

Counting and equidistribution over primes in hyperbolic groups

Yiannis N. Petridis and Morten S. Risager

Abstract. We consider equidistribution of angles for certain hyperbolic lattice points in the upper half-plane. Extending work of Friedlander and Iwaniec, we show that for the full modular group equidistribution persists for matrices with $a^2 + b^2 + c^2 + d^2 = p$ with p prime; at least if we assume sufficiently good lower bounds in the hyperbolic prime number theorem by Friedlander and Iwaniec. We also investigate related questions for a specific arithmetic co-compact group and its double cosets by hyperbolic subgroups. The general equidistribution problem was studied by Good, and in this case, we show, that equidistribution holds unconditionally when restricting to primes.

1. Introduction

Let X be a compact topological space equipped with a non-negative measure μ , normalized such that $\mu(X) = 1$. It is an important problem in number theory to determine if a (generalized) sequence $S = (x_i)_{i \in I} \subseteq X$ is (asymptotically) equidistributed on X (with respect to μ), i.e., if for every $f \in C(X)$, we have that

$$\frac{1}{N_S(x)} \sum_{\nu(i) \leq x} f(x_i) \rightarrow \int_X f d\mu \quad \text{as } x \rightarrow \infty.$$

Here we assume that I is equipped with a (size) function $\nu: I \rightarrow \mathbb{N}$ with the property that $N_S(x) := \#\{i \in I : \nu(i) \leq x\}$ is finite for all $x \in \mathbb{R}$.

It is an interesting question to see how much we can shrink the index set I and still have (asymptotic) equidistribution. We say that a sequence $(x_i)_{i \in I}$ is (asymptotically) equidistributed on X over primes if for every $f \in C(X)$, we have that

$$\frac{1}{\pi_S(x)} \sum_{\substack{\nu(i) \leq x \\ \nu(i) \text{ prime}}} f(x_i) \rightarrow \int_X f d\mu \quad \text{as } x \rightarrow \infty.$$

Mathematics Subject Classification 2020: 11N45 (primary); 11J71, 11N36 (secondary).

Keywords: hyperbolic primes, equidistribution of angles.

Here

$$\pi_S(x) = \#\{i \in I : v(i) \leq x, v(i) \text{ prime}\}.$$

Example 1.1 (Angles of lattice points in $\mathbb{Z}^2$). Consider the sequence of (normalized) angles of the square lattice $A = (\arg(v)/2\pi)_{v \in \mathbb{Z}^2} \subseteq \mathbb{R}/\mathbb{Z}$ with $v(v) = \|v\|^2$. In the 19th century, Gauss [13] noticed that

$$N_A(x) = \pi x + O(x^{1/2}); \quad (1)$$

see, e.g., [2] for a description of Gauss' elementary method. His method is flexible enough to show that the normalized angles are equidistributed with respect to Lebesgue measure on $\mathbb{R}/\mathbb{Z}$. It was observed by Landau [28] that $\pi_A(x)$ can be estimated, using the analytic properties of the Dedekind zeta-function $\zeta_K(s)$ for the number field $K = \mathbb{Q}(i)$; in particular, its pole at $s = 1$ and the fact that it has a zero-free region. He found that

$$\pi_A(x) = \sum_{p \leq x} r(p) = 4 \operatorname{li}(x) + O\left(\frac{x}{(\log(x))^4}\right),$$

where $\operatorname{li}(x) = \int_2^x 1/(\log t) dt$ is the logarithmic integral function. The factor 4 occurs since we are really counting prime ideal with multiplicity 4. In order to determine the angular distribution of these 'prime lattice points', Hecke [17] introduced his Grössen-characters

$$\xi_k((z)) = \left(\frac{z}{|z|}\right)^{4k},$$

proved the analytic continuation of the corresponding Hecke L -functions $L(s, \xi_k)$ and also proved, via Weyl's equidistribution criterion, that $\arg(v)/2\pi$ equidistributes on primes; see [17, eq. (52)]. See also the work of Kubilius [27] for a statement with error term.

Example 1.2 (The sequence αn modulo 1 for α irrational). Using his equidistribution theorem, Weyl [45, Satz 2] proved that, if $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, then $(\alpha n)_{n \in \mathbb{N}} \subseteq \mathbb{R}/\mathbb{Z}$ is equidistributed with respect to the Lebesgue measure on $\mathbb{R}/\mathbb{Z}$. Understanding what happens when restricting to primes is much harder, but Vinogradov famously proved that $(\alpha n)_{n \in \mathbb{N}}$ is indeed equidistributed over primes; see [25, Theorem 21.3] for a proof.

Analogous statements hold for $q(n)$ with $q(x)$ a non-constant real polynomial with some condition on the coefficients (the leading coefficient being irrational suffices). For more on this, consult [25, Proposition 21.1] and [37, Theorem 1].

1.1. Main results

In this paper we investigate equidistribution over primes for various quantities in specific arithmetic subgroups of $\mathrm{SL}_2(\mathbb{R})$. Anton Good [14] studied nine different types of decomposition of cofinite Fuchsian groups corresponding to double coset spaces $\Gamma_\xi \backslash \Gamma / \Gamma_\chi$ for Γ_ξ, Γ_χ pairs of stabilizers of ξ resp. χ . Here ξ, χ can be cusps (parabolic subgroups), points in $\mathbb{H}$ (elliptic subgroups), or geodesics between two points on the boundary of $\mathbb{H}$ (hyperbolic subgroups). Using the spectral theory of automorphic forms he proved [14, Corollary, p. 119] an equidistribution result for each of these nine types of decomposition. Good's results hold for any co-finite discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$, as their proof utilize the spectral theory of the corresponding automorphic Laplacian, and not any arithmetic. Parkkonen and Paulin proved more general equidistribution results for endpoints of common perpendiculars in negative curvature; see [34].

For certain arithmetic subgroups of $\mathrm{SL}_2(\mathbb{Z})$ Duke, Friedlander and Iwaniec [8] proved equidistribution over primes in the parabolic-elliptic case of Good's theorem, while Tóth [41] proved equidistribution over primes in the parabolic-hyperbolic case of Good's theorem. In this paper we consider arithmetic examples of the three diagonal cases $\xi = \chi$ and investigate what happens when we restrict the counting functions to primes.

1.1.1. The parabolic case. Consider $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, and the parabolic subgroup $\Gamma_\infty = \left(\begin{smallmatrix} 1 & \\ 0 & 1 \end{smallmatrix}\right)$. We consider the sequence

$$P = \left(\left(\frac{a}{c}, \frac{d}{c} \right) \right) \subseteq (\mathbb{R}/\mathbb{Z})^2$$

indexed over $\gamma \in \Gamma_\infty \backslash \Gamma / \Gamma_\infty$ with $0 < c$, and with size function $v(\gamma) = c$.

In this case, Good's theorem (see also Selberg's unpublished notes [39]) implies that

$$N_P(x) = \frac{3}{\pi^2} x^2 + O(x^{4/3}),$$

and P is equidistributed on $(\mathbb{R}/\mathbb{Z})^2$. Here and elsewhere equidistribution on $(\mathbb{R}/\mathbb{Z})^2$ is understood to be with respect to Lebesgue measure. For this specific group, much better error terms are known using different methods; see [44, eq. (2), p. 114] and [30].

The sequence P is straightforward to analyze over primes: Using the prime number theorem it follows that

$$\pi_P(x) = \mathrm{li}(x^2) + O\left(\frac{x^2}{\log^A(x)}\right).$$

Any non-trivial bound on the classical Kloosterman sums gives that P is equidistributed on $(\mathbb{R}/\mathbb{Z})^2$ over primes. We will not dwell on the details. The relevant decompos-

ition is a Bruhat-type decomposition; see [24, Section 1.4]. Humphries [22] proved several refined equidistribution results in this case, using different notation.

1.1.2. The elliptic case. Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, which acts on the upper half-plane $\mathbb{H}$. Consider the hyperbolic length $d_{\mathbb{H}}(\gamma i, i)$ between γi and i , and the angle of the hyperbolic geodesic from i to γi against the vertical geodesic from i . If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we let

$$v_{\mathbb{H}}(\gamma) = a^2 + b^2 + c^2 + d^2 = 2 \cosh d_{\mathbb{H}}(\gamma i, i).$$

Selberg [39], Nicholls [33], and Good [14] proved asymptotic equidistribution of angles related to $\gamma \in \Gamma$ with $v_{\mathbb{H}}(\gamma) \leq x$. In fact, Selberg and Good proved something even stronger. For $I \neq \gamma \in \mathrm{SL}_2(\mathbb{R})$, the Cartan decomposition allows us to write

$$\gamma = k(\theta_1(\gamma))a(e^{-r})k(\theta_2(\gamma)),$$

where

$$k(\theta) = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}, \quad a(e^{-r}) = \begin{pmatrix} e^{-r/2} & \\ & e^{r/2} \end{pmatrix}.$$

Here $r = d_{\mathbb{H}}(\gamma i, i) > 0$ is uniquely determined, and $\theta_1(\gamma), \theta_2(\gamma)$ are determined modulo π . The works of Selberg [39] and Good [14] imply that if we consider the sequence

$$E = (\theta(\gamma))_{\gamma \in \Gamma} = \left(\left(\frac{\theta_1(\gamma)}{\pi}, \frac{\theta_2(\gamma)}{\pi} \right) \right) \quad (2)$$

indexed over Γ and with counting function $v(\gamma) = v_{\mathbb{H}}(\gamma)$, then

$$N_E(x) = 6x + O(x^{2/3}),$$

and E is equidistributed on $(\mathbb{R}/\mathbb{Z})^2$; see also [14, 24, 35, 39].

In order to understand what happens when we restrict to primes, we recall that Friedlander and Iwaniec [12] studied what they call a ‘hyperbolic prime number theorem’. In our notation this means understanding $\pi_E(x)$. Conditional on a conjecture weaker than the Elliott–Halberstam conjecture (see (17) below for the precise conjecture), they used sieving techniques to prove that

$$\pi_E(x) \asymp \frac{x}{\log x}. \quad (3)$$

Here $\asymp$ means that the quotient of the two sides is bounded from above and below by strictly positive constants. In this paper we show, conditional on the same conjecture, that E is equidistributed over primes, analogously to Hecke’s result for $\mathbb{Z}^2$.

Theorem 1.3. *Let E be the sequence (2), i.e., the pair of normalized angles from the Cartan decomposition for $\mathrm{SL}_2(\mathbb{Z})$. Assume $\pi_E(x)$ satisfies (3). Then E is equidistributed on $(\mathbb{R}/\mathbb{Z})^2$ over primes.*

We remark that in Theorem 1.3, we do not need the full force of (3). Our proof only requires

$$\frac{\pi_E(x)}{x/\log(x)}(\log x)^{1-2\pi^{-1}} \rightarrow \infty \quad (4)$$

to conclude equidistribution over primes, which is much weaker than the conditional lower bound in (3). It would be interesting to see if (4) can be proved unconditionally, and/or if the exponent of $1 - 2\pi^{-1}$ may be improved.

Friedlander and Iwaniec also considered a related but different counting function, namely,

$$\pi_{E'}(x) = \#\{\gamma \in \Gamma \mid v_{\mathbb{H}}(\gamma) = p - 2 \leq x\}.$$

This is equivalent to considering the sequence

$$E' = (\theta(\gamma))_{\gamma \in \Gamma} = \left(\left(\frac{\theta_1(\gamma)}{\pi}, \frac{\theta_2(\gamma)}{\pi} \right) \right) \quad (5)$$

with modified counting function $v'(\gamma) = v_{\mathbb{H}}(\gamma) + 2$. Clearly, we have $N_{E'}(x) = N_E(x) + O(x^{2/3})$ and E' is also equidistributed on $(\mathbb{R}/\mathbb{Z})^2$.

For this slightly modified sequence, they found precise unconditional asymptotics

$$\pi_{E'}(x) = 8\pi \prod_p \left(1 + \frac{\chi_4(p)}{p(p-1)} \right) \text{li}(x) + O_A(x(\log x)^{-A}) \quad (6)$$

for any $A > 0$. Note that there is an obvious factor of 8 missing in going from (1.16) to (1.17) in [12]. Here χ_4 is the primitive Dirichlet character modulo 4. Our method is flexible enough to allow considering the angle distribution in this case, and we arrive at the following unconditional result.

Theorem 1.4. *Let E' be the modified sequence (5), i.e., the pair of normalized angles from the Cartan decomposition with the modified ordering. Then E' is equidistributed on $(\mathbb{R}/\mathbb{Z})^2$ over primes.*

The hyperbolic prime number theorem (3) of Friedlander and Iwaniec is hard. It is equivalent to the following statement:

$$\sum_{p \leq x} r(p+2)r(p-2) \asymp \frac{x}{\log x}, \quad (7)$$

with $r(n)$ the sum of two squares counting function. This highlights the similarity to the twin prime conjecture, and why (7) and (3) currently cannot be proved unconditionally. They are only proved conditionally on a weak form of the Elliott–Halberstam conjecture; see (17).

It turns out that, using Proposition 3.2 below, Theorems 1.3 and 1.4 can be reformulated in terms of Gaussian integers. A Gaussian integer w is called primary if

$w = 1 \pmod{(1+i)^3}$. Consider the following sets of pairs of primary Gaussian integers with norms differing by 4:

$$C_n = \{z_1 \in \mathbb{Z}[i] \mid z_1 \bar{z}_1 = n + 2, z_1 \text{ primary}\} \times \{z_2 \in \mathbb{Z}[i] \mid z_2 \bar{z}_2 = n - 2, z_2 \text{ primary}\}.$$

Note that for n odd, we have $\#C_n = r(n+2)r(n-2)$. For $z = (z_1, z_2)$, denote by $\theta(z) = (\theta(z_1), \theta(z_2))^t$ the corresponding set of angles. Consider

$$M = \frac{1}{2\pi} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

and observe that $M\theta(z)$ is the (normalized) sum and difference of the two angles. Consider the two sequences $\mathcal{E}$ resp. $\mathcal{E}'$ both defined to be the sum and the difference of the normalized angles of z_1 and $z_2 \pmod{1}$, i.e.,

$$(M\theta(z) \pmod{\mathbb{Z}^2}) \text{ indexed over } C_n \text{ with } n \in \mathbb{N},$$

but with size function $v(z) = n$ resp. $v'(z) = n + 2$.

