

COUNTING SALEM NUMBERS OF ARITHMETIC HYPERBOLIC 3-ORBIFOLDS

MIKHAIL BELOLIPETSKY, MATILDE LALÍN, PLINIO G. P. MURILLO, AND LOLA THOMPSON

ABSTRACT. It is known that the lengths of closed geodesics of an arithmetic hyperbolic orbifold are related to Salem numbers. We initiate a quantitative study of this phenomenon. We show that any non-compact arithmetic 3-dimensional orbifold defines $cQ^{1/2} + O(Q^{1/4})$ square-rootable Salem numbers of degree 4 which are less than or equal to Q . This quantity can be compared to the total number of such Salem numbers, which is shown to be asymptotic to $\frac{4}{3}Q^{3/2} + O(Q)$. Assuming the gap conjecture of Marklof, we can extend these results to compact arithmetic 3-orbifolds.

1. INTRODUCTION

A *Salem number* is a real algebraic integer $\lambda > 1$ such that all of its Galois conjugates except λ^{-1} have absolute value equal to 1. Salem numbers appear in many areas of mathematics including algebra, geometry, dynamical systems, and number theory. They are closely related to the celebrated Lehmer's problem about the smallest Mahler measure of a non-cyclotomic polynomial. We refer to [Smy15] for a survey of research on Salem numbers.

It has been known for some time that the exponential lengths of the closed geodesics of an arithmetic hyperbolic n -dimensional manifold or orbifold are given by Salem numbers. For $n = 2$ and 3 this relation is described in the book by C. Maclachlan and A. Reid [MR03, Chapter 12]. More recently, it was elaborated upon and generalized to higher dimensions by V. Emery, J. Ratcliffe, and S. Tschantz in [ERT19]. In particular, their Theorem 1.1 implies that, for a non-compact arithmetic hyperbolic n -orbifold \mathcal{O} , a closed geodesic of length ℓ corresponds to a Salem number $\lambda = e^\ell$ if the dimension n is even, and to a so called square-rootable Salem number $\lambda = e^{2\ell}$ if n is odd. The degrees of these Salem numbers satisfy $\deg(\lambda) \leq n+1$. A natural question arises: *What proportion of Salem numbers of a given degree are associated to a fixed orbifold \mathcal{O} ?*

To this end, let us recall some results about the distribution of algebraic integers. This field has a long history, so we will mention only the more recent results which are relevant to our work. In a beautiful paper [Thu14], W. Thurston, motivated by the study of entropy of one-dimensional dynamical systems, encountered limiting distributions of conjugates of Perron numbers, a class which includes Salem numbers as a subset. His experiments led to a set of interesting problems and conjectures, some of which were successfully resolved by F. Calegari and Z. Huang in [CH17]. Later on, some ideas from their approach helped F. Götzte and A. Gusakova to compute the asymptotic growth of Salem numbers in [GG19]. The precise form of their result is given in Theorem 2. It is remarkable that this result was established only very recently, as it allows us to play the asymptotic formula against the distribution of closed geodesics of an arithmetic n -orbifold with $n = 2m + 1$. We also come up with a related question about the distribution of square-rootable Salem numbers. We were able to answer these questions in the first non-trivial case, when the degree of the Salem numbers is 4 and the corresponding dimension of the arithmetic orbifolds is 3.

The main result of this paper is the following theorem:

Theorem 1.

A. Let \mathcal{O}_D be a non-compact arithmetic hyperbolic 3-orbifold associated to a Bianchi group $\Gamma_D = \mathrm{PSL}(2, \mathfrak{o}_K)$, where \mathfrak{o}_K is the ring of integers of an imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-D})$, and D is a square-free positive integer. Then \mathcal{O}_D generates

$$cQ^{1/2} + O(Q^{1/4})$$

2010 Mathematics Subject Classification. 11R06, 20H05, 20H10.

Key words and phrases. arithmetic 3-orbifold; closed geodesic; Salem number.

square-rootable Salem numbers of degree 4 which are less or equal to Q , where $c = \frac{\pi}{4\sqrt{D}}$ if $D \equiv 1, 2 \pmod{4}$ and $c = \frac{\pi}{2\sqrt{D}}$ if $D \equiv 3 \pmod{4}$.

- B. The number of Salem numbers of degree 4 that are square-rootable over \mathbb{Q} and less than or equal to Q is

$$\frac{4}{3}Q^{3/2} + O(Q).$$

This theorem together with a special case of the theorem of Götze and Gusakova implies that, in the logarithmic scale, a given 3-orbifold \mathcal{O}_D generates asymptotically $1/4$ of all Salem numbers of degree 4 and asymptotically $1/3$ of the square-rootable Salem numbers of degree 4.

The proof of the first part of the theorem uses the work of J. Marklof on multiplicities in length spectra of arithmetic hyperbolic 3-orbifolds [Mar96]. For proving part B we take advantage of some special properties of Salem numbers of degree 4. Extending these results to higher degrees would require an extension of Marklof's length spectrum asymptotic to arithmetic orbifolds of dimension greater than 3 and an analogue of the Götze–Gusakova theorem for square-rootable Salem numbers of higher degree. While we do not handle the higher-dimensional case in this paper, we are able to extend Theorem 1 to compact arithmetic 3-orbifolds and associated Salem numbers of degree $4d$, $d \geq 1$, square-rootable over an intermediate field L of degree d — see Theorem 8.

