TRACES IN ARITHMETIC FUCHSIAN GROUPS

STEFAN JOHANSSON

Introduction

Let Γ be a Fuchsian group of the first kind in $SL_2(\mathbb{R})$. The purpose of this paper is to investigate the set of traces

$$\mathcal{T}^{\Gamma} = \{t : t = \mathrm{trace}(\gamma),\, \gamma \in \Gamma\}.$$

This set is very important for several reasons. It is well known that the orbifold $\Gamma\backslash\mathcal{H}$, where $\mathcal{H}$ is the upper half-plane model of the hyperbolic plane, has a natural structure of a Riemann surface. The geometry of this surface is closely related to the arithmetical properties of the trace set $\mathcal{T}^{\Gamma}$. For example, there is a natural one-to-one correspondence between traces of conjugacy classes of hyperbolic elements in Γ, and the geodesic length spectrum $\mathcal{L}(\Gamma)$ on the corresponding Riemann surface: To each conjugacy class $[\gamma]$ of hyperbolic elements in Γ corresponds a unique closed geodesic on the Riemann surface, whose length l_γ satisfies

$$|Tr(\gamma)| = 2\cosh\frac{l_\gamma}{2}.$$

Furthermore, the spectrum of the Laplacian on $\Gamma\backslash\mathcal{H}$ is totally determined by $\mathcal{L}(\Gamma)$ through the Selberg trace formula, see [5].

When $\Gamma = SL_2(\mathbb{Z})$, it is trivial that $\mathcal{T}^{\Gamma} = \mathbb{Z}$. It is also easy to determine $\mathcal{T}^{\Gamma}$ for many groups Γ commensurable with $SL_2(\mathbb{Z})$, but in general it is not a trivial task to describe the trace set $\mathcal{T}^{\Gamma}$.

There is a significant difference between $\mathcal{T}^{\Gamma}$ for arithmetic and non-arithmetic Fuchsian groups. Indeed it is possible to characterise arithmetic Fuchsian groups in terms of $\mathcal{T}^{\Gamma}$ [11]. In geometrical terms, this translates to a significant difference in the statistics of the length spectrum of closed geodesics on $\Gamma\backslash\mathcal{H}$ when Γ is arithmetic, compared to what is expected and has been found numerically for non-arithmetic groups. This special behaviour of the spectral statistics when Γ is arithmetic is an example of what has recently been named arithmetic chaos [9].

In [1], Bolte gave a conjectural explicit formula for the asymptotic behaviour of $\mathcal{T}^{\Gamma}$, when Γ is arithmetic. However, this formula relied on a hypothesis, which proved to be false.

The main purpose of this paper is to determine the asymptotic behaviour of $\mathcal{T}^{\Gamma}$ when Γ is arithmetic, and thereby prove a corrected version of the formula in [1]. It will be shown that the only correction needed in [1] is the coefficient of the leading term.

Sections 1 and 2 contain some notational conventions and a number of auxiliary results.

In section 3, we reformulate the problem in terms of representations by quadratic forms on lattices. Using the theory of quadratic forms, we show that it is possible to localise the problem. With this, we are able to explicitly determine the asymptotic behaviour of $\mathcal{T}^\Gamma$, when Γ are unit groups in quaternion orders. This is done in section 4 for a large family of orders, including maximal orders and Eichler orders. For many of these orders, we are also able to exactly determine $\mathcal{T}^\Gamma$.

1. Background and notations

Let F be a totally real algebraic number field with $[F:\mathbb{Q}] = n < \infty$, and let R denote the algebraic integers in F. Let Ω be the set of normalised valuations on F, Ω_f the non-archimedean and Ω_∞ the archimedean ones. If $\mathfrak{p} \in \Omega_f$, then $F_\mathfrak{p}$ will denote the completion of F with respect to $\mathfrak{p}$, and $R_\mathfrak{p}$ the integers in $F_\mathfrak{p}$. The discriminant of F will be denoted by D_F, and the different embeddings of F in $\mathbb{R}$ by $\sigma_1, \dots, \sigma_n$. We will consider F embedded in $\mathbb{R}^n$ by

$$x \longmapsto \sigma(x) = (\sigma_1(x), \dots, \sigma_n(x)).$$

If $\mathfrak{I}$ is an ideal in R, then $N\mathfrak{I}$ is the cardinality of $R/\mathfrak{I}$.

Let $\mathfrak{A}$ be a quaternion algebra over F. This will always be assumed to satisfy

$$\mathfrak{A} \otimes_\mathbb{Q} \mathbb{R} \cong M_2(\mathbb{R}) \times \mathbb{H}^{n-1}, \tag{1.1}$$

where $\mathbb{H}$ are the Hamiltonian quaternions. The algebra $\mathfrak{A}$ will be considered embedded in $M_2(\mathbb{R})$, through a map corresponding to σ_1.

It is always possible to find an F-basis $1, i, j, ij$ of $\mathfrak{A}$, such that

$$i^2 = a,\ j^2 = b,\ ij = -ji, \text{ where } a, b \in R \text{ and } ab \neq 0.$$

This algebra will be denoted $(a,b)_F$. There is a natural anti-involution in $\mathfrak{A} \cong (a,b)_F$ given by

$$q = x_0 + x_1 i + x_2 j + x_3 ij \longmapsto \bar{q} = x_0 - x_1 i - x_2 j - x_3 ij.$$

The (reduced) norm $N : \mathfrak{A} \longrightarrow F$ and (reduced) trace $Tr : \mathfrak{A} \longrightarrow F$ are defined by

$$\begin{aligned} N(q) &= q\bar{q} = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 \\ Tr(q) &= q + \bar{q} = 2x_0. \end{aligned}$$

From the embeddings σ_i we get $\sigma_i N : \mathfrak{A} \longrightarrow \mathbb{R}$ and $\sigma_i Tr : \mathfrak{A} \longrightarrow \mathbb{R}$. The condition (1.1) is equivalent to $\sigma_i N$ being indefinite when $i = 1$, and positive definite otherwise. In terms of a and b, this corresponds to $\sigma_i(a)$ and $\sigma_i(b)$ both negative iff $2 \leq i \leq n$.

An order $\mathcal{O}$ in $\mathfrak{A}$ is a subring of $\mathfrak{A}$, such that $1 \in \mathcal{O}$, $\mathcal{O}$ is a finitely generated R-module and $\mathcal{O}$ contains an F-basis of $\mathfrak{A}$. If $\nu \in \Omega$, then $\mathfrak{A}_\nu := \mathfrak{A} \otimes_F F_\nu$ and $\mathcal{O}_\nu := \mathcal{O} \otimes_R R_\nu$.

If $\mathcal{O}$ is an order in a quaternion algebra, then the (reduced) discriminant of $\mathcal{O}$, $d(\mathcal{O})$, is defined to be the R-ideal which is the square root of the ideal generated by $\det[Tr(x_i\bar{x}_j)]$, where $x_i \in \mathcal{O}$.

The set $\mathcal{O}^1 = \{q \in \mathcal{O} : N(q) = 1\}$ is embedded in $SL_2(\mathbb{R})$, and is always a Fuchsian group of the first kind. A Fuchsian group is called arithmetic iff it is commensurable with any such $\mathcal{O}^1$.

When S is a finite set, then $|S|$ will denote the cardinality of S. Observe that in order to determine $\mathcal{T}^\Gamma$, we may restrict to elements γ with $Tr(\gamma) > 0$, since if $\gamma \in \mathcal{O}^1$ then $-\gamma \in \mathcal{O}^1$. When we determine the asymptotics of the trace set, it does not matter if we include non-hyperbolic traces ($|Tr(\gamma)| \leq 2$) or not. Hence if

$$\mathcal{T}^{\mathcal{O}}(r) = \left\{Tr(q) : 2 < Tr(q) \leq 2r,\ q \in \mathcal{O}^1\right\},$$

then our main goal is to determine the asymptotic behaviour of $|\mathcal{T}^{\mathcal{O}}(r)|$, when $r \longrightarrow \infty$.