Theorem 1.5. *The sequences $\mathcal{E}$ and $\mathcal{E}'$ are equidistributed on $(\mathbb{R}/\mathbb{Z})^2$. Assume $\pi_E(x)$ satisfies (7), then $\mathcal{E}$ is equidistributed on $(\mathbb{R}/\mathbb{Z})^2$ over primes. Unconditionally, $\mathcal{E}'$ is equidistributed on $(\mathbb{R}/\mathbb{Z})^2$ over primes.*

Remark 1. Chatzakos, Kurlberg, Lester, and Wigman [5] proved, for points on hyperbolic circles, the existence of a full density subsequence of $n \in \mathcal{N}$ such that the angle $\theta_1(\gamma)$, for $\gamma \in \Gamma$ with $v_{\mathbb{H}}(\gamma) = n$ equidistributes as $n \rightarrow \infty$ with $n \in \mathcal{N}$. Here

$$\mathcal{N} = \{n \in \mathbb{N} \mid n = a^2 + b^2 + c^2 + d^2 \text{ for some } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma\}.$$

They also show that exceptional radii *do* exist. Similar questions for Euclidean circles were considered by Kátai and Környei [26] and Erdős and Hall [9]. Our method of proof is indeed inspired by [5].

Cherubini and Fazzari [6] extended [5] in a different direction by considering other CM-points with class number $h = 1$. The techniques we are using probably generalize to congruence groups and other CM-points, but probably not to general cofinite subgroups of $\mathrm{PSL}_2(\mathbb{R})$.

1.1.3. The hyperbolic case. The final case we analyze relates to the quaternion group

$$\Gamma(2, 5) = \left\{ \begin{pmatrix} x_0 + x_1\sqrt{2} & \sqrt{5}(x_2 + x_3\sqrt{2}) \\ \sqrt{5}(x_2 - x_3\sqrt{2}) & x_0 - x_1\sqrt{2} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) \mid x_i \in \mathbb{Z} \right\}$$

and its hyperbolic subgroup

$$H = \left\langle \begin{pmatrix} \varepsilon^2 & 0 \\ 0 & \varepsilon^{-2} \end{pmatrix} \right\rangle.$$

Here $\varepsilon = 1 + \sqrt{2}$ is the totally positive fundamental unit in the ring of integers of $\mathbb{Q}(\sqrt{2})$. If $\gamma \in \Gamma(2, 5)$ has strictly positive integer entries, then there exist unique $y_1, y_2 > 0, v > 0$ such that

$$\gamma = \begin{pmatrix} \sqrt{y_1} & 0 \\ 0 & 1/\sqrt{y_1} \end{pmatrix} \begin{pmatrix} \cosh v & \sinh v \\ \sinh v & \cosh v \end{pmatrix} \begin{pmatrix} \sqrt{y_2} & 0 \\ 0 & 1/\sqrt{y_2} \end{pmatrix};$$

see Lemma 4.3. Geometrically, $v(\gamma)$ equals half the distance between the infinite vertical geodesic $\mathcal{I}$ from 0 to $i\infty$ and its image under γ . In terms of the entries one shows that $(\cosh(2v(\gamma)) - 1)/10 = bc/5$.

Consider the sequence

$$h = (\psi(\gamma)) = \left(\left(\frac{\log y_1}{2 \log \varepsilon^2}, \frac{\log y_2}{2 \log \varepsilon^2} \right) \right) \subseteq (\mathbb{R}/\mathbb{Z})^2, \quad (8)$$

indexed over the set of all $\gamma \in H \backslash \Gamma(2, 5)/H$ with all four entries strictly positive. Equip this index set with the size function $v(\gamma) = bc/5$. Good [14] and Hejhal ([19], [21, Theorem 8]) proved that

$$N_h(x) = \frac{10(\log \varepsilon)^2}{\pi^2} X + O(X^{2/3}).$$

If there are non-zero eigenvalues of the automorphic Laplacian less than $1/4$, there are additional main terms, but these are not expected to exist in this case, as follows from Selberg's eigenvalue conjecture. Good [14, Theorem 4] further proved that h is equidistributed on $(\mathbb{R}/\mathbb{Z})^2$. When restricting to primes we prove the following result.

Theorem 1.6. *Consider the sequence h in (8). Then*

$$\pi_h(x) = C \operatorname{li}(x) + O\left(\frac{x}{\log^A(x)}\right),$$

and h is equidistributed on $(\mathbb{R}/\mathbb{Z})^2$ over primes. Here

$$C = \frac{12 \log \varepsilon}{5 \sqrt{2}} \prod_{p \neq 5} \left(1 + \frac{\chi_8(p)}{p(p-1)} \right),$$

where χ_8 is the even primitive Dirichlet character modulo 8.

Remark 2. The sequence h in (8) has a natural geometric interpretation: The geodesic segment minimizing the distance from the imaginary axis $\mathcal{I}$ and $\gamma\mathcal{I}$ meets $\mathcal{I}$ at iy_1 and $\gamma\mathcal{I}$ at γiy_2^{-1} . The length of the geodesic corresponding to H is $2\log(\varepsilon^2)$. The signed distance from i to iy_1 is $\log y_1$. So Good's theorem proves the (joint) equidistribution of the endpoints of the distance minimizing geodesic segments corresponding to the double cosets $H\backslash\Gamma(2, 5)/H$.

We can formulate the equidistribution statement entirely in terms of quantities defined using the ring of integers of the real quadratic field $K = \mathbb{Q}(\sqrt{2})$. Let

$$\sigma(a + \sqrt{2}b) = a - \sqrt{2}b$$

be the non-trivial Galois automorphism, and consider

$$D_n = D_K(5n + 1) \times D_K(n).$$

Here $D_K(n)$ is the set of classes of totally positive elements of $\mathcal{O}_K$ with field norm n modulo the following equivalence relation: $z_1 \sim z_2$ if and only if $z_1 = \varepsilon^{2m} z_2$ for some $m \in \mathbb{Z}$. Therefore,

$$D_K(n) = \{z \in \mathcal{O}_K \mid z \cdot \sigma z = n, z > 0, \sigma(z) > 0\} / \sim.$$

For $z \in (z_1, z_2) \in D_n$, denote

$$\theta'(z) = \left(\frac{\log|z_1/\sigma z_1|}{2\log \varepsilon^2}, \frac{\log|z_2/\sigma z_2|}{2\log \varepsilon^2} \right),$$

and let $M' = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Then we may consider the sequence $\mathcal{H}$ defined to be the (normalized) sum and difference of these quantities mod 1, i.e.,

$$(M'\theta'(z) \bmod \mathbb{Z}^2) \text{ indexed over } D_n \text{ with } n \in \mathbb{N},$$

and with size function $v(z) = n$.

Theorem 1.7. *The sequence $\mathcal{H}$ is equidistributed on $(\mathbb{R}/\mathbb{Z})^2$, and equidistributed on $(\mathbb{R}/\mathbb{Z})^2$ over primes.*

Remark 3. In a nutshell, the main theorems are proved by translating the statistics of the problem in question to a number field setting, where we can apply Hecke's theory of Größencharacters, and extensions thereof. We then combine with various bounds on sums involving multiplicative functions due to Nair and Tenenbaum, and use Weyl's equidistribution criterium.

In Section 2 we state the relevant various bounds on sums of multiplicative functions. In Section 3 we translate the elliptic case to statistics of Gaussian integers on

two circles, and analyze the relevant Weyl sums leading to Theorem 1.5. In Section 4 we translate the hyperbolic case to statistics of the integers of the real quadratic field $\mathbb{Q}(\sqrt{2})$ on two hyperbolas. The counting problem can then be translated to an analogue of the Titchmarsh divisor problem, which we solve using recent results by Assing, Blomer and Li. The equidistribution result can be deduced using the techniques of Section 2. This leads to a proof of Theorem 1.6.

2. Bounding sums of multiplicative functions

A crucial ingredient in our proofs of equidistribution over primes are certain bounds on sums of multiplicative function. In this section we recall a few useful results in this direction.

Nair and Tennenbaum [32] developed a general and very flexible method to harvest the power of multiplicativity to bound specific sums of multiplicative or approximately multiplicative non-negative functions of various types. Here we state a small part of a simplified version of [32, Theorem 3].

Theorem 2.1. *Consider two non-negative multiplicative functions g_1, g_2 satisfying $g_i(n) \leq d(n)$ and a_i, b_i satisfying $(a_i, b_i) = 1$ and $b_1 a_2 \neq b_2 a_1$. Then*

$$\sum_{p \leq x} g_1(|a_1 p + b_1|) g_2(|a_2 p + b_2|) \ll_{a_i, b_i} \frac{x}{\log(x)} \prod_{2 < p \leq x} \left(1 - \frac{2}{p}\right) \sum_{n_1 \leq x} \frac{g_1(n_1)}{n_1} \sum_{n_2 \leq x} \frac{g_2(n_2)}{n_2}. \quad (9)$$

It is well known that

$$\prod_{p \leq x} \left(1 - \frac{2}{p}\right) = O((\log x)^{-2}),$$

e.g., it follows easily from the prime number theorem. Therefore, the right-hand side of (9) is bounded by a constant times

$$\frac{x}{\log^3(x)} \sum_{n_1 \leq x} \frac{g_1(n_1)}{n_1} \sum_{n_2 \leq x} \frac{g_2(n_2)}{n_2}.$$

Another useful bound is the following weak form of a Halberstam–Richert inequality [16]. We quote from [10, Theorem 7].

Theorem 2.2. *Let f be a non-negative multiplicative function satisfying that*

$$\sum_{n \leq x} f(n) = O(x), \quad \text{and} \quad f(p^k) = O(k)$$

for all primes p and $k \geq 1$. Then

$$\frac{1}{x} \sum_{n \leq x} f(n) \ll \exp \left(\sum_{p \leq x} \frac{f(p) - 1}{p} \right) + \frac{1}{\log x}.$$

The implied constant in the conclusion only depends on the implied constants of the assumptions.

3. The elliptic case

In this section we consider the modular group $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. We recall the Cartan decomposition and its relation to angles.

3.1. Cartan decomposition and angles between lattice points

For a group element $\gamma \in \mathrm{SL}_2(\mathbb{R}) = G$, the point $\gamma i \in \mathbb{H}$ is determined by the hyperbolic distance $d_{\mathbb{H}}(i, \gamma i)$ and the angle $\nu(\gamma)$ between the vertical geodesic from i to $i\infty$ and the geodesic between i and γi . To give a clear geometric picture, we map the upper half-plane $\mathbb{H}$ to the Poincaré disc $\mathbb{D}$ using the Cayley map

$$f(z) = \frac{z - i}{z + i}.$$

This is a holomorphic diffeomorphism with $f(i) = 0$. Since it is conformal, it preserves angles. It maps the vertical geodesic from i to the geodesic $[0, 1)$ in the Poincaré disc, so that $\nu(\gamma)$ is the argument of the complex number $f(\gamma i)$, i.e.,

$$f(\gamma i) = |f(\gamma i)|e^{i\nu(\gamma)}.$$

By the Cartan decomposition $G = KAK$, we may write

$$\gamma = k(\theta_1(\gamma))a(e^{-r})k(\theta_2(\gamma)),$$

where

$$k(\theta) = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \in K = \mathrm{SO}_2(\mathbb{R}),$$

which is the stabilizer of i in $\mathrm{SL}_2(\mathbb{R})$, and

$$a(e^{-r}) = \begin{pmatrix} e^{-r/2} & \\ & e^{r/2} \end{pmatrix} \in A = \left\{ \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \mid a > 0 \right\}.$$

Here $r = d_{\mathbb{H}}(\gamma i, i) \geq 0$ is uniquely determined and, if $r > 0$, the numbers $\theta_1(\gamma)$, $\theta_2(\gamma)$ are determined modulo π , while $\theta_1(\gamma) + \theta_2(\gamma)$ is determined modulo 2π . A straightforward computation shows that

$$f(\gamma i) = \frac{e^{-r} - 1}{e^{-r} + 1} e^{2i\theta_1(\gamma)},$$

so $2\theta_1(\gamma) = v(\gamma)$. We note also that

$$\gamma^{-1} = k\left(\frac{\pi}{2} - \theta_2(\gamma)\right) a(e^{-r}) k\left(-\frac{\pi}{2} - \theta_1(\gamma)\right),$$

so $2\theta_2(\gamma) = \pi - 2\theta_1(\gamma^{-1}) = \pi - v(\gamma^{-1})$. When studying the joint distribution of $\theta_1(\gamma)$, $\theta_2(\gamma) \bmod \pi$, we want to consider the corresponding Weyl sums, which in this case are

$$S_e(m_1, m_2, n) = \sum_{\substack{\gamma \in \Gamma \\ v_{\mathbb{H}}(\gamma) = n}} \exp(i(2\theta_1(\gamma)m_1 + 2\theta_2(\gamma)m_2)). \quad (10)$$

This may be thought of as a Kloosterman-type sum related to the Cartan decomposition, in the same way that the standard Kloosterman sum is related to a Bruhat-type decomposition $G = N\omega AN$, where N consists of upper triangular matrices with 1 on the diagonal and $\omega = k(-\pi/2)$.

It is convenient to mod out on the right and left by of stabilizer Γ_i of i in Γ acting on $\mathbb{H}$. One finds that Γ_i is cyclic of order 4 generated by the elliptic element

$$\gamma_i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = k\left(\frac{\pi}{2}\right),$$

so that

$$\gamma_i^{j_1} \gamma \gamma_i^{j_2} = k\left(\theta_1(\gamma) + j_1 \frac{\pi}{2}\right) a(e^{-r}) k\left(\theta_2(\gamma) + j_2 \frac{\pi}{2}\right). \quad (11)$$

Since if $\gamma \neq \pm I$, the double coset $\Gamma_i \gamma \Gamma_i$ contains precisely 8 elements; these can, e.g., be parametrized by $\gamma_i^{j_1} \gamma \gamma_i^{j_2}$ for $j_1 = 0, \dots, 3$, and $j_2 = 0, 1$. Another possible parametrization is $j_1 = 0, 1$, $j_2 = 0, \dots, 3$. Fixing representatives for the double coset $\Gamma_i \backslash \Gamma / \Gamma_i$ and using (11), we find that

$$S_e(m_1, m_2, n) = \delta_{2|m_1} \delta_{2|m_2} 8 S'_e(m_1, m_2, n), \quad (12)$$

where

$$S'_e(m_1, m_2, n) = \sum_{\substack{\gamma \in \Gamma_i \backslash \Gamma / \Gamma_i \\ v_{\mathbb{H}}(\gamma) = n}} \exp(i(2\theta_1(\gamma)m_1 + 2\theta_2(\gamma)m_2)).$$

Note that the relation (12) shows that we only need to bound the Kloosterman-type sum $S'_e(m_1, m_2, n)$ when m_1, m_2 are even. It also shows that in this case $S'_e(m_1, m_2, n)$ is independent of the choice of representatives for the double coset.

3.2. The Gaussian integers

It is a remarkable fact, observed in part in [12] and [5] that for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ the data $\{(v_{\mathbb{H}}(\gamma), \theta_1(\gamma), \theta_2(\gamma)) \mid \gamma \in \Gamma\}$ can be parametrized in terms of angles and lengths of Gaussian integers on two Euclidean circles with distance 4 apart.

Before we explain this observation in detail, we recall some results about Gaussian integers. For more information the reader may consult [23, 25].

