THE GENERALIZED ARTIN CONJECTURE AND ARITHMETIC ORBIFOLDS

M. RAM MURTY* AND KATHLEEN L. PETERSEN†

ABSTRACT. Let K be a number field with positive unit rank, and let $\mathcal{O}_K$ denote the ring of integers of K. A generalization of Artin's primitive root conjecture is that that $\mathcal{O}_K^\times$ is a primitive root set for infinitely many prime ideals. We prove this with additional conjugacy conditions in the case when K is Galois with unit rank greater than three. This was previously known under the assumption of the Generalized Riemann Hypothesis. From our result, we deduce a topological corollary about the structure of quotients of $\mathrm{PSL}_2(\mathcal{O}_K)$.

1. INTRODUCTION

It is a classical result that the modular group, $\mathrm{PSL}_2(\mathbb{Z})$, does not have the congruence subgroup property (CSP). That is, that there are finite index subgroups which do not contain the kernel of the entrywise modulo n map for any integer $n \in \mathbb{N}$. Petersson proved that, although there are infinitely many subgroups of the modular group whose quotient by $\mathbb{H}$ has only one cusp, only finitely many of these are congruence subgroups. He showed that the index of these groups are exactly the factors of $55440 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$, a divisor of the order of the monster group. This theorem is a consequence of the fact, famously noticed by Galois, that $\mathrm{PSL}_2(\mathbb{F}_p)$ has an index p subgroup only for $p \leq 11$. There appears to be a connection between this and moonshine. Moreover, the groups commensurable with the modular group that appear in moonshine have a cusp transitivity condition which suggests a connection with the one cusped congruence subgroups (see [3]). Petersson's result has been generalized to the Bianchi groups (see [12]) which also fail to have the CSP. In contrast, for number fields K with positive unit rank, such that $\sqrt{-1} \notin K$, there are infinitely many maximal (necessarily congruence) subgroups of $\mathrm{PSL}_2(\mathcal{O}_K)$ whose quotient has a minimal number of cusps. (See section 2 for details.) This result is conditional, under the assumption of a form of Artin's primitive root conjecture (to be specified below). In this paper we prove this

1991 *Mathematics Subject Classification.* 11A07, 11N36, 22E40.

Key words and phrases. Large Sieve, Hyperbolic Spaces, Orbifolds, Euclidean Algorithm.

∗Research partially supported by an NSERC Research grant.

†Coleman post-doctoral fellow.

primitive root conjecture for Galois K with unit rank greater than 3, which was previously known only under the assumption of the generalized Riemann hypothesis (GRH) (see [11]).

We now describe the primitive root conjectures. An integer s is called a primitive root modulo the prime p if s has order $p-1$ modulo p. To be primitive modulo $p > 2$ it is necessary that s is not a square or -1. Artin conjectured a specific density for the set of primes for which s is a primitive root. This density is positive if s is not a square or -1. We will refer to the conjecture that given an integer s other than -1 or a square there are infinitely many primes p for which s is a primitive root as Artin's primitive root conjecture. In 1967 this was proved conditionally, under the assumption of the GRH by Hooley [6]. There are many unconditional results related to Artin's primitive root conjecture (See [9] for a good exposition.) but at present there are no integers for which the conjecture is known to be true.

This classical primitive root conjecture has been generalized to number fields as follows. Let K be a number field with ring of integers $\mathcal{O}_K$. Let π be a prime ideal in $\mathcal{O}_K$ and φ_π be the reduction modulo π map from $\mathcal{O}_K$ to $\mathcal{O}_K/\pi$. Given a multiplicative set S in $\mathcal{O}_K$, $\varphi_\pi(S)$ is contained in $(\mathcal{O}_K/\pi)^\times$. We say that S is a *primitive root set modulo* π if $\varphi_\pi(S) = (\mathcal{O}_K/\pi)^\times$. If S is generated by an element s, we say that s is a *primitive root modulo* π. One generalization of the classical conjecture is that if K has positive unit rank, then $\mathcal{O}_K^\times$ is a primitive root set for infinitely many prime ideals. One can add congruence conditions to the above to get the following conjecture. We will use ζ_q to denote a primitive q^{th} root of unity.

