DESY 92-104 ISSN 0418-9833
July 1992

Periodic Orbits in Arithmetical Chaos

Jens Bolte

II. Institut für Theoretische Physik
Universität Hamburg
Luruper Chaussee 149, 2000 Hamburg 50
Fed. Rep. Germany

Abstract

Length spectra of periodic orbits are investigated for some chaotic dynamical systems whose quantum energy spectra show unexpected statistical properties and for which the notion of arithmetical chaos has been introduced recently. These systems are defined as the unconstrained motions of particles on two dimensional surfaces of constant negative curvature whose fundamental groups are given by number theoretical statements (arithmetic Fuchsian groups). It is shown that the mean multiplicity of lengths l of periodic orbits grows asymptotically like $c \cdot e^{l/2}/l$, $l \to \infty$. Moreover, the constant c (depending on the arithmetic group) is determined.

1 Introduction

In the semiclassical analysis of quantum mechanical systems one is interested in detecting traces of the properties of the underlying classical systems. These may either be integrable or totally chaotic, or their phase spaces consist of regions that are in some intermediate stage. Many investigators in the field for example have worked on the problem how to distinguish statistical properties of semiclassical energy spectra in the two extreme cases of integrable and strongly chaotic classical systems. It has been found [1] that the existence of action–angle variables for integrable systems leads to a Poissonian statistics for the nearest–neighbour spacings distribution in the (semiclassical) energy spectrum. (For rigorous results, see [2].) Concerning chaotic systems, however, no such result exists, although it is generally believed that the energy level statistics for classically chaotic systems may be described by the distribution of eigenvalues of large random hermitian matrices. This *random matrix theory* (RMT) [3] offers a phenomenological description of energy spectra and has been confirmed empirically in many examples [4].

Recently, a class of strongly chaotic systems has been found with energy spectra that do not fit into the universal scheme of RMT [5], but rather appear to be more like ones of classically integrable systems. These exceptional systems consist of single particles sliding freely on special two dimensional hyperbolic surfaces, i.e. surfaces endowed with a metric of constant negative curvature. In more sophisticated terms, the classical dynamics are defined by the geodesic flows on those surfaces. One realizes hyperbolic surfaces as quotients of the upper complex half–plane $\mathcal{H} = \{z = x + iy \,|\, y > 0\}$, with Poincaré metric $ds^2 = y^{-2}(dx^2 + dy^2)$ of constant Gaussian curvature $K = -1$, by discrete subgroups Γ of $PSL(2, I\!R)$, known as *Fuchsian groups* (of the first kind). Γ operates on $\mathcal{H}$ by fractional linear transformations: for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, $z \in \mathcal{H}$, one sets $\gamma z = (az + b)(cz + d)^{-1}$. The quantum versions of these systems are governed by the Hamiltonian $H = -\Delta$, where $\Delta = y^2(\partial_x^2 + \partial_y^2)$ is the hyperbolic Laplacian ($\hbar = 1 = 2m$). H is an operator on the Hilbert space $L^2(\Gamma\backslash\mathcal{H})$ of square integrable functions that are invariant under the Γ–operation on $\mathcal{H}$, i.e. $\psi(\gamma z) = \psi(z)$ for all $\gamma \in \Gamma$. For a certain subclass of these systems, characterized by number theoretical properties of the Fuchsian group, the notion of *arithmetical chaos* has been introduced recently [5] and it has been noted that the energy level statistics of these systems violate the universal laws of RMT. Several peculiarities appearing in arithmetical chaos have been worked out, e.g. the presence of an infinite algebra of hermitian operators commuting with the Hamiltonian (the *Hecke operators*) and an exponential growth of the multiplicities of lengths of classical periodic orbits.

Since Gutzwiller invented his by now famous trace formula [6], *periodic orbit theory* (POT) has been developed into a major and powerful tool to investigate the semiclassical quantization of chaotic dynamical systems. POT connects the energy spectrum of a quantum system to the set of periodic orbits of the underlying classical system. Because of this relationship one could hope to trace back the peculiarities of the energy spectra in arithmetical chaos to properties of the classical periodic orbits. For the geodesic flows on hyperbolic surfaces POT is even exact and not only a semiclassical approximation. The trace formula was known as the *Selberg trace formula* [7] in mathematics long before Gutzwiller treated the more general physical systems. It is the geodesic length spectrum that in these cases exactly determines the eigenvalues of the Laplacian. These facts may serve as a motivation to study length spectra of periodic orbits in arithmetical chaos more thoroughly.

The aim of this article now is to first explain the exact definition of arithmetical chaos in more detail and then to prove the law for the growth of the multiplicities of lengths of periodic orbits, a result which has been announced before independently in the two papers of ref. [5]. In addition we are now able to derive the constant multiplying the exponential, a problem which was left open in [5].

This paper is organized in the following way. The next section will contain a discussion of geodesic length spectra of general hyperbolic surfaces. It will introduce the necessary notation for subsequent considerations and relate length spectra of surfaces whose Fuchsian groups are commensurable. A collection of relevant definitions and facts from algebraic number theory will be presentd in section 3. These are needed to formulate the definition of arithmetic Fuchsian groups. The next section then will be devoted to a detailed discussion of length spectra that occur on hyperbolic surfaces with arithmetic Fuchsian groups. Out of this the main result on the mean multiplicities of geodesic lengths in the case of arithmetic groups will grow. This statement will be followed by a presentation of two explicit examples for which our result will be checked. A final discussion will then close the present article.

2 Length Spectra of Hyperbolic Surfaces

Since according to the Selberg trace formula [7] the spectrum of the Laplacian on a hyperbolic surface $M = \Gamma\backslash\mathcal{H}$ is determined by its geodesic length spectrum, we are interested in the geometry of such surfaces when Γ is a Fuchsian group of the first kind, i.e. a discrete subgroup of $PSL(2,\mathbb{R})$ such that M has finite hyperbolic area. In some loose notation the elements $\gamma \in \Gamma$ will also be viewed as matrices in $SL(2,\mathbb{R})$ and the identification of the matrices γ and $-\gamma$ in $PSL(2,\mathbb{R}) = SL(2,\mathbb{R})/\{\pm\mathbb{1}\}$ will be understood automatically. Thus $tr\,\gamma$ denotes the corresponding matrix–trace and we agree to choose it always non–negative.

The fundamental group of M is isomorphic to Γ, where the (free) homotopy classes in the fundamental group correspond to conjugacy classes of hyperbolic elements in Γ. ($\gamma \in \Gamma$ is called hyperbolic if $tr\,\gamma > 2$.) Each hyperbolic conjugacy class in Γ represents a closed geodesic on M and its length $l(\gamma)$, where γ is a representative from the appropriate conjugacy class $\{\gamma\}_\Gamma$ in Γ, is related to the trace of γ by

$$tr\,\gamma = 2\cosh\left(\frac{l(\gamma)}{2}\right) \ . \tag{1}$$

The determination of the geodesic length spectrum thus is equivalent to describing the set of traces of inconjugate hyperbolic elements in the Fuchsian group Γ. In section 4 we therefore will study which traces of group elements will occur for arithmetic Fuchsian groups.