The Gaussian integers $\mathbb{Z}[i]$ is the ring of integers of the imaginary quadratic field $\mathbb{Q}(i)$. The field is equipped with two important multiplicative maps; complex conjugation $z \mapsto \bar{z}$, and the norm map $N(z) = z\bar{z}$. It is a Euclidean domain with respect to this norm. The group of units satisfies

$$\mathbb{Z}[i]^\times = \{z \in \mathbb{Z}[i] \mid N(z) = 1\} = \{\pm 1, \pm i\}.$$

The ring of integers is a unique factorisation domain and the irreducible elements are, up to multiplication by a unit,

- (i) $(1 + i)$;
- (ii) $Q_p, \bar{Q}_p$, where $Q_p = x + iy$ with $x^2 + y^2 = p \equiv 1 \pmod{4}$;
- (iii) $p = 3 \pmod{4}$.

A Gaussian integer $\alpha \in \mathbb{Z}[i]$ is called *primary* if $\alpha \equiv 1 \pmod{(1 + i)^3}$. Note that with this definition the only primary unit is 1. For α not divisible by $(1 + i)$, there exists a unique unit u such that $u\alpha$ is primary. Every primary element can be written uniquely as a product of primary irreducible elements. A primary element z satisfies $N(z) \equiv 1 \pmod{4}$.

We fix a specific set of irreducible elements by fixing $(1 + i)$ and for the other irreducible elements we choose the primary irreducible. Note that Q is primary if and only if $\bar{Q}$ is primary. For any of these specific irreducible elements Q , we write

$$Q = |Q|e^{i\theta_Q}.$$

Note that, if $p \equiv 3 \pmod{4}$, then the corresponding primary irreducible is $Q = -p$, and $\theta_Q = \pi$. If, on the other hand, $p \equiv 1 \pmod{4}$ and $p = Q\bar{Q}$ is the factorisation into primary irreducibles, we disambiguate the choice of Q vs $\bar{Q}$ by assuming $\theta_Q > 0$. We denote $\theta_p = \theta_Q$.

The angles θ_Q of the primary irreducibles are asymptotically equidistributed modulo 2π . This can be seen by using Weyl's equidistribution criterion. To see why this applies, one considers the set of primitive Hecke Grössencharacters described in [25, Example 1, p. 62], the analytic properties of the corresponding Hecke L -function $L(s, \xi_k)$ (see [25, Theorem 3.8]), and a standard zero-free region for these functions. Note that for $Q = p \equiv 3 \pmod{4}$ we have $\theta_Q = \pi$, but since $N(Q) = p^2$ these do not affect the equidistribution.

3.3. Analysis on Weyl sums in $\mathbb{Z}[i]$

We now describe certain Weyl sums related the Gaussian integers. Consider

$$W_m(n) = \frac{1}{4} \sum_{\substack{z \in \mathbb{Z}[i] \\ N(z)=n}} \left(\frac{z}{|z|} \right)^m \quad \text{for } n \in \mathbb{N},$$

$$W_m^P(n) = W_m^P(2^l) W_m^P(n') \quad \text{if } n = 2^l n' \text{ with } n' \text{ odd,}$$

where

$$W_m^P(n) = \sum_{\substack{z \in \mathbb{Z}[i] \\ N(z)=n \\ z \text{ primary}}} \left(\frac{z}{|z|} \right)^m \quad \text{for } n \text{ odd,} \quad W_m^P(2^l) = \left(\frac{1+i}{\sqrt{2}} \right)^{lm} = e^{i(\pi/4)lm}.$$

Note that, for n odd,

$$W_m^P(n) = \sum_{\substack{z \in \mathbb{Z}[i]/\mathbb{Z}[i]^\times \\ N(z)=n}} \left(\frac{z}{|z|} \right)^m$$

for a specific choice of representatives of $\mathbb{Z}[i]/\mathbb{Z}[i]^\times$. It follows that

$$W_m(n) = \frac{1}{4} \sum_{u \in \mathbb{Z}[i]^\times} u^m W_m^P(n) = \begin{cases} W_m^P(n) & \text{if } m \equiv 0 \pmod{4}, \\ 0 & \text{otherwise.} \end{cases}$$

The functions $W_m(n)$ and $W_m^P(n)$ are multiplicative, i.e.,

$$W_m(n_1 n_2) = W_m(n_1) W_m(n_2),$$

$$W_m^P(n_1 n_2) = W_m^P(n_1) W_m^P(n_2),$$

if $(n_1, n_2) = 1$. The statement for W_m follows from unique factorisation into irreducible elements in $\mathbb{Z}[i]$ up to associates, and the statement for W_m^P follows from unique factorisation into primary irreducibles. Furthermore, we have the trivial bound

$$|W_m^P(n)| \leq W_0^P(n) = \frac{r(n)}{4} \leq d(n) = O_\varepsilon(n^\varepsilon) \quad \text{as } n \rightarrow \infty. \quad (13)$$

We also note that, if $p \equiv 3 \pmod{4}$, then

$$W_m^P(p^l) = \begin{cases} 0 & \text{if } l \text{ is odd,} \\ 1 & \text{if } l \text{ is even,} \end{cases} \quad (14)$$

and, if $p \equiv 1 \pmod{4}$, then

$$W_m^P(p^l) = \sum_{j=0}^l e^{i(2j-k)m\theta_p}.$$

In particular, we have for any odd rational prime

$$W_m^P(p) = \begin{cases} 2 \cos(m\theta_p) & \text{if } p \equiv 1 \pmod{4}, \\ 0 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

For $m = 0$, the result (1) of Gauss gives

$$\sum_{n \leq x} W_0^P(n) = \frac{\pi}{4}x + O(x^{1/2}).$$

Proposition 3.1. *Let m be an even non-zero integer. Then*

$$\sum_{n \leq x} |W_m^P(n)| = O\left(x \left(\frac{\log^2 |m|}{\log x}\right)^{1-2/\pi}\right).$$

Proof. When $m \equiv 0 \pmod{4}$ we have $W_m(n) = W_m^P(n)$, and in this case the claim is [10, Proposition 6].

To handle the general situation we note the following. For every even m , we have that, if $z_j \in \mathbb{Z}[i]$, $j = 1, 2$ are associated, and have angles determined by $z_j = |z|e^{i\theta(z_j)}$, then there exists an $r = 0, \dots, 3$ such that $\theta(z_1) = \theta(z_2) + r\pi/2 \pmod{2\pi}$. It follows that

$$|\cos(m\theta(z_1))| = |\cos(m\theta(z_2))|.$$

In particular, if $v_p = \arctan(y/x)$, where $p = x^2 + y^2 \equiv 1 \pmod{4}$ with $0 \leq y \leq x$, then we have

$$|\cos(m\theta_p)| = |\cos(mv_p)|.$$

With this observation (see also [5, p. 2367]), we can repeat the argument given by Erdős and Hall in [9, pp. 91–92] for every even non-zero m , and find

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{4}}} \frac{|\cos(m\theta_p)|}{p} \leq \frac{1}{\pi} \log \log x + \left(1 - \frac{2}{\pi}\right) \log \log m + O(1),$$

when $\log m \leq b\sqrt{\log x}$. Notice that our v_p is equivalent to $\theta(p)$ in [9]. Once this has been established, the proof in [10, Proposition 6] carries through verbatim and gives the result. ■

3.4. Parametrization of Γ in terms of Gaussian integers

We can now explain a parametrization of the elements of Γ in terms of Gaussian integers with various norms. The basic map (15) below is a variation of the one in [5, 12].

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, we define two Gaussian integers

$$\begin{aligned} z_1(\gamma) &= (a + d) + i(b - c) \in \mathbb{Z}[i], \\ z_2(\gamma) &= (a - d) - i(b + c) \in \mathbb{Z}[i]. \end{aligned} \quad (15)$$

It is straightforward to verify the following proposition, whose proof we leave as an exercise.

Proposition 3.2. *The following statements hold.*

- (1) *The map $\gamma \mapsto (z_1(\gamma), z_2(\gamma))$ is injective.*
- (2) *If $\nu_{\mathbb{H}}(\gamma) = n$, then $N(z_1(\gamma)) = n + 2$ and $N(z_2(\gamma)) = n - 2$.*
- (3) *If $\gamma' = \gamma_i^{j_1} \gamma \gamma_i^{j_2}$, then*

$$z_1(\gamma') = i^{j_1 + j_2} z_1(\gamma), \quad z_2(\gamma') = i^{j_1 - j_2} z_2(\gamma).$$

- (4) *We have*

$$f(\gamma i) = \frac{z_2(\gamma)}{\overline{z_1(\gamma)}}, \quad f(\gamma^{-1} i) = -\frac{z_2(\gamma)}{z_1(\gamma)}.$$

- (5) *We have*

$$\exp(2i\theta_1(\gamma)) = \frac{z_1(\gamma)}{|z_1(\gamma)|} \frac{z_2(\gamma)}{|z_2(\gamma)|}, \quad \exp(2i\theta_2(\gamma)) = \frac{z_1(\gamma)}{|z_1(\gamma)|} \frac{|z_2(\gamma)|}{z_2(\gamma)}.$$

We note that Proposition 3.2 (5) can be formulated as follows: the angles $2\theta_1(\gamma)$, $2\theta_2(\gamma)$ can be identified as the sum and difference of the arguments of $z_1(\gamma)$, $z_2(\gamma)$, i.e.,

$$\begin{aligned} 2\theta_1(\gamma) &= \arg(z_1(\gamma)) + \arg(z_2(\gamma)) \bmod 2\pi, \\ 2\theta_2(\gamma) &= \arg(z_1(\gamma)) - \arg(z_2(\gamma)) \bmod 2\pi. \end{aligned}$$

Proposition 3.2 (1), (2) raises the question of determining the precise image of the map $\gamma \mapsto (z_1(\gamma), z_2(\gamma))$ when restricted to the finite set consisting of $\gamma \in \Gamma$ with $\nu_{\mathbb{H}}(\gamma) = n$. Since an invertible 2×2 matrix must have at least two non-zero entries consider $n \geq 2$. We consider this question separately for the four different values of $n \bmod 4$.

Let $S_2 = \{n \in \mathbb{Z} \mid r(n) > 0\}$ be the set of integers expressible as a sum of two squares. Recall that S_2 consists precisely of integers n satisfying that any prime $p = 3 \bmod 4$ occurs an even number of times in the factorisation of n into rational primes, so an odd number cannot be in S_2 unless it is $1 \bmod 4$.

Lemma 3.3. *If $n = 0 \bmod 4$ or $n = 1 \bmod 4$, then*

$$\{\gamma \in \Gamma \mid \nu_{\mathbb{H}}(\gamma) = n\} = \emptyset.$$

Proof. *Case:* $n = 0 \pmod{4}$. Proposition 3.2 (2) implies that if $\{\gamma \in \Gamma \mid v_{\mathbb{H}}(\gamma) = n\} \neq \emptyset$, then $n \pm 2 \in S_2$. We have $n = 4m$, so $n \pm 2 = 2(2m \pm 1)$. Clearly, one of $2m \pm 1$ is equal to 3 mod 4, so one of them is not in S_2 . This implies that the prime factorisation of that number contains a prime $p = 3 \pmod{4}$ occurring an odd number of times. But then the same is true for the corresponding $n \pm 2 = 2(2m \pm 1)$, so one of $n \pm 2$ is not in S_2 . This implies that, in this case,

$$\{\gamma \in \Gamma \mid v_{\mathbb{H}}(\gamma) = n\} = \emptyset.$$

Case: $n = 1 \pmod{4}$. Again, Proposition 3.2 (2) implies that if $\{\gamma \in \Gamma \mid v_{\mathbb{H}}(\gamma) = n\} \neq \emptyset$, then $n \pm 2 \in S_2$. When $n = 1 \pmod{4}$, we have that $n + 2 \notin S_2$, so also in this case $\{\gamma \in \Gamma \mid v_{\mathbb{H}}(\gamma) = n\} = \emptyset$. ■

Let $B_n = \{z_1 \in \mathbb{Z}[i] \mid N(z_1) = n + 2\} \times \{z_2 \in \mathbb{Z}[i] \mid N(z_2) = n - 2\}$.

Lemma 3.4. *Let $n \geq 2$ with $n = 2 \pmod{4}$. Then the map*

$$\begin{aligned} \{\gamma \in \Gamma \mid v_{\mathbb{H}}(\gamma) = n\} &\rightarrow B_n, \\ \gamma &\mapsto (z_1(\gamma), z_2(\gamma)) \end{aligned}$$

is an isomorphism.

Proof. We can define an inverse map from B_n . Proposition 3.2 gives that the assignment $\gamma \mapsto (z_1(\gamma), z_2(\gamma))$ maps $\{\gamma \in \Gamma \mid v_{\mathbb{H}}(\gamma) = n\}$ into B_n , so we have an injective map into B_n .

To see that it is surjective we note that if $(z_1, z_2) \in B_n$ with $z_j = x_j + iy_j$, then

$$\begin{aligned} N(z_1) &= n + 2 = 0 \pmod{4}, \\ N(z_2) &= n - 2 = 0 \pmod{4}. \end{aligned}$$

But this is only possible if all of x_1, x_2, y_1, y_2 are even. To see this, write

$$x_1 = \delta_x + 2m_x, \quad y_1 = \delta_y + 2m_y,$$

with m_x, m_y integers and $\delta_x, \delta_y \in \{0, 1\}$. Then

$$\begin{aligned} x_1^2 + y_1^2 &= \delta_x^2 + 4\delta_x m_x + 4m_x^2 + \delta_y^2 + 4\delta_y m_y + 4m_y^2 \\ &= \delta_x^2 + \delta_y^2 \pmod{4}, \end{aligned}$$

which implies $\delta_x = \delta_y = 0$, since $N(z_1) = 0 \pmod{4}$.

We now define a map $B_n \rightarrow \{\gamma \in \Gamma \mid v_{\mathbb{H}}(\gamma) = n\}$ as follows: Let

$$a = \frac{x_1 + x_2}{2}, \quad b = \frac{y_1 - y_2}{2}, \quad c = \frac{-y_1 - y_2}{2}, \quad d = \frac{x_1 - x_2}{2}. \quad (16)$$

Since all the coordinates of z_1, z_2 are even, a, b, c, d are all integers, and we easily find $ad - bc = 1$ and $a^2 + b^2 + c^2 + d^2 = n$. Setting

$$\gamma(z_1, z_2) := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,$$

we verify that $z_i(\gamma(z_1, z_2)) = z_i$, i.e., we have constructed an inverse to the map $\gamma \mapsto (z_1(\gamma), z_2(\gamma))$.