Conjecture 1.1. *Let K be a number field with positive unit rank. Then $\mathcal{O}_K^\times$ is a primitive root set for infinitely many prime ideals. Moreover, given integers $1 \leq a < q$ with $(a,q) = 1$, if $\mathbb{Q}(\zeta_q) \cap K = \mathbb{Q}$ then there are infinitely many prime ideals π such that $|N_{K/\mathbb{Q}}(\pi)| \equiv a \pmod{q}$ and $\mathcal{O}_K^\times$ is a primitive root set modulo π.*

Extending Hooley's conditional proof, this was proven under the assumption of the GRH by Weinberger in 1973 [15]. We provide an unconditional proof of Conjecture 1.1, in the case where K is Galois with unit rank greater than three. Specifically, we show the following.

Theorem 1.2. *Let $K/\mathbb{Q}$ be finite Galois of unit rank greater than three. Let a and q be integers such that $1 \leq a < q$ and $(a,q) = 1$. Assume that $\mathbb{Q}(\zeta_q) \cap K = \mathbb{Q}$. Then there are infinitely many degree one prime ideals π in $\mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\pi)| \equiv a \pmod{q}$ and $\mathcal{O}_K^\times$ is a primitive root set modulo π.*

In Section 2 we describe a topological application of Theorem 1.2, in Section 3 we discuss some preliminaries needed for the proof, in Section 4 we prove Theorem 1.2, and in Section 5 we make some concluding remarks.

2. A Topological Application

Let K be a number field with r_1 real places, and r_2 complex places, and let $\mathcal{O}_K$ denote the ring of integers of K. Then group $\mathrm{PSL}_2(\mathcal{O}_K)$ embeds discretely in $\mathrm{PSL}_2(\mathbb{R})^{r_1} \times \mathrm{PSL}_2(\mathbb{C})^{r_2}$ via the map

$$\pm \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \prod_{\sigma} \pm \begin{pmatrix} \sigma(\alpha) & \sigma(\beta) \\ \sigma(\gamma) & \sigma(\delta) \end{pmatrix}$$

where the product is taken over all infinite places σ of K. The product $\mathrm{PSL}_2(\mathbb{R})^{r_1} \times \mathrm{PSL}_2(\mathbb{C})^{r_2}$ is isomorphic to the orientation preserving isometries of $H_{r_1,r_2} = [\mathbb{H}^2]^{r_1} \times [\mathbb{H}^3]^{r_2}$ where $\mathbb{H}^2$ is the hyperbolic plane, and $\mathbb{H}^3$ is hyperbolic 3-space. This follows from the fact that $\mathrm{Isom}^+(\mathbb{H}^2) \cong \mathrm{PSL}_2(\mathbb{R})$ and $\mathrm{Isom}^+(\mathbb{H}^3) \cong \mathrm{PSL}_2(\mathbb{C})$. The quotient $M_K = H_{r_1,r_2}/\mathrm{PSL}_2(\mathcal{O}_K)$ is a finite volume $(2r_1 + 3r_2)$-dimensional orbifold equipped with a metric inherited from H_{r_1,r_2}. This orbifold has h_K cusps where h_K is the class number of K. If Γ is a finite index subgroup of $\mathrm{PSL}_2(\mathcal{O}_K)$ the quotient $M_\Gamma = H_{r_1,r_2}/\Gamma$ is a finite volume $(2r_1 + 3r_2)$-dimensional orbifold with finitely many cusps. If M_Γ has n cusps, we say that Γ is *n-cusped.* Any such Γ has at least h_K cusps and M_Γ covers M_K.

The groups $\mathrm{PSL}_2(\mathcal{O}_K)$ and the quotients M_K exhibit vastly different behavior depending on whether or not the unit rank of K is positive. Only when $K = \mathbb{Q}$ or an imaginary quadratic field is the unit rank zero, and these quotients are the prototypes for non-compact arithmetic hyperbolic 2- and 3-orbifolds, as all such orbifolds are commensurable to one of these. (Two orbifolds are commensurable if they share a finite sheeted cover.) A principal congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_K)$ is the kernel of the entry-wise modulo $\mathcal{J}$ map for some non-zero ideal $\mathcal{J}$ in $\mathcal{O}_K$ and is denoted $\Gamma(\mathcal{J})$. A finite index subgroup of $\mathrm{PSL}_2(\mathcal{O}_K)$ is a *congruence subgroup* if it contains a principal congruence subgroup, and $\mathrm{PSL}_2(\mathcal{O}_K)$ is said to have the *congruence subgroup property (CSP)* if all finite index subgroups are congruence subgroups. Only when the unit rank of K is zero does $\mathrm{PSL}_2(\mathcal{O}_K)$ fail to have the CSP.