By $P(r)$, we will denote the parallelotope

$$P(r) = \{x \in \mathbb{R}^n : 2 < x_1 \leq 2r,\ |x_i| < 2,\ 2 \leq i \leq n\},$$

where $n = [F : \mathbb{Q}]$. More generally, $P_y(r)$ will denote the translation of $P(r)$ given by $P_y(r) = \{x \in \mathbb{R}^n : x - y \in P(r)\}$.

2. Auxiliary results

We will need some simple results in section 4, which we record for convenience. First the trivial observation, that if a and b are elements in a field, then

$$a + a^{-1} = b + b^{-1} \Longrightarrow a = b \text{ or } a = b^{-1}. \tag{2.1}$$

(2.2) Lemma. *Let R be a complete discrete valuation ring and let $\mathfrak{p}$ be the maximal ideal in R. Suppose that $x \in R$ is such that there exists $a \in R$ with $x \equiv a + a^{-1}$ mod $\mathfrak{p}$ and $a \not\equiv \pm 1$ mod $\mathfrak{p}$. Then there is $b \in R$ such that $x = b + b^{-1}$.*

Proof. The conclusion of the lemma is equivalent to the following: For every $n \geq 1$, there exist $b_n, b_n' \in R$ such that $a \equiv b_n + b_n'$ mod $\mathfrak{p}^n$ and $b_n b_n' \equiv 1$ mod $\mathfrak{p}^n$, with $b_n - b_{n+1} \in \mathfrak{p}^n$ and $b_n' - b_{n+1}' \in \mathfrak{p}^n$.

We give an inductive proof on n. It is true for $n = 1$ by assumption. Let π be a generator of $\mathfrak{p}$, $b = b_n$ and $b' = b_n'$. Suppose that

$$bb' = 1 + \pi^n r_1 \text{ and } b + b' = x + \pi^n r_2, r_i \in R.$$

Then we have

$$\begin{cases} (b + k\pi^n)(b' + l\pi^n) \equiv 1 + (r_1 + b'k + bl)\pi^n \text{ mod } \pi^{n+1} \\ (b + k\pi^n) + (b' + l\pi^n) = x + (r_2 + k + l)\pi^n. \end{cases}$$

Hence it suffices to show that $k + l$ assumes all values modulo π under the restriction $r_1 + b'k + bl \equiv 0$ mod π. But

$$r_1 + b'k + bl \equiv 0 \Longleftrightarrow k + l \equiv -br_1 - l(b^2 - 1),$$

and the result follows, since $b^2 - 1 \in R^*$. □

The following lemma is a special case of a well known result about representations by quadratic forms over finite fields [10, Ch.4, Prop.4.4].

(2.3) Lemma. *Let $\mathbb{F}_q$ denote a finite field with q elements. If q is odd, then*

$$\left|\{x \in \mathbb{F}_q : x^2 - 1 \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2\}\right| = \frac{q-1}{2}.$$

(2.4) Lemma. *Let R be the integers in a totally real algebraic number field F. If $\mathfrak{I}$ is an ideal in R and $\alpha, \beta \in R$, then*

$$|\sigma(\mathfrak{I}) \cap P_y(r)| = \frac{2^{2n-1}}{N\mathfrak{I}\sqrt{|D_F|}} \cdot r + O(r^{1-\frac{1}{n}}), \text{ when } r \longrightarrow \infty.$$

In particular, this implies that the different classes modulo $\mathfrak{I}$ are equally distributed in $P(r)$ in the sense that

$$\lim_{r\to\infty} \frac{|\sigma(\alpha+\mathfrak{I}) \cap P(r)|}{|\sigma(\beta+\mathfrak{I}) \cap P(r)|} = 1.$$

Proof. If $y = 0$, then the first statement is a special case of [7, Ch.V, Th.1]. But it is easy to adopt the proof of this theorem to a translated parallelotope, since one only makes use of the structure of the boundary and the volume of the parallelotope, which of course are independent of y.

The second statement follows since $|\sigma(\alpha+\mathfrak{I}) \cap P(r)| = |\sigma(\mathfrak{I}) \cap P_{-\alpha}(r)|$. □

(2.5) Lemma. *Let R be the integers in an algebraic number field, let $\alpha \in R$ be given, and $X_\alpha = \sigma\left(\{x \in R : \exists t \in R,\, x^2 - \alpha t^2 = 1\}\right)$. Then*

$$f(r) = \frac{|X_\alpha \cap P(r)|}{|\sigma(R) \cap P(r)|} \longrightarrow 0, \text{ when } r \longrightarrow \infty.$$

Proof. Let $\mathfrak{p}$ be a prime ideal in R, with $N\mathfrak{p}$ odd. According to (2.3),

$$x^2 - \alpha t^2 \equiv 1 \bmod \mathfrak{p}$$

has at most $\frac{N\mathfrak{p}+1}{2}$ solutions x inequivalent modulo $\mathfrak{p}$. Hence, if

$$X_{\alpha,\mathfrak{p}} = \sigma\left(\{x \in R : \exists t \in R,\, x^2 - \alpha t^2 \equiv 1 \bmod \mathfrak{p}\}\right),$$

then there exists $r_\mathfrak{p}$, such that

$$\frac{|X_{\alpha,\mathfrak{p}} \cap P(r)|}{|\sigma(R) \cap P(r)|} < \frac{N\mathfrak{p}+2}{2N\mathfrak{p}}, \text{ when } r > r_\mathfrak{p}.$$

This is true since the classes modulo $\mathfrak{p}$ are equally distributed according to (2.4). It is clear that $X_\alpha \subseteq \bigcap_\mathfrak{p} X_{\alpha,\mathfrak{p}}$. So by the Chinese Remainder Theorem, we get

$$f(r) \le \frac{|\bigcap_\mathfrak{p} X_{\alpha,\mathfrak{p}} \cap P(r)|}{|\sigma(R) \cap P(r)|} < \prod_\mathfrak{p} \frac{N\mathfrak{p}+2}{2N\mathfrak{p}} \text{ for } r > s,$$

where the product is over all $\mathfrak{p}$ with $r_\mathfrak{p} < s$. When $s \longrightarrow \infty$, then the number of factors in the product also approaches infinity, so $f(r) \longrightarrow 0$. □

3. Reformulation and localisation

The promised reformulation of the problem is the following obvious one. Let $\mathcal{O}$ be an order in $\mathfrak{A} \cong (a,b)_F$. The question whether $2x_0 \in Tr(\mathcal{O}^1)$ is equivalent to, whether there exists $q = x_0 + x_1 i + x_2 j + x_3 ij \in \mathcal{O}$, such that $N(x_1 i + x_2 j + x_3 ij) = 1 - x_0^2$.

(3.1) Proposition. *Let $L_{\mathcal{O}} = L = \{\lambda \in \mathfrak{A}_0 : \exists c \in F,\, c + \lambda \in \mathcal{O}\}$, where $\mathfrak{A}_0 = \{q \in \mathfrak{A} : Tr(q) = 0\}$. Then L is a lattice on $\mathfrak{A}_0$ and*

$$Tr(\mathcal{O}^1) = \left\{2x : \exists \lambda \in L,\, N(\lambda) = 1 - x^2\right\} =: S.$$

Proof. The inclusion $Tr(\mathcal{O}^1) \subseteq S$ is obvious, and so is the other inclusion when $\mathcal{O} = R \oplus L$. In general, let $\lambda \in L$ be such that $N(\lambda) = 1 - x^2$. Then there is a $c \in F$, such that $c + \lambda \in \mathcal{O}$. It is enough to show that $x + \lambda \in \mathcal{O}$, since $N(x + \lambda) = 1$ then implies $2x \in Tr(\mathcal{O}^1)$.