This section, however, will be devoted to a detailed investigation of length spectra of general hyperbolic surfaces to prepare for the more specific later considerations. Such a length spectrum may be degenerate, i.e. there possibly exist distinct geodesics on the surface sharing the same length l. In this case the multiplicity of l will be denoted by $g(l) \in \mathbb{N}$. In addition we will call a geodesic *primitive* if it is traversed only once. Then a corresponding representative $\gamma \in \Gamma$ is also primitive, i.e. it is not a power (≥ 2) of some other element in Γ. The primitive geodesics give rise to the primitive length spectrum, which is the object we are primarily interested in. The knowledge of the sets of distinct lengths $\mathcal{L}(\Gamma)$ and of distinct primitive lengths $\mathcal{L}_p(\Gamma)$ then allows to investigate the mean multiplicities $< g(l) >$ and $< g_p(l) >$, respectively. This is possible since for all Fuchsian groups *Huber's law* [8] universally determines the proliferation of geodesic lengths. It states, using the notations $\mathcal{L}(\Gamma) = \{l_1 < l_2 < l_3 \ldots\}$ and $\mathcal{L}_p(\Gamma) = \{l_{p,1} < l_{p,2} < l_{p,3} < \ldots\}$, that

$$\begin{aligned} N_p(l) &:= \#\{\,\{\gamma_p\}_\Gamma \subset \Gamma \,|\, l(\gamma_p) \le l\,\} \\ &= \sum_{l_{p,n} \le l} g_p(l_{p,n}) \;\sim\; \frac{1}{l}\, e^l \;, \quad l \to \infty \;. \end{aligned} \tag{2}$$

We now define the counting function $\hat{N}_p(l)$ of distinct primitive lengths,

$$\begin{aligned} \hat{N}_p(l) &:= \#\{\, n \,|\, l_{p,n} \le l\,\} \\ &= \sum_{l_{p,n} \le l} 1 \;, \end{aligned} \tag{3}$$

and, analogously, $\hat{N}(l)$ as a counting function for $\mathcal{L}(\Gamma)$. Knowing $\hat{N}_p(l)$ for $l \to \infty$ in addition to Huber's law (2) permits to find the asymptotics of the local average $< g_p(l) >$ of the multiplicities of primitive lengths as in [9].

In section 4 we mainly will not deal with the primitive but rather with the complete length spectrum. But we observe that

$$\hat{N}(l) = \sum_{l_n \le l} 1 = \sum_{r=1}^{[l/l_1]} \sum_{r l_{p,n} \le l} 1 = \sum_{r=1}^{[l/l_1]} \hat{N}_p(l/r) \;. \tag{4}$$

Since $\hat{N}_p(l)$ is positive and monotonically increasing, asymptotically for $l \to \infty$ the sum on the very right of (4) is dominated by the first term $r = 1$. Thus $\hat{N}(l) \sim \hat{N}_p(l)$ for $l \to \infty$. We conclude that in order to gain information on the asymptotics of $< g_p(l) >$ for $l \to \infty$ one has to count the distinct geodesic lengths up to l in the limit $l \to \infty$. Performing this for arithmetic Fuchsian groups will be the main task in section 4.

It is known that for general hyperbolic surfaces $g_p(l)$ is always unbounded [10]. A crude estimate of how frequently high values for $g_p(l)$ might occur shows that these will show up very scarcely. Numerical computations of the lower parts of length spectra for several arbitrarily chosen compact surfaces of genus two show [11] that $g_p(l)$ never exceeds four in the computed range, a value expected by symmetry arguments. One might therefore speculate that high values for the multiplicities of primitive lengths are so much suppressed that they do not influence the asymptotics of their mean $< g_p(l) >$. The latter rather seems to approach a constant value determined only by the order of the group of geometric symmetries (isometries) of M. The situation, however, changes drastically if Γ is an arithmetic group. For $\Gamma = PSL(2,\mathbb{Z})$ e.g. it has been found that $< g_p(l) >\sim 2\,e^{l/2}/l$, $l \to \infty$. Another example of an arithmetic group that has been treated before is that of the *regular octagon group*. In [12] it is shown that $< g_p(l) >\sim 8\sqrt{2}\,e^{l/2}/l$, $l \to \infty$, for this surface. The observation appearing in [5] now states that for every arithmetic Fuchsian group $< g_p(l) >\sim const.\, e^{l/2}/l$, $l \to \infty$, is realized. This is significantly different from what is found in the "generic" cases mentioned before.

For reasons that will become clear in section 4, we are interested in the relation of length spectra for commensurable Fuchsian groups. (We remark that two subgroups H_1 and H_2 of a group G are said to be *commensurable* if their intersection is a subgroup of finite index in both H_1 and H_2.) But let us first consider the case of a Fuchsian group Γ_1 that is a subgroup of finite index d in some other Fuchsian group (of the first kind) Γ_2. The generalization of the result on the relation of the counting functions $\hat{N}(l)$, to be achieved in the subsequent reasoning, to the case of commensurable groups will then easily follow, see (9)–(11).

The first step will be to notice that if $\gamma \in \Gamma_2$ then there exists a $k \in \mathbb{N}$ such that $\gamma^k \in \Gamma_1$. To see this take any $\gamma \in \Gamma_2$ and form $\cup_{m\in\mathbb{Z}}\, \Gamma_1\gamma^m \subset \Gamma_2$. The union cannot be disjoint since Γ_1 is of finite index in Γ_2. Therefore there exists a $\gamma_0 \in \Gamma_1\gamma^r \cap \Gamma_1\gamma^s$ for some pair $r \neq s$. Thus γ^{r-s} and γ^{s-r} lie in Γ_1. Choosing $k = |r-s|$ then proves the assertion.

The set of all distinct primitive lengths derived from Γ_2 will be denoted by

$$\mathcal{L}_p(\Gamma_2) = \{l_{p,1} < l_{p,2} < l_{p,3} < \ldots\}\ , \tag{5}$$

and one would now like to determine $\mathcal{L}_p(\Gamma_1)$ in terms of the $l_{p,n} \in \mathcal{L}_p(\Gamma_2)$. This can be achieved by what has just been proven. Let therefore γ_p be a primitive hyperbolic element in Γ_2, hence $l(\gamma_p) \in \mathcal{L}_p(\Gamma_2)$. Then either *i)* $\gamma_p \in \Gamma_1$: γ_p is also primitive hyperbolic in Γ_1 and $l(\gamma_p) \in \mathcal{L}_p(\Gamma_1)$, or *ii)* $\gamma_p \notin \Gamma_1$. Then, by the above remark, there exists a $k \in \mathbb{N}$ with $\gamma_p^k \in \Gamma_1$. The minimal such k takes care for $l(\gamma_p^k) = k\,l(\gamma_p)$ to be an element of $\mathcal{L}_p(\Gamma_1)$. Altogether, the set of primitive lengths referring to Γ_1 can be characterized by

$$\mathcal{L}_p(\Gamma_1) = \{k_1\, l_{p,1}\, ,\ k_2\, l_{p,2}\, ,\ k_3\, l_{p,3}\, , \ldots\} \tag{6}$$

with positive integers k_j. Since the k_j's can take arbitrary values in $\mathbb{N}$, this enumeration of elements of $\mathcal{L}_p(\Gamma_1)$, however, is not an ordered one.

Next we are going to discuss the counting functions $\hat{N}_p^{(1)}(l)$ and $\hat{N}_p^{(2)}(l)$ for distinct primitive lengths derived from Γ_1 and Γ_2, respectively. Given the above representations for $\mathcal{L}_p(\Gamma_1)$ and $\mathcal{L}_p(\Gamma_2)$, the problem consists of determining the asymptotics of $\hat{N}_p^{(1)}(l)$ for $l \to \infty$ in terms of the behaviour of $\hat{N}_p^{(2)}(l)$. In this context there arises the question how often a certain value for the k_j's in (6) occurs.