The paper is organized as follows. In Section 2 we recall definitions and some properties of Salem numbers and arithmetic groups. In Section 3 we prove Theorem 1. In Section 4 we prove Theorem 8. In Section 5 we briefly discuss some other examples and open problems.

2. PRELIMINARIES

2.1. Salem numbers. A *Salem number* is a real algebraic integer $\lambda > 1$ such that all of its Galois conjugates have absolute value less than or equal to 1, and at least one of them has absolute value equal to 1. Let λ' denote a Galois conjugate of the Salem number λ with $|\lambda'| = 1$. Since λ' and its complex conjugate $\overline{\lambda}' = (\lambda')^{-1}$ are Galois conjugates we conclude that the minimal polynomial p_λ of a Salem number λ is self-reciprocal, i.e., $p_\lambda(x) = x^{\deg(p_\lambda)} p_\lambda(x^{-1})$. This means that its coefficients form a palindromic sequence. Moreover, the polynomial p_λ is of even degree $n = 2(m+1)$ because otherwise $p_\lambda(-1) = -p_\lambda(-1) = 0$, which contradicts its irreducibility. Thus, all Galois conjugates of a Salem number λ (except for λ^{-1}) have absolute value 1 and lie on the unit circle in the complex plane. We used this property as the first definition of Salem numbers in the introduction. For convenience in this paper we will also allow Salem numbers to have degree 2 (where λ has λ^{-1} as its only conjugate). We do this so that our definition of Salem numbers aligns with that used in [ERT19].

The celebrated Lehmer's problem asks about the existence of a smallest Salem number $\lambda > 1$ and gives the conjectural candidate $\lambda = 1.176\dots$ of degree 10 found by D. H. Lehmer in 1933 [Leh33]. We refer to [Smy15] and the references therein for more about Lehmer's problem. In this paper we will be interested in a somewhat opposite question about how quickly the number of Salem numbers grows when their values tend to infinity.

We denote by Sal_m the set of all Salem numbers of degree $2(m+1)$ and let

$$\text{Sal}_m(Q) := \{\lambda \in \text{Sal}_m : \lambda \leq Q\}.$$

It is not hard to find examples of Salem numbers of any even degree. One of the basic facts proved by Salem is that if λ is a Salem number of degree n , then so is λ^k for all $k \in \mathbb{N}$ (see [Smy15, Lemma 2]). This implies that the counting function $\#\text{Sal}_m(Q)$ grows at least as fast as $c \log Q$. However, the actual growth of Salem numbers is much faster. A precise result for their asymptotic growth was recently proved by Götze and Gusakova:

Theorem 2 ([GG19], Theorem 1.1). *For any positive integer m we have*

$$\#\text{Sal}_m(Q) = \omega_m Q^{m+1} + O(Q^m),$$

as $Q \rightarrow \infty$, where

$$\omega_m := \frac{2^{m(m+1)}}{m+1} \prod_{k=0}^{m-1} \frac{k!^2}{(2k+1)!}.$$

We remark for future reference that $\omega_1 = 2$.

In this paper, we will encounter a special class of Salem numbers that are called *square-rootable*.

Definition 3. Let λ be a Salem number, let L be a subfield of $\mathbb{Q}(\lambda + \lambda^{-1})$, and let $p(x)$ be the minimal polynomial of λ over L . We say that λ is square-rootable over L via α if there exist a totally positive element $\alpha \in L$ and a monic palindromic polynomial $q(x)$, whose even degree coefficients are in L and whose odd degree coefficients are in $\sqrt{\alpha}L$, such that $q(x)q(-x) = p(x^2)$.

The square-rootable Salem numbers were first defined by Emery, Ratcliffe, and Tschantz in [ERT19]. They are of interest because they are associated to geodesic lengths of odd-dimensional arithmetic orbifolds.

2.2. Arithmetic orbifolds. Let us recall the definition of an arithmetic Kleinian group. Let K be a number field with exactly one complex place, \mathfrak{o}_K its ring of integers, and A a quaternion algebra over K ramified at all real places of K . Let \mathfrak{D} be an \mathfrak{o}_K -order of A , and denote by \mathfrak{D}^1 its group of elements of norm 1. Consider a K -embedding $\rho : A \hookrightarrow M(2, \mathbb{C})$ associated with the complex place of K . The group

$$\Gamma_{\mathfrak{D}} = P\rho(\mathfrak{D}^1) < \mathrm{PSL}(2, \mathbb{C}),$$

where $P : \mathrm{SL}(2, \mathbb{C}) \rightarrow \mathrm{PSL}(2, \mathbb{C})$ is the natural projection, is then a discrete finite covolume subgroup of $\mathrm{PSL}(2, \mathbb{C})$. Following [Mar96], we will call $\Gamma_{\mathfrak{D}}$ an *arithmetic quaternion group*. A subgroup $\Gamma < \mathrm{PSL}(2, \mathbb{C})$ which is commensurable with some such group $\Gamma_{\mathfrak{D}}$ is called an *arithmetic Kleinian group*. The associated quotient space $\mathcal{O} = \mathbb{H}^3/\Gamma$ is an *arithmetic hyperbolic 3-orbifold*.