In 1971 Petersson [13] proved that in the case of the modular group, $\mathrm{PSL}_2(\mathbb{Z})$, there are only finitely many one-cusped congruence subgroups, although there are infinitely many maximal one-cusped subgroups. The Bianchi groups are the groups $\mathrm{PSL}_2(\mathcal{O}_d)$ where $\mathcal{O}_d$ is the ring of integers of the imaginary quadratic $\mathbb{Q}(\sqrt{-d})$. The quotients $M_{\mathbb{Q}(\sqrt{-d})}$ are hyperbolic 3-orbifolds. The class number of $\mathcal{O}_d$ is one precisely when $d = 1$, 2, 3, 7, 11, 19, 43, 67, or 163, so only for these values of d can $\mathrm{PSL}_2(\mathcal{O}_d)$ have one-cusped subgroups. Of these, if $d \neq 1$ or 3 there are infinitely many maximal one-cusped subgroups, and for $d = 1$ and 3 there are infinitely many one-cusped subgroups. However, for $d = 11$, 19, 43, 67, or 163 there are only finitely many one-cusped congruence

subgroups, and for $d = 1$, 2, 3, and 7, there are only finitely many maximal one-cusped subgroups (see [12]).

If $\mathcal{O}_K$ has positive unit rank, the situation is quite different. Let π be a prime ideal in $\mathcal{O}_K$ with odd norm $|N_{K/\mathbb{Q}}(\pi)| = q$, let $\varphi_\pi : \mathcal{O}_K \to \mathcal{O}_K/\pi$ denote the reduction modulo π map, and $\Phi_\pi : \mathrm{PSL}_2(\mathcal{O}_K) \to \mathrm{PSL}_2(\mathbb{F}_q)$ be the induced map with the identification $\mathcal{O}_K/\pi \cong \mathbb{F}_q$. Since φ_π maps $\mathcal{O}_K^\times$ into $(\mathcal{O}_K/\pi)^\times$ we will also use φ_π to denote this restriction and let $l = [(\mathcal{O}_K/\pi)^\times : \varphi_\pi(\mathcal{O}_K^\times)]$. If q is odd, there is a subgroup of $\mathrm{PSL}_2(\mathbb{F}_q)$ isomorphic to the dihedral group with $q+1$ elements. Let $\Gamma_\pi < \mathrm{PSL}_2(\mathcal{O}_K)$ be the φ_π pull-back of this group. For π large enough, the principal congruence subgroup $\Gamma(\pi)$ has $h_K l(q+1)$ cusps where h_K is the class number of K. From this, one can show that Γ_π has $h_K l$ cusps if $q \equiv 3 \pmod 4$. (See [11] for details.) Therefore, $\mathrm{PSL}_2(\mathcal{O}_K)$ contains infinitely many maximal h_K-cusped (congruence) subgroups if there are infinitely many prime ideals π in $\mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\pi)| \equiv 3 \pmod 4$ and $\varphi_\pi(\mathcal{O}_K^\times) = (\mathcal{O}_K/\pi)^\times$. If $\sqrt{-1} \notin K$, a conditional proof of this under the assumption of the GRH, is a corollary of Weinberger's result [15]. Theorem 1.2 immediately implies the following corollary.

Corollary 2.1. *Let K be Galois with unit rank greater than three, and such that $\sqrt{-1} \notin K$. There are infinitely many maximal h_K-cusped subgroups of $\mathrm{PSL}_2(\mathcal{O}_K)$, where h_K is the class number of K.*

3. Preliminaries

In this section we collect various results that we will use in the proof of Theorem 1.2. Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ and let C be a conjugacy class in G. Let a and q be positive integers with $1 \le a < q$ and $(a,q) = 1$. We denote by $\pi_C(x,q,a)$ the number of primes $p \le x$ which are unramified in K such that $p \equiv a \pmod q$ and such that the Artin symbol $(p, K/\mathbb{Q}) = C$.