To answer this question, one decomposes Γ_2 into cosets of Γ_1. Since Γ_1 was assumed to be a subgroup of index $d < \infty$ in Γ_2, the decomposition looks like

$$\Gamma_2 = \Gamma_1 \,\dot{\cup}\, \Gamma_1\gamma_1 \,\dot{\cup} \ldots \dot{\cup}\, \Gamma_1\gamma_{d-1} \;, \tag{7}$$

with $\gamma_i \in \Gamma_2$, $\gamma_i \notin \Gamma_1$. Going through the set of inconjugate primitive hyperbolic elements of Γ_2 (in ascending order of the corresponding lengths) then yields for $l \to \infty$ a fraction of $1/d$ of those to lie in Γ_1; a fraction of $1 - 1/d$ does not fall into Γ_1. Thus a fraction of $1/d$ of the k_j's in (6) equals one; a fraction of $(1 - 1/d)/d$ of the k_j's equal two, and so on. One thus concludes, looking at the subsequence of $k_j = 1$ in (6), that for $l \to \infty$

$$d^{-1}\,\hat{N}_p^{(2)}(l) \le \hat{N}_p^{(1)}(l) \le \hat{N}_p^{(2)}(l) \;. \tag{8}$$

The inequality on the right follows trivially from (5) and (6). On the left we give an inequality rather than an equality, because there might be some $k_j \ge 2$ such that $k_j\, l_{p,j} \le l$. The number of $k_j = k \ge 2$ such that $k\, l_{p,j} \le l$ is, however, bounded by $\hat{N}_p^{(2)}(l/k)$ and therefore subdominant compared to the contribution coming from $k = 1$. Thus asymptotically for $l \to \infty$ one finds the result

$$\hat{N}_p^{(1)}(l) \sim d^{-1}\,\hat{N}_p^{(2)}(l) \;. \tag{9}$$

This is the relation that we were seeking for. Because of (4) the same relation also holds for the corresponding quantities $\hat{N}^{(i)}(l)$ of the complete length spectra.

Finally, a comment on the case of two commensurable Fuchsian groups Γ_a and Γ_b will be added. Their intersection $\Gamma_0 := \Gamma_a \cap \Gamma_b$ shall be a subgroup of index d_a in Γ_a and of index d_b in Γ_b. Introducing an obvious notation for the counting functions of the primitive length spectra corresponding to Γ_0, Γ_a and Γ_b, and using (9), shows that for $l \to \infty$

$$\hat{N}_p^{(0)}(l) \;\;\sim\;\; d_a^{-1}\,\hat{N}_p^{(a)}(l) \;,$$

$$\hat{N}_p^{(0)}(l) \;\; \sim \;\; d_b^{-1}\, \hat{N}_p^{(b)}(l) \; . \tag{10}$$

¿From this observation one draws the main result of this section, namely

$$\hat{N}_p^{(a)}(l) \sim (d_a/d_b) \, \cdot \, \hat{N}_p^{(b)}(l) \; , \quad l \to \infty \; . \tag{11}$$

Therefore, given two commensurable Fuchsian groups, their numbers of distinct (primitive) lengths up to a given value l are, in the limit $l \to \infty$, proportional to one another. The factor of proportionality is given by the ratio of the indices with which the two groups contain their intersection as a subgroup. This nice result will find an application in section 4.

3 Arithmetic Fuchsian Groups

In this section we want to recall the definition of *arithmetic Fuchsian groups* that give rise to the chaotic systems showing arithmetical chaos. They are Fuchsian groups of the first kind that have special properties due to their number theoretical nature.

In general it will not be possible to define an arbitrary Fuchsian group by giving rules that determine the matrix entries of the group elements explicitly. Usually, Γ will be characterized by some explicit generator matrices, which in many cases are constrained by one or several relations. One of the most prominent examples of a Fuchsian group is the modular group $PSL(2,\mathbb{Z})$. This, however, can easily be characterized since it consists of all 2×2–matrices of unit determinant with integer entries. These matrix entries are therefore given by a simple arithmetic statement. The most general possible extension of this example now is formed by the arithmetic Fuchsian groups. Their group elements are given by matrices with certain entries from an algebraic number field. The precise definition of these groups requires some algebraic number theory, and for the convenience of the reader, this section contains a short survey of those aspects of algebraic number theory that are relevant for the subsequent discussion. For a further reference, see [13, 14, 15].

An extension K of finite degree n of the field of rational numbers $\mathbb{Q}$ is a field that contains $\mathbb{Q}$ as a subfield and, viewed as a vector space over $\mathbb{Q}$ (in the obvious manner), is of finite dimension n. Let $\mathbb{Q}[x]$ denote the ring of polynomials in a variable x with rational coefficients. $\alpha \in K$ will be called *algebraic*, if it is a zero of some polynomial from $\mathbb{Q}[x]$. The *minimal* *polynomial* of α is the (unique) element in $\mathbb{Q}[x]$ of lowest degree, and with leading coefficient one, that has α as a root. The field K is called an *algebraic number field*, if every $\alpha \in K$ is algebraic. Every extension K of $\mathbb{Q}$ of finite degree is known to be algebraic.

If M is some arbitrary subset of K, $\mathbb{Q}(M)$ is defined to be the smallest subfield of K that contains both M and $\mathbb{Q}$. It is given by all values of all polynomials in the elements of M with rational coefficients, and all possible quotients thereof. $\mathbb{Q}(M)$ is called the *adjunction* of M to $\mathbb{Q}$. One can now show that every algebraic number field K of finite degree over $\mathbb{Q}$ can be realized as an adjunction of a single algebraic number $\alpha \in K$ to $\mathbb{Q}$; therefore $K = \mathbb{Q}(\alpha)$.

Since K is a vector space of dimension n over $\mathbb{Q}$, the $n+1$ algebraic numbers $1, \alpha, \ldots, \alpha^n$ have to be linearly dependent and thus to obey a relation

$$a_n \alpha^n + \ldots + a_1 \alpha + a_0 = 0 \tag{12}$$

with rational coefficients a_i and $a_n \neq 0$. Normalizing the leading coefficient to one leaves α as a root of an irreducible polynomial $f_\alpha(x) \in \mathbb{Q}[x]$ of degree n. $f_\alpha(x)$ is the minimal polynomial of α. Since $\{1, \alpha, \ldots, \alpha^{n-1}\}$ may serve as a basis for K over $\mathbb{Q}$, any $x \in K$ may be expanded as a linear combination of powers of α up to the order $n-1$,

$$x = b_{n-1} \alpha^{n-1} + \ldots + b_1 \alpha + b_0 \ , \tag{13}$$

with rational coefficients b_i.

The polynomial $f_\alpha(x)$ has n different complex roots $\alpha_1, \ldots, \alpha_n$ ($\alpha_1 = \alpha$). One can thus define n different homomorphisms $\varphi_i : \ K \longrightarrow \mathbb{C}$, $i = 1, \ldots, n$, that leave $\mathbb{Q}$ invariant, by

$$\varphi_i(x) := b_{n-1} \alpha_i^{n-1} + \ldots + b_1 \alpha_i + b_0 \ , \tag{14}$$

$\varphi_1(x) = x$. The φ_i's are called the *conjugations* of K. If all images of K under these homomorphisms are contained in the real numbers, K is said to be *totally real*.

On $\mathbb{Q}$ the usual absolute value $\nu_1(x) = |x|$, $x \in \mathbb{Q}$, introduces a topology, which is, however, not complete. The n conjugations φ_i offer n distinct ways to embed K into $\mathbb{R}$. Thus n different absolute values ν_i are given on K by $\nu_i(x) := |\varphi_i(x)|$, and these can be used to complete K to $K_{\nu_i} \cong \mathbb{R}$. The ν_i's are also called the (archimedean) *infinite primes* of K.