Since $c+\lambda$ and $x+\lambda$ commute, we have $x+\lambda \in F(c+\lambda)$. Both $c+\lambda$ and $x+\lambda$ are integral over R, since $c+\lambda \in \mathcal{O}$ and $N(x+\lambda) = 1$, $Tr(x+\lambda) = 2x$. ($2x \in R$ since $N(c+\lambda) = 1 - x^2 + c^2 \in R$ and $2c \in R$.) Hence $x - c$ is integral over R, so $x - c \in R$. But then

$$x + \lambda = (x - c) + (c + \lambda) \in \mathcal{O}.$$

□

The problem is thus formulated in terms of representations by ternary quadratic forms on lattices, since $L_{\mathcal{O}}$ is a ternary lattice with quadratic structure given by N.

The question of representations in the global case is not directly manageable. Since we are mainly considering asymptotics, it will be shown that local considerations will suffice. Therefore we introduce the following sets. Let $\nu \in \Omega$.

$$\begin{aligned} \mathcal{T}_\nu^{\mathcal{O}}(r) &= \left\{2x \in R :\ 1 < \sigma_1(x) \le r,\ 1 - x^2 \in N(L_{\mathcal{O}_\nu})\right\}, \\ \mathcal{T}_\Omega^{\mathcal{O}}(r) &= \textstyle\bigcap_{\nu \in \Omega} \mathcal{T}_\nu^{\mathcal{O}}(r), \\ \mathcal{T}_\infty^{\mathcal{O}}(r) &= \textstyle\bigcap_{\nu \in \Omega_\infty} \mathcal{T}_\nu^{\mathcal{O}}(r). \end{aligned}$$

If $\nu = \mathfrak{p} \in \Omega_f$, then we also define

$$\mathcal{T}_{\mathfrak{p},\infty}^{\mathcal{O}}(r) = \mathcal{T}_{\mathfrak{p}}^{\mathcal{O}}(r) \cap \mathcal{T}_\infty^{\mathcal{O}}(r).$$

When the argument r is excluded, we will mean the corresponding infinite set, which we get when the restriction on $\sigma_1(x)$ is replaced by $\sigma_1(x) > 1$. Here $L_{\mathcal{O}_\nu}$ is defined similarly as $L_{\mathcal{O}}$ in (3.1). Also observe that $L_{\mathcal{O}_\nu} = (L_{\mathcal{O}})_\nu$. Since $\sigma_i N$ is positive definite iff $2 \le i \le n$, $\mathcal{T}_\infty^{\mathcal{O}}$ only depends on F and we get that

$$\mathcal{T}_\infty^{\mathcal{O}}(r) = R \cap P(r).$$

Hence by (2.4), we get

$$|\mathcal{T}_{\infty}^{\mathcal{O}}(r)| = \frac{2^{2n-1}}{\sqrt{|D_F|}} \cdot r + O(r^{1-\frac{1}{n}}), \text{ when } r \longrightarrow \infty. \tag{3.2}$$

The hypothesis in [1] was that $|\mathcal{T}^{\mathcal{O}}(r)|$ and a natural modification of $|\mathcal{T}_{\infty}^{\mathcal{O}}(r)|$ depending on $\mathcal{O}$, have the same asymptotics when $r \longrightarrow \infty$. But this is too much to hope for, since we only have taken into account the archimedean completions. However, it is true that $|\mathcal{T}^{\mathcal{O}}(r)|$ and $|\mathcal{T}_{\Omega}^{\mathcal{O}}(r)|$ have the same asymptotics, when $r \longrightarrow \infty$. If $\mathcal{O}$ is a maximal order, or more generally an Eichler order, in a quaternion division algebra, then $\mathcal{T}^{\mathcal{O}} = \mathcal{T}_{\Omega}^{\mathcal{O}}$ [12, Ch.III, Prop.5.10]. To show that $|\mathcal{T}^{\mathcal{O}}(r)|$ and $|\mathcal{T}_{\Omega}^{\mathcal{O}}(r)|$ have the same asymptotics in general, we first need a known result from the theory of quadratic forms. An argument is included, since it does not seem to exist a complete argument in the literature in the general case. Though everything of importance is included in [6].

Before the statement of the proposition, we need some background. Let Q be a quadratic form on an R-lattice L. An element $\alpha \in F$ is represented by Q on $L_{\mathfrak{p}}$ $\forall \mathfrak{p} \in \Omega$ iff α is represented by a lattice in gen$L$, the genus of L. Suppose that $\alpha \in F$ is represented by a lattice in gen$L$, but not by all classes (resp. spinor genera) in gen$L$. Then α is called an exception (resp. spinor exception) of gen$L$. It is well known, that if dim$FL \geq 3$ and Q is not totally definite, then α is an exception of gen$L$ iff α is a spinor exception of gen$L$ [4].

The notation and terminology in the proof of (3.3) will follow [8]. The spinor norm will be denoted by θ. The idèle group of F will be denoted by J_F, and the subgroups J_F^L and P_D of J_F are defined by

$$\begin{aligned} J_F^L &= \left\{ i = (i_{\mathfrak{p}}) \in J_F : i_{\mathfrak{p}} \in \theta(O^+(L_{\mathfrak{p}}))\, \forall \mathfrak{p} \in \Omega \right\} \\ P_D &= \left\{ i = (i_{\mathfrak{p}}) \in J_F : i_{\mathfrak{p}} = \alpha,\ \alpha \in \theta(O^+(V)) \right\}, \end{aligned}$$

where $V = FL$.

(3.3) Proposition. *Let F be an arbitrary algebraic number field with integers R, and let Q be a quadratic form on an R-lattice L, with rk$L = 3$. Then all spinor exceptions of gen$L$ in F are included in a finite set of classes in $F^*/(F^*)^2$.*

Proof. Suppose that $\alpha \in F$ is represented by gen$L$. Let $E = F(\sqrt{d})$, where $d \in -\alpha\cdot$disc(V). Here disc$(V) \in F^*/(F^*)^2$ is the discriminant of the quadratic space (V, Q), where $V = FL$. According to Theorem 2 in [6], α can be a spinor exception only if

$$[J_F : P_D N_{E/F}(J_E) J_F^L] = 2.$$

Let $T = \{\mathfrak{p} \in \Omega_\infty : (V_{\mathfrak{p}}, Q) \text{ is anisotropic}\}$, and let

$$I_F(\mathfrak{p}) = \left\{ i \in J_F : i_{\mathfrak{q}} = 1,\ \forall \mathfrak{q} \in \Omega \setminus \{\mathfrak{p}\} \right\}.$$

If $I_F = \prod_{\mathfrak{p}\in T} I_F(\mathfrak{p})$, then according to the proof of Theorem 2 in [6]

$$[J_F : P_D N_{E/F}(J_E) I_F] = 2.$$

If

$$J_F^{L'} = \{i \in J_F^L : i_{\mathfrak{p}} = 1 \,\forall \mathfrak{p} \in T\},$$

then $J_F^L = J_F^{L'} I_F$ and $J_F^{L'} \cap I_F = 1$. Hence

$$2 = [J_F : P_D N_{E/F}(J_E) J_F^L] = [J_F : P_D N_{E/F}(J_E) J_F^{L'} I_F]$$

iff

$$J_F^{L'} \subseteq P_D N_{E/F}(J_E).$$

By exactly the same argument as in the lemma preceding Theorem 2 in [6], one gets that

$$J_F^{L'} \subseteq P_D N_{E/F}(J_E) \Longleftrightarrow J_F^{L'} \subseteq N_{E/F}(J_E).$$