Arithmetic hyperbolic orbifolds can be compact or non-compact with cusps and finite volume. In dimension 3 the non-compact orbifolds correspond to the arithmetic Kleinian groups which are commensurable with the Bianchi groups $\Gamma_D = \mathrm{PSL}(2, \mathfrak{o}_K)$, where \mathfrak{o}_K is the ring of integers of an imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-D})$ and D is a square-free positive integer (cf. [MR03, Theorem 8.2.3]).

An important subclass of arithmetic groups of hyperbolic isometries is defined by admissible quadratic forms. For this definition let L be a totally real number field with ring of integers \mathfrak{o}_L , and let f be a quadratic form of signature $(n, 1)$ defined over L such that, for every non-identity embedding $\sigma : L \rightarrow \mathbb{R}$, the form f^σ is positive definite. The group $\Gamma = O_0(f, \mathfrak{o}_L)$ of the integral automorphisms of f is a discrete subgroup of $O_0(n, 1)$, which is the full group of isometries of the hyperbolic n -space \mathbb{H}^n (the group $O_0(n, 1)$ is the subgroup of the orthogonal group $O(n, 1)$ that preserves the upper cone in the vector model of \mathbb{H}^n). It can be shown by using reduction theory that such groups Γ have finite covolume. The groups Γ obtained in this way and subgroups of $\mathrm{Isom}(\mathbb{H}^n)$ which are commensurable with them are called *arithmetic subgroups of the simplest type*.

It is a well-known consequence of [Wei60] that every non-cocompact arithmetic Γ in dimension $n \neq 7$ is commensurable with the group of units of a quadratic form over \mathbb{Q} . A more careful analysis implies that the same is true for $n = 7$ but we will not consider this case here. For the purpose of this paper we record a corollary that the Bianchi groups are arithmetic subgroups of the simplest type. Indeed, it is not hard to write down the corresponding quadratic forms for each Γ_D , which we leave as an exercise for the interested reader.

3. PROOF OF THEOREM 1

3.1. Proof of part A. In [ERT19], V. Emery, J. Ratcliffe and S. Tschantz obtained the following result.

Theorem 4 (cf. [ERT19], Theorem 1.6). *Let $\Gamma \subseteq \mathrm{Isom}(\mathbb{H}^n)$ be an arithmetic lattice, with n odd, of the simplest type defined over a totally real number field L . Let γ be a hyperbolic element of Γ , and let $\lambda = e^{2\ell(\gamma)}$. Then λ is a Salem number which is square-rootable over L .*

Recall from the previous section that in dimension $n = 3$ the Bianchi groups correspond to arithmetic lattices of the simplest type defined over $L = \mathbb{Q}$.

Now recall a result of Marklof on counting geodesic lengths in the spectrum of Bianchi orbifolds [Mar96]. It is important for us that the lengths are counted without multiplicities, as it is well-known that multiplicities in the spectrum of arithmetic orbifolds can grow very rapidly. We have:

Theorem 5 (cf. [Mar96], Theorem 4(b)). *Let $\Gamma_D = \mathrm{SL}(2, \mathfrak{o}_K)$, $K = \mathbb{Q}(\sqrt{-D})$, $D \in \mathbb{Z}_{>0}$ square-free. Then the number of distinct real lengths of closed geodesics less than or equal to ℓ in \mathbb{H}^3/Γ_D is given by*

$$\mathcal{N}_r(\ell) = \begin{cases} \frac{\pi}{4\sqrt{D}} e^\ell + O(e^{\ell/2}), & D \equiv 1, 2 \pmod{4}, \\ \frac{\pi}{2\sqrt{D}} e^\ell + O(e^{\ell/2}), & D \equiv 3 \pmod{4}. \end{cases}$$

Combining Theorems 4 and 5, we obtain that a non-compact arithmetic hyperbolic 3-orbifold generates

$$\mathcal{N}(Q) = \mathcal{N}_r\left(\frac{1}{2} \log Q\right) \sim cQ^{1/2}$$

square-rootable Salem numbers $\lambda \leq Q$ of degree ≤ 4 , where c is the constant given by Theorem 5.

Going more carefully through the proof of Marklof's theorem allows us to conclude that most of these Salem numbers have degree equal to 4. Indeed, the proof of Theorem 4(b) (loc.cit.) shows that the main contribution to the counting function $\mathcal{N}_r(\ell)$ comes from the ellipses $e(y)$ with $y \leq x$, $y \notin \mathbb{Q}$ and sums up to $\frac{1}{4}\mathcal{E}(x)$, $x = 2 \cosh \ell$ different lengths. The corresponding Salem numbers λ are square-rootable, hence $\deg(\lambda) = \deg(\lambda^{\frac{1}{2}})$ (by [ERT19, Lemmas 7.4 and 7.2]). On the other hand, we have $\lambda^{\frac{1}{2}} + \lambda^{-\frac{1}{2}} = y \notin \mathbb{Q}$, hence $\deg(\lambda) > 2$.

This completes the proof of part A of the theorem.