All algebraic numbers in K whose minimal polynomials have coefficients in the rational integers $\mathbb{Z}$ form a ring $\mathcal{R}_K$, which is called the *ring of integers of* K. An element $x \in \mathcal{R}_K$ is also called an *algebraic integer.* A $\mathbb{Z}$–module (i.e. an additive abelian group) $o \subset K$ of (the maximal possible) rank n that at the same time is a subring of K is called an *order* of K. Since we understand a ring to contain a unity, every order $o \subset K$ contains the rational integers $\mathbb{Z}$. Further it is known that there exists a *maximal order* in K that contains all other orders, and that this maximal order is just the ring of algebraic integers $\mathcal{R}_K$. An order o possesses a module–basis of n algebraic numbers $\omega_1, \ldots, \omega_n$ that are linearly independent over $\mathbb{Z}$ and hence also, equivalently, over $\mathbb{Q}$,

$$o = \mathbb{Z}\omega_1 \oplus \ldots \oplus \mathbb{Z}\omega_n \ . \tag{15}$$

The *discriminant* of o is defined to be $D_{K/\mathbb{Q}}(o) := [det(\varphi_j(\omega_i))]^2 \neq 0$. In complete analogy one can also define a discriminant for any $\mathbb{Z}$–module of rank n in K.

Another important notion, to be introduced now, is that of a *quaternion algebra*. In doing so, we will mainly follow [14, 15]. An algebra A over a field K is called *central*, if K is its center; it is said to be *simple*, if it contains no two–sided ideals besides $\{0\}$ and A itself. A quaternion algebra then is defined to be a central simple algebra A of dimension four over K. In more explicit terms A may be visualized as follows: the elements of a basis $\{1, \alpha, \beta, \gamma\}$ of A over K have to obey the relations $\gamma = \alpha\beta = -\beta\alpha$, $\alpha^2 = a$, $\beta^2 = b$; $a, b \in K\backslash\{0\}$. Any $X \in A$ may then be expanded as

$$X = x_0 + x_1\alpha + x_2\beta + x_3\gamma \ , \tag{16}$$

with $x_0, \ldots, x_3 \in K$. On A there exists an involutory anti–automorphism, called the *conjugation* of A, that maps X to $\bar{X} := x_0 - x_1\alpha - x_2\beta - x_3\gamma$. Thus $\bar{\bar{X}} = X$ and $\overline{X \cdot Y} = \bar{Y} \cdot \bar{X}$. The conjugation enables one to define the *reduced trace* and the *reduced norm* of A,

$$\begin{aligned} tr_A(X) &:= X + \bar{X} = 2x_0 \ , \\ n_A(X) &:= X \cdot \bar{X} = x_0^2 - x_1^2 a - x_2^2 b + x_3^2 ab \ . \end{aligned} \tag{17}$$

If A is a division algebra, i.e. if every $X \neq 0$ in A possesses an inverse, $n_A(X) = 0$ implies $X = 0$. The inverse is then given by $X^{-1} = \frac{1}{n_A(X)}\bar{X}$.

A $\mathbb{Z}$–module $\mathcal{O} \subset A$ of (the maximal possible) rank $4n$ that also is a subalgebra in A is called an *order* of A. The introduction of a module–basis $\{\tau_1, \ldots, \tau_{4n}\}$ turns the order into

$$\mathcal{O} = \mathbb{Z}\tau_1 \oplus \ldots \oplus \mathbb{Z}\tau_{4n} \ . \tag{18}$$

We further introduce the *group of units of norm one* $\mathcal{O}^1 := \{\varepsilon \in \mathcal{O} \,|\, \varepsilon^{-1} \in \mathcal{O},\ n_A(\varepsilon) = 1\,\}$.

A well–known example of a (division) quaternion algebra is given by *Hamilton's quaternions*

$$\mathbb{H} := \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \mid z, w \in \mathbb{C} \right\} \ .$$

$\mathbb{H}$ is a four dimensional $\mathbb{R}$–subalgebra of $M(2, \mathbb{C})$, the algebra of complex 2×2– matrices, characterized by the parameters $a = b = -1$. The subgroup of elements of reduced norm one is just $SU(2, \mathbb{C})$. An even simpler example of a (non–division) quaternion algebra over $\mathbb{R}$ is $M(2, \mathbb{R})$. In fact, $\mathbb{H}$ and $M(2, \mathbb{R})$ are the only quaternion algebras over $\mathbb{R}$.

A classification of quaternion algebras over K can now be achieved by looking at the corresponding algebras over $\mathbb{R}$ with the help of the n completions $K_{\nu_i} \cong \mathbb{R}$. Define $A_i := A \otimes_{\mathbb{Q}} K_{\nu_i} \cong A \otimes_{\mathbb{Q}} \mathbb{R}$, which is a quaternion algebra over $\mathbb{R}$. Hence it is either isomorphic to $\mathbb{H}$ (if it is a division algebra), or to $M(2, \mathbb{R})$ (if it is a non–division algebra). For the definition of arithmetic Fuchsian groups (see [14, 16]) we consider the case $A_1 \cong M(2, \mathbb{R})$ and $A_i \cong \mathbb{H}$ for $i = 2, \ldots, n$. Therefore there exists an isomorphism

$$\rho : \quad A \otimes_{\mathbb{Q}} \mathbb{R} \longrightarrow M(2, \mathbb{R}) \oplus \mathbb{H} \oplus \ldots \oplus \mathbb{H} \ , \tag{19}$$

where there occur $n - 1$ summands of $\mathbb{H}$. ρ_j will denote the restriction of ρ to A followed by a projection onto the j-th summand in (19). The several reduced traces and norms for $X \in A$ in (19) are related by

$$\begin{aligned} tr\,\rho_1(X) &= tr_A(X) \ , \\ det\,\rho_1(X) &= n_A(X) \ , \\ tr_{\mathbb{H}}\rho_j(X) &= \varphi_j(tr_A(X)) = \varphi_j(tr\,\rho_1(X)) \ , \\ n_{\mathbb{H}}(\rho_j(X)) &= \varphi_j(n_A(X)) = \varphi_j(det\,\rho_1(X)) \ , \qquad j = 2, \ldots, n \ . \end{aligned} \tag{20}$$

The image of A under ρ_1 in $M(2,I\!R)$ may also be expressed in more explicit terms by using the basis $\{1,\alpha,\beta,\alpha\beta\}$ for A, see (16): $\rho_1(1)$ is the 2×2 unit matrix; $\rho_1(\alpha)$ and $\rho_1(\beta)$ may be represented, by using the parameters $a,b>0$, as

$$\rho_1(\alpha)=\begin{pmatrix}\sqrt{a} & 0\\ 0 & -\sqrt{a}\end{pmatrix}\,, \qquad \rho_1(\beta)=\begin{pmatrix}0 & \sqrt{b}\\ \sqrt{b} & 0\end{pmatrix}\,. \tag{21}$$

For $X=x_0+x_1\alpha+x_2\beta+x_3\alpha\beta\in A$ the matrix $\rho_1(X)$ in this representation takes the form

$$\rho_1(X)=\begin{pmatrix}x_0+x_1\sqrt{a} & x_2\sqrt{b}+x_3\sqrt{ab}\\ x_2\sqrt{b}-x_3\sqrt{ab} & x_0-x_1\sqrt{a}\end{pmatrix}\,. \tag{22}$$

We are now seeking for a subset in A whose image under ρ_1 in $M(2,I\!R)$ gives a Fuchsian group Γ. Therefore $\rho_1^{-1}(\Gamma)$ must be a discrete multiplicative subgroup of A. Furthermore, for $\rho_1(X)=\gamma\in\Gamma$ the condition $det\,\gamma=1$ must be fulfilled. Thus by (20) $n_A(X)=1$ has to be required. Hence we are led to look at groups of units of norm one $\mathcal{O}^1$ of orders $\mathcal{O}\subset A$. Regarding their images under ρ_1 one finds in [15, 16] the following

PROPOSITION: Let A be a quaternion algebra over the totally real algebraic number field K of degree n. Let $\mathcal{O}\subset A$ be an order and $\mathcal{O}^1$ be its group of units of norm one. Then $\Gamma(A,\mathcal{O}):=\rho_1(\mathcal{O}^1)$ is a Fuchsian group of the first kind. Moreover, $\Gamma(A,\mathcal{O})\backslash\mathcal{H}$ is compact if A is a division algebra. A change of the isomorphism ρ in (19) amounts to a conjugation of $\Gamma(A,\mathcal{O})$ in $SL(2,I\!R)$.