Classically, in the case where $K = \mathbb{Q}$, Dirichlet density theorems state that

$$\pi(x,q,a) \sim \frac{\pi(x)}{\phi(q)}$$

where $\pi(x,q,a)$ denotes the number of primes $\le x$ with the required congruence condition, $\pi(x)$ denotes the number of primes $\le x$, and ϕ is Euler's function. Estimates of the error term, $\pi(x,q,a) - \pi(x)/\phi(q)$ have proven to be very important in many applications. The Riemann Hypothesis for Dirichlet L-functions implies that it is $O\left(x^{1/2}\log qx\right)$. Bombieri [1] and Vinogradov [14] have proven that this estimate holds on the average.. That is, for any $A > 0$

there is a $B > 0$ depending on A so that

$$\sum_{q \le Q} \max_{y \le x} \max_{(a,q)=1} \left| \pi(y,q,a) - \frac{\pi(y)}{\phi(q)} \right| \ll \frac{y}{(\log x)^A}$$

where $Q = x^{1/2}(\log x)^{-B}$. (The notation $f \ll g$ means that $|f/g|$ is bounded.)

In general, the Chebotarev density theorem states that

$$\pi_C(x,q,a) \sim \delta(C,q,a)\phi(q)$$

for some density $\delta(C,q,a) \ge 0$. In fact, if $K \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$ where ζ_q is a primitive q^{th} root of unity, then $\delta(C,q,a) = |C|/|G|\phi(q)$. Murty and Murty [10] have shown the following average formulation.

Proposition 3.1. *Let $L/\mathbb{Q}$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$. Let C be a conjugacy class in G and let a and q be positive integers with $1 \le a < q, (a,q) = 1$. There exist numbers $\delta(C,q,a) \ge 0$ such that for any $\epsilon > 0$ and $A > 0$, we have*

$$\sum_{q \le Q} \max_{(a,q)=1} \max_{y \le x} |\pi_C(y,q,a) - \delta(C,q,a)\pi(y)| \ll \frac{x}{(\log x)^A}$$

with $Q = x^{1/\eta - \epsilon}$ where $\eta \ge \max(|G|/2, 2)$ and the summation is over q such that $L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$.

If A is an abelian subgroup of G with $A \cap C \ne \varnothing$, and $d = [G : A]$. We can improve the above by taking

$$\eta = \begin{cases} d-2 & \text{if } d \ge 4 \\ 2 & \text{if } d \le 4. \end{cases}$$

Moreover, we may replace d above by d^* where $d^* = \min_H \max_\omega [G : H]\omega(1)$ where the minimum is taken over all subgroups H satisfying the following two conditions

- *$H \cap C \ne \varnothing$*
- *For every irreducible character ω of H and any non-trivial Dirichlet character χ, then Artin L-series $L(s, \omega \otimes \chi)$ is entire.*

The maximum above is over all irreducible characters of H. In particular, if Artin's holomorphy conjecture is true for $L/\mathbb{Q}$ then we may take $d^* = \max_\chi \chi(1)$ where the maximum is over all irreducible characters of G.

If $\pi_q(x)$ denotes the number of primes $p \le x$ which split completely in $\mathbb{Q}(\zeta_q, \sqrt[q]{s})$, an estimate of the form

$$\sum_{q \le Q} \left| \pi_q(x) - \frac{\pi(x)}{q(q-1)} \right| \ll \frac{x}{(\log x)^2}$$

with Q about $x^{1/2}$ is sufficient to imply Artin's primitive root conjecture for s (see [8]). At present, such a result seems to be beyond the reach of modern technology.

We will also need the following, whose proof is analogous to that of Lemma 2 in [4].

Proposition 3.2. *Let K be an algebraic number field. Let M be a monoid in $\mathcal{O}_K$ and π be coprime to the elements of M. If M contains r multiplicatively independent elements, then*

$$\#\{\pi : |\varphi_\pi(M)| \leq Y\} \ll Y^{(r+1)/r}.$$

The proof is essentially combinatorial in nature. If $\{b_1, \ldots, b_r\}$ is an independent set of generators for M, and if $|\varphi_\pi(M)| \leq Y$ then for $|N_{K/\mathbb{Q}}(\pi)|$ large enough, there are r-tuples $b_1^{a_1} \ldots b_r^{a_r} \equiv b_1^{\alpha_1} \ldots b_r^{\alpha_r} (\text{mod } \pi)$. Hence $N_{K/\mathbb{Q}}(\pi)$ divides the numerator of $b_1^{a_1-\alpha_1} \ldots b_r^{a_r-\alpha_r} - 1$. The fact that $|\varphi_\pi(M)| \leq Y$ bounds $|a_1| + \cdots + |a_r|$. Together with the divisibility condition this results in the required bound.