Finally, we note that both sides of the map might be empty, e.g., if $n = 10$, since $12 \notin S_2$. ■

Recall that we have defined

$$\begin{aligned} C_n &= \{z_1 \in \mathbb{Z}[i] \mid N(z_1) = n + 2, z_1 \text{ primary}\} \\ &\quad \times \{z_2 \in \mathbb{Z}[i] \mid N(z_2) = n - 2, z_2 \text{ primary}\}. \end{aligned}$$

Lemma 3.5. *Let $n \geq 2$ with $n \equiv 3 \pmod{4}$. Then there exist unique representatives for the double cosets in $\Gamma_i \backslash \Gamma / \Gamma_i$ with $v_{\mathbb{H}}(\gamma) = n$ such that*

$$\begin{aligned} \{\gamma \in \Gamma_i \backslash \Gamma / \Gamma_i \mid v_{\mathbb{H}}(\gamma) = n\} &\rightarrow C_n, \\ \gamma &\mapsto (z_1(\gamma), z_2(\gamma)) \end{aligned}$$

is an isomorphism.

Proof. If a Gaussian integer is primary then its imaginary part is even and its real part is odd [23, p. 121]. With these parity conditions the numbers a, b, c, d defined by (16) are again all integers, and we have

$$ad - bc = 1 \quad \text{and} \quad a^2 + b^2 + c^2 + d^2 = n.$$

Setting $\gamma(z_1, z_2) := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, we again easily verify that $z_i(\gamma(z_1, z_2)) = z_i$. However, the map from $\{\gamma \in \Gamma \mid v_{\mathbb{H}}(\gamma) = n\}$ does not always land in C_n so we need to restrict our mapping a bit.

We claim that any double cosets in $\Gamma_i \backslash \Gamma / \Gamma_i$ has a unique representative γ such that $(z_1(\gamma), z_2(\gamma)) \in C_n$. To see this, we first take any representative γ'' for a given double coset. Then $N(z_2(\gamma'')) = 1 \pmod{4}$ so $z_2(\gamma'')$ is not divisible by $(1 + i)$. It follows that there exists a unique $k \pmod{4}$ such that $i^k z_2(\gamma'')$ is primary. Let $\gamma' = \gamma_i^k \gamma''$. Then by Proposition 3.2 (3), we have that $z_2(\gamma') = i^k z_2(\gamma'')$, so

$$z_2(\gamma') \in \{z_2 \in \mathbb{Z}[i] \mid N(z_2) = n - 2, z_2 \text{ primary}\}.$$

We now claim that $z_1(\gamma') = \pm 1 \pmod{(1 + i)^3}$.

To see this, we first note that any $w \in \mathbb{Z}[i]$ is congruent to 0 or 1 $\pmod{(1 + i)}$. This follows from observing that Euclidean division in $\mathbb{Z}[i]$ gives that $w = q(1 + i) + r$

for some $q \in \mathbb{Z}[i]$, where r is either zero or a unit. Noting that all units are equivalent modulo $(1+i)$ shows that $w = 0, 1 \bmod (1+i)$.

To prove that $z_1(\gamma') = \pm 1 \bmod (1+i)^3$ we note that, by construction, we have

$$z_2(\gamma') = 1 \bmod (1+i)^3,$$

and from the general definition (15), we see that

$$z_1(\gamma') = z_2(\gamma') + 2w,$$

where $w \in \mathbb{Z}[i]$. Since $2w$ equals 0 or 2 $\bmod (1+i)^3$, as follows from the above observation that any $w \in \mathbb{Z}[i]$ is 0, 1 $\bmod (1+i)$, it follows that

$$z_1(\gamma) = \pm 1 \bmod (1+i)^3.$$

If $z_1(\gamma') = 1 \bmod (1+i)^3$, then the only other representative in the same double coset that map to the same point is $\gamma = \gamma_i^2 \gamma' \gamma_i^2$; see again Proposition 3.2 (3). Since $\gamma_i^2 = -I$ this is really the same representative, i.e., $\gamma = \gamma_i^2 \gamma' \gamma_i^2 = \gamma'$.

If $z_1(\gamma') = -1 \bmod (1+i)^3$, then the only representatives in the same double coset that maps to C_n is $\gamma = \gamma_i^1 \gamma' \gamma_i^1$ or $\gamma = \gamma_i^3 \gamma' \gamma_i^3$. But since $\gamma_i^2 = -I$ this is again really the same representative. This finishes the proof.

Note that also in this case we may have $\{\gamma \in \Gamma \mid v_{\mathbb{H}}(\gamma) = n\} = \emptyset$, e.g., when $n = 19$, since $21 \notin S_2$. ■

We can now use the bijections of the above lemmata to connect the hyperbolic Kloosterman sum with products of Weyl sums related to Gaussian integers with norms with distance 4 apart.

Lemma 3.6. *If m_1 or m_2 is odd, then $S_e(m_1, m_2, n) = 0$. If not, then*

$$S_e(m_1, m_2, n) = \begin{cases} 16W_{m_1+m_2}(n+2)W_{m_1-m_2}(n-2) & \text{if } n = 2 \bmod 4, \\ 8W_{m_1+m_2}^P(n+2)W_{m_1-m_2}^P(n-2) & \text{if } n = 3 \bmod 4, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. For $n = 0, 1 \bmod 4$, this follows from Lemma 3.3. For $n = 2 \bmod 4$, it follows from Lemma 3.4 and Proposition 3.2 (5). For $n = 3 \bmod 4$, it follows from (12), Lemma 3.5, and Proposition 3.2 (5). ■

3.5. Counting group elements along primes in the elliptic case

Friedlander and Iwaniec considered

$$\pi_{\Gamma}(x) = \#\{\gamma \in \Gamma \mid v_{\mathbb{H}}(\gamma) = p \leq x\}.$$

We note that $\pi_\Gamma(x) = \pi_E(x)$. In order to give good estimates on $\pi_E(x)$, they introduced for $0 < \theta \leq 1$ an assumption $A(\theta)$ as follows. Let $\Lambda(n)$ denote the von Mangoldt function and

$$\psi(x, a, q) = \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n),$$

which by the prime number theorem for primes in arithmetic progression is asymptotic to $x/\varphi(q)$. Consider the level Q remainder

$$E(x, Q) = \sum_{q \leq Q} \max_{(a, q)=1} \max_{y \leq x} \left| \psi(y, a, q) - \frac{y}{\varphi(q)} \right|.$$

Then $A(\theta)$ is the assumption that, for any $A, \varepsilon > 0$,

$$E(x, Q) = O_{\varepsilon, A}(x(\log x)^{-A}) \quad \text{when } Q = x^{\theta - \varepsilon}.$$

We note that $A(1/2)$ is the Bombieri–Vinogradov theorem, and $A(1)$ is the Elliott–Halberstam conjecture.

Friedlander and Iwaniec proved that there exists a $\theta_0 < 1$ such that, if $A(\theta_0)$ is true, then

$$\pi_E(x) \asymp \frac{x}{\log x}. \quad (17)$$

They furthermore conjectured that $\pi_E(x) \sim c(x/\log x)$ for some constant $c > 0$.

3.6. Equidistribution over primes in the elliptic case

To prove equidistribution over primes in this case we use the following result.

Theorem 3.7. *If $m = (m_1, m_2) \in \mathbb{Z}^2 \setminus \{0\}$ and l is a non-negative even integer, then*

$$\sum_{\substack{\gamma \in \Gamma \\ v_{\mathbb{H}}(\gamma) + l = p \leq x}} \exp(i(2\theta_1(\gamma)m_1 + 2\theta_2(\gamma)m_2)) = O_m\left(\frac{x}{\log x} \frac{1}{\log^{1-2/\pi} x}\right).$$

Proof. Let

$$A(m_1, m_2, x) = \sum_{\substack{\gamma \in \Gamma \\ v_{\mathbb{H}}(\gamma) + l = p \leq x}} \exp(i(2\theta_1(\gamma)m_1 + 2\theta_2(\gamma)m_2)).$$

Then, by (10), we have

$$A(m_1, m_2, x) = \sum_{p \leq x} S_e(m_1, m_2, p - l).$$

By using (12), we may assume that m_1, m_2 are both even. We then use Lemma 3.6 to deduce that

$$|A(m_1, m_2, x)| \leq 4 + 8 \sum_{\substack{p \leq x \\ p+l \equiv 3 \pmod{4}}} |W_{m_1+m_2}^P(p-l+2)| |W_{m_1-m_2}^P(p-l-2)|.$$

Note that, since $W_m^P(n) = 0$ for $n \equiv 3 \pmod{4}$, as follows from multiplicativity and (14), we may as well sum over all odd primes $p \leq x$.

Applying Theorem 2.1 with the non-negative multiplicative functions, we have

$$g_1(n) = |W_{m_1+m_2}^P(n)|, \quad g_2(n) = |W_{m_1-m_2}^P(n)|,$$

and $(a_1, b_1) = (1, -l+2)$, $(a_2, b_2) = (1, -l-2)$, we arrive at

$$|A(m_1, m_2, x)| \ll_l \frac{x}{(\log x)^3} \sum_{n \leq x} \frac{|W_{m_1+m_2}^P(n)|}{n} \sum_{n \leq x} \frac{|W_{m_1-m_2}^P(n)|}{n}.$$

From the bound $W_0^P(n) \leq r(n)/4$ (see formula (13)), we can bound the two sums by $O(\log(x))$. Since m_1, m_2 are not both zero, at least one of $m_1 + m_2, m_1 - m_2$ is non-zero. Call this non-zero integer m' . It is even, since both of m_1, m_2 are even. It now follows from Proposition 3.1 that

$$\sum_{n \leq x} \frac{|W_{m'}^P(n)|}{n} = O_{m'}((\log x)^{2/\pi}),$$

which gives the result. ■

Since $1 - 2/\pi > 0$, we can now conclude Theorems 1.3 and 1.4 by specializing to $l = 0$ and $l = 2$, using Weyl's equidistribution criterion in combination with (3) and (6).

It follows from Theorem 3.7 that, if m_1, m_2 are not both zero, then, conditional on the lower bound in (17), we have

$$\frac{1}{\pi_E(x)} \sum_{\nu_{\mathbb{H}}(\gamma) = p \leq x} \exp(i(2\theta_1(\gamma)m_1 + 2\theta_2(\gamma)m_2)) = O_m((\log x)^{2/\pi-1}),$$

which, via Weyl's equidistribution theorem, gives Theorem 1.3.

Remark 4. Note that we do not really need the full force of the lower bound in (17); we only need

$$\frac{1}{\pi_E(x)} = o(x^{-1}(\log x)^{2(1-\pi^{-1})})$$

to conclude equidistribution.

4. The hyperbolic case

We now shift our attention to a different subgroup of $G = \mathrm{SL}_2(\mathbb{R})$; we consider the quaternion group

$$\Gamma(2, 5) = \left\{ \begin{pmatrix} x_0 + x_1\sqrt{2} & \sqrt{5}(x_2 + x_3\sqrt{2}) \\ \sqrt{5}(x_2 - x_3\sqrt{2}) & x_0 - x_1\sqrt{2} \end{pmatrix} \in G \mid x_i \in \mathbb{Z} \right\}. \quad (18)$$

This is an embedding in G of the standard order $\mathcal{O} = \mathbb{Z}[1, i, j, k]$ in

$$\left(\frac{2, 5}{\mathbb{Q}} \right) = \{q_0 + q_1i + q_2j + q_3k \mid q_i \in \mathbb{Q}\},$$

where $i^2 = 2$, $j^2 = 5$, $ij = -ji = k$.

It is well known that $\Gamma(2, 5)$ is a discrete strictly hyperbolic co-compact subgroup of G ; see [18, pp. 302–303]. It has genus 3 and co-volume 8π . It contains the primitive hyperbolic subgroup

$$H = \langle h_0 \rangle \text{ generated by } h_0 = \begin{pmatrix} \varepsilon^2 & \\ & \varepsilon^{-2} \end{pmatrix},$$

where $\varepsilon = 1 + \sqrt{2}$ is the fundamental unit for the ring of integers of the number field $\mathbb{Q}(\sqrt{2})$.

4.1. Hyperbolic decomposition in $\mathrm{SL}_2(\mathbb{R})$ and Good's equidistribution

In this section, we make a simplified exposition of the decomposition given in [14, Lemma 1] leading up to Good's theorem in the case of both subgroups being hyperbolic.

Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G = \mathrm{SL}_2(\mathbb{R})$ and consider

$$\begin{aligned} s &= \{g \in G \mid gz_1 = z_2 \text{ for some } z_1, z_2 \in \{0, i\infty\}\}, \\ S &= s \cup \{g \in G \mid g(iy_1) = iy_2 \text{ for some } y_1, y_2 \in \mathbb{R}_+\}. \end{aligned}$$

It is straightforward to check that $s = \{g \in G \mid abcd = 0\}$.

Lemma 4.1. *Let $g \in G \setminus s$. Then there exist unique $y_1, y_2 > 0$ such that*

$$g = \begin{pmatrix} y_1^{1/2} & \\ & y_1^{-1/2} \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} y_2^{1/2} & \\ & y_2^{-1/2} \end{pmatrix}$$

with the middle matrix satisfying $|\alpha| = |\delta|$, $|\beta| = |\gamma|$.

Proof. Since $abcd \neq 0$, the matrix

$$\begin{pmatrix} y_1^{-1/2} & \\ & y_1^{1/2} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} y_2^{-1/2} & \\ & y_2^{1/2} \end{pmatrix} = \begin{pmatrix} (y_1 y_2)^{-1/2} a & (y_2 / y_1)^{1/2} b \\ (y_1 / y_2)^{1/2} c & (y_2 y_1)^{1/2} d \end{pmatrix}$$

has the desired form if and only if $y_1 y_2 = |a/d|$ and $y_1 / y_2 = |b/c|$. This has a unique strictly positive solution given by

$$y_1 = \left| \frac{ab}{cd} \right|^{1/2}, \quad y_2 = \left| \frac{ac}{bd} \right|^{1/2}.$$

■

Recall the matrix $\omega = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Lemma 4.2. *Let $g \in G \setminus s$ and assume that $|a| = |d|$, $|b| = |c|$. Then either $g \in K$ or there exist uniquely determined numbers $\delta_1, \delta_2 \in \{0, 1\}$, $v > 0$, and a sign $\pm$ such that*

$$g = \pm \omega^{\delta_1} \begin{pmatrix} \cosh v & \sinh v \\ \sinh v & \cosh v \end{pmatrix} \omega^{\delta_2}.$$

Moreover, the matrix $g \in K$ if and only if $g \in S \setminus s$, which happens if and only if $abcd < 0$.

Proof. By the given assumptions, we are in exactly one of the following four cases:

- (1) $a = d$ and $b = -c$, such that $c^2 + d^2 = 1$;
- (2) $a = d$ and $b = c$, such that $d^2 - c^2 = 1$;
- (3) $a = -d$ and $b = -c$, such that $-d^2 + c^2 = 1$;
- (4) $a = -d$ and $b = c$, such that $-d^2 - c^2 = 1$.

In case (1), $g \in K$.