3.2. Proof of part B. Here, we are interested in the case where $L = \mathbb{Q}$ and $\deg(\lambda) = 4$. We begin by recalling the following lemma of Emery, Ratcliffe, and Tschantz:

Lemma 6 ([ERT19], Lemma 8.2 (2)). *Let λ be a Salem number of degree 4 and $p(x)$ its minimal polynomial. Then λ is square-rootable over \mathbb{Q} if and only if $p(-1)$ is a square in \mathbb{Z} .*

Our goal is to count those λ 's of degree 4 that are square-rootable. Thus, we wish to count polynomials

$$p(x) = x^4 + ax^3 + bx^2 + ax + 1 \in \mathbb{Z}[x]$$

such that

- (a) $p(x)$ is irreducible;
- (b) $p(x)$ is a Salem polynomial, that is, its roots are $\lambda, \lambda^{-1}, \mu, \mu^{-1}$ with $\lambda \in \mathbb{R}_{>1}$ and $\mu \notin \mathbb{R}, |\mu| = 1$;
- (c) $p(-1) = k^2$ for $k \in \mathbb{Z}$;
- (d) $\lambda \leq Q$.

We remark that k above must be different from 0, since -1 cannot be a root of $p(x)$. Thus we can assume that $k > 0$.

Condition (c) is equivalent to

$$(1) \quad 2 + b - 2a = k^2, \text{ for } k \in \mathbb{Z}, k > 0.$$

Now we focus on condition (b). Our first observation is that

$$-a = \lambda + \lambda^{-1} + \mu + \mu^{-1} < \lambda + 3 \leq Q + 3.$$

In addition, $\lambda + \lambda^{-1} \geq 2$ implies that

$$-a = \lambda + \lambda^{-1} + \mu + \mu^{-1} > 0.$$

Therefore,

$$(2) \quad 0 < -a < Q + 3.$$

Write $y = x + x^{-1}$ and consider the polynomial

$$r(y) = y^2 + ay + b - 2.$$

Then it is immediate to see that $x^2 r(x + x^{-1}) = p(x)$. Condition (b) is equivalent to asking that $r(y)$ has two real roots, with one > 2 and the other in the interval $(-2, 2)$. Writing the roots as

$$\frac{-a \pm \sqrt{a^2 - 4(b-2)}}{2},$$

we see that we need

$$(3) \quad a^2 > 4b - 8.$$

Combining with condition (1), we have

$$(4) \quad (a - 4)^2 > 4k^2.$$

In addition,

$$\begin{aligned} 2 < \frac{-a + \sqrt{a^2 - 4(b-2)}}{2} &\iff 4 + a < \sqrt{a^2 - 4(b-2)}, \\ 2 > \frac{-a - \sqrt{a^2 - 4(b-2)}}{2} > -2 &\iff 4 - a > \sqrt{a^2 - 4(b-2)} > -4 - a. \end{aligned}$$

Combining the above lower bounds for the square-root, we have

$$(5) \quad a^2 - 4(b-2) > (4+a)^2 \iff -2a > 2+b.$$

Similarly, the upper bound gives us

$$(4-a)^2 > a^2 - 4(b-2) \iff 2+b > 2a,$$

but this condition is already a consequence of (1).

Combining (1) with (5) we obtain

$$(6) \quad k^2 < -4a.$$

Notice that $-16a < (a-4)^2$, and therefore equations (3) and (4) are consequences of (6).

In sum, we have the following conditions

$$b = k^2 + 2a - 2, \quad k^2 < -4a, \quad 0 < -a < Q+3.$$

The number of solutions for this is given by

$$\sum_{j=1}^{Q+2} (\lceil \sqrt{4j} \rceil - 1) = 2 \int_1^{Q+2} \sqrt{x} dx + O(Q) = \frac{4}{3} Q^{3/2} + O(Q).$$

We have not yet taken into account condition (a). The only way for $p(x)$ to be reducible is that

$$p(x) = (x^2 + \alpha x + 1)(x^2 + \beta x + 1)$$

in $\mathbb{Z}[x]$, where one of the factors (say, the first) is the minimal polynomial of μ . Since $|\mu| = 1$, we conclude that $|\alpha| < 2$ and therefore the only possible values for α are $0, \pm 1$. Choosing the value of α and comparing the conditions on the coefficients a, b of $p(x)$, we have

$$\begin{aligned} \alpha = 0 &\iff b = 2, \\ \alpha = 1 &\iff b = a + 1, \\ \alpha = -1 &\iff 1 = a + b. \end{aligned}$$

There are $O(Q)$ choices of a and b satisfying the three equations above, which completes the proof of part B. \square

3.3. We remark that we can simplify our reasoning from the previous section to recover the result of Götze and Gusakova for the case where $m = 1$ (which corresponds to Salem numbers of degree 4). Indeed, we must again count the possible polynomials $p(x)$, this time without condition (c). From the previous discussion, we have the conditions

$$-2a > 2+b > 2a, \quad 0 < -a < Q+3.$$

We also have $a^2 > 4b - 8$, but it is easy to see that this condition is a consequence of the first equation above.

The number of solutions for the above inequalities is

$$\sum_{j=1}^{Q+2} (4j - 1) = 2Q^2 + O(Q),$$

and this recovers Theorem 2 for $m = 1$.