We also require an application of the lower bound sieve. The conditions we need are a slight modification of those in [2]. The proof relies upon the linear sieve in the form given by Iwaniec [7], and the estimates from the Bombieri-Vinogradov theorem, as extended by Murty and Murty [10].

Proposition 3.3. *Let $K/\mathbb{Q}$ be a finite Galois extension, such that $\mathbb{Q}(\zeta_q) \cap K = \mathbb{Q}$ and let $t_K = \max_m\{m : K \supseteq \mathbb{Q}(\zeta_m)\}$. Denote by L the Galois extension $K(\zeta_q)$. For a such that $(a, q) = 1$, let C be a conjugacy class of the form $(a, 1)$ in $\mathrm{Gal}(L/\mathbb{Q})$. For η as in Proposition 3.1 the number of primes $p \leq x$ with Artin symbol $(p, L/\mathbb{Q}) = C$ such that for all primes ℓ dividing $(p-1)/t_K$, $\ell > x^{1/2\eta-\epsilon}$ is $\gg x/\log^2 x$.*

4. Proof of Theorem 1.2

We form the compositum, L, of $\mathbb{Q}(\zeta_q)$ and K, which is Galois over $\mathbb{Q}$ as both K and $\mathbb{Q}(\zeta_q)$ are Galois. Let $G = \mathrm{Gal}(L/\mathbb{Q})$ and $H = \mathrm{Gal}(K/\mathbb{Q})$. Notice that $G \cong \mathbb{Z}/\phi(q)\mathbb{Z} \times H$. Let $C \in G$ be the conjugacy class $(a, 1)$. For η and ϵ as in Proposition 3.1, let S be the set of all primes $p \leq x$ such that $(p, L/\mathbb{Q}) \in C$ and such that for all primes ℓ which divide $(p-1)/t_K$, $\ell > x^{1/2\eta-\epsilon}$. The value η is given in Proposition 3.1 for the number field L. Proposition 3.3 implies that $\#S \gg x/\log^2 x$. Notice that the condition that $(p, L/\mathbb{Q}) = C$ insures that all prime ideals π in K lying over p are degree one and have the required congruence condition.

For p in S, t_K divides $|\varphi_\pi(\mathcal{O}_K^\times)|$ as the roots of unity in $\mathcal{O}_K^\times$ inject into $\mathcal{O}_K/\pi$ for $p = N_{K/\mathbb{Q}}(\pi)$ large enough. Therefore, if ℓ divides $(p-1)/|\varphi_\pi(\mathcal{O}_K^\times)|$ then ℓ divides $(p-1)/t_K$ and is greater than $x^{1/2\eta-\epsilon}$. As a result, the index

$(p-1)/|\varphi_\pi(\mathcal{O}_K^\times)|$ is either one or greater than $x^{1/2\eta-\epsilon}$. If the index is not one then $|\varphi_\pi(\mathcal{O}_K^\times)| < x^{1-1/2\eta+\epsilon}$.

By Proposition 3.2 $\#\{\pi : |\mathcal{O}_K^\times/\pi| \leq x^{1-1/2\eta+\epsilon}\} \ll x^{(1-1/2\eta+\epsilon)(r+1)/r}$ where r is the rank of $\mathcal{O}_K^\times$. It suffices to show that

$$O(x^{(1-1/2\eta+\epsilon)(r+1)/r}) = o\left(\frac{x}{\log^2 x}\right).$$

This occurs when $2\eta < r+1$.