Since $L_{\mathfrak{p}}$ is unimodular for almost all $\mathfrak{p} \in \Omega_f$, $\theta(O^+(L_{\mathfrak{p}})) \supseteq R_{\mathfrak{p}}^*$ for almost all $\mathfrak{p} \in \Omega_f$. Hence $J_F^{L'} \subseteq N_{E/F}(J_E)$ implies that the ramified primes of E/F are included in a fixed finite set. Therefore only a finite number of extensions E/F is possible for α being a spinor exception, and the result follows. □

Since $L_{\mathcal{O}_{\mathfrak{p}}}$ is unimodular with respect to N for all $\mathfrak{p} \nmid d(\mathcal{O})$, we get $N(L_{\mathcal{O}_{\mathfrak{p}}}) = R_{\mathfrak{p}}$ for almost all $\mathfrak{p} \in \Omega_f$ [8, 92:1b] and

$$\mathcal{T}_\Omega^{\mathcal{O}}(r) = \bigcap_{\mathfrak{p}|d(\mathcal{O})} \mathcal{T}_{\mathfrak{p},\infty}^{\mathcal{O}}(r).$$

Since $\mathcal{T}_{\mathfrak{p}}^{\mathcal{O}}$ contains a whole class modulo $\mathfrak{p}^n$ for some n, it follows that $\mathcal{T}_\Omega^{\mathcal{O}}$ contains a whole class modulo some ideal. Hence

$$\frac{|\mathcal{T}_\Omega^{\mathcal{O}}(r)|}{|\mathcal{T}_\infty^{\mathcal{O}}(r)|} \geq C > 0, \tag{3.4}$$

for some constant C if r is big enough.

Now we are able to formulate and prove the first of the main results:

(3.5) Theorem. *The sets $\mathcal{T}^{\mathcal{O}}(r)$ and $\mathcal{T}_\Omega^{\mathcal{O}}(r)$ satisfy*

$$\lim_{r\to\infty} \frac{|\mathcal{T}^{\mathcal{O}}(r)|}{|\mathcal{T}_\Omega^{\mathcal{O}}(r)|} = 1.$$

Proof. If $[\alpha]$ denotes a class in $F^*/(F^*)^2$, then let

$$E_{[\alpha]}(r) = \left\{2x \in \mathcal{T}_\Omega^{\mathcal{O}}(r) : 1 - x^2 \in [\alpha]\right\}.$$

Then by (3.3)

$$\mathcal{T}^{\mathcal{O}}(r) \supseteq \mathcal{T}_\Omega^{\mathcal{O}}(r) \setminus \bigcup_{i=1}^{m} E_{[\alpha_i]}(r),$$

where m is a positive integer. Hence it suffices to show that

$$\lim_{r\to\infty}\frac{|E_{[\alpha]}(r)|}{|\mathcal{T}_{\Omega}^{\mathcal{O}}(r)|}=0.$$

Let X_α be as in (2.5). Then $E_{[\alpha]}\subseteq R\cap X_\alpha$, and the result follows from (2.5) and (3.4) since

$$\frac{|E_{[\alpha]}(r)|}{|\mathcal{T}_{\Omega}^{\mathcal{O}}(r)|}\le\frac{|R\cap X_\alpha|}{|\mathcal{T}_{\infty}^{\mathcal{O}}(r)|}\frac{|\mathcal{T}_{\infty}^{\mathcal{O}}(r)|}{|\mathcal{T}_{\Omega}^{\mathcal{O}}(r)|}\le\frac{|R\cap X_\alpha|}{|\mathcal{T}_{\infty}^{\mathcal{O}}(r)|}\frac{1}{C}.$$

□

We will conclude this section with an explanation of how to use (3.5) and local computations to determine at least the asymptotics of $\mathcal{T}^{\mathcal{O}}(r)$.

If $x\in R$, then let $[x]_{\mathfrak{p}^n}$ be the elements in R, which are congruent to x modulo $\mathfrak{p}^n$. We define the sequences $m_{\mathfrak{p}}^{(n)}(\mathcal{O})$ and $M_{\mathfrak{p}}^{(n)}(\mathcal{O})$ in n as

$$m_{\mathfrak{p}}^{(n)}(\mathcal{O})=\frac{1}{(N\mathfrak{p})^n}\cdot\left|\left\{[x]_{\mathfrak{p}^n}:[x]_{\mathfrak{p}^n}\subseteq\mathcal{T}_{\mathfrak{p}}^{\mathcal{O}}\right\}\right| \tag{3.6}$$

and

$$M_{\mathfrak{p}}^{(n)}(\mathcal{O})=\frac{1}{(N\mathfrak{p})^n}\cdot\left|\left\{[x]_{\mathfrak{p}^n}:\exists y\in[x]_{\mathfrak{p}^n},\,y\in\mathcal{T}_{\mathfrak{p}}^{\mathcal{O}}\right\}\right|. \tag{3.7}$$

Then $m_{\mathfrak{p}}^{(n)}(\mathcal{O})$ is an increasing sequence with an upper bound and $M_{\mathfrak{p}}^{(n)}(\mathcal{O})$ is a decreasing sequence with a lower bound. Hence the limits

$$m_{\mathfrak{p}}(\mathcal{O})=\lim_{n\to\infty}m_{\mathfrak{p}}^{(n)}(\mathcal{O})\text{ and }M_{\mathfrak{p}}(\mathcal{O})=\lim_{n\to\infty}M_{\mathfrak{p}}^{(n)}(\mathcal{O}) \tag{3.8}$$

exist.

To prove that $m_{\mathfrak{p}}(\mathcal{O})=M_{\mathfrak{p}}(\mathcal{O})$, we introduce the unique additive Haar measure μ on $F_{\mathfrak{p}}$ normalised so that $\mu(R_{\mathfrak{p}})=1$. Let S_n be the set of elements in $R_{\mathfrak{p}}$, which are included in a class modulo $\mathfrak{p}^n$, so that this class is partly included in $\mathcal{T}_{\mathfrak{p}}^{\mathcal{O}}$. Then by definition

$$\mu(S_n)=M_{\mathfrak{p}}^{(n)}(\mathcal{O})-m_{\mathfrak{p}}^{(n)}(\mathcal{O}).$$

The sets S_n are open, decreasing and $\bigcap_{n=1}^{\infty}S_n=\emptyset$. In fact suppose that $x\in\bigcap_{n=1}^{\infty}S_n$. Then

$$N(\lambda_n)\equiv 1-x^2 \bmod \mathfrak{p}^n$$

has a solution $\lambda_n\in L_{\mathcal{O}_{\mathfrak{p}}}$ for all n. But then there is a $\lambda\in L_{\mathcal{O}_{\mathfrak{p}}}$, such that $N(\lambda)=1-x^2$. If an element x is represented by a quadratic form, then there is an open set containing x which is represented by this form, and hence there is n such that $x\notin S_n$.

Hence

$$0=\mu(\bigcap_{n=1}^{\infty}S_n)=\lim_{n\to\infty}\mu(S_n),$$

and we get $m_{\mathfrak{p}}(\mathcal{O})=M_{\mathfrak{p}}(\mathcal{O})$.