The proposition now tells us that we have found what we were looking for: a class of arithmetically defined Fuchsian groups.

We are aiming at counting the numbers of distinct primitive lengths to gain information on the mean multiplicities in the length spectra derived from the Fuchsian groups under consideration. For this purpose (11) allows to enlarge the class of groups appearing in the proposition a little.

DEFINITION: A Fuchsian group Γ that is a subgroup of finite index in some $\Gamma(A,\mathcal{O})$ will be called a *Fuchsian group derived from the quaternion algebra* A. (The shorthand phrase *quaternion group* will also be sometimes used instead.) A Fuchsian group Γ that is commensurable with some $\Gamma(A,\mathcal{O})$ will be called an *arithmetic Fuchsian group.*

Finally, we mention that in [16] a characterization of arithmetic Fuchsian groups Γ is presented in terms of an adjunction of $tr\,\Gamma = \{tr\,\gamma\,|\,\gamma \in \Gamma\}$ to $\mathbb{Q}$. This already shows that the traces of elements of arithmetic groups (and hence also the lengths of closed geodesics on $\Gamma\backslash\mathcal{H}$) share special features that distinguish them from the non–arithmetic case.

4 Counting Traces in Arithmetic Groups

After having discussed length spectra of hyperbolic surfaces and having introduced the concept of arithmetic Fuchsian groups, we want to investigate the length spectra, i.e. the sets of traces occurring in these groups. As in the preceding section, take A to be a quaternion algebra over a totally real algebraic number field K of degree n and $\mathcal{O}$ as some order in A. By the proposition from section 4 $\Gamma := \Gamma(A, \mathcal{O}) = \rho_1(\mathcal{O}^1)$ is a Fuchsian group of the first kind. For $X = x_0 + x_1\alpha + x_2\beta + x_3\alpha\beta \in \mathcal{O}$ denote $\rho_1(X) = \gamma \in \Gamma$. By (22) one sees that $\frac{1}{2}tr\,\gamma = x_0 \in \mathcal{O}|_K =: \mathcal{M}$. Thus

$$tr\,\Gamma = tr_A\mathcal{O}^1 \subset tr_A\mathcal{O} = 2\mathcal{M}\ . \tag{23}$$

The inclusion $tr_A\mathcal{O}^1 \subset tr_A\mathcal{O}$ will in general be a proper one and we will return to this problem later. The aim now is to determine the number $\hat{N}_p(l)$ of distinct primitive lengths on $\Gamma\backslash\mathcal{H}$ for $l \to \infty$. By (1) one hence has to count the number of distinct traces in Γ with $2 < tr\,\gamma \leq 2R$, $R := \cosh(l/2) \to \infty$.

First we want to describe the set $\mathcal{M}$ a little bit further. To this end we have to introduce some more notation. Let $\{\omega_1, \ldots, \omega_n\}$ be a basis for K (as a vector space) over $\mathbb{Q}$. With the help of the basis $\{1, \alpha, \beta, \gamma\}$ of A over K then $\{\chi_1, \ldots, \chi_{4n}\} := \{\omega_1 \cdot 1, \ldots, \omega_n \cdot \gamma\}$ is a basis of A over $\mathbb{Q}$. On the other hand the module–basis $\{\tau_1, \ldots, \tau_{4n}\}$ of $\mathcal{O}$ (see (18)) consists of $4n$ linearly independent (over $\mathbb{Z}$ as over $\mathbb{Q}$) elements of A and thus may also serve as a basis for A over $\mathbb{Q}$. The two $\mathbb{Q}$–bases of A are therefore related by

$$\tau_i = \sum_{j=1}^{4n} M_{i,j}\,\chi_j\ , \tag{24}$$

where $(M_{i,j}) \in GL(4n,\mathbb{Q})$. The order $\mathcal{O} \subset A$ then takes the form

$$\mathcal{O} = \mathbb{Z} \sum_{j=1}^{4n} M_{1,j}\, \chi_j \oplus \ldots \oplus \mathbb{Z} \sum_{j=1}^{4n} M_{4n,j}\, \chi_j \tag{25}$$

after inserting (24) into (18). As the center K of A is spanned by $\{\chi_1, \ldots, \chi_n\} \cong \{\omega_1, \ldots, \omega_n\}$, it turns out that

$$\mathcal{M} = \mathbb{Z} \sum_{j=1}^{n} M_{1,j}\, \omega_j + \ldots + \mathbb{Z} \sum_{j=1}^{n} M_{4n,j}\, \omega_j \ . \tag{26}$$

Obviously, $\mathcal{M}$ is a $\mathbb{Z}$–module in K. Since $(M_{i,j}) \in GL(4n,\mathbb{Q})$, out of the $4n$ algebraic numbers $\sum_{j=1}^{n} M_{i,j}\omega_j$, $i = 1, \ldots, 4n$, n are linearly independent. One can therefore choose the module–basis $\{\mu_1, \ldots, \mu_n\}$ among them,

$$\mathcal{M} = \mathbb{Z}\mu_1 \oplus \ldots \oplus \mathbb{Z}\mu_n \ . \tag{27}$$

In general, however, $\mathcal{M}$ is not a subring and hence no order in K, because the multiplication in it need not close. But in [16] one finds that $tr\,\Gamma = 2 \cdot \mathcal{M}$ is contained in the ring $\mathcal{R}_K$ of integers of K. Defining $\hat{\mu}_i := 2\mu_i$ for $i = 1, \ldots, n$ then yields

$$2\mathcal{M} = \mathbb{Z}\hat{\mu}_1 \oplus \ldots \oplus \mathbb{Z}\hat{\mu}_n \subset \mathcal{R}_K \ . \tag{28}$$

By (1) this means for the geodesic length spectrum $\mathcal{L}(\Gamma)$ that $2\cosh(l/2) \in 2\mathcal{M} \subset \mathcal{R}_K$ is an algebraic integer for every $l \in \mathcal{L}(\Gamma)$.

Now we return to discussing the difference between $tr\,\Gamma = tr_A\mathcal{O}^1$ and $tr_A\mathcal{O}$. The condition that characterizes $\mathcal{O}^1$ as a subset of $\mathcal{O}$ is that $n_A(X) = 1$ (i.e. $det\,\gamma = 1$) has to be required for $X \in \mathcal{O}^1$, $\gamma = \rho_1(X)$. By (19) and (20) this implies that $n_{\mathbb{H}}(\rho_j(X)) = \varphi_j(n_A(X)) = 1$, $j = 2, \ldots, n$. Therefore $\rho_j(X) \in SU(2,\mathbb{C})$ and hence $tr_{\mathbb{H}}\rho_j(X) = \varphi_j(tr\,\gamma) \in [-2, +2]$ for $j = 2, \ldots, n$. We will now call

$$tr_I\Gamma := \{2\varepsilon \,|\, \varepsilon \in \mathcal{M},\ |\varphi_j(\varepsilon)| \leq 1,\ j = 2, \ldots, n\,\} \tag{29}$$

the *idealized set of traces* of Γ, and will refer to $2\varepsilon \in tr_I\Gamma$, $2\varepsilon \notin tr\,\Gamma$ as a *gap* in the set of traces of Γ.