4. COCOMPACT CASE

In this section we consider a generalization of Theorem 1 to compact orbifolds. Here the results are less precise and conditional on the *gap conjecture* of Marklof:

Conjecture 7 ([Mar96], Conjecture 1). *Let $\Gamma_{\mathfrak{D}}$ be an arithmetic quaternion group. Then the number of gaps in the complex length spectrum of $\mathbb{H}^3/\Gamma_{\mathfrak{D}}$ up to length $\ell = \log x$ is given by*

$$\mathcal{G}(x) = \kappa x + o(x), \quad x \rightarrow \infty,$$

where $\kappa \geq 0$ is a constant depending only on $\Gamma_{\mathfrak{D}}$, and small compared to $2^{2d-3}\pi|D_{\mathfrak{a}}|^{-1/2}$. It could even be the case that $\kappa = 0$ for all $\Gamma_{\mathfrak{D}}$. (Here d denotes the degree of the field of definition K and $D_{\mathfrak{a}}$ is the discriminant of $\mathfrak{a} = \text{tr } \mathfrak{D}$.)

The conjecture is known to be true (with $\kappa = 0$) when $\Gamma_{\mathfrak{D}} = \text{PSL}(2, \mathfrak{o}_K)$ is a Bianchi group, but it remains open even for the other arithmetic groups of the simplest type. The main result of this section is the following theorem.

Theorem 8. A. *Let $\Gamma_{\mathfrak{D}}$ be an arithmetic quaternion group of the simplest type with the totally real field of definition L , and let $\mathcal{O}_{\mathfrak{D}} = \mathbb{H}^3/\Gamma_{\mathfrak{D}}$. Assume that Conjecture 7 holds for $\Gamma_{\mathfrak{D}}$. Then $\mathcal{O}_{\mathfrak{D}}$ generates*

$$c_1 Q^{1/2} + o(Q^{1/2}), \quad Q \rightarrow \infty$$

Salem numbers of degree 4 over L that are square-rootable over L , where $c_1 = \frac{2^{2d-3}\pi}{|D_{\mathfrak{a}}|} - \frac{\kappa}{4}$ with the notation as in Conjecture 7.

B. *Let L be a totally real number field. There exists a constant $c_2 = c_2(L) \geq 0$ such that the number of Salem numbers of degree 4 over L that are square-rootable over L and less than or equal to Q is*

$$c_2 Q^{3/2} + o(Q^{3/2}).$$

Proof. A. This part of the proof is similar to the argument in Section 3.1. The only difference is that instead of Marklof's Theorem 4(b) cited there we now apply his Theorem 4(a) together with the gap conjecture [Mar96]. Note that in Theorem 4(a) [loc. cit.] there is an additional assumption that the set of traces $\text{tr } \mathfrak{D}^1$ is invariant under complex conjugation. This assumption allows us to prove Lemma 2 [loc. cit.] which is then used in the proof of the theorem. It is well known that arithmetic groups of the simplest type always have a totally real index two subfield of their complex field of definition (see [MR03, Section 10.2]). Therefore, we are not required to impose the aforementioned extra assumption on the traces. The rest of the argument is the same as in Section 3.1.

B. We now use the general form of square-rootable Salem numbers given in Definition 3. We work over an arbitrary totally real field L , but consider only the Salem numbers λ with $\deg_L(\lambda) = 4$. The latter assumption allows us to apply the method from Section 3.2.

First recall a more general lemma from [ERT19] (compare with Lemma 6):

Lemma 9 ([ERT19], Lemma 8.2 (1)). *Let λ be a Salem number, let $L \subset \mathbb{Q}(\lambda + \lambda^{-1})$ a subfield, and let $p(x)$ be the minimal polynomial of λ over L . If $p(x) = x^4 + ax^3 + bx^2 + ax + 1 \in \mathfrak{o}_L[x]$, then λ is square-rootable over L if and only if there is a positive element k of L such that $p(-1) = k^2$ and $4 - a \pm 2k$ is a totally positive element of L , in which case λ is square-rootable over L via $4 - a \pm 2k$.*

As before, we seek to count the Salem numbers λ of degree 4 over L that are square-rootable. This amounts to counting the polynomials

$$p(x) = x^4 + ax^3 + bx^2 + ax + 1 \in \mathfrak{o}_L[x]$$

for which

- (a) $p(x)$ is irreducible;
- (b) its root λ is a Salem number of degree $4[L : \mathbb{Q}]$, that is, the roots are $\lambda, \lambda^{-1}, \mu, \mu^{-1}$ with $\lambda \in \mathbb{R}_{>1}$ and $\mu \notin \mathbb{R}, |\mu| = 1$, and for all non-identity places $\sigma : L \rightarrow \mathbb{R}$ the roots of $p^{\sigma}(x)$ have absolute value one (cf. [ERT19, Proof of Theorem 5.2(1)]);
- (c) $p(-1) = k^2$ for $k \in \mathfrak{o}_L$, $k > 0$;
- (d) $4 - a + 2k$ or $4 - a - 2k$ is totally positive;

(e) $\lambda \leq Q$.

The proof proceeds much as in Section 3.2. Here, condition (c) is equivalent to

$$(7) \quad 2 + b - 2a = k^2, \text{ for } k \in \mathfrak{o}_L, k > 0.$$

Now we turn our attention to condition (b), which allows us to deduce that

$$-a = \lambda + \lambda^{-1} + \mu + \mu^{-1} < \lambda + 3 \leq Q + 3,$$

where the final inequality follows from condition (e). Moreover, since λ is a Salem number, we know that $\lambda + \lambda^{-1} \geq 2$, hence

$$-a = \lambda + \lambda^{-1} + \mu + \mu^{-1} > 0.$$

Combining the two displayed inequalities for $-a$ yields

$$(8) \quad 0 < -a < Q + 3.$$

Furthermore, since $p^\sigma(x)$ has all of the roots with absolute value one, it must be the case that $|a^\sigma| < 4$ for any non-identity $\sigma : L \rightarrow \mathbb{R}$.