Recall from Proposition 3.1 that if A is an abelian subgroup of G such that $A \cap C \neq \varnothing$, setting $d = [G : A]$

$$\eta = \begin{cases} d-2 & \text{if } d \geq 4 \\ 2 & \text{if } d \leq 4. \end{cases}$$

Taking A isomorphic to $\mathbb{Z}/\phi(q)\mathbb{Z} \times B$ where B is an abelian subgroup of H, $d = [H : B]$. Notice that $A \cap C \neq \varnothing$. If $d \leq 4$, then the inequality is satisfied when $r > 3$. If $d \geq 4$ then the inequality is $2|H| < |B|(r+5)$. Let r_1 be the number of real places of K and r_2 be the number of complex places of K. Then $r = r_1 + r_2 - 1$ and $|H| = r_1 + 2r_2$. With this substitution the inequality becomes $0 < (|B|-2)r_1 + (|B|-4)r_2 + 4|B|$. This is satisfied if there is an abelian subgroup B of H with $|B| \geq 4$, which is the case unless $|H|$ divides 6. If $|H| \leq 3$ then $r \leq 3$. If $|H| = 6$ we let $|B| = 2$ and satisfy the inequality if $r > 3$.

The following two corollaries follow immediately.

Corollary 4.1. *Let $K/\mathbb{Q}$ be finite Galois of unit rank greater than three. Then there are infinitely many degree one prime ideals π in $\mathcal{O}_K$ such that $\mathcal{O}_K^\times$ is a primitive root set modulo π.*

Corollary 4.2. *Let $K/\mathbb{Q}$ be finite Galois of unit rank greater than three such that $i \notin K$. Fix $a = \pm 1$. Then there are infinitely many degree one prime ideals π in $\mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\pi)| \equiv a \pmod 4$ and $\mathcal{O}_K^\times$ is a primitive root set modulo π.*

5. Concluding Remarks

There are two possible avenues for further research. The first is the problem when the unit rank is 1, 2 or 3. This problem may be approached by refining the techniques of [5], but this refinement will not be straightforward. These techniques may allow us to treat the case of rank 3. The second problem to address is the case when K is not Galois. To treat this case, one would have to extend the results of [10] to the non-Galois situation. This can be done, in

principle, though again there are several technical difficulties that need to be addressed. We hope to investigate both of these problems in future work.

References

[1] E. Bombieri. On the large sieve. *Mathematika*, 12:201–225, 1965.

[2] David A. Clark and M. Ram Murty. The Euclidean algorithm for Galois extensions of $\mathbf{Q}$. *J. Reine Angew. Math.*, 459:151–162, 1995.

[3] John Conway, John McKay, and Abdellah Sebbar. On the discrete groups of Moonshine. *Proc. Amer. Math. Soc.*, 132(8):2233–2240 (electronic), 2004.

[4] Rajiv Gupta and M. Ram Murty. A remark on Artin's conjecture. *Invent. Math.*, 78(1):127–130, 1984.

[5] Malcolm Harper and M. Ram Murty. Euclidean rings of algebraic integers. *Canad. J. Math.*, 56(1):71–76, 2004.

[6] Christopher Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.

[7] Henryk Iwaniec. Rosser's sieve. *Acta Arith.*, 36(2):171–202, 1980.

[8] M. Ram Murty. On Artin's conjecture. *J. Number Theory*, 16(2):147–168, 1983.

[9] M. Ram Murty. Artin's conjecture for primitive roots. *Math. Intelligencer*, 10(4):59–67, 1988.

[10] M. Ram Murty and V. Kumar Murty. A variant of the Bombieri-Vinogradov theorem. In *Number theory (Montreal, Que., 1985)*, volume 7 of *CMS Conf. Proc.*, pages 243–272. Amer. Math. Soc., Providence, RI, 1987.

[11] K. L. Petersen. Counting cusps of subgroups of $\mathrm{PSL}_2(\mathcal{O}_K)$. *to appear in Proc AMS.*

[12] K. L. Petersen. One-cusped congruence subgroups of Bianchi groups. *Math. Ann.*, 338(2):249–282, 2007.

[13] Hans Petersson. Über die Konstruktion zykloider Kongruenzgruppen in der rationalen Modulgruppe. *J. Reine Angew. Math.*, 250:182–212, 1971.

[14] A. I. Vinogradov. The density hypothesis for Dirichet L-series. *Izv. Akad. Nauk SSSR Ser. Mat.*, 29:903–934, 1965.

[15] Peter J. Weinberger. On Euclidean rings of algebraic integers. In *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 321–332. Amer. Math. Soc., Providence, R. I., 1973.

Department of Mathematics and Statistics, Queen's University
Kingston, ON K7L 3N6, Canada
email: murty@mast.queensu.ca, petersen@mast.queensu.ca