It seems at least plausible to expect these gaps because the question regarding their existence means the following: We are given $\varepsilon \in \mathcal{M}$, $2\varepsilon \in$

$tr_I\Gamma$. By (26) this can be represented as $\varepsilon = \sum_{i=1}^{4n}\sum_{j=1}^{n} r_i M_{i,j}\omega_j$ with $r_i \in \mathbb{Z}$, $i = 1,\ldots,4n$. This $\varepsilon \in \mathcal{M}$ can be viewed (see (25)) as the K–part of

$$X_\varepsilon := \sum_{i,j=1}^{4n} r_i M_{i,j}\chi_j \in \mathcal{O} \ . \tag{30}$$

The choice of the $(r_1,\ldots,r_{4n})$, however, is not unique, as $\mathcal{M}$ has only rank n. But still X_ε ranges over a discrete set when varying $(r_1,\ldots,r_{4n})$ in $\mathbb{Z}^{4n}$ to produce the same ε. Hence one cannot expect for every such ε to be able to find some X_ε in the just described discrete set that matches with the condition $n_A(X_\varepsilon) = 1$ and therefore falls into $\mathcal{O}^1$. A failure of this procedure then leads to a gap. In section 5 two explicit examples of arithmetic groups will be discussed, and one of these indeed shows gaps.

Since we do not have a suitable description of $tr\,\Gamma$ (i.e. of $\mathcal{O}^1|_K$) at hand, we neglect the possible occurrence of gaps and rather work with the idealized traces $tr_I\Gamma$ instead. Our strategy therefore is to substitute the determinantal condition on $\gamma = \rho_1(X)$ for $X \in \mathcal{O}$ by the somewhat weaker conditions on the $n-1$ conjugations of its traces. We thus define

$$\mathcal{N}(R) := \frac{1}{2}\cdot \#\{\varepsilon \in \mathcal{M} \mid |\varepsilon| \le R,\ |\varphi_j(\varepsilon)| \le 1,\ j = 2,\ldots,n\} \ , \tag{31}$$

for $R = \cosh(l/2)$. The factor of $\frac{1}{2}$ takes care of the overcounting by admitting both signs for ε.

The determination of the asymptotics of $\mathcal{N}(R)$ for $R \to \infty$ will now be achieved by investigating the number of certain lattice points in some parallelotope. The procedure we are going to follow uses some standard receipt from algebraic number theory, see [13] and [17]. At first K is being mapped to $K_{\nu_1} \times \ldots \times K_{\nu_n} \cong \mathbb{R}^n$ by: $x \in K$, $x \mapsto \mathbf{x} = (x_1,\ldots,x_n) := (\varphi_1(x),\ldots,\varphi_n(x))$. In $\mathbb{R}^n$ we consider, given n linearly independent vectors $\mathbf{e}_1,\ldots,\mathbf{e}_n$, a lattice

$$L := \mathbb{Z}\mathbf{e}_1 \oplus \ldots \oplus \mathbb{Z}\mathbf{e}_n \tag{32}$$

with fundamental cell

$$F := I\mathbf{e}_1 \oplus \ldots \oplus I\mathbf{e}_n \ , \tag{33}$$

$I := [0,1)$. In $\mathbb{R}^n$ we shall consider usual euclidean volumes. F then has a volume of $vol(F) = det(e_{ij})$, where (e_{ij}) denotes the $n\times n$ matrix formed by the n row vectors $\mathbf{e}_j \in \mathbb{R}^n$. We further introduce the parallelotope

$$P_R := \{\mathbf{x} \in \mathbb{R}^n \mid |x_1| \le R,\ |x_j| \le 1,\ j = 2,\ldots,n\} \tag{34}$$

of volume $vol(P_R) = 2^n \cdot R$. In a first obvious approximation, the number $n_L(R)$ of lattice points in P_R is given by $vol(P_R)/vol(F)$. Corrections to this result are caused by contributions of the surface of P_R; this is of dimension $n-1$ (in $\mathbb{R}^n$), whereas P_R itself is of dimension n. One therefore expects the corrections to be of the order of $vol(P_R)^{(n-1)/n}$. Indeed, in [17] it is shown that

$$n_L(R) = \frac{vol(P_R)}{vol(F)} + c \cdot vol(P_R)^{1-1/n} \ , \tag{35}$$

with some constant c. The surface correction is therefore subdominant in the limit $R \to \infty$ and one finds that

$$n_L(R) = \frac{2^n}{det(e_{ij})} \cdot R + O(R^{1-1/n}) \ . \tag{36}$$

One can now construct an appropriate lattice L that allows to represent $\mathcal{N}(R)$ as the corresponding $\frac{1}{2}n_L(R)$. To this end one notices that the module basis $\{\mu_1, \ldots, \mu_n\}$ of $\mathcal{M} \subset K$ is being mapped to a set of n linearly independent vectors $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$, with $\mathbf{e}_j := (\varphi_1(\mu_j), \ldots, \varphi_n(\mu_j))$. The independence may be seen by $[det(e_{ij})]^2 = [det(\varphi_i(\mu_j))]^2 = D_{K/\mathbb{Q}}(\mathcal{M}) \neq 0$. One can thus use these $\mathbf{e}_j$'s to define a lattice L as in (32). Its fundamental cell F has volume $vol(F) = \sqrt{D_{K/\mathbb{Q}}(\mathcal{M})}$. An element $\varepsilon = k_1\mu_1 + \ldots + k_n\mu_n \in \mathcal{M}$, $k_j \in \mathbb{Z}$, is being mapped to $\varepsilon = k_1\mathbf{e}_1 + \ldots + k_n\mathbf{e}_n \in L$, and this relation is clearly bijective. One can thus embed $\mathcal{M}$ as L in $\mathbb{R}^n$, and hence (see (31)) $\mathcal{N}(R) = \frac{1}{2}n_L(R)$. Using $R = \cosh(l/2) \sim \frac{1}{2}e^{l/2}$, $l \to \infty$, and (36), one concludes that

$$\mathcal{N}(\cosh(l/2)) \sim 2^{n-2} \, [D_{K/\mathbb{Q}}(\mathcal{M})]^{-1/2} \, e^{l/2} \ , \quad l \to \infty \ . \tag{37}$$

As already mentioned, we are not able to pin down the exact number of gaps that might occur for a general Fuchsian group of the type $\Gamma = \Gamma(A, \mathcal{O})$. We are, however, quite confident that the following hypothesis holds true:

HYPOTHESIS: Asymptotically, for $l \to \infty$,

$$\hat{N}(l) \sim \mathcal{N}(\cosh(l/2)) \ . \tag{38}$$

In other words, we assume that the number of gaps grows at most like $O(e^{(1/2-\delta)l})$, $\delta > 0$, $l \to \infty$.

We are now in a position to state our main result as the

THEOREM: Let Γ be an arithmetic Fuchsian group, commensurable with the group $\Gamma(A,\mathcal{O})$ derived from the quaternion algebra A over the totally real algebraic number field K of degree n. Denote by d_1 the index of the subgroup $\Gamma_0 := \Gamma \cap \Gamma(A,\mathcal{O})$ in Γ, and by d_2 the respective index of Γ_0 in $\Gamma(A,\mathcal{O})$. Let $D_{K/\mathbb{Q}}(\mathcal{M})$ be the discriminant of the module $\mathcal{M} \subset K$ that contains $\frac{1}{2} tr\, \Gamma(A,\mathcal{O})$. Then, under the hypothesis (38), the number $\hat{N}_p(l)$ of distinct primitive lengths on $\Gamma\backslash\mathcal{H}$ up to l grows asymptotically like

$$\hat{N}_p(l) \sim 2^{n-2} \cdot (d_1/d_2) \cdot [D_{K/\mathbb{Q}}(\mathcal{M})]^{-1/2} \cdot e^{l/2} , \quad l \to \infty . \tag{39}$$

PROOF: Assume the validity of the hypothesis (38) and recall the asymptotic relation $\hat{N}_p(l) \sim \hat{N}(l)$, $l \to \infty$, from section 2. Therefore also $\hat{N}_p(l) \sim \mathcal{N}(\cosh(l/2))$. Using (11) and (37) then leads to the assertion.