Next, we perform a change of variable, writing $y = x + x^{-1}$. Then, if we define

$$r(y) = y^2 + ay + b - 2,$$

we see that $p(x)$ can be expressed in terms of this new polynomial: $x^2 r(x + x^{-1}) = p(x)$. In other words, condition (b) amounts to requiring that $r(y)$ has two real roots, with one > 2 and the other in the interval $(-2, 2)$, whose σ -conjugates are all in the interval $(-2, 2)$. By applying the quadratic formula, we see that the roots of $r(y)$ are of the form

$$\frac{-a \pm \sqrt{a^2 - 4(b-2)}}{2}.$$

As a result, we need

$$(9) \quad (a^\sigma)^2 > 4b^\sigma - 8 \text{ for all } \sigma : L \rightarrow \mathbb{R}.$$

Combining this with condition (7) yields

$$(10) \quad (a^\sigma - 4)^2 > 4(k^\sigma)^2.$$

Hence, from (8), for all non-identity $\sigma : L \rightarrow \mathbb{R}$ we have

$$(11) \quad -4 < k^\sigma < 4.$$

We need to impose some additional assumptions on k^σ in order to satisfy condition (d). More precisely, we have that either

$$\frac{a^\sigma - 4}{2} < k^\sigma < 4$$

for all non-identity $\sigma : L \rightarrow \mathbb{R}$ or that

$$-4 < k^\sigma < \frac{4 - a^\sigma}{2}$$

for all non-identity $\sigma : L \rightarrow \mathbb{R}$. In both cases, this condition replaces (11).

Furthermore, taking into account the roots of $r(y)$ and the intervals that they live in, we deduce the following inequalities:

$$\begin{aligned} 2 &< \frac{-a + \sqrt{a^2 - 4(b-2)}}{2} \iff 4 + a < \sqrt{a^2 - 4(b-2)}, \\ 2 &> \frac{-a - \sqrt{a^2 - 4(b-2)}}{2} > -2 \iff 4 - a > \sqrt{a^2 - 4(b-2)} > -4 - a, \text{ and} \\ &\text{for all non-identity } \sigma : L \rightarrow \mathbb{R} \text{ have } 4 \pm a^\sigma > \sqrt{(a^\sigma)^2 - 4(b^\sigma - 2)} > -4 \pm a^\sigma. \end{aligned}$$

Next, we combine the lower bounds for the square-root that we obtained above, which yields

$$(12) \quad a^2 - 4(b-2) > (4+a)^2 \iff -2a > 2+b.$$

Likewise, we combine the upper bounds, which gives us

$$(4-a)^2 > a^2 - 4(b-2) \iff 2+b > 2a.$$

Note that this inequality is already a consequence of (7).

For the conjugates, taking into account (8), we only have a non-trivial upper bound for the square root, which gives

$$2 + b^\sigma > \pm 2a^\sigma.$$

Next, we combine (7) with (12), which produces a simple inequality

$$(13) \quad k^2 < -4a.$$

Observe that $-16a < (a - 4)^2$, which means that equations (9) and (10) are consequences of (13).

To summarize, we have shown that the following inequalities must simultaneously hold:

$$(14) \quad \begin{aligned} b &= k^2 + 2a - 2; \\ k^2 &< -4a; \\ \frac{a^\sigma - 4}{2} &< k^\sigma < 4 \text{ or } -4 < k^\sigma < \frac{4 - a^\sigma}{2}; \\ 0 < -a < Q + 3, \quad -4 &< a^\sigma < 4. \end{aligned}$$

Condition (14) should be interpreted as $\frac{a^\sigma - 4}{2} < k^\sigma < 4$ for all non-identity σ or $-4 < k^\sigma < \frac{4 - a^\sigma}{2}$ for all non-identity σ .

The number of solutions can be counted in a manner similar to [Mar96, p. 525], following standard methods from the geometry of numbers (see, for example, [Lan94, Theorem 1, Chapter V]). The count that we obtain is of the form $c_2 Q^{3/2} + o(Q^{3/2})$, where c_2 is a nonnegative constant. We include some details of this computation in the next lemma.

Observe that we still have not used condition (a) in our count. As in the previous section, the only way for $p(x)$ to be reducible is for it to factor into a product of quadratics, i.e.,

$$p(x) = (x^2 + \alpha x + 1)(x^2 + \beta x + 1)$$

in $\mathfrak{o}_L[x]$, with one of them being the minimal polynomial of μ . Without loss of generality, suppose that the first factor has this property. Since its roots have absolute value 1 for all $\sigma : L \rightarrow \mathbb{R}$, we conclude that $|\alpha^\sigma| < 2$ for all σ . This gives finitely many choices for $\alpha \in \mathfrak{o}_L$, and hence $O(Q)$ choices for $p(x)$. \square

In fact, we can use the geometry of numbers to give a bound for c_2 . Let $h = [L : \mathbb{Q}]$. Then we have h embeddings of L into \mathbb{R} given by $\sigma_1 = 1, \sigma_2, \dots, \sigma_h$. Consider the function

$$\varphi : L \rightarrow \mathbb{R}^h$$

$$\varphi(x) = (x^{\sigma_1}, x^{\sigma_2}, \dots, x^{\sigma_h}).$$

It is well-known that the image of \mathfrak{o}_L is a full lattice whose fundamental domain ϕ_L is a parallelotope of volume $|D_L|^{1/2}$.