For any $\epsilon > 0$, we get by (2.4) that

$$m_{\mathfrak{p}}^{(n)}(\mathcal{O}) - \epsilon < \frac{|\mathcal{T}_{\mathfrak{p},\infty}^{\mathcal{O}}(r)|}{|\mathcal{T}_{\infty}^{\mathcal{O}}(r)|} < M_{\mathfrak{p}}^{(n)}(\mathcal{O}) + \epsilon, \text{ if } r > r_n$$

for some r_n depending on n. Hence from the argument above, we get that

$$\lim_{r\to\infty} \frac{|\mathcal{T}_{\mathfrak{p},\infty}^{\mathcal{O}}(r)|}{|\mathcal{T}_{\infty}^{\mathcal{O}}(r)|} = \lim_{n\to\infty} m_{\mathfrak{p}}^{(n)}(\mathcal{O}) = m_{\mathfrak{p}}(\mathcal{O}).$$

By the Chinese Remainder Theorem and the same argument as above with $\mathfrak{p}$ replaced by, for example, $\mathfrak{I} = \prod_{\mathfrak{p}|d(\mathcal{O})} \mathfrak{p}$, we get the following result:

(3.9) Proposition. *Let $m_{\mathfrak{p}}(\mathcal{O})$ be defined by* (3.6) *and* (3.8)*. Then*

$$\lim_{r\to\infty} \frac{|\mathcal{T}_{\Omega}^{\mathcal{O}}(r)|}{|\mathcal{T}_{\infty}^{\mathcal{O}}(r)|} = \prod_{\mathfrak{p}|d(\mathcal{O})} m_{\mathfrak{p}}(\mathcal{O}).$$

From (3.2), (3.5) and (3.9), we derive the following result on the asymptotics for the trace set of $\mathcal{O}^1$.

(3.10) Theorem. *Let $\mathcal{O}$ be an arbitrary order in a quaternion algebra satisfying* (1.1)*. Then*

$$\lim_{r\to\infty} \frac{|\mathcal{T}^{\mathcal{O}}(r)|}{r} = \frac{2^{2n-1}}{\sqrt{|D_F|}} \prod_{\mathfrak{p}|d(\mathcal{O})} m_{\mathfrak{p}}(\mathcal{O}).$$

4. Local computations

The goal of this section is to determine the numbers $m_{\mathfrak{p}}(\mathcal{O})$ for some important classes of orders. We will achieve a complete answer in the case of Bass orders $\mathcal{O}$ with Eichler invariant $e(\mathcal{O}) = \pm 1$. These include maximal orders and so called Eichler orders, since Eichler orders are Bass orders with Eichler invariant $e(\mathcal{O}) = 1$. The Eichler invariant depends on the structure of $\mathcal{O}/J(\mathcal{O})$, where $J(\mathcal{O})$ is the Jacobson radical and was introduced in [3]. All necessary information about (Bass) orders in quaternion algebras can be found in [2].

In this section F will denote a $\mathfrak{p}$-adic field with integers R and prime ideal $\mathfrak{p}$. Furthermore, we define $F_t(x)$ to be the quadratic extension of F, with x satisfying $x^2 - tx + 1 = 0$.

Sums with the lower bound greater than the upper bound will be considered empty, and $[x]$ will denote the greatest integer less than or equal to x.

(4.1) Remark. To determine how many of the elements $t \equiv \pm a \bmod \mathfrak{p}^m$ that are traces, we may always restrict to $t \equiv a \bmod \mathfrak{p}^m$ and multiply the result by 2, since $t \in Tr(\mathcal{O}^1)$ iff $-t \in Tr(\mathcal{O}^1)$. □

The following observations will reduce the amount and difficulty of the computations needed.

(4.2) Proposition. *Let E_n be an Eichler order in $M_2(F)$ with discriminant $d(E_n) = \mathfrak{p}^n$. Then $t \in Tr(E_n^1)$ for all $n \geq 1$ iff $F_t(x)$ is not a field.*

Proof. We have that E_n is isomorphic to the order, which consists of all elements

$$\begin{pmatrix} a & b \\ c\pi^n & d \end{pmatrix} \in M_2(R),$$

where $a, b, c, d \in R$ and π is a generator of $\mathfrak{p}$. Hence

$$t \in Tr(E_n^1),\ \forall n \geq 1 \iff \exists a \in R,\ a(t-a) \equiv 1 \bmod \mathfrak{p}^n,\ \forall n \geq 1.$$

But by Hensel's lemma [8, 13:8], this is equivalent to $F_t(x)$ not being a field. □

(4.3) Proposition. *Let E_n be an Eichler order in $M_2(F)$ with $d(E_n) = \mathfrak{p}^n$, and let $\mathcal{O}$ be the maximal order in the unique quaternion division algebra over F. Then $t \in R$ $(t \neq \pm 2)$ is either in $Tr(\mathcal{O}^1)$ or in $Tr(E_n^1)$ for all $n \geq 1$, but not in both. In particular*

$$m_{\mathfrak{p}}(\mathcal{O}) + \lim_{n\to\infty} m_{\mathfrak{p}}(E_n) = 1.$$

Proof. According to [12, Ch.II, Cor.1.9], $t \in Tr(\mathcal{O}^1)$ iff $F_t(x)$ is a field (if we exclude ± 1 from $\mathcal{O}^1$). Hence an element ($\neq \pm 2$) in R is either a trace in $\mathcal{O}^1$ or in E_n^1 for all $n \geq 1$ but not in both, and the result follows. □

In the dyadic case, which is the problematic one, it seems easier to deal with Eichler orders in general than with the maximal order in the division algebra. Therefore we start with calculating $m_{\mathfrak{p}}(E_n)$ for Eichler orders E_n.

(4.4) Proposition. *Let E_n be an Eichler order in $M_2(F)$ with $d(E_n) = \mathfrak{p}^n$ $(n \geq 1)$, and let $q = N\mathfrak{p}$.*

If $\mathfrak{p}$ is non-dyadic, then

$$m_{\mathfrak{p}}(E_n) = \frac{q-3}{2q} + \varphi_{\mathfrak{p}}(n),$$

where

$$\varphi_{\mathfrak{p}}(n) = \frac{2}{q^n} + \sum_{i=1}^{\left[\frac{n-1}{2}\right]} \frac{q-1}{q^{2i+1}}.$$

If $\mathfrak{p}$ is dyadic with $(2) = \mathfrak{p}^e$, then

$$m_{\mathfrak{p}}(E_n) = \frac{q-2}{2q} + \varphi_{\mathfrak{p}}(n),$$

where

$$\varphi_{\mathfrak{p}}(n) = \begin{cases} \displaystyle\sum_{i=1}^{\left[\frac{n-1}{4}\right]} \frac{q-1}{2q^{3i+1}} + \frac{1}{q^{\left[\frac{3n+2}{4}\right]}}, & \textit{if } n \leq 4e, \\ \displaystyle\sum_{i=1}^{e-1} \frac{q-1}{2q^{3i+1}} + \frac{q-2}{2q^{3e+1}} + \sum_{i=0}^{\left[\frac{n-(4e+3)}{2}\right]} \frac{q-1}{q^{3(e+1)+2i}} + \frac{2}{q^{n-e}}, & \textit{if } n \geq 4e+1. \end{cases}$$

Proof. From the proof of (4.2), it follows that $m_{\mathfrak{p}}(E_n) = m_{\mathfrak{p}}^{(n)}(E_n)$.