In [9] it was shown how to derive the asymptotics for $l \to \infty$ of the local average $< g_p(l) >$ of the multiplicities in the primitive length spectrum from that of $\hat{N}_p(l)$ for cases like (39). We thus observe the

COROLLARY: The local average of the primitive multiplicities in the cases described in the theorem behaves asymptotically like

$$< g_p(l) > \sim 2^{3-n} \, \frac{d_2}{d_1} \, \sqrt{D_{K/\mathbb{Q}}(\mathcal{M})} \cdot \frac{e^{l/2}}{l} , \quad l \to \infty . \tag{40}$$

5 Two Examples of Arithmetic Fuchsian Groups

In this section we would like to discuss two examples of arithmetic Fuchsian groups for which the asymptotic behaviour of $< g_p(l) >$ was known before.

The first example will be the prototype one, namely the modular group $\Gamma = PSL(2,\mathbb{Z})$. In this case the relevant number field K is just the field of rational numbers $\mathbb{Q}$ itself, which obviously has degree $n = 1$. There is only one order in $\mathbb{Q}$, the maximal one $\mathcal{R}_K = \mathbb{Z}$ of rational integers. The quaternion algebra A is characterized by the two parameters $a = b = 1$; thus $A = M(2,\mathbb{Q})$. (We remark that A is a non–division algebra in accordance with the non–compactness of $\Gamma\backslash\mathcal{H}$.) The order $\mathcal{O}\subset A$ is determined by the four elements

$$\tau_1=\begin{pmatrix}1&0\\0&0\end{pmatrix}\ ,\quad \tau_2=\begin{pmatrix}0&1\\0&0\end{pmatrix}\ ,\quad \tau_3=\begin{pmatrix}0&0\\1&0\end{pmatrix}\ ,\quad \tau_4=\begin{pmatrix}0&0\\0&1\end{pmatrix} \tag{41}$$

of the $\mathbb{Z}$–basis for $\mathcal{O}$. By (18) therefore $\mathcal{O}=M(2,\mathbb{Z})$, which obviously leads to $\mathcal{O}^1=SL(2,\mathbb{Z})$. Expand $X\in\mathcal{O}$ into the basis (41), $X=k_1\tau_1+\ldots+k_4\tau_4$, $k_i\in\mathbb{Z}$, from which one observes that $\frac{1}{2}tr_A X=x_0=\frac{1}{2}(k_1+k_4)$. This yields $\mathcal{M}=\frac{1}{2}\mathbb{Z}$ and $\mu_1=\frac{1}{2}$, see (27). It is known [18] that for the modular group $tr\,\Gamma=\mathbb{Z}=2\mathcal{M}$ and therefore no gaps in the set of traces occur. The discriminant of $\mathcal{M}$ now is trivially obtained, and $\sqrt{D_{\mathbb{Q}}(\mathcal{M})}=\mu_1=\frac{1}{2}$. As the modular group itself is the group $\mathcal{O}^1=\Gamma(A,\mathcal{O})$ just defined, one concludes using $d_1=d_2=1$,

$$\begin{aligned}\hat{N}_p(l) &\sim e^{l/2}\ ,\\ <g_p(l)> &\sim \frac{e^{l/2}}{l/2}\ ,\quad l\to\infty\ ,\end{aligned} \tag{42}$$

which agrees with the previously known result.

As a second example we would like to introduce the regular octagon group Γ_{reg}, see [9, 12]. This is a Fuchsian group that leads to a compact surface $\Gamma_{reg}\backslash\mathcal{H}$ of genus two, which is the most symmetric one of this type. Γ_{reg} is a normal subgroup of index 48 in another Fuchsian group. Including orientation–reversing diffeomorphisms the group of isometries of this surface thus is of order 96. As an arithmetic group Γ_{reg} may be obtained in the following way. The algebraic number field $K=\mathbb{Q}(\sqrt{2})$ to be considered is of degree $n=2$. The ring of integers in it is $\mathcal{R}_K=\mathbb{Z}[\sqrt{2}]=\{m+n\sqrt{2}\,|\,m,n\in\mathbb{Z}\}$. A basis $\{\omega_1,\omega_2\}$ for K which at the same time is a module–basis for $\mathcal{R}_K$ is given by $\{1,\sqrt{2}\}$. The two parameters determining the quaternion algebra A are $a=1+\sqrt{2}$ and $b=1$. We now characterize the relevant order $\mathcal{O}$ in A by specifying the module–basis $\{\tau_1,\ldots,\tau_8\}$ for $\mathcal{O}$ as $\{\omega_1\cdot 1,\ldots,\omega_2\cdot\alpha\beta\}$. Therefore, by (18), an element $\gamma=\rho_1(X)$ for $X\in\mathcal{O}$ can be identified as

$$\gamma=\begin{pmatrix}x_0+x_1\sqrt{1+\sqrt{2}} & x_2+x_3\sqrt{1+\sqrt{2}}\\ x_2-x_3\sqrt{1+\sqrt{2}} & x_0-x_1\sqrt{1+\sqrt{2}}\end{pmatrix}\ , \tag{43}$$

with $x_i=m_i+n_i\sqrt{2}$, $m_i,n_i\in\mathbb{Z}$. From this one concludes that $x_0\in\mathcal{M}=\mathbb{Z}[\sqrt{2}]$. In this (exceptional) case therefore $\mathcal{M}$ is an order in K; it even is the maximal one. A basis for $\mathcal{M}$ then is given by $\{\mu_1, \mu_2\} = \{1, \sqrt{2}\}$ and thus $\mathbf{e}_1 = (1,1)$ and $\mathbf{e}_2 = (\sqrt{2}, -\sqrt{2})$. This allows to determine the discriminant of $\mathcal{M}$, leading to $\sqrt{D_{K/\mathbb{Q}}(\mathcal{M})} = |det(e_{ij})| = 2\sqrt{2}$. The group $\Gamma(A, \mathcal{O})$ now is formed by all matrices (43) of unit determinant. In [19] it is shown that this group may also be obtained by adjoining an additional element $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ to Γ_{reg}. Therefore, $\Gamma(A, \mathcal{O}) = \Gamma_{reg} \,\dot{\cup}\, \Gamma_{reg} S$, and Γ_{reg} is a subgroup of index two in $\Gamma(A, \mathcal{O})$. From the theorem one hence concludes (using $d_1 = 1$, $d_2 = 2$)

$$\begin{aligned} \hat{N}_p(l) &\sim \frac{1}{4\sqrt{2}} \cdot e^{l/2} \ , \\ < g_p(l) > &\sim 8\sqrt{2} \cdot \frac{e^{l/2}}{l} \ , \quad l \to \infty \ . \end{aligned} \tag{44}$$

This is exactly the result found in [9, 12]. We remark that in this example there do exist gaps in the length spectrum. These have been identified in [9, 12], where it was further shown by a numerical calculation of the geodesic length spectrum up to $l = 18$ that these do not alter the result and that therefore our hypothesis (38) is fulfilled.

6 Discussion

This article contained a study of geodesic length spectra on hyperbolic surfaces $\Gamma\backslash\mathcal{H}$, where Γ is a Fuchsian group of the first kind. In the first part of this investigation we discussed how the counting functions for distinct lengths and for distinct primitive lengths, respectively, on such a surface are asymptotically related. Moreover, we looked at relations among the counting functions for two different surfaces whose Fuchsian groups are commensurable. It was found that these share essentially the same asymptotic behaviour (besides explicitly known factors of proportionality).

After this discussion we continued in explaining the definition of arithmetic Fuchsian groups and provided definitions and properties of the relevant quantities from number theory. In doing so we tried to be as explicit as possible and to avoid unnecessary generality.