Lemma 10. *Let c_2 be as in Theorem 8.B. Then*

$$c_2 \leq \frac{2^{2h+2}(12 + 7\delta + \delta^2)^{h-1}}{3|D_L|},$$

where

$$\delta = 2 \min_{\phi_L} \max_{\text{diagonal}} \phi_L.$$

In other words, δ is twice the minimal value of the maximal diagonals of all the possible parallelotopes ϕ_L corresponding to fundamental domains of the lattice given by \mathfrak{o}_L .

Proof. We concentrate on counting the number of $a, k \in \mathfrak{o}_L$ such that

$$(15) \quad \begin{cases} 0 < -a < Q + 3, \\ -4 < a^\sigma < 4 & \forall \sigma \neq 1, \\ k^2 < -4a, \\ \frac{a^\sigma - 4}{2} < k^\sigma < 4 & \forall \sigma \neq 1. \end{cases}$$

The result with $-4 < k^\sigma < \frac{4 - a^\sigma}{2}$ is analogous and will yield the same number.

Now we consider two coordinates, namely $\tilde{\varphi} : L \times L \rightarrow \mathbb{R}^{2h}$ given by $\tilde{\varphi}(a, k) = (\varphi(a), \varphi(k))$. The image of $\mathfrak{o}_L \times \mathfrak{o}_L$ is a full lattice in \mathbb{R}^{2h} whose fundamental parallelopiped $\tilde{\phi}_L$ has volume $|D_L|$.

The number of solutions to (15) is approximated by the number of translates of $\tilde{\phi}_L$ by the image of $\mathfrak{o}_L \times \mathfrak{o}_L$ that fit in the set $S_L(Q, 0)$, where

$$S_L(Q, \delta) = \left\{ (\mathbf{x}, \mathbf{y}) \in \mathbb{R}^{2h} \mid -\delta < -x_1 < Q + 3 + \delta, |x_i| < 4 + \delta, |y_1| < \sqrt{-4x_1} + \delta, \frac{x_i - 4}{2} - \delta < y_i < 4 + \delta, i = 2, \dots, h \right\}.$$

More precisely, let $n(Q, \delta)$ be the number of translations of $\tilde{\phi}_L$ which are contained in $S_L(Q, \delta)$, and let $m(Q, \delta)$ be the number of translations of $\tilde{\phi}_L$ which intersect $S_L(Q, \delta)$. Let $\ell(Q)$ be the number of lattice points in $S_L(Q, 0)$. Then we have

$$(16) \quad n(Q, \delta) \text{Vol}(\tilde{\phi}_L) \leq \text{Vol}(S(Q, \delta)) \leq m(Q, \delta) \text{Vol}(\tilde{\phi}_L)$$

and

$$n(Q, 0) \leq \ell(Q) \leq m(Q, 0).$$

Let δ be equal to the length of the longest diagonal of $\tilde{\phi}_L$. Thus $m(Q, 0) \leq n(Q, \delta)$. This yields

$$(17) \quad n(Q, 0) \leq \ell(Q) \leq m(Q, 0) \leq n(Q, \delta).$$

In textbook applications, one also normally writes $m(Q, -\delta) \leq n(Q, 0)$. However, we are not able to do this here because our set $S_L(Q, \delta)$ is thin compared with the size of δ in the directions where $\sigma \neq 1$. This is the reason why we get an upper bound, but no lower bound.

Combining equations (16) and (17), we obtain

$$(18) \quad \ell(Q) \leq \frac{\text{Vol}(S(Q, \delta))}{\text{Vol}(\tilde{\phi}_L)}.$$

Notice that

$$\begin{aligned} \text{Vol}(S_L(Q, \delta)) &= \int_{-Q-3-\delta}^{\delta} \int_{-4-\delta}^{4+\delta} \cdots \int_{-4-\delta}^{4+\delta} 2(\sqrt{-4x_1} + \delta) \prod_{i=2}^h \left(6 - \frac{x_i}{2} + 2\delta \right) dx_1 \dots dx_h \\ &= (48 + 28\delta + 4\delta^2)^{h-1} \frac{8}{3} Q^{3/2} + O_\delta(Q). \end{aligned}$$

Combining with (18), we arrive at the claimed expression for δ , which is the maximal diagonal of $\tilde{\phi}_L$ and can therefore be bounded by twice the maximal diagonal of ϕ_L . □

5. COMMENTS ABOUT OTHER DEGREES

5.1. We can consider the degree 2 case using the previous work of Bolte [Bol93] instead of Marklof. Let \mathcal{O} be a non-compact arithmetic 2-orbifold with associated group Γ . By [ERT19, Theorem 1.1], for every hyperbolic element $\gamma \in \Gamma$ with $\lambda = e^{\ell(\gamma)}$, we have that λ is a Salem number of degree 2 (recall that the Salem numbers have even degree). It follows that a non-compact arithmetic hyperbolic 2-orbifold generates $Q^{1/2} + O(1)$ different Salem numbers of degree 2 that are less than or equal to Q .