In cases (2) and (3), we compute $\omega^{-\delta_1} g \omega^{-\delta_2}$ for all four values of δ_1, δ_2 . In case (2), these are

$$\begin{aligned} g &= \begin{pmatrix} d & c \\ c & d \end{pmatrix}, & \omega^{-1} g &= \begin{pmatrix} c & d \\ -d & -c \end{pmatrix}, \\ g \omega^{-1} &= \begin{pmatrix} -c & d \\ -d & c \end{pmatrix}, & \omega^{-1} g \omega^{-1} &= \begin{pmatrix} -d & c \\ c & -d \end{pmatrix}. \end{aligned}$$

Precisely one choice of δ_1, δ_2 has all entries to be of the same sign, namely $(\delta_1, \delta_2) = (0, 0)$ if c and d already have the same sign, and $(\delta_1, \delta_2) = (1, 1)$ if they have opposite sign. With this choice, we have

$$g = \pm \omega^{\delta_1} \begin{pmatrix} |d| & |c| \\ |c| & |d| \end{pmatrix} \omega^{\delta_2}$$

for a unique choice of $\pm$. Since $d^2 - c^2 = 1$, we have that $|d| > 1$, and we have the claimed decomposition with $v = \log(|d| + |c|) > 0$.

Similarly in case (3),

$$\begin{aligned} g &= \begin{pmatrix} -d & -c \\ c & d \end{pmatrix}, & \omega^{-1}g &= \begin{pmatrix} c & d \\ d & c \end{pmatrix}, \\ g\omega^{-1} &= \begin{pmatrix} c & -d \\ -d & c \end{pmatrix}, & \omega^{-1}g\omega^{-1} &= \begin{pmatrix} -d & c \\ -c & d \end{pmatrix}. \end{aligned}$$

Again, precisely one choice of δ_1, δ_2 has all entries to be of the same sign, namely $(\delta_1, \delta_2) = (1, 0)$ if c and d already have the same sign, and $(\delta_1, \delta_2) = (0, 1)$ if they have opposite signs. With this choice, we have

$$g = \pm \omega^{\delta_1} \begin{pmatrix} |c| & |d| \\ |d| & |c| \end{pmatrix} \omega^{\delta_2}.$$

Since $c^2 - d^2 = 1$, we have that $|c| > 1$ getting the claimed decomposition again with $v = \log(|d| + |c|) > 0$.

Case (4) does not happen since $-c^2 - d^2 = 1$ does not have any real solutions.

To see the final claim, note that if $g \in K$, then $gi = i$, so $g \in S \backslash s$. If, on the other hand, $g \in S \backslash s$, then there exist $y_1, y_2 > 0$ such that $g(iy_1) = iy_2$, which implies

$$aiy_1 + b = -cy_1y_2 + diy_2.$$

It follows that

$$ay_1 - dy_2 = 0 = -b - cy_1y_2,$$

which is only possible if a, d has the same sign, and b, c has opposite signs. Hence, we are in case (1) and $g \in K$. Finally, we finish the proof by noting that $abcd < 0$ precisely in case (1). ■

Noticing that s and $S \backslash s$ are closed under multiplication from the left and the right by multiplication by $\begin{pmatrix} y_1^{1/2} & \\ & y_1^{-1/2} \end{pmatrix}$, we may use the previous lemmata and the formulas in their proofs to conclude the following lemma.

Lemma 4.3. *For $g \in G \backslash s$, we have $g \in S$ if and only if $|ad| + |bc| = 1$. If $g \notin S$, then there exist uniquely determined numbers $y_1, y_2 > 0$, $\delta_1, \delta_2 \in \{0, 1\}$, $v > 0$, and sign $\pm$ such that*

$$g = \pm \begin{pmatrix} y_1^{1/2} & \\ & y_1^{-1/2} \end{pmatrix} \omega^{\delta_1} \begin{pmatrix} \cosh v & \sinh v \\ \sinh v & \cosh v \end{pmatrix} \omega^{\delta_2} \begin{pmatrix} y_2^{1/2} & \\ & y_2^{-1/2} \end{pmatrix}.$$

Concretely,

$$y_1 = \left| \frac{ab}{cd} \right|^{1/2}, \quad y_2 = \left| \frac{ac}{bd} \right|^{1/2},$$

$$v = \log(|ad|^{1/2} + |cb|^{1/2}),$$

$$(\delta_1, \delta_2) = \begin{cases} (0, 0) & \text{if } \text{sign}(a, b, c, d) = \pm(+, +, +, +), \\ (1, 1) & \text{if } \text{sign}(a, b, c, d) = \pm(+, -, -, +), \\ (1, 0) & \text{if } \text{sign}(a, b, c, d) = \pm(+, +, -, -), \\ (0, 1) & \text{if } \text{sign}(a, b, c, d) = \pm(+, -, +, -). \end{cases}$$

Proof. To see the condition for g to be in S , we apply Lemma 4.1 to g . Let

$$g' = \begin{pmatrix} y_1^{-1/2} & \\ & y_1^{1/2} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} y_2^{-1/2} & \\ & y_2^{1/2} \end{pmatrix}$$

$$= \begin{pmatrix} a|d|^{1/2}/|a|^{1/2} & b|c|^{1/2}/|b|^{1/2} \\ c|b|^{1/2}/|c|^{1/2} & d|a|^{1/2}/|d|^{1/2} \end{pmatrix}.$$

Then $g \in S$ if and only if $g' \in S \setminus s$. Since g' satisfies the assumptions of Lemma 4.2, $g' \in S \setminus s$ if and only if $g' \in K$. This is equivalent to a, d having the same sign and b, c having opposite signs. But then the determinant condition gives

$$|ad| + |bc| = ad - bc = 1.$$

In the opposite direction, if we assume that $|ad| + |bc| = 1$, then combining this with the determinant condition, we find that

$$|ad| - ad = -(bd + |bd|).$$

But since the left-hand side is non-negative and the right-hand side is non-positive, both sides are zero. This implies that a, d have the same sign, and b, d have opposite signs. Hence, $g' \in K$ and we conclude that $g \in S$. Alternatively, we may use Lemma 4.2 to conclude that $g \in S$ if and only if ad and cd has opposite signs, which by the determinant condition happens precisely if $ad > 0$, so that

$$1 = ad - bc = |ad| + |bc|.$$

To see the decomposition of $g \notin S$, we apply Lemma 4.2 to g' . ■

For the decomposition of a matrix $g \in G$, we will often write the parameters $v = v(g)$, $y_i = y_i(g)$, and $\delta_i = \delta_i(g)$.

Martin, McKee, and Wambach [31] introduced a different parameter

$$\delta(g) = 2|ad + bc|.$$

The parameter $\delta(g)$ should not be confused with the integers $\delta_i(g) \in \{0, 1\}$. We now describe how $\delta(g)$ relates to $v(g)$ when $g \in G \setminus S$. Since $\gamma \notin S$, we have $abcd > 0$, so ad and bc have the same sign. We deduce that

$$\begin{aligned} 1 < e^{2v(g)} &= (|ad|^{1/2} + |bc|^{1/2})^2 \\ &= |ad| + |bc| + \sqrt{4abcd} \\ &= |ad + bc| + \sqrt{|ad + bc|^2 - 1} \\ &= \frac{\delta(g)}{2} + \sqrt{\left(\frac{\delta(g)}{2}\right)^2 - 1} = e^{\operatorname{arccosh} \delta(g)/2}, \end{aligned}$$

so that

$$v(g) = \frac{1}{2} \operatorname{arccosh}\left(\frac{\delta(g)}{2}\right). \quad (19)$$

We use this to give the following geometric interpretation of the parameter $v(g)$ as the closest hyperbolic distance between the vertical geodesic from 0 to $i\infty$ and its image under g .

Proposition 4.4. *Let $g \in G \setminus S$. Then*

$$v(g) = \frac{1}{2} d_{\mathbb{H}}(gi\mathbb{R}_+, i\mathbb{R}_+) > 0.$$

Proof. This follows from [31, Lemma 1] and the above identification. ■

Martin, McKee, and Wambach [31, Proof of Lemma 1] found that if $g \in G \setminus S$ is decomposed as in Lemma 4.3, then the distance $d_{\mathbb{H}}(gi\mathbb{R}_+, i\mathbb{R}_+)$ is attained between iy_1 on the vertical geodesic and giy_2^{-1} on the second, i.e.,

$$d_{\mathbb{H}}(i\mathbb{R}_+, \gamma(i\mathbb{R}_+)) = d_{\mathbb{H}}(iy_1, giy_2^{-1}).$$

We can now describe Good's theorem. Let Γ be a discrete co-finite subgroup of $\operatorname{SL}_2(\mathbb{R})$, and let $\gamma_1, \gamma_2 \in \Gamma$ be primitive hyperbolic elements. Fix scaling elements $\sigma_1, \sigma_2 \in G$ satisfying

$$\gamma_l = \sigma_l^{-1} \begin{pmatrix} m_l & \\ & m_l^{-1} \end{pmatrix} \sigma_l$$

with $1 < |m_l| < \infty$, and write $\Gamma_{m_l} = \sigma_l \langle \gamma_l \rangle \sigma_l^{-1}$. Let

$$0 = \lambda_0 < \lambda_1 \leq \dots \leq \lambda_N < \frac{1}{4}$$

be the eigenvalues of the automorphic Laplacian on $\Gamma \setminus \mathbb{H}$ below $1/4$, and write $\lambda_j = s_j(1 - s_j)$ with $s_j > 1/2$. We now quote Good [14, Theorem 4, p. 116] in this special case.

Theorem 4.5. *Let $\delta_1, \delta_2 \in \{0, 1\}$, and $n = (n_1, n_2) \in \mathbb{Z}^2$. There exist explicit complex constants $c_1, \dots, c_N$ such that*

$$\begin{aligned} & \sum_{\substack{\delta_l(\gamma)=\delta_l \\ e^{v(\gamma)} \leq X^{1/2}}} e\left(n_1 \frac{\log y_1(\gamma)}{\log m_1^2} + n_2 \frac{\log y_2(\gamma)}{\log m_2^2}\right) \\ &= \delta_{n,0} \frac{\log m_1^2 \log m_2^2}{4\pi \operatorname{vol}(\Gamma \backslash \mathbb{H})} X + \sum_{j=1}^N c_j X^{s_j} + O_n(X^{2/3}). \end{aligned}$$

Here the sum is over double cosets of $\Gamma_{m_1} \backslash (\sigma_1 \Gamma \sigma_2^{-1} \cap S^c) / \Gamma_{m_2}$.

By Weyl's equidistribution theorem, it follows that

$$\left(\frac{\log y_1(\gamma)}{\log m_1^2}, \frac{\log y_2(\gamma)}{\log m_2^2} \right)$$

is equidistributed on $(\mathbb{R}/\mathbb{Z})^2$.

4.2. The ring of integers of $\mathbb{Q}(\sqrt{2})$

The arithmetic properties of $\Gamma(2, 5)$ are to a large extent controlled by the real quadratic field $K = \mathbb{Q}(\sqrt{2})$, and its ring of integers $\mathcal{O}_K$.

The ring is a principal ideal domain, has regulator $\log(\varepsilon)$, discriminant 8, class number one, and has ± 1 as its only roots of unity. Moreover, any unit $u \in \mathcal{O}_K$ is of the form $u = \pm \varepsilon^n$ for some $n \in \mathbb{Z}$. The ring of integers $\mathcal{O}_K$ comes equipped with an element norm

$$N(z) = z \cdot \sigma z \in \mathbb{Z},$$

where $\sigma(x + \sqrt{2}y) = x - \sqrt{2}y$, and an ideal norm $N(\mathfrak{z}) = |N(z)|$. The Galois group is generated by the involution σ .

Recall that $\mathcal{O}_K$ is Euclidean and, therefore, a unique factorisation domain; its irreducible elements are:

- (i) $\sqrt{2}$;
- (ii) $\rho = a + \sqrt{2}b$ with $N(\rho) = p = \pm 1 \pmod{8}$;
- (iii) $p = \pm 3 \pmod{8}$;

and their associates.

The Dedekind zeta function of K factors as

$$\zeta_K(s) = \zeta(s)L(s, \chi_8),$$

where $\chi_8(n) = (8/n)$ is the Kronecker symbol. The character $\chi_8(n)$ is the unique primitive even Dirichlet character modulo 8. By the class number formula

$$L(1, \chi_8) = \frac{\log \varepsilon}{\sqrt{2}}. \quad (20)$$

Proposition 4.6. *Every ideal $I \subset \mathcal{O}_K$ has a totally positive generator, i.e.,*

$$I = (z) \quad \text{for some } z \in \mathcal{O}_K \text{ with } z, \sigma(z) > 0.$$

Given two such generators z_1, z_2 , there exists $m \in \mathbb{Z}$ such that $z_1 = \varepsilon^{2m} z_2$.

Proof. Since $\mathcal{O}_K$ is a principal ideal domain, the ideal I has a generator w . For any unit u , the element uw is another generator, and if $w, \sigma(w)$ has different signs, then $\varepsilon w, \sigma(\varepsilon w)$ has the same sign since $\sigma(\varepsilon)$ is negative. So, without loss of generality, we may assume that $w, \sigma(w)$ has the same sign. If this sign is positive we are done, and if not $-w$ has the desired property.

If two z_1, z_2 are totally positive generators for I , then $z_1 = uz_2$ for some unit $u = \pm \varepsilon^n$. Since z_1 and z_2 are totally positive, this is only possible if $u = \varepsilon^{2m}$. ■

Consider now the set of classes of totally positive elements of $\mathcal{O}_K$ with norm n modulo the equivalence relation $z_1 \sim z_2$ if and only if $z_1 = \varepsilon^{2m} z_2$ for some $m \in \mathbb{Z}$:

$$D_K(n) = \{z \in \mathcal{O}_K \mid N(z) = n, z > 0, \sigma(z) > 0\} / \sim.$$

For $n > 0$, this is in bijection with the set of ideals of $\mathcal{O}_K$ with norm n via the map $z \mapsto (z)$, as follows from Proposition 4.6. In particular,

$$\mathcal{N}_2(n) := \#D_K(n) = \#\{I \subseteq \mathcal{O}_K \mid N(I) = n\} = \sum_{d|n} \chi_8(d). \quad (21)$$

The last equality follows from the divisibility theory of K ; see [29, Satz 882].