First suppose that $\mathfrak{p}$ is non-dyadic. Then there are $\frac{q-3}{2}$ pairs (a, a^{-1}) in $\mathbb{F}_q^*$, such that $a \neq a^{-1}$. From (2.1) and (2.2), it follows that

$$m_{\mathfrak{p}}(E_n) = \frac{q-3}{2q} + \varphi_{\mathfrak{p}}(n),$$

where $q^n \cdot \varphi_{\mathfrak{p}}(n)$ is the number of classes t modulo $\mathfrak{p}^n$, such that

$$t \equiv a + d \bmod \mathfrak{p}^n$$

has solutions, which satisfy $a \equiv d \equiv \pm 1 \bmod \mathfrak{p}$ and $ad \equiv 1 \bmod \mathfrak{p}^n$. These correspond to the classes for which $F_t(x)$ is ramified.

According to (4.1), we may restrict to $a \equiv 1$ and multiply by 2. We claim that

$$\text{(4.5)} \qquad t \in Tr(E_n^1),\ t \equiv 2 \bmod \mathfrak{p} \Longleftrightarrow t \equiv 2 \bmod \mathfrak{p}^n \text{ or } t \equiv 2 + \alpha^2\pi^{2m},$$

where $2 \leq 2m \leq n-1$, $\alpha \in R^*$. The result follows from (4.5) by adding the number of different classes and multiplying by 2.

To prove (4.5), we first remark that clearly $t \equiv 2 \bmod \mathfrak{p}^n$ is a trace, since $(1 + O(\pi^n))^2 = 1 + O(\pi^n)$. Suppose that $t \not\equiv 2 \bmod \mathfrak{p}^n$. Let

$$a = 1 + \sum_{i=1}^{\infty} a_i \pi^i \text{ and } d = 1 + \sum_{i=1}^{\infty} d_i \pi^i,$$

where a_i and d_i belong to a set of representatives modulo $\mathfrak{p}$ including 0. We have to investigate, which values $a_i + d_i$ assumes under the restriction $1 = ad$. Let m be the least integer i such that $a_i \neq 0$. If we multiply a and d and identify coefficients, we see that m is also the least integer i such that $d_i \neq 0$. Furthermore, we get a system:

$$\text{(4.6)} \quad \begin{cases} a_m + d_m & = & a_{m+1} + d_{m+1} = \ldots = a_{2m-1} + d_{2m-1} = 0 \\ a_{2m} + d_{2m} & = & -a_m d_m = a_m^2 \\ a_{2m+1} + d_{2m+1} & = & -a_{m+1}d_m - a_m d_{m+1} = 2a_m a_{m+1} + f_1(a_m) \\ & \vdots & \\ a_{2m+k} + d_{2m+k} & = & 2a_m a_{m+k} + f_k(a_m, \cdots, a_{m+k-1}), \end{cases}$$

where f_i are polynomials. Now (4.5) follows immediately from (4.6), since we may vary a_i freely and 2 is a unit.

Now suppose that $\mathfrak{p}$ is dyadic with $(2) = \mathfrak{p}^e$. Then there are $\frac{q-2}{2}$ pairs (a, a^{-1}) in $\mathbb{F}_q^*$, such that $a \neq a^{-1}$. From (2.1) and (2.2), it follows that

$$m_{\mathfrak{p}}(E_n) = \frac{q-2}{2q} + \varphi_{\mathfrak{p}}(n),$$

where $\varphi_{\mathfrak{p}}(n)$ is defined as above. Though in this case of course $1 \equiv -1 \bmod \mathfrak{p}$ so $\varphi_{\mathfrak{p}}(1) = \frac{1}{q}$.

To determine $\varphi_{\mathfrak{p}}(n)$ in the dyadic case, we use the same method. However, it will get more complicated, since 2 is no longer a unit. We will give a thorough proof in the special case $e = 2$ and indicate how to generalise. This is probably the most illuminating, since $e = 2$ involves all complications and a proof with general e might be hard to follow. So assume that $2 = \pi^2\beta$, where $\beta \in R^*$, and let a and d be as above. By multiplying a and d and identifying coefficients, we get

$$(4.7) \qquad \begin{cases} a_1 + d_1 & = & 0 \\ a_2 + d_2 & = & a_1^2 \\ a_3 + d_3 & = & 2a_1a_2 - a_1^3 = a_1^3 \\ a_4 + d_4 & = & 2a_1a_3 + a_2^2 - a_2a_1^2 = a_2^2 + a_2a_1^2 \\ a_5 + d_5 & = & a_3a_1^2 + a_1a_2\beta + a_1a_2^2 \\ & \vdots & \\ a_{2+k} + d_{2+k} & = & a_ka_1^2 + f_k(a_1, \dots, a_{k-1}). \end{cases}$$

From this, we immediately get $\varphi_{\mathfrak{p}}(2) = \varphi_{\mathfrak{p}}(3) = \frac{1}{q^2}$ and $\varphi_{\mathfrak{p}}(4) = \frac{1}{q^3}$. If $a_1 = 0$, then $a_4 + d_4$ assumes all possible values, but $a_5 + d_5$ only one. On the other hand, if $a_1 \neq 0$, then $a_4 + d_4$ assumes half of the possible values and $a_k + d_k$ assumes all possible values for $k \geq 5$. Hence

$$\varphi_{\mathfrak{p}}(5) = \frac{q-1}{2q^4} + \frac{1}{q^4},\ \varphi_{\mathfrak{p}}(6) = \frac{q-1}{2q^4} + \frac{1}{q^5} \text{ and } \varphi_{\mathfrak{p}}(k) = \frac{q-1}{2q^4} + \varphi_{\mathfrak{p}}^{'}(k),$$

where $k \geq 7$ and $q^k \cdot \varphi_{\mathfrak{p}}^{'}(k)$ is the number of classes modulo $\mathfrak{p}^k$ with $a_1 = 0$.

Now assume that $a_1 = 0$. Then we get the following system:

$$(4.8) \qquad \begin{cases} a_2 + d_2 & = & a_3 + d_3 = 0 \\ a_4 + d_4 & = & a_2^2 \\ a_5 + d_5 & = & 2a_2a_3 = 0 \\ a_6 + d_6 & = & 2a_2a_4 + a_2^3 - a_3^2 = a_2^3 + a_3^2 \\ a_7 + d_7 & = & a_2a_3\beta + a_3a_2^2 \\ a_8 + d_8 & = & a_4^2 + a_4(a_2\beta + a_2^2) + f_4(a_2, a_3) \\ a_9 + d_9 & = & a_5^2(a_2\beta + a_2^2) + f_5(a_2, \dots, a_4) \\ & \vdots & \\ a_{4+k} + d_{4+k} & = & a_k^2(a_2\beta + a_2^2) + f_k(a_2, \dots, a_{k-1}) \end{cases}$$

From this, we get $\varphi_{\mathfrak{p}}(7) = \varphi_{\mathfrak{p}}(6) = \frac{q-1}{2q^4} + \frac{1}{q^5}$ and $\varphi_{\mathfrak{p}}(8) = \frac{q-1}{2q^4} + \frac{1}{q^6}$. If $a_2 = 0$ or $a_2 = \beta$, then $a_8 + d_8$ assumes all possible values, but $a_9 + d_9$ only one. On the other hand, if $a_2 \neq 0$ and $a_2 \neq \beta$, then $a_8 + d_8$ assumes half of the possible values and $a_k + d_k$ assumes all possible values for $k \geq 9$. Hence

$$\varphi_{\mathfrak{p}}(9) = \frac{q-1}{2q^4} + \frac{q-2}{2q^7} + \frac{2}{q^7},\ \varphi_{\mathfrak{p}}(10) = \frac{q-1}{2q^4} + \frac{q-2}{2q^7} + \frac{2}{q^8} \text{ and}$$

$$\varphi_{\mathfrak{p}}(k) = \frac{q-1}{2q^4} + \frac{q-2}{2q^7} + \varphi_{\mathfrak{p}}^{''}(k),$$

where $k \geq 11$ and $q^k \cdot \varphi_{\mathfrak{p}}^{''}(k)$ is the number of classes modulo $\mathfrak{p}^k$ with $a_1 = 0$ and $a_2 = 0$ or $a_2 = \beta$.

