrix} : b \in S(\mathfrak{p}, n)^\times, 1 \leqslant l \leqslant n-1 \right\};$$

the total number of them are $p^{f(n-1)}(p^f + 1)$.

Proof. The second part follows from the first part trivially. Let $\mathfrak{a} = \mathcal{O}_\mathfrak{p}\alpha$ be any integral ideal of norm $\mathfrak{p}^n$ and assume

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad a, b, c, d \in R_\mathfrak{p}.$$

If $v_\mathfrak{p}(a) \geqslant v_\mathfrak{p}(c)$, then let

$$\beta = \begin{pmatrix} 0 & 1 \\ 1 & -c^{-1}a \end{pmatrix} \in \mathcal{O}_\mathfrak{p}^\times$$

and $\beta\alpha$ has zero left lower element. If on the other hand $v_{\mathfrak{p}}(a) < v_{\mathfrak{p}}(c)$, then let

$$\beta = \begin{pmatrix} 1 & 0 \\ -a^{-1}c & 1 \end{pmatrix} \in \mathcal{O}_{\mathfrak{p}}^{\times}$$

and $\beta\alpha$ also has zero left lower element. So we may assume $c = 0$. Assume $v_{\mathfrak{p}}(a) = l$ and hence $v_{\mathfrak{p}}(d) = n - l$. Let

$$\beta = \begin{pmatrix} a^{-1}\pi^{l} & 0 \\ 0 & d^{-1}\pi^{n-l} \end{pmatrix} \in \mathcal{O}_{\mathfrak{p}}^{\times}$$

and $\beta\alpha$ has diagonal elements π^l and π^{n-l} respectively. We can assume $a = \pi^l$ and $d = \pi^{n-l}$. There is a unique $x \in S(\mathfrak{p}, n-l)$ such that $b - x = -y\pi^{n-l} \in \mathfrak{p}^{n-l}$ with $y \in R_{\mathfrak{p}}$. Let

$$\beta = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in \mathcal{O}_{\mathfrak{p}}^{\times} \qquad \text{and} \qquad \beta\alpha = \begin{pmatrix} \pi^{l} & x \\ 0 & \pi^{n-l} \end{pmatrix}.$$

Now it suffices to show that all ideals in part one are distinct. Suppose

$$\beta = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \in \mathcal{O}_{\mathfrak{p}}^{\times} \qquad \text{and} \qquad \beta \begin{pmatrix} \pi^{l} & b \\ 0 & \pi^{n-l} \end{pmatrix} = \begin{pmatrix} \pi^{l'} & b' \\ 0 & \pi^{n-l'} \end{pmatrix}.$$

Comparing the left lower elements gives us $c_1 = 0$, hence $a_1, d_1 \in R_{\mathfrak{p}}^{\times}$. Now equalities of the diagonal elements imply that $a_1 = d_1 = 1$ and $l = l'$. Finally the right upper elements equal and implies $b \cong b' \bmod \mathfrak{p}^{n-l}$; so by the choices of b and b', they have to be the same. Done. ■

Lemma 36. *Any primitive ideal $\mathfrak{a}$ has a unique decomposition into a proper product of maximal ideals; consequently, $d(\mathfrak{a}) = m + 1$ if $N(\mathfrak{a}) = \mathfrak{p}^m$.*

Proof. As usual, we may assume the left order of $\mathfrak{a}$ is $M(2, R_{\mathfrak{p}})$. We see that $\mathfrak{a}$ is left divisible by a uniquely determined norm $\mathfrak{p}$ ideal; indeed this is easy to verify by using the explicit expression in Lemma 35 and passing to right divisibility of corresponding elements. From this we know that the norm $\mathfrak{p}$ ideals are precisely the maximal ideals and the lemma follows. Done. ■

We say an ideal is of signature (n, m) if $N(\mathfrak{a}) = \mathfrak{p}^{2n+m}$ and $\mathfrak{p}^n \mid_l \mathfrak{a}$ with n maximal. We define

$$c(\mathfrak{a}) = c(n, m) = \#\{(\mathfrak{b}, \mathfrak{c}) : \mathfrak{a} = \mathfrak{b}\mathfrak{c} \text{ with } \mathfrak{b}, \mathfrak{c} \text{ primitive}\}.$$

Again we will see in the following lemma that this number only depends on the signature, which justifies the notation we used here. Similarly we will use $d(n, m) = d(\mathfrak{a})$.