4.3. Analysis of Weyl sums in $\mathcal{O}_K$

Consider, for k even,

$$U_k(n) = \sum_{z \in D_K(n)} \lambda(z)^k,$$

where

$$\lambda(z) = \left| \frac{z}{\sigma z} \right|^{\pi i / (4 \log(\varepsilon))} \quad (22)$$

is the square root of the basic Grössencharacter in $\mathcal{O}_K$; see [17, Section 10]. It is straightforward to verify that this is well defined, and that for $n > 0$,

$$|U_k(n)| \leq U_0(n) = \#\{I \subseteq \mathcal{O}_K \mid N(I) = n\} = \sum_{d|n} \chi_8(d),$$

as follows from (21). In particular, $|U_k(p^l)| \leq l + 1$ and $\sum_{n \leq x} |U_k(n)| = O(x)$. If $n_1, n_2 \in \mathbb{N}$ are coprime, then the map

$$\begin{aligned} D_K(n_1) \times D_K(n_2) &\rightarrow D_K(n_1 n_2), \\ (z_1, z_2) &\mapsto z_1 z_2 \end{aligned}$$

is an isomorphism. This implies that $U_k(n)$ is multiplicative as a function of n . Using the factorisation into irreducible elements, we see that

$$U_k(p) = \begin{cases} 1 & \text{if } p = 2, \\ 2 \cos\left(\frac{\pi k}{4 \log \varepsilon} \log |\rho_p / \sigma(\rho_p)|\right) & \text{if } p \equiv \pm 1 \pmod{8}, \\ 0 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Here the element ρ_p is any of the two totally positive elements modulo $\sim$ satisfying $N(\rho_p) = p \equiv \pm 1 \pmod{8}$, i.e., ρ_p is any of the two elements of $D_K(p)$. The Galois element σ permutes these elements. Since cosine is an even function, the expression above is independent of the element we choose.

In anticipation of using Theorem 2.2, we find the average size of $|U_k(p)|$. This can be done using an effective version of Hecke's equidistribution theorem [17, Section 7]. The following is an adaptation of a classical result due to Rademacher. Rademacher proved it using good zero-free regions for Hecke L -series; a more precise error term was found by Urbjalis [42].

Theorem 4.7 (Rademacher [36]). *There exists a constant $b > 0$ such that for an interval $I \subseteq \mathbb{R}/\mathbb{Z}$, we have*

$$\#\left\{\rho \in D_K(p) \mid p \equiv \pm 1 \pmod{8} \leq x, \frac{\log |\rho / \sigma(\rho)|}{2 \log \varepsilon^2} \in I\right\} = |I| \operatorname{li}(x) + O(xe^{-b\sqrt{\log x}}).$$

The implied constant depends only on K .

Using this effective equidistribution theorem, we can prove the following result.

Lemma 4.8. *For a non-zero $k \in 2\mathbb{Z}$ with $\log |k| \leq b\sqrt{\log x}$, we have*

$$\sum_{\substack{p \leq x \\ p \equiv \pm 1 \pmod{8}}} \frac{\left|\cos\left(\frac{\pi k}{4 \log \varepsilon} \log |\rho_p / \sigma(\rho_p)|\right)\right|}{p} \leq \frac{1}{\pi} \log \log x + \left(1 - \frac{2}{\pi}\right) \log \log k + O(1).$$

Proof. We follow the strategy in [9, pp. 91–92]. By possibly shifting to $-k$, we may assume $k > 0$. We start by showing that, for all even k , we have

$$\frac{1}{2} \sum_{\substack{p \leq x \\ p \equiv \pm 1 \pmod{8} \\ \rho \in D_K(p)}} |\cos(v_k(\rho))| = \frac{1}{\pi} \operatorname{li}(x) + O(kxe^{-b\sqrt{\log x}}), \quad (23)$$

where $v_k(\rho) = \frac{\pi k}{4 \log \varepsilon} \log |\rho / \sigma(\rho)|$. Note that we are summing over both ρ_p and $\sigma(\rho_p)$. This makes it easier to use Rademacher's theorem. We choose representatives for ρ such that $v_k(\rho) \in [-\pi/2, \pi k - \pi/2[= E$. We split this interval as a disjoint union according to the sign of $\cos(v)$, i.e.,

$$E = \bigcup_{n=0}^{k-1} E_n,$$

where $E_n = [-\pi/2 + n\pi, \pi/2 + n\pi[$, and note that

$$|\cos(v)| = (-1)^n \cos(v) = (-1)^n \int_v^{\pi/2+n\pi} \sin(\theta) d\theta$$

for $v \in E_n$. It follows that

$$\begin{aligned} \sum_{\substack{p \leq x \\ p \equiv \pm 1 \pmod{8} \\ \rho \in D_K(p)}} |\cos(v_k(\rho))| &= \sum_{n=0}^{k-1} (-1)^n \sum_{\substack{p \leq x \\ p \equiv \pm 1 \pmod{8}}} \sum_{\substack{\rho \in D_K(p) \\ v_k(\rho) \in E_n}} \int_{v_k(\rho)}^{\pi/2+n\pi} \sin(\theta) d\theta \\ &= \sum_{n=0}^{k-1} (-1)^n \int_{E_n} \left(\sum_{\substack{p \leq x \\ p \equiv \pm 1 \pmod{8}}} \sum_{\substack{\rho \in D_K(p) \\ -\pi/2+n\pi \leq v_k(\rho) \leq \theta}} 1 \right) \sin(\theta) d\theta. \end{aligned}$$

Using Theorem 4.7 on the inner sum, we find

$$= \sum_{n=0}^{k-1} (-1)^n \int_{E_n} \left(\left(\frac{\theta}{k\pi} - \frac{n-1/2}{k} \right) \text{li}(x) + O(xe^{-c\sqrt{\log x}}) \right) \sin(\theta) d\theta.$$

Using

$$\int_{E_n} \sin(\theta) d\theta = 0 \quad \text{and} \quad \int_{E_n} \theta \sin(\theta) d\theta = 2(-1)^n,$$

we arrive at (23). It follows that, for any $2 < w \leq x$, we have

$$\begin{aligned} \sum_{\substack{p \leq x \\ p \equiv \pm 1 \pmod{8}}} \frac{1}{p} \left| \cos \left(\frac{\pi k}{4 \log \varepsilon} \log \left| \frac{\rho_p}{\sigma(\rho_p)} \right| \right) \right| \\ \leq \frac{1}{2} \log \log w + O(1) + \frac{1}{\pi} \log \left(\frac{\log x}{\log w} \right) + O(ke^{-b\sqrt{\log w}}). \end{aligned}$$

Here we have estimated the sum up w trivially, and used partial summation and (23) on the rest. After that, we used

$$\int \frac{\text{li}(x)}{x^2} dx = \log \log x + O(1).$$

If we choose w subject to $\log(w) = (b^{-1} \log k)^2$, then the last term is bounded. The condition $w \leq x$ gives the condition on k , and we arrive at the claim. ■

Lemma 4.9. *Let k be an even non-zero integer. Then there exists a constant b such that, for $\log|k| \leq b\sqrt{\log x}$, we have*

$$\sum_{n \leq x} |U_k(n)| = O\left(x \left(\frac{\log^2 |k|}{\log x}\right)^{1-2/\pi}\right).$$

Proof. We use Theorem 2.2 with $f(n) = |U_k(n)|$. The relevant assumptions were checked above. Using

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + O(1)$$

and Lemma 4.8, the claim follows. ■

4.4. Parametrization of $\Gamma(2, 5)$

In this section, we return to the quaternion group $\Gamma(2, 5)$ (see (18)), and show how we can parametrize parts of it using $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{2})$. Consider for $\gamma \in \Gamma(2, 5)$ the two algebraic integers

$$\begin{aligned} z_1(\gamma) &= x_0 + x_1 \sqrt{2} \in \mathcal{O}_K, \\ z_2(\gamma) &= x_2 + x_3 \sqrt{2} \in \mathcal{O}_K. \end{aligned}$$

By the determinant condition, we deduce that $N(z_1(\gamma)) - 5N(z_2(\gamma)) = 1$, so

$$N(z_1(\gamma)) = 5N(z_2(\gamma)) + 1.$$

It is now straightforward to verify the following proposition.

Proposition 4.10. *The following statements hold.*

- (1) *The map $\gamma \mapsto (z_1(\gamma), z_2(\gamma))$ is injective.*
- (2) *If $\gamma \in \Gamma \cap S^c$, then $N(z_1(\gamma))$, $N(z_2(\gamma))$ are non-zero and have the same sign. Writing $N(z_1(\gamma)) = 5N(z_2(\gamma)) + 1 = 5n + 1$, we have the following statements:*
 - (a) *if $\delta_1(\gamma) + \delta_2(\gamma)$ is even, then $n \in \mathbb{N}$ and $\delta(\gamma) = 20n + 2$;*
 - (b) *if $\delta_1(\gamma) + \delta_2(\gamma)$ is odd, then $n \in -\mathbb{N}$ and $\delta(\gamma) = -20n - 2$.*
- (3) *If $\gamma' = h_0^{j_1} \gamma h_0^{j_2}$, then*

$$z_1(\gamma') = \varepsilon^{2(j_1+j_2)} z_1(\gamma), \quad z_2(\gamma') = \varepsilon^{2(j_1-j_2)} z_2(\gamma).$$

(4) We have

$$e\left(\frac{\log y_1(\gamma)}{\log \varepsilon^4}\right) = (\lambda(z_1(\gamma))\lambda(z_2(\gamma))), \quad e\left(\frac{\log y_2(\gamma)}{\log \varepsilon^4}\right) = \left(\frac{\lambda(z_1(\gamma))}{\lambda(z_2(\gamma))}\right),$$

where $\lambda(z)$ is the square root of the basic Grössencharacter in $\mathcal{O}_K$; see (22) and [17, Section 10].

Note that Proposition 4.10 (4) implies that

$$\begin{aligned} \frac{\log y_1(\gamma)}{\log \varepsilon^4} &= \frac{1}{2} \left(\frac{\log |z_1(\gamma)/\sigma z_1(\gamma)|}{\log \varepsilon^4} + \frac{\log |z_2(\gamma)/\sigma z_2(\gamma)|}{\log \varepsilon^4} \right) \pmod{1}, \\ \frac{\log y_2(\gamma)}{\log \varepsilon^4} &= \frac{1}{2} \left(\frac{\log |z_1(\gamma)/\sigma z_1(\gamma)|}{\log \varepsilon^4} - \frac{\log |z_2(\gamma)/\sigma z_2(\gamma)|}{\log \varepsilon^4} \right) \pmod{1}. \end{aligned}$$

We want to describe the intersection of $\Gamma(2, 5)$ with $S \backslash s$ and s . Note that if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then

$$abcd = N(z_1)5N(z_2) = (5N(z_2) + 1)5N(z_2).$$

If $N(z_2) \leq 0$, then $(5N(z_2) + 1) < 0$, so we have $abcd \geq 0$. If, on the other hand, $N(z_2) \geq 0$, then $(5N(z_2) + 1) > 0$, so also in this case $abcd \geq 0$.

We see that $abcd$ vanishes if and only in $N(z_2) = 0$. This happens precisely if $N(z_1) = 1$, i.e., if z_1 is a unit with norm 1. But this means that γ is a power of h_0 .

Summarizing, we have shown that

$$\Gamma(2, 5) \cap s = H \quad \text{and} \quad \Gamma(2, 5) \cap (S \backslash s) = \emptyset.$$

For a double coset $[\gamma] \in H \backslash (\Gamma(2, 5) - H) / H$, we note that $\delta_1(\gamma) = \delta_2(\gamma) = 0$ precisely if all four entries of γ have the same sign.

Theorem 4.11. *The map*

$$\begin{aligned} \psi: \{[\gamma] \mid \delta_1(\gamma) = \delta_2(\gamma) = 0, bc = 5n\} / \{\pm I\} &\rightarrow D_K(5n + 1) \times D_K(n), \\ \gamma &\mapsto (|z_1(\gamma)|, |z_2(\gamma)|) \end{aligned}$$

is well defined, two-to-one, and surjective.

Proof. It follows from Proposition 4.10 that ψ is well defined.

Given $(z_1, z_2) \in D_K(5n + 1) \times D_K(n)$, we consider the matrix

$$\gamma = \begin{pmatrix} z_1 & \sqrt{5}z_2 \\ \sqrt{5}\sigma(z_2) & \sigma(z_1) \end{pmatrix} \in \Gamma,$$

which satisfies that $\delta_1(\gamma) = \delta_2(\gamma) = 0$ and $\sqrt{5}z_2\sqrt{5}\sigma(z_2) = 5n$. This shows ψ is surjective.

To see that ψ is two-to-one, we note that the two matrices in $\Gamma(2, 5)$ given by

$$\gamma = \begin{pmatrix} z_1 & \sqrt{5}z_2 \\ \sqrt{5}\sigma(z_2) & \sigma(z_1) \end{pmatrix}, \quad \gamma' = \begin{pmatrix} z_1\varepsilon^2 & \sqrt{5}z_2 \\ \sqrt{5}\sigma(z_2) & \sigma(z_1\varepsilon^2) \end{pmatrix} \quad (24)$$

represent different double cosets and map to the same element in

$$D_K(5n+1) \times D_K(n).$$

Assume now that $\psi(\gamma_1) = \psi(\gamma_2)$. By possibly taking minus the matrix, we may assume that all entries of γ_1 and γ_2 are positive. It follows that there exist integers n_1, n_2 such that

$$z_1(\gamma_2) = z_1(\gamma_1)\varepsilon^{2n_1}, \quad z_2(\gamma_2) = z_2(\gamma_1)\varepsilon^{2n_2}.$$

Write $z_i(\gamma_1) = z_i$. Using that

$$h_0^{j_1} \gamma_1 h_0^{j_2} = \gamma = \begin{pmatrix} z_1 \varepsilon^{2(j_1+j_2)} & \sqrt{5}z_2 \varepsilon^{2(j_1-j_2)} \\ \sqrt{5}\sigma(z_2 \varepsilon^{2(j_1-j_2)}) & \sigma(z_1 \varepsilon^{2(j_1+j_2)}) \end{pmatrix},$$

we see that if n_1, n_2 have the same parity, then γ_1 and γ_2 are in the same double coset, and if n_1, n_2 have different parity, then γ_2 is in the same double coset as the second matrix in (24). This shows that the map is two-to-one. ■

4.5. Counting double cosets with prime norm in the hyperbolic case

In order to find asymptotics for the number of double cosets with prime norm in the hyperbolic case, we first prove a variant of the Titchmarsh divisor problem. Recall that in the Titchmarsh divisor problem [40] we want to determine asymptotics for sums like

$$\sum_{n \leq x} 1 * 1(n+1) \Lambda(n),$$

where $*$ denotes the usual Dirichlet convolution between arithmetical functions.

Consider

$$\psi(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n).$$

The famous Bombieri–Vinogradov theorem [3] (see also [43]) states that, for every $A > 0$, there exists a $B > 0$ such that

$$\sum_{q \leq Q} \max_{\substack{(a,q)=1 \\ y \leq x}} \left| \psi(y, q, a) - \frac{y}{\varphi(q)} \right| = O_A \left(\frac{x}{\log^A(x)} \right) \quad (25)$$

for $Q = O(x^{1/2}/\log^B(x))$. This suffices, when combined with the Brun–Titchmarsh inequality

$$\pi(x+y, q, a) - \pi(x, q, a) < \frac{2y}{\varphi(q) \log(y/q)} \quad \text{for } (a, q) = 1, q < y \quad (26)$$

(see [25, Theorem 6.6]), to find the main term and an error term of the form

$$\frac{x \log \log x}{\log x};$$

see [15, Theorem 3.9] and [38]. In order to get better error term estimates, one needs to extend the validity of bounds like (25). In the case of the classical Titchmarsh divisor problem this was done independently by Fouvry [11] and by Bombieri, Friedlander and Iwaniec [4]. They found that, for any $A > 0$,

$$\sum_{n \leq x} 1 * 1(n+1) \Lambda(n) = c_1 x \log x + c_2 x + O\left(\frac{x}{\log^A(x)}\right).$$

Here,

$$c_1 = \frac{\zeta(2)\zeta(3)}{\zeta(6)}, \quad c_2 = c_1 \left(2\gamma - 1 - 2 \sum_p \frac{\log p}{p^2 - p + 1} \right).$$

Drappeau [7, Theorem 1.2] found improvements on the error term above, and showed that getting better estimates is related to the existence of Siegel zeroes.