Since $1 \equiv -(1+\beta\pi^2) \bmod \mathfrak{p}^3$, we may restrict to $a_2 = 0$ and multiply the result by 2, when determining $\varphi''_{\mathfrak{p}}(k)$. If we assume $a_1 = a_2 = 0$, then we get the following system:

$$(4.9) \qquad \left\{ \begin{array}{rcl} a_3 + d_3 & = & a_4 + d_4 = a_5 + d_5 = 0 \\ a_6 + d_6 & = & a_3^2 \\ a_7 + d_7 & = & 2a_3a_4 = 0 \\ a_8 + d_8 & = & 2a_3a_5 + a_4^2 = a_4^2 \\ a_9 + d_9 & = & a_3a_4\beta + a_3^3 \\ a_{10} + d_{10} & = & a_5^2 + a_5a_3\beta + f_5(a_3, a_4) \\ a_{11} + d_{11} & = & a_6a_3\beta + f_6(a_3, \dots, a_5) \\ & \vdots & \\ a_{5+k} + d_{5+k} & = & a_ka_3\beta + f_k(a_3, \dots, a_{k-1}) \end{array} \right.$$

If $a_3 = 0$, then $a_{10} + d_{10}$ assumes all possible values, but $a_{11} + d_{11}$ only one. On the other hand, if $a_3 \neq 0$, then $a_{10} + d_{10}$ assumes half of the possible values and $a_k + d_k$ assumes all possible values for $k \geq 11$. Hence

$$\begin{aligned} \varphi_{\mathfrak{p}}(11) &= \frac{q-1}{2q^4} + \frac{q-2}{2q^7} + 2\left(\frac{q-1}{2q^9} + \frac{1}{q^9}\right), \\ \varphi_{\mathfrak{p}}(12) &= \frac{q-1}{2q^4} + \frac{q-2}{2q^7} + \frac{q-1}{q^9} + \frac{2}{q^{10}}, \\ \varphi_{\mathfrak{p}}(k) &= \frac{q-1}{2q^4} + \frac{q-2}{2q^7} + \frac{q-1}{q^9} + 2\varphi_{\mathfrak{p}}^{(3)}(k), \end{aligned}$$

where $k \geq 13$ and $q^k \cdot \varphi_{\mathfrak{p}}^{(3)}(k)$ is the number of classes modulo $\mathfrak{p}^k$ with $a_1 = a_2 = a_3 = 0$.

To conclude the proof in the case $e = 2$, we write the corresponding system when one assumes $a_1 = \ldots = a_{m-1} = 0$ for $m > 3$. One sees that this shows the same pattern as (4.9) and the formula follows by induction on m.

For a general e the pattern in (4.7) will occur $e-1$ times before we get a system with the pattern (4.8). This gives the first sum in the formula. As soon as the case $e = 2$ is fully understood, it is not too difficult to work through the general case.

Observe that the formula in the dyadic case with $e = 0$ is the same as the one in the non-dyadic case, except for the leading term. □

The following result, we get directly from (4.3) and (4.4).

(4.10) Proposition. *Let $\mathcal{O}$ be the maximal order in the unique quaternion division algebra $\mathfrak{A}$ over F, and let $q = N\mathfrak{p}$.*

If $\mathfrak{p}$ is non-dyadic, then

$$m_{\mathfrak{p}}(\mathcal{O}) = \frac{q^2 + 4q + 1}{2q(q+1)}.$$

If $\mathfrak{p}$ *is dyadic with* $(2) = \mathfrak{p}^e$, *then*

$$m_{\mathfrak{p}}(\mathcal{O}) = \frac{q^2+3q+2}{2q(q+1)} - \frac{1}{2q^{3e}(q+1)}\left(q^2(q^2-1)\frac{(q^{3(e-1)}-1)}{q^3-1} + q - 1\right).$$

We observe that the formula in the non-dyadic case agrees with the one in the dyadic case with $e = 0$.

(4.11) Remark. Let $\mathcal{O}$ be an Eichler order in a quaternion division algebra over an algebraic number field, such that $d(\mathcal{O})$ is square free. This is equivalent to that every localisation $\mathcal{O}_{\mathfrak{p}}$ is either maximal or isomorphic to $E_{\mathfrak{p}}$. Then according to [12, Ch.III, Prop.5.16], we have $t \in Tr(\mathcal{O})$ iff $t \in Tr(\mathcal{O}_{\mathfrak{p}})$ $\forall \mathfrak{p} \in \Omega_f$. Hence in this case, we can determine $Tr(\mathcal{O})$ exactly with the help of the proofs of (4.3) and (4.4).

For example, assume $\mathcal{O} \subset \mathfrak{A}$ with $\mathfrak{A}$ the algebra over $\mathbb{Q}$ which is ramified only at 3 and 5. Furthermore, assume that $d(\mathcal{O}) = 3\cdot 5\cdot 7$ and that $\mathcal{O}_7 \cong E_7$. Then $t \notin Tr(\mathcal{O})$ $(t \neq \pm 2)$ iff one of the following congruences is satisfied:

$$\begin{aligned} t &\equiv 0, \pm 3 \bmod 7 \\ t &\equiv \pm(2+3^{2m}) \bmod 3^{2m+1} \\ t &\equiv \pm(2 \pm 5^{2m}) \bmod 5^{2m+1} \\ t &\equiv 0 \bmod 5. \end{aligned}$$

□

Next we will investigate Bass orders $\mathcal{O}$ with $e(\mathcal{O}) = -1$. The proof of (4.12) will show an interesting 'anti-relation' between the traces for these orders and the traces for Eichler orders. We remark, that the discriminant of a Bass order with $e(\mathcal{O}) = -1$ is always a square if $\mathcal{O} \in M_2(F)$ and always a non-square if $\mathcal{O}$ is in the division algebra. Furthermore, there is only one isomorphism class for a given discriminant [2].

(4.12) Proposition. *Let* G_n *be an arbitrary Bass order in* $M_2(F)$, *with* $e(G_n) = -1$ $(n \geq 1)$ *and* $d(G_n) = \mathfrak{p}^{2n}$. *Furthermore let* $q = N\mathfrak{p}$ *and let* $\varphi_{\mathfrak{p}}$ *be as in* (4.4).

If $\mathfrak{p}$ *is non-dyadic, then*

$$m_{\mathfrak{p}}(G_n) = \frac{q-1}{2q} + \varphi_{\mathfrak{p}}(2n).$$

If $\mathfrak{p}$ *is dyadic with* $(2) = \mathfrak{p}^e$, *then*

$$m_{\mathfrak{p}}(G_n) = \frac{1}{2} + \varphi_{\mathfrak{p}}(2n).$$

Proof. With a slight change of notations compared to the result in [2, (5.4)], we get that G_n is isomorphic to the order consisting of all elements

$$\begin{pmatrix} a+b & b+(d-c)\pi^n \\ -\epsilon(b-c\pi^n) & a \end{pmatrix} \in M_2(R),\ a,b,c,d \in R,$$

where $X^2 - X + \epsilon$ is irreducible over R and π is a generator of $\mathfrak{p}$.

First we observe that if $F_t(x)$ is an unramified field, then $t \in Tr(G_n)$ for all $n \geq 1$. This can be proved in the same manner as (2.2) or (4.2). Furthermore, if $F_t(x)$ is not a field and unramified, then $t \notin Tr(G_n)$ for any n. This gives the first term in the formulas.