Lemma 37. *Let $\mathfrak{a}$ be of signature (n, m).*

$$c(n, m) = \begin{cases} p^{f(n-1)}((m+1)(p^f - 1) + 2), & n \geqslant 1, \\ m + 1, & n = 0. \end{cases}$$

Proof. The proof of this lemma is essentially the same as the proof of Lemma 11 in [4]; indeed Lemma 8 and Lemma 10 in [4] still hold here and this is nearly the only things that we need in the proof. More specifically, we use the same arguments to show first

$$c(1, m) = (m + 1)(p^f - 1) + 2$$

and then for $n \geqslant 1$

$$c(n + 1, m) = p^f c(n, m),$$

which completes the proof. See [4] for details. Done. ■

Proposition 38. *Let $\mathfrak{a}$ be of signature (n, m).*

$$d(\mathfrak{a}) = \frac{p^{f(n+1)} - 1}{p^f - 1}(m + 1) - \frac{2(n + 1)}{p^f - 1} + \frac{2(p^{f(n+1)} - 1)}{(p^f - 1)^2}.$$

Proof. This follows trivially from $d(\mathfrak{a}) = \sum_{l=0}^{n}(l + 1)c(n - l, m)$. Done. ■

Let us denote by $a(n, m)$ the number of left $\mathcal{O}_{\mathfrak{p}}$-ideals with signature (n, m). Then

Proposition 39.

$$a(n, m) = \begin{cases} p^{f(m-1)}(p^f + 1), & m \geqslant 1, \\ 1, & 0. \end{cases}$$

Proof. It is obvious that $a(0, m) = a(n, m)$ which follows from the bijective map $\mathfrak{a} \to (\pi)^n\mathfrak{a}$; the formula for $a(0, m)$ is given by Lemma 35. Done. ■

For convenience, let us group some series identities as a lemma:

Lemma 40.

(1)

$$\sum_{n=0}^{\infty}(n + 1)^2 X^{-ns} = (1 - X^{-2s})(1 - X^{-s})^{-4};$$

(2) *If*

$$a_{n,m} = \begin{cases} X^{m-1}(X + 1), & m > 0, \\ 1, & m = 0. \end{cases}$$

and

$$d_{n,m} = \frac{X^{n+1} - 1}{X - 1}(m + 1) - \frac{2(n + 1)}{X - 1} + \frac{2(X^{n+1} - 1)}{(X - 1)^2},$$

then

$$\sum_{m,n=0}^{\infty} a_{n,m} d_{n,m}^2 X^{-(m+2n)s} = (1+X^{-s})(1-X^{1-2s})(1-X^{-s})^{-3}(1-X^{1-s})^{-4}.$$

Proof. These identities are the same as those in the proof of Theorem 1 in [4]. See the computations there for details. Done. ■

Define the zeta function for the maximal order $\mathcal{O}$ as follows:

$$\zeta_{\mathcal{O}}(s) = \sum_{\mathfrak{a}}{}' N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s},$$

where the sum is over all nontrivial integral left $\mathcal{O}$-ideals. Since both the norms are multiplicative and by Lemma 31, we can write the zeta function as an Euler product

$$\zeta_{\mathcal{O}}(s) = \prod_{\mathfrak{p},\ \text{prime}} \zeta_{\mathcal{O},\mathfrak{p}}(s),$$

where

$$\zeta_{\mathcal{O},\mathfrak{p}}(s) = \sum_{\mathfrak{a}}{}' N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s},$$

and the sum is taken over all non-zero integral left $\mathcal{O}$-ideals of norm $\mathfrak{p}$-powers.

Lemma 41.

$$\zeta_{\mathcal{O}}(s) = \zeta_F(s)\zeta_F(s-1) \prod_{\mathfrak{p},\mathfrak{A}\ \textit{ramifies at}\ \mathfrak{p}} (1 - p^{f(1-s)}),$$

where $\zeta_F(s)$ is the Dedekind zeta function for F, $\mathfrak{p} \mid p$ and $f = f(\mathfrak{p}/p)$ is the residue degree of $F_{\mathfrak{p}}/\mathbb{Q}_p$.