4.5.1. A variant of the Titchmarsh divisor problem. We need a variant of the Titchmarsh divisor problem. Let

$$L_5(s, \chi_8) = (1 + 5^{-s})L(s, \chi_8)$$

be the L -function related to χ_8 with the Euler factor at 5 removed, and let

$$C' = L_5(1, \chi_8) \prod_{p \neq 5} \left(1 + \frac{\chi_8(p)}{p(p-1)} \right).$$

Using (20), we see that

$$C' = \frac{6 \log \varepsilon}{5 \sqrt{2}} \prod_{p \neq 5} \left(1 + \frac{\chi_8(p)}{p(p-1)} \right).$$

Theorem 4.12. *Let $a = \pm 1 \pmod{8}$. Then, for any $A > 0$,*

$$\sum_{\substack{n \leq x \\ n \equiv a \pmod{8}}} \mathcal{N}_2(5n+1) \Lambda(n) = \frac{C'}{\varphi(8)} x + O\left(\frac{x}{\log^A(x)}\right).$$

Remark 5. Theorem 4.12 is analogous to the Titchmarsh divisor problem in the following sense: The Titchmarsh divisor problem asks for asymptotics with error terms of $\sum_{n \leq x} 1 * 1(n+1)\Lambda(n)$, and since $\mathcal{N}_2(5n+1) = 1 * \chi_8(5n+1)$, the first expression in Theorem 4.12 is an analogous sum over a linear shift with n in an arithmetic progression. Assing, Blomer and Li [1] studied such sums with 5 replaced by ± 1 and without the arithmetic progression. We use a variant of their method. One can prove, using a slight variation of the proof given for Theorem 4.12 that the same asymptotics hold, when $a = \pm 3 \pmod 8$ proving equidistribution among the four residue classes modulo 8.

The proof of Theorem 4.12 uses a recent result by Assing, Blomer and Li. Here we write $a|b^\infty$ to mean that a has only prime divisors of b .

Theorem 4.13 ([1, Theorem 2.1]). *There exist $0 < \delta < 1/2$ with the following property: Let*

- (1) $x \geq 2$ and $Q \leq x^{1/2+\delta}$, $A, C > 0$;
- (2) $c, d \in \mathbb{N}$ with $d|c^\infty$, and $c, d \leq \log^C x$;
- (3) $c_0, d_0 \in \mathbb{Z}$ with $(c, c_0) = (d, d_0) = 1$;
- (4) $a_1, a_2 \in \mathbb{Z} \setminus \{0\}$ with $|a_1| \leq x^{1-\delta}$, $|a_2| \leq x^\delta$.

Then

$$\sum_{\substack{q \leq Q \\ (q, a_1 a_2) = 1 \\ q = c_0 \pmod c}} \left(\sum_{\substack{n \leq x \\ n = a_1 \bar{a}_2 \pmod q \\ n = d_0 \pmod d}} \Lambda(n) - \frac{x}{\varphi(qd)} \right) = O_{A,C} \left(\frac{x}{\log^A(x)} \right).$$

This theorem is particularly useful because the error term allows for varying a_i , c, d in certain ranges. We have applied the prime number theorem and [1, Lemma 5.1] to get it in this form.

Proof of Theorem 4.12. We first note that since $\Lambda(n) \leq \log(n)$, we have trivially

$$\sum_{\substack{n \leq y \\ n = a \pmod 8}} \mathcal{N}_2(5n+1)\Lambda(n) = O(y \log y). \quad (27)$$

Let $L = \log^B(x)$ for a suitably chosen B . It follows from (27) that, up to an error of size $O_B(x/\log^{B-1}(x))$, the sum in (4.12) equals

$$\sum_{\substack{x/L < n \leq x \\ n = a \pmod 8}} \mathcal{N}_2(5n+1)\Lambda(n).$$

The arithmetic function $\mathcal{N}_2(m)$ is multiplicative and equal to 1 on powers of 2, so we may always remove the 2-part of m .

If $n = 1 \pmod{8}$, then $5n + 1$ is divisible by 2 exactly once.

To simplify notation, we introduce the function

$$y(x) = \sqrt{\frac{5x+1}{2}}, \quad \text{with inverse } x(y) = \frac{2y^2-1}{5}.$$

For simplicity, we denote $y(n)$ by y_n . We can use Dirichlet's hyperbola method to get

$$\mathcal{N}_2(5n+1) = \mathcal{N}_2\left(\frac{5n+1}{2}\right) = \sum_{\substack{k|y_n^2 \\ k < y_n}} \chi_8(k)(1 + \chi_8(y_n^2)) + \chi_8(y_n).$$

Here we have set $\chi(y) = 0$, if $y \notin \mathbb{N}$. Note that $5n + 1$ is never twice a square since two times a square is 0, 2, or 3 mod 5. It follows that

$$\mathcal{N}_2(5n+1) = \begin{cases} 0 & \text{if } n = 1 \pmod{16}, \\ 2 \sum_{\substack{k|y_n^2 \\ k < y_n}} \chi_8(k) & \text{if } n = 9 \pmod{16}. \end{cases} \quad (28)$$

We can now use these expressions to see that

$$\begin{aligned} \sum_{\substack{x/L < n \leq x \\ n \equiv 1 \pmod{8}}} \mathcal{N}_2(5n+1) \Lambda(n) &= 2 \sum_{\substack{x/L < n \leq x \\ n \equiv 9 \pmod{16}}} \sum_{\substack{k|y_n^2 \\ k < y_n}} \chi_8(k) \Lambda(n) \\ &= 2 \sum_{k \leq y(x)} \chi_8(k) \sum_{\substack{\max(x/L, x(k)) < n \leq x \\ n \equiv 9 \pmod{16} \\ 5n \equiv -1 \pmod{2k}}} \Lambda(n). \end{aligned}$$

When k is divisible by 5, the inner sum is void, and when k is odd, $n = 9 \pmod{16}$ implies $5n = -1 \pmod{2}$. Therefore, the two congruence conditions reduce to $n = 9 \pmod{16}$ and $n = -\bar{5} \pmod{k}$, and we get

$$\begin{aligned} &= 2 \sum_{\substack{k \leq y(x) \\ (k,5)=1}} \chi_8(k) \sum_{\substack{\max(x/L, x(k)) < n \leq x \\ n \equiv 9 \pmod{16} \\ n \equiv -\bar{5} \pmod{k}}} \Lambda(n) \\ &= 2(\Sigma_1 + \Sigma_2). \end{aligned}$$

Here we have split the outer sum into two sums: Σ_1 equals the sum over $k \leq y(x/L)$, and Σ_2 denotes the rest. We have

$$\begin{aligned} \Sigma_1 &= \sum_{\substack{k \leq y(x/L) \\ (k,5)=1}} \chi_8(k) \sum_{\substack{x/L < n \leq x \\ n \equiv 9 \pmod{16} \\ n \equiv -\bar{5} \pmod{k}}} \Lambda(n) \\ &= \sum_{b \pmod{8}} \chi_8(b) \sum_{\substack{k \leq y(x/L) \\ (k,5)=1 \\ k \equiv b \pmod{8}}} \sum_{\substack{x/L < n \leq x \\ n \equiv 9 \pmod{16} \\ n \equiv -\bar{5} \pmod{k}}} \Lambda(n). \end{aligned}$$

We can now apply Theorem 4.13 twice with x equal to x and x/L , respectively, both times with $Q = y(x/L)$, $a_1 = -1$, $a_2 = 5$, $d_0 = 9$, $d = 16$, $c_0 = b$, $c = 8$. This gives

$$\begin{aligned}
 &= \sum_{b \bmod 8} \chi_8(b) \sum_{\substack{k \leq y(x/L) \\ (k,5)=1 \\ k \equiv b \pmod{8}}} \left(\frac{x}{\varphi(16k)} - \frac{x/L}{\varphi(16k)} \right) + O\left(\frac{x}{\log^A(x)} \right) \\
 &= \sum_{\substack{k \leq y(x/L) \\ (k,5)=1}} \chi_8(k) \left(\frac{x}{\varphi(16k)} - \frac{x/L}{\varphi(16k)} \right) + O\left(\frac{x}{\log^A(x)} \right) \\
 &= \frac{C'}{\varphi(16)} x + O\left(\frac{x}{\log^A(x)} \right),
 \end{aligned}$$

where in the last line we have used [1, Lemma 5.2].

We now want to show that $\Sigma_2 \ll x / \log^A x$:

$$\Sigma_2 = \sum_{\substack{y(x/L) < k \leq y(x) \\ (k,5)=1}} \chi_8(k) \sum_{\substack{x(k) < n \leq x \\ n \equiv 9 \pmod{16} \\ n \equiv -5 \pmod{k}}} \Lambda(n).$$

We want to apply Theorem 4.13, so we need to deal with the fact that the inner sum is over an interval depending on k . To address this, we let

$$V = (1 - \Delta) \text{ with } \Delta = \log^{-A/2} x,$$

and split the inner sum in intervals roughly of the form $yV < n \leq y$ as follows:

$$\sum_{\substack{x(k) < n \leq x \\ n \equiv 9 \pmod{16} \\ n \equiv -5 \pmod{k}}} \Lambda(n) = \sum_{r=0}^{R(k,x)} \sum_{\substack{\max(x(k), xV^{r+1}) < n \leq xV^r \\ n \equiv 9 \pmod{16} \\ n \equiv -5 \pmod{k}}} \Lambda(n),$$

where $R(k, x) = \min\{r \mid xV^{r+1} < x(k)\}$,

$$= \sum_{r=0}^{R(k,x)-1} \sum_{\substack{xV^{r+1} < n \leq xV^r \\ n \equiv 9 \pmod{16} \\ n \equiv -5 \pmod{k}}} \Lambda(n) + \sum_{\substack{x(k) < n \leq xV^{R(k,x)} \\ n \equiv 9 \pmod{16} \\ n \equiv -5 \pmod{k}}} \Lambda(n).$$

Observing that for $k \in \Sigma_2$ we have $xV^{r+1} < x/L$, implies $xV^{r+1} < x(k)$. Therefore, $R(k, x) = O(\log L/\Delta)$ uniformly in k . Trivially, we have

$$x - x(k) = \sum_{r=0}^{R(k,x)-1} (xV^r - xV^{r+1}) + (xV^{R(k,x)} - x(k)),$$

so we arrive at

$$\begin{aligned}
 \Sigma_2 &= \sum_k \chi_8(k) \sum_{\substack{x(k) < n \leq x \\ n \equiv 9 \pmod{16} \\ n \equiv -5 \pmod{k}}} \Lambda(n) = \sum_k \chi_8(k) \frac{x - x(k)}{\varphi(16k)} \\
 &\quad + \sum_k \chi_8(k) \left(\sum_{r=0}^{R(k,x)-1} \sum_{\substack{xV^{r+1} < n \leq xV^r \\ n \equiv 9 \pmod{16} \\ n \equiv -5 \pmod{k}}} \Lambda(n) - \frac{xV^r - xV^{r+1}}{\varphi(16k)} \right) \\
 &\quad + \sum_k \chi_8(k) \left(\sum_{\substack{x(k) < n \leq xV^{R(k,x)} \\ n \equiv 9 \pmod{16} \\ n \equiv -5 \pmod{k}}} \Lambda(n) - \frac{xV^{R(k,x)} - x(k)}{\varphi(16k)} \right) \\
 &= \Sigma_{2,1} + \Sigma_{2,2} + \Sigma_{2,3}.
 \end{aligned}$$

Here, all k -sums are over $y(x/L) < k \leq y(x)$ with $(k, 5) = 1$. Using summation by parts, we see that $\Sigma_{2,1} = O(x/L)$. The contribution from $\Sigma_{2,3}$ is bounded as follows: By Brun–Titchmarsh (26) and the definition of $R(k, x)$, the sum that comes after the character is bounded by $O(x\Delta/\varphi(k))$. Summing this over the relevant k , and using

$$\sum_{k \leq x} \varphi^{-1}(k) = O(\log x)$$

(see [1, Lemma 5.1]), gives a contribution of $\Sigma_{2,3} = O(x \log^{1-A/2} x)$.

Finally, to estimate $\Sigma_{2,2}$, we first split the k sum according to its value mod 8. Then we notice that as a function of k with $y(x/L) < k \leq y(x)$, we have that $R(k, x)$ is decreasing. We then interchange the k and the r sum, and we find

$$\begin{aligned}
 \Sigma_{2,2} &= \sum_{b \pmod{8}} \chi_8(k) \sum_{k=b \pmod{8}} \sum_{r=0}^{R(k,x)-1} \Sigma_{2,2}(n, k, r) \\
 &= \sum_{b \pmod{8}} \chi_8(k) \sum_{r=0}^{R(k,x)-1} \sum_{\substack{y(x/L) < k \leq K(x,r) \\ (k,5)=1 \\ k \equiv b \pmod{8}}} \Sigma_{2,2}(n, k, r).
 \end{aligned}$$

Here,

$$\Sigma_{2,2}(n, k, r) = \sum_{\substack{xV^{r+1} < n \leq xV^r \\ n \equiv 9 \pmod{16} \\ n \equiv -5 \pmod{k}}} \Lambda(n) - \frac{xV^r - xV^{r+1}}{\varphi(16k)},$$

$$R(x) = R\left(y\left(\frac{x}{L}\right), x\right) = O\left(\frac{\log L}{\Delta}\right),$$

$$K(x, r) = \max\{k \mid r \leq R(k, x)\}.$$

We may now use Theorem 4.13, and we find that

$$\begin{aligned}\Sigma_{2,2} &= O\left(\sum_{b \bmod 8} \sum_{r=0}^{R(x)} \frac{x V^r}{\log^A(x V^r)}\right) \\ &= O\left(\frac{x}{\log^A(x/L)} \Delta\right) = O\left(\frac{x}{\log^{A(1/2-\varepsilon)}(x)}\right).\end{aligned}$$

Here we have used that for r in the sum, we have $x/L \leq x V^r$. Summarizing, we have shown that, for every $A > 0$, we have

$$\sum_{\substack{n \leq x \\ n \equiv 1 \pmod{8}}} \mathcal{N}_2(5n+1) \Lambda(n) = \frac{C'}{\varphi(8)} x + O\left(\frac{x}{\log^A(x)}\right).$$

This proves the bound for $n \equiv 1 \pmod{8}$.