On the arithmetic side, the counting here is very simple. For degree 2, we have $m = 0$, and the problem of counting Salem number reduces to counting irreducible polynomials of the form $x^2 + ax + 1 \in \mathbb{Z}[x]$ under the condition that $0 < -a < Q + 1$. It is also easy to see that the case $a = -1$ does not yield real roots, while $a = -2$ gives $\lambda = 1$. It follows that the number of Salem numbers of degree 2 less than or equal to Q is $Q - 2$.

So, in the logarithmic scale, a given non-compact arithmetic 2-orbifold \mathcal{O} generates asymptotically $1/2$ of all Salem numbers of degree 2.

5.2. From what we see in degrees 2 and 4 it is hardly possible to predict the general distribution. In order to attack this problem one would need to generalize the Bolte–Marklof results to higher dimensional arithmetic orbifolds and obtain an analogue of the Götze–Gusakova theorem for square-rootable Salem numbers. Each of these problems is difficult. We leave them for future research.

Let us mention in passing that the prime geodesic theorem proved by Margulis in [Mar69] applies to counting geodesics of bounded length in any negatively curved closed manifold. However, this result and its generalizations to orbifolds (compact and non-compact finite volume) do not take multiplicity into account. It is a well-known phenomenon that geodesic lengths in the spectrum of an arithmetic space tend to have large multiplicity. For instance, in hyperbolic dimension 3 the leading term in the Margulis theorem is $e^{2\ell}/2\ell$, while the Marklof result yields a growth rate for the number of distinct lengths that is about e^ℓ , which is much smaller. This explains why we cannot use the prime geodesic theorems in our counting.

Acknowledgements. The authors would like to thank Chris Smyth for very helpful comments on an earlier draft of this manuscript. This project was started at the BIRS-CMO workshop “Number Theory in the Americas” in Oaxaca, Mexico. We sincerely thank the organizers of the workshop, and the Casa Matemática Oaxaca, for making it possible for us to work together.

MB is partially supported by CNPq and FAPERJ research grants. ML is partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant 355412-2013 and by the Fonds de recherche du Québec – Nature et technologies (FRQNT) Projet de recherche en équipe 256442. PM has been supported by the KIAS Individual Grant MG072601 at the Korea Institute for Advanced Study. LT is partially supported by the Max Planck Institute for Mathematics.

REFERENCES

- [Bol93] Jens Bolte, *Periodic orbits in arithmetical chaos on hyperbolic surfaces*, Nonlinearity **6** (1993), no. 6, 935–951. MR 1251251
- [CH17] Frank Calegari and Zili Huang, *Counting Perron numbers by absolute value*, J. Lond. Math. Soc. (2) **96** (2017), no. 1, 181–200. MR 3687945
- [ERT19] Vincent Emery, John G. Ratcliffe, and Steven T. Tschantz, *Salem numbers and arithmetic hyperbolic groups*, Trans. Amer. Math. Soc. **372** (2019), no. 1, 329–355. MR 3968771
- [GG19] Friedrich Götze and Anna Gusakova, *On the distribution of Salem numbers*, 2019.
- [Lan94] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR 1282723
- [Leh33] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2) **34** (1933), no. 3, 461–479. MR 1503118
- [Mar69] G. A. Margulis, *Certain applications of ergodic theory to the investigation of manifolds of negative curvature*, Funkcional. Anal. i Prilozhen. **3** (1969), no. 4, 89–90. MR 0257933
- [Mar96] J. Marklof, *On multiplicities in length spectra of arithmetic hyperbolic three-orbifolds*, Nonlinearity **9** (1996), no. 2, 517–536. MR 1384490
- [MR03] Colin Maclachlan and Alan W. Reid, *The arithmetic of hyperbolic 3-manifolds*, Graduate Texts in Mathematics, vol. 219, Springer-Verlag, New York, 2003. MR 1937957
- [Smy15] Chris Smyth, *Seventy years of Salem numbers*, Bull. Lond. Math. Soc. **47** (2015), no. 3, 379–395. MR 3354434
- [Thu14] William P. Thurston, *Entropy in dimension one*, Frontiers in complex dynamics, Princeton Math. Ser., vol. 51, Princeton Univ. Press, Princeton, NJ, 2014, pp. 339–384. MR 3289916
- [Wei60] André Weil, *Algebras with involutions and the classical groups*, J. Indian Math. Soc. (N.S.) **24** (1960), 589–623 (1961). MR 0136682

IMPA, ESTRADA DONA CASTORINA, 110, 22460-320 RIO DE JANEIRO, BRAZIL
Email address: mbel@impa.br

UNIVERSITE DE MONTRÉAL, PAVILLON ANDRÉ-AISENSTADT, DÉPT. DE MATHÉMATIQUES ET DE STATISTIQUE, CP 6128, SUCC. CENTRE-VILLE MONTRÉAL, QUÉBEC, H3C 3J7, CANADA
Email address: mlalin@dms.umontreal.ca

SCHOOL OF MATHEMATICS, KOREA INSTITUTE FOR ADVANCED STUDY, HEOGIRO 85, DONGDAEMUN-GU, SEOUL, 02455, REPUBLIC OF KOREA
Email address: plinio@kias.re.kr

DEPARTMENT OF MATHEMATICS, OBERLIN COLLEGE, 10 N. PROFESSOR ST., OBERLIN, OH 44074, USA
Email address: lola.thompson@oberlin.edu