Proof. If $\mathfrak{p}$ ramifies in $\mathfrak{A}$, by Lemma 33,

$$\zeta_{\mathcal{O},\mathfrak{p}}(s) = \sum_{n=0}^{\infty} p^{-fns} = (1 - p^{-fs})^{-1};$$

if $\mathfrak{p}$ splits in $\mathfrak{A}$, by Lemma 35,

$$\zeta_{\mathcal{O},\mathfrak{p}}(s) = \sum_{n=0}^{\infty} \frac{p^{f(n+1)} - 1}{p^f - 1} p^{-fns} = (1 - p^{-fs})^{-1}(1 - p^{f(1-s)}).$$

Our lemma follows. Done. ■

Theorem 42.

$$\sum_{\mathfrak{a}}{}' (d(\mathfrak{a}))^2 N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s} = \frac{\zeta_{\mathcal{O}}(s)^4}{\zeta_{\mathcal{O}}(2s)},$$

where the sum is over all nonzero integral left $\mathcal{O}$-ideals.

Proof. To prove the identity, we only need to show the identity for local factors, since the left side also has a Euler product because of the multiplicativity of the divisor function.

If $\mathfrak{p}$ ramifies in $\mathfrak{A}$, by Lemma 33 and Proposition 34, we need to show

$$\sum_{n=0}^{\infty}(n+1)^2 p^{-fns} = (1-p^{-2fs})(1-p^{-fs})^4,$$

which follows from Lemma 40, by replacing X by p^f.

If $\mathfrak{p}$ splits in $\mathfrak{A}$, we need to show

$$\sum_{n,m=0}^{\infty} a(n,m)(d(n,m))^2 p^{-(2n+m)fs}$$
$$= (1+p^{-fs})(1-p^{f(1-2s)})(1-p^{-fs})^{-3}(1-p^{f(1-s)})^{-4}.$$

This follows directly from Propositions 38, 39 and Lemma 40. Done. ■

Corollary 43.

$$\sum_{N_{F/\mathbb{Q}}(N(\mathfrak{a}))\leqslant x} (d(\mathfrak{a}))^2 \sim Ax^2\log^3(x),$$

for some positive A.

Proof. Let

$$f(s) = \sum_{n=0}^{\infty} a_n n^{-s} := \sum_{\mathfrak{a}}{}' (d(\mathfrak{a}))^2 N_{F/\mathbb{Q}}(N(\mathfrak{a}))^{-s}.$$

Since $\zeta_F(s)$ only has a simple pole at $s=1$ on the right half plane $Re(s) > 1-1/N$ where $N=[F:\mathbb{Q}]$, $\zeta_{\mathcal{O}}(s)$ only has a simple pole at $s=2$ on the right half plane $Re(s) > 2-1/N$. Moreover $\zeta_F(2s)$ is regular and non-vanishing there, so by Theorem 42, $f(s)$ is regular on $Re(s) > 2-1/N$ except a unique pole at $s=2$ of order 4. Apply Perron's formula to $f(s)$, and the result is obvious. ■

References

[1] W. Duke, *Fourth moments of L-functions attached to newforms*, Comm. Pure Appl. Math **41** (1988), 815–831.

[2] M. Eichler, *Lectures on modular correspondences*, Tata Institute of Fundamental Research, Bombay, 1965.

[3] M. Eichler, *The basis problem for modular forms and the traces of the Hecke operators*, Lecture Notes in Mathematics, no. 320 (1972), Springer-Verlag, 75–151.

[4] H. H. Kim and Y. Zhang, *Divisor function for quaternion algebras and application to fourth moments of L-functions*, Journal of Number Theory, to appear.

[5] H. Maass, *Automorphe Funktionen von mehreren Veränderlichen und Dirichletsche Reihen*, Abh. Math. Seminar Hansischen Univ. **16** (1949), 72–100.

[6] A. Pizer, *An algorithm for computing modular forms on $\Gamma_0(N)$*, J. of Algebra **64** (1980), 340–390.

[7] A. Pizer, *The action of the canonical involution on modular forms of weight 2 on* $\Gamma_0(M)$, Math. Ann. **226** (1977), 99–116.
[8] A. Pizer, *Theta series and modular forms of level* p^2M, Comp. Math. **40** (1980), 177–241.
[9] P. Ponomarev, *Newforms of squarefree level and theta series*, Math. Ann. **345** (2009), 185–193.
[10] I. Reiner, *Maximal orders*, Academic Press, 1975.
[11] P. Sarnak, *Fourth moments of Grössencharakeren zeta functions*, Comm. Pure Appl. Math. **38** (1985), 167–178.

Address: Yichao Zhang: Department of Mathematics, University of Connecticut, 196 Auditorium Road, Unit 3009, Storrs, CT 06269-3009.

E-mail: yichao.zhang@uconn.edu

Received: 9 March 2011