We were then able to count the number of different geodesic lengths asymptotically up to a given (large) value. This was possible, since we could identify the set of traces that occurs for an arithmetic group as being (the essential part of) a module in the field of algebraic numbers used in the definition of the group. We were able to map this module to a lattice in $\mathbb{R}^n$. The counting problem was thus reformulated as a lattice point problem.

It was found that the number of distinct lengths up to a value of l grows like $e^{l/2}$ for $l \to \infty$, whereas by Huber's law the number of geodesics with lengths up to l grows like e^l/l, which is exceptionally strong compared to the case of non–arithmetic groups. The reason for this difference –the number of different lengths proliferates only like, roughly speaking, the square root of the number of geodesics– is caused by the arithmetic restriction on the set of possible lengths, which does not exist for non–arithmetic groups. For these, however, such a quite general description as we presented it here in the arithmetic case seems not to be possible.

In proving our result we also gave a receipt to find the complete asymptotic expression for the mean multiplicity $< g_p(l) >$ of primitive lengths, including the overall constant. First, given an arithmetic Fuchsian group Γ, one has to know the quaternion group $\Gamma(A, \mathcal{O})$ commensurable with it. Once one has this at hand one also knows the indices d_1 and d_2 describing $\Gamma \cap \Gamma(A, \mathcal{O})$ as a subgroup in Γ and in $\Gamma(A, \mathcal{O})$. In [16] it is shown that one can get the relevant number field K by adjoining $tr\, \Gamma(A, \mathcal{O})$ to $\mathbb{Q}$. Furthermore, the algebra A can be received as the linear span of $\Gamma(A, \mathcal{O})$ over K. Analogously, the order $\mathcal{O} \subset A$ is obtained as the linear span of $\Gamma(A, \mathcal{O})$ over $\mathcal{R}_K$. One then has to find the module–basis $\{\tau_1, \ldots, \tau_{4n}\}$ of $\mathcal{O}$. This can be used to obtain the matrix $(M_{i,j})$ appearing in (24). Given this one has to identify the module $\mathcal{M}$ containing $\frac{1}{2} tr\, \Gamma(A, \mathcal{O})$ (see (26) and (27)) in order to determine its discriminant $D_{K/\mathbb{Q}}(\mathcal{M})$. One can now plug all this information into (40) to get the answer to the problem.

The arithmetic nature of the groups considered in this article does also produce restrictions on the quantum systems that arise as quantizations of the geodesic flows on the corresponding surfaces. The already mentioned existence of the infinitely many self–adjoint Hecke operators commuting with the Hamiltonian leads to correlations among the values in each wavefunction, see the first paper of ref. [5]. This is in sharp contrast to the non–arithmetic case where at most a finite number of such Hecke operators can exist and thus the correlations in the wavefunctions are by far weaker (if present at all). In [5] it was argued that this was the reason why the statistical properties of the energy spectra in the arithmetical case are different from "generic" chaotic systems. As the Selberg trace formula connects the geodesic length spectrum to the spectrum of the hyperbolic Laplacian, one could expect a link between the exceptional status' of surfaces with arithmetic Fuchsian groups in both the classical and quantum context. This, however, has still to be made more explicit.

Acknowledgements

I would like to thank Prof. F. Steiner for useful discussions and for reading the manuscript. Further I want to thank Holger Ninnemann for helpful discussions.

References

[1] M.V. Berry and M. Tabor, Proc. Roy. Soc. London **A356**(1977)375

[2] Ya.G. Sinai, *Mathematical problems in the theory of quantum chaos*, Distinguished Raimond and Beverly Sackler lectures, Tel Aviv University, 1990 (to appear in Springer Lecture Notes in Mathematics)
P.M. Bleher, in *Mathematical Physics X*, Proc. of the X^{th} Congress on Mathematical Physics, Leipzig 1991, p. 298, ed.: K. Schmüdgen (Springer, Berlin–Heidelberg–New York, 1992)

[3] M.L. Mehta, *Random Matrices and the Statistical Theory of Energy Levels* (Academic Press, New York, 1967); new revised and enlarged edition (Academic Press, New York, 1990)
O. Bohigas, in *Chaos and Quantum Physics*, Proc. of the Les Houches Summer School 1989, eds.: M.-J. Giannoni, A. Voros and J. Zinn-Justin (Elsevier Science Publ., Amsterdam, 1991)
F. Haake, *Quantum Signatures of Chaos* (Springer, Berlin–Heidelberg, 1991)

[4] S.W. McDonald and A.N. Kaufmann, Phys. Rev. Lett. **42**(1979)1189
M.V. Berry, Ann. Phys. **131**(1981)163
O. Bohigas, M.-J. Giannoni and C. Schmit, Phys. Rev. Lett. **52**(1984)1
M.V. Berry and M. Robnik, J. Phys. **A19**(1985)649
R. Aurich and F. Steiner, Physica **D43**(1990)155
M. Sieber and F. Steiner, Phys. Lett. **A148**(1990)415

[5] J. Bolte, G. Steil and F. Steiner, *Arithmetical Chaos and Violation of Universality in Energy Level Statistics*, DESY–preprint, DESY 92-061, April 1992
E.B. Bogomolny, B. Georgeot, M.-J. Giannoni and C. Schmit, *Arithmetical Chaos*, preprint IPNO/TH 92-23

[6] M.C. Gutzwiller, J. Math. Phys. **8**(1967)1979; **10**(1969)1004; **11**(1970)1791; **12**(1971)343
M.C. Gutzwiller, *Chaos in Classical and Quantum Mechanics* (Springer, New York, 1990)

[7] A. Selberg, J. Indian Math. Soc. **20**(1956)47
D.A. Hejhal, *The Selberg Trace Formula for* $PSL(2, I\!R)$*, vol. I and II*, Springer Lecture Notes in Mathematics **548**(1976) and **1001**(1983)
A.B. Venkov, *Spectral Theory of Automorphic Functions and its Applications* (Kluwer Academic Publ., Dordrecht–Boston–London, 1990)

[8] H. Huber, Math. Annalen **138**(1959)1

[9] R. Aurich and F. Steiner, Physica **D32**(1988)451

[10] R.D. Horowitz, Commun. Pure Appl. Math. **25**(1972)635
B. Randol, Proc. Amer. Math. Soc. **78**(1980)455

[11] R. Aurich, private communication

[12] R. Aurich, E.B. Bogomolny and F. Steiner, Physica **D48**(1991)91

[13] B.L. van der Waerden, *Algebra I*, 5. Auflage (Springer, Berlin–Göttingen–Heidelberg, 1960)
S.I. Borewicz and I.R. Šafarevič, *Zahlentheorie* (Birkhäuser, Basel–Stuttgart, 1966)

[14] M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions*, Springer Lecture Notes in Mathematics **800**(1980)

[15] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions* (Princeton University Press, Princeton, 1971)

[16] K. Takeuchi, J. Fac. Sci. Univ. Tokyo **16**(1969)97; J. Math. Soc. Japan **27**(1975)600

[17] S. Lang, *Algebraic Numbers* (Addison–Wesley, Reading–Palo Alto–London, 1964)

[18] G. Handke, *Über Streuzustände in einem klassisch chaotischen System* (Diploma Thesis, Univ. Hamburg, 1989)
D. Schleicher, *Bestimmung des Energiespektrums in einem chaotischen System mit Hilfe der Selbergschen Spurformel* (Diploma Thesis, Univ. Hamburg, 1991)

[19] T. Pignataro, *Hausdorff Dimension, Spectral Theory and Applications to the Quantization of Geodesic Flows on Surfaces of Constant Negative Curvature* (PhD Thesis, Princeton Univ., 1984)