It remains to investigate the cases when $F_t(x)$ is ramified. The calculations are similar to the ones for Eichler orders. The number of classes are the same as in the case of Eichler orders, and the trace sets are in some sense complimentary. For example, if $t \in Tr(G_n)$ for all $n \geq 1$ then $F_t(x)$ is a field (or $t = \pm 2$), and in the non-dyadic case

$$t \in Tr(G_n^1),\ t \equiv 2 \bmod \mathfrak{p} \Longleftrightarrow t \equiv 2 \bmod \mathfrak{p}^{2n} \text{ or } t \equiv 2 + \beta\pi^{2m},$$

where $2 \leq 2m < 2n$, $\beta \in R^* \setminus (R^*)^2$. □

(4.13) Proposition. *Let Γ_n be an arbitrary Bass order in the unique quaternion division algebra over F, with $e(\Gamma_n) = -1$ $(n \geq 1)$ and $d(\Gamma_n) = \mathfrak{p}^{2n+1}$. Furthermore, let $\mathcal{O}$ be the maximal order in the quaternion division algebra over F, $q = N\mathfrak{p}$ and let $\varphi_\mathfrak{p}$ be as in* (4.4).

If $\mathfrak{p}$ is non-dyadic, then

$$m_\mathfrak{p}(\Gamma_n) = \frac{q^2+1}{2q(q+1)} + \frac{2}{q^{2n}(q+1)}.$$

If $\mathfrak{p}$ is dyadic with $(2) = \mathfrak{p}^e$, then

$$m_\mathfrak{p}(\Gamma_n) = \begin{cases} m_\mathfrak{p}(\mathcal{O}) + 2\varphi_\mathfrak{p}(2n+1) - \frac{1}{q} - \frac{1}{q^{\left[\frac{6n+5}{4}\right]}} & \text{if } n < 2e, \\ m_\mathfrak{p}(\mathcal{O}) + 2\varphi_\mathfrak{p}(2n+1) - \frac{1}{q} - \frac{2}{q^{2n+1-e}}, & \text{if } n \geq 2e. \end{cases}$$

Proof. From the explicit description in [2], we get that the norm and trace for elements in Γ_n is given by

$$N(\gamma) = a^2 + ab + \epsilon b^2 - \pi^{2n+1}(c^2 + cd + \epsilon d^2) \text{ and } Tr(\gamma) = 2a + b,$$

where $X^2 - X + \epsilon$ is irreducible over R, π is a generator of $\mathfrak{p}$ and a, b, c and d are arbitrary elements in R. Observe that this is very similar to the case of G_n. An important remark is that $\mathcal{O} = \Gamma_0$. It is trivial to check that $t \in Tr(\Gamma_n^1)$ iff $t \in Tr(\mathcal{O}^1)$ and $t = 2a + b$ for some $a, b \in R$ satisfying $a^2 + ab + \epsilon b^2 \equiv 1 \bmod \mathfrak{p}^{2n+1}$.

We give a complete argument in the non-dyadic case. It is exactly the same in the dyadic case, except for some details which will be clear from the remark below and the formula in the proposition.

It is easy to check that $t \in Tr(\Gamma_n^1)$ if $F_t(x)$ is an unramified field or $t \equiv \pm 2 \bmod \mathfrak{p}^{2n+1}$. It remains to check the case when $t \equiv \pm 2 \bmod \mathfrak{p}$, but $t \not\equiv \pm 2 \bmod \mathfrak{p}^{2n+1}$. The elements $t \in Tr(\mathcal{O}^1)$ which satisfy this, correspond to the summand

$$\left(\frac{2}{q} - \frac{2}{q^{2n+1}}\right) - \left(\varphi_\mathfrak{p}(2n+1) - \frac{2}{q^{2n+1}}\right) = \frac{2}{q} - \varphi_\mathfrak{p}(2n+1).$$

(This is where the dyadic case is slightly different.) Exactly the same calculation as in (4.13) reveals the same one-to-one correspondence between traces in E^1_{2n+1} and Γ^1_n. Hence we get the summand $\varphi_{\mathfrak{p}}(2n+1) - \frac{2}{q^{2n+1}}$ for $t \in Tr(\Gamma^1_n)$ with $t \equiv \pm 2 \bmod \mathfrak{p}$ but $t \not\equiv \pm 2 \bmod \mathfrak{p}^{2n+1}$. Summing up, we get

$$\begin{aligned} m_p(\Gamma_n) &= m_{\mathfrak{p}}(\mathcal{O}) - \left(\tfrac{2}{q} - \varphi_{\mathfrak{p}}(2n+1)\right) + \left(\varphi_{\mathfrak{p}}(2n+1) - \tfrac{2}{q^{2n+1}}\right) = \\ &= m_{\mathfrak{p}}(\mathcal{O}) + 2\varphi_{\mathfrak{p}}(2n+1) - \tfrac{2}{q} - \tfrac{2}{q^{2n+1}}. \end{aligned}$$

If we evaluate this, we get the desired formula. □

For the remaining Bass orders, those with Eichler invariant equal to 0, the situation is more complex. Then there are in general several different isomorphism classes for a given discriminant. Calculations similar to those of the proof of (4.4) have revealed, that there are Bass orders $\mathcal{O}_1$, $\mathcal{O}_2$, such that $d(\mathcal{O}_1) = d(\mathcal{O}_2)$, $e(\mathcal{O}_1) = e(\mathcal{O}_2) = 0$ but $m_{\mathfrak{p}}(\mathcal{O}_1) \neq m_{\mathfrak{p}}(\mathcal{O}_2)$ even in the non-dyadic case. It seems very hard to find general formulas for $m_{\mathfrak{p}}(\mathcal{O})$ for Bass orders with Eichler invariant equal to 0. Although, given such an order, it is of course possible to use the methods of this section to compute $m_{\mathfrak{p}}(\mathcal{O})$.

References

[1] J. Bolte, Periodic orbits in arithmetical chaos on hyperbolic surfaces, *Nonlinearity*, **6** (1993), 935–951.

[2] J. Brzezinski, On orders in quaternion algebras, *Comm. Algebra*, **11** (1983), 501–522.

[3] M. Eichler, Untersuchungen in der Zahlentheorie der rationalen Quaternionalgebren, *J. Reine Angew. Math.*, **174** (1936), 129–159.

[4] M. Eichler, Die Änlichkeitsklassen indefiniter Gitter, *Math. Z.*, **55** (1952), 216–252.

[5] D. A. Hejhal, "The Selberg Trace Formula for $PSL(2,\mathbb{R})$ vol. 1, 2," Lecture Notes in Mathematics 548, 1001, Springer-Verlag, Berlin-Heidelberg-New York, 1976, 1983.

[6] J. S. Hsia, Representations by spinor genera, *Pacific J. Math.*, **63** (1976), 147–152.

[7] S. Lang, "Algebraic Number Theory," Springer-Verlag, Berlin-Heidelberg-New York, 2nd ed., 1994.

[8] O. O'Meara, "Introduction to Quadratic Forms," Springer-Verlag, Berlin-Heidelberg-New York, 1973.

[9] P. Sarnak, "Arithmetic quantum chaos," R. A. Blyth Lectures, University of Toronto, 1993.

[10] C. Small, "Arithmetic of Finite Fields," Marcel Dekker, Inc., New York, Basel, Hong Kong, 1991.

[11] K. Takeuchi, A characterisation of arithmetic Fuchsian groups, *J. Math. Soc. Japan*, **27** (1975), 600–612.

[12] M.-F. Vigneras, "Arithmétique des Algèbres de Quaternions," Lecture Notes in Math. 800, Springer-Verlag, Berlin-Heidelberg-New York, 1980.