To deal with the case of $n \equiv 7 \pmod{8}$ we note that in this case $5n+1$ is divisible by 2 exactly twice and the same procedure that led to (28) leads to the following expression in this case:

$$\mathcal{N}_2(5n+1) = \begin{cases} 0 & \text{if } n \equiv 15, 23 \pmod{32}, \\ 2 \sum_{\substack{k|w_n^2 \\ k < w_n}} \chi_8(k) + \chi_8(w_n) & \text{if } n \equiv 7, 31 \pmod{32}. \end{cases}$$

Here, $w_n = \sqrt{(5n+1)/4}$. We then deal separately with the cases $a = 7, 31$ of

$$\sum_{\substack{n \leq x \\ n \equiv a \pmod{32}}} \mathcal{N}_2(5n+1) \Lambda(n).$$

The term $\chi_8(w_n)$ introduces a negligible error term, and the same technique, which we employed above, leads to

$$\sum_{\substack{n \leq x \\ n \equiv a \pmod{32}}} \mathcal{N}_2(5n+1) \Lambda(n) = \frac{1}{2} \frac{C'}{\varphi(8)} x + O\left(\frac{x}{\log^A(x)}\right),$$

when $a = 7$ or $a = 31$. Summing the contributions together, we find

$$\sum_{\substack{n \leq x \\ n \equiv 7 \pmod{8}}} \mathcal{N}_2(5n+1) \Lambda(n) = \frac{C'}{\varphi(8)} x + O\left(\frac{x}{\log^A(x)}\right),$$

which finishes the proof. ■

4.5.2. Counting over primes in the hyperbolic case. We are now ready to prove the first part of Theorem 1.6. Recall that we are considering the sequence

$$h = (\psi(\gamma)) = \left(\left(\frac{\log y_1}{2 \log \varepsilon^2}, \frac{\log y_2}{2 \log \varepsilon^2} \right) \right) \subseteq (\mathbb{R}/\mathbb{Z})^2, \quad (29)$$

indexed over the set of all $\gamma \in H \backslash \Gamma(2, 5)/H$ with all four entries strictly positive. Equip this index set with the size function $v(\gamma) = bc/5$, and recall from Proposition 4.10 (a) and (19) that $v(\gamma) = (\cosh(2v(\gamma)) - 1)/10$.

Theorem 4.14. *Consider the sequence h in (29). Then*

$$\pi_h(x) = C \operatorname{li}(x) + O\left(\frac{x}{\log^A(x)}\right),$$

where

$$C = \frac{12 \log \varepsilon}{5 \sqrt{2}} \prod_{p \neq 5} \left(1 + \frac{\chi_8(p)}{p(p-1)} \right).$$

Here, χ_8 is the even primitive Dirichlet character modulo 8.

Note that by Lemma 4.3 and the discussion before Theorem 4.11, the set we are indexing over corresponds precisely to $\pm H \Gamma H$ with $\pm \gamma \notin H$ and $\delta_1(\gamma) = \delta_2(\gamma) = 0$. We can therefore parametrize this set using Theorem 4.11. Let γ, γ' be the two matrices from (24), which map to the same element under ψ in Theorem 4.11. Observing that

$$e\left(n_1 \frac{\log y_1(\gamma')}{\log \varepsilon^4} + n_2 \frac{\log y_2(\gamma')}{\log \varepsilon^4}\right) = (-1)^{n_1+n_2} e\left(n_1 \frac{\log y_1(\gamma)}{\log \varepsilon^4} + n_2 \frac{\log y_2(\gamma)}{\log \varepsilon^4}\right),$$

we see that if $n > 0$, then the Kloosterman-type sum

$$S_h(n_1, n_2, n) = \sum_{\substack{[\gamma] \\ \delta_i(\gamma)=0 \\ (\cosh 2v(\gamma)-1)/10=n}} e\left(n_1 \frac{\log y_1(\gamma)}{\log \varepsilon^4} + n_2 \frac{\log y_2(\gamma)}{\log \varepsilon^4}\right)$$

vanishes, unless n_1, n_2 have the same parity. If they do have the same parity, Theorem 4.11 gives

$$\begin{aligned} S_h(n_1, n_2, n) &= 2 \sum_{(z_1, z_2) \in D_K(5n+1) \times D_K(n)} \lambda(z_1)^{n_1+n_2} \lambda(z_2)^{n_1-n_2} \\ &= 2U_{n_1+n_2}(5n+1)U_{n_1-n_2}(n). \end{aligned} \quad (30)$$

It follows from Theorem 4.5 that if $m = (n_1, n_2) \in \mathbb{Z}^2$, then

$$\begin{aligned} \sum_{n \leq X} S_h(n_1, n_2, n) &= \sum_{\substack{[\gamma] \\ \delta_i(\gamma)=0 \\ e^{2v(\gamma)} + O(1) \leq 20X+2}} e \left(n_1 \frac{\log y_1(\gamma)}{\log \varepsilon^4} + n_2 \frac{\log y_2(\gamma)}{\log \varepsilon} \right) \\ &= \delta_{m,0} \frac{(\log \varepsilon)^2}{\pi^2} 10X + O_m(X^{2/3}). \end{aligned} \quad (31)$$

The $n_1 = n_2 = 0$ case reduces, via (30) and (21), to

$$\sum_{n \leq X} \mathcal{N}_2(5n+1) \mathcal{N}_2(n) = \frac{5(\log \varepsilon)^2}{\pi^2} X + O(X^{2/3}).$$

The same asymptotics were found by Hejhal ([19, Théorème 2], [20, eq. (1)]), see also [21, Théorème 8].

Proof of Theorem 4.14. To investigate what happens if we only sum over primes in equation (31), we define

$$\psi_h(x) = \sum_{n \leq x} S_h(0, 0, n) \Lambda(n),$$

where Λ is the von Mangoldt function. Since $S_h(n_1, n_2, n) \ll n^\varepsilon$ it is easy to verify that the asymptotical expansion of $\pi_h(x, 0, 0)$ is equivalent to

$$\psi_h(x) = C \cdot x + O\left(\frac{x}{(\log(x))^A}\right),$$

which we will prove. Since by (30) and (21),

$$S_h(0, 0, p) = 2\mathcal{N}_2(p)\mathcal{N}_2(5p+1) = 4\delta_{p \equiv \pm 1(8)}\mathcal{N}_2(5p+1),$$

we have

$$\psi_h(x) = 4 \sum_{\substack{n \leq x \\ n \equiv \pm 1 \pmod{8}}} \mathcal{N}_2(5n+1) \Lambda(n) + O\left(\frac{x}{\log^A(x)}\right).$$

It now follows from Theorem 4.12 that

$$\psi_h(x) = \frac{8}{\varphi(8)} cx + O\left(\frac{x}{\log^A(x)}\right),$$

from which the claim follows. ■

4.6. Equidistribution over primes in the hyperbolic case

We can now finally prove equidistribution over primes of the sequence h in (29). We first give upper bounds for the Weyl sums.

Theorem 4.15. *Consider the sequence h in (29), and consider integers m_1, m_2 not both zero. Then*

$$\sum_{\substack{\delta_i(\gamma)=0 \\ v(\gamma)=p \leq x}} e\left(m_1 \frac{\log y_1(\gamma)}{\log \varepsilon^4} + m_2 \frac{\log y_2(\gamma)}{\log \varepsilon^4}\right) = O\left(\frac{x}{\log x} \frac{1}{\log^{1-2/\pi} x}\right).$$

Proof. Denoting the sum we want to bound by $B(m_1, m_2, x)$, we see that

$$B(m_1, m_2, x) = \sum_{p \leq x} S_h(m_1, m_2, p).$$

Since $S_h(m_1, m_2, p) = 0$ except when m_1, m_2 have the same parity, we may assume that m_1, m_2 have the same parity. We deduce from (30) that

$$B(m_1, m_2, x) \leq 2 \sum_{p \leq x} |U_{n_1+n_2}(p)| |U_{n_1-n_2}(5p+1)|.$$

We now let $(a_1, b_1) = (1, 0)$, $(a_2, b_2) = (5, 1)$ and $g_1(n) = |U_{m_1+m_2}(n)|$, $g_2(n) = |U_{m_1-m_2}(n)|$. We verified in Section 4.3 that the functions g_i are multiplicative and satisfies $|g_i(n)| \leq d(n)$. It now follows from Theorem 2.1 that

$$|B(m_1, m_2, x)| \ll \frac{x}{\log^3(x)} \sum_{n_1 \leq x} \frac{g_1(n_1)}{n_1} \sum_{n_2 \leq x} \frac{g_2(n_2)}{n_2}.$$

Since $g_i(n) \leq 1 * \chi_8$, we have trivially

$$\sum_{n \leq x} \frac{g_i(n)}{n} = O(\log x).$$

Since m_1 and m_2 are non-zero with the same parity, $m_1 - m_2, m_1 + m_2$ are even with at least one of them being non-zero. Let $g = g_i$, where i is chosen such that $g_i = |U_k|$ for some non-zero even k . We can then use Lemma 4.9 and summation by parts to conclude that

$$\sum_{n \leq x} \frac{g(n)}{n} = O_k(\log^{2/\pi}(x)),$$

which proves the claimed bound. ■

Using Weyl's equidistribution criterion and Theorem 4.14, we get the following corollary from Theorem 4.15.

Corollary 4.16. *Consider the sequence h given in (29). Then h is equidistributed on $(\mathbb{R} \setminus \mathbb{Z})^2$ over primes.*

Funding. Morten S. Risager was supported by the Grant DFF-3103-00074B from Independent Research Fund Denmark. Both authors were supported by the Swedish Research Council under grant no. 2021-06594, while in residence at Institut Mittag-Leffler in Djursholm, Sweden during the Analytic Number Theory programme in the spring of 2024.

References

- [1] E. Assing, V. Blomer, and J. Li, [Uniform Titchmarsh divisor problems](#). *Adv. Math.* **393** (2021), article no. 108076 Zbl [1484.11194](#) MR [4339529](#)
- [2] B. C. Berndt, S. Kim, and A. Zaharescu, [The circle problem of Gauss and the divisor problem of Dirichlet—still unsolved](#). *Amer. Math. Monthly* **125** (2018), no. 2, 99–114 Zbl [1396.11001](#) MR [3756337](#)
- [3] E. Bombieri, [On the large sieve](#). *Mathematika* **12** (1965), 201–225 Zbl [0136.33004](#) MR [0197425](#)
- [4] E. Bombieri, J. B. Friedlander, and H. Iwaniec, [Primes in arithmetic progressions to large moduli](#). *Acta Math.* **156** (1986), no. 3–4, 203–251 Zbl [0588.10042](#) MR [0834613](#)
- [5] D. Chatzacos, P. Kurlberg, S. Lester, and I. Wigman, [On the distribution of lattice points on hyperbolic circles](#). *Algebra Number Theory* **15** (2021), no. 9, 2357–2380 Zbl [1490.11044](#) MR [4355477](#)
- [6] G. Cherubini and A. Fazzari, [Hyperbolic angles from Heegner points](#). *Michigan Math. J.* **75** (2025), no. 5, 943–970 Zbl [8124644](#) MR [4979921](#)
- [7] S. Drapeau, [Sums of Kloosterman sums in arithmetic progressions, and the error term in the dispersion method](#). *Proc. Lond. Math. Soc. (3)* **114** (2017), no. 4, 684–732 Zbl [1392.11059](#) MR [3653244](#)
- [8] W. Duke, J. B. Friedlander, and H. Iwaniec, [Equidistribution of roots of a quadratic congruence to prime moduli](#). *Ann. of Math. (2)* **141** (1995), no. 2, 423–441 Zbl [0840.11003](#) MR [1324141](#)
- [9] P. Erdős and R. R. Hall, [On the angular distribution of Gaussian integers with fixed norm](#). *Discrete Math.* **200**, no. 1–3, 87–94 Zbl [1044.11073](#) MR [1692282](#)
- [10] L. Fainsilber, P. Kurlberg, and B. Wennberg, [Lattice points on circles and discrete velocity models for the Boltzmann equation](#). *SIAM J. Math. Anal.* **37** (2006), no. 6, 1903–1922 Zbl [1141.11046](#) MR [2213399](#)
- [11] É. Fouvry, [Sur le problème des diviseurs de Titchmarsh](#). *J. Reine Angew. Math.* **357** (1985), 51–76 Zbl [0547.10039](#) MR [0783533](#)
- [12] J. B. Friedlander and H. Iwaniec, [Hyperbolic prime number theorem](#). *Acta Math.* **202** (2009), no. 1, 1–19 Zbl [1278.11089](#) MR [2486486](#)

- [13] C. F. Gauss, [De nexu inter multitudinem classium in quas formae binariae secundi gradus distribuuntur earumque determinantem \(1834\)](#). In *Werke*. Vol. 2, pp. 269–291, Camb. Libr. Collect., Math., Cambridge University Press, Cambridge 2011
- [14] A. Good, [Local analysis of Selberg's trace formula](#). Lecture Notes in Math. 1040, Springer, Berlin, 1983 Zbl 0525.10013 MR 0727476
- [15] H. Halberstam and H.-E. Richert, *Sieve methods*. Lond. Math. Soc. Monogr. 4, Academic Press, London-New York, 1974 Zbl 0298.10026 MR 0424730
- [16] H. Halberstam and H.-E. Richert, [On a result of R. R. Hall](#). *J. Number Theory* **11** (1979), no. 1, 76–89 Zbl 0395.10048 MR 0527762
- [17] E. Hecke, [Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen](#). *Math. Z.* **6** (1920), no. 1-2, 11–51 Zbl 47.0152.01 MR 1544392
- [18] D. A. Hejhal, [The Selberg trace formula for \$\mathrm{PSL}\(2, \mathbf{R}\)\$](#) . Vol. I. Lect. Notes Math. 548, Springer, Berlin-New York, 1976 Zbl 0347.10018 MR 0439755
- [19] D. A. Hejhal, [Sur certaines séries de Dirichlet dont les pôles sont sur les lignes critiques](#). *C. R. Acad. Sci. Paris Sér. A-B* **287** (1978), no. 6, A383–A385 Zbl 0392.10025 MR 0498439
- [20] D. A. Hejhal, [Quelques exemples de séries de Dirichlet dont les pôles ont un rapport étroit avec les valeurs propres de l'opérateur de Laplace-Beltrami hyperbolique](#). *C. R. Acad. Sci. Paris Sér. I Math.* **294** (1982), no. 19, 637–640 Zbl 0487.10026 MR 0664638
- [21] D. A. Hejhal, [Sur quelques propriétés asymptotiques des périodes hyperboliques et des invariants algébriques d'un sous-groupe discret de \$\mathrm{PSL}\(2, \mathbf{R}\)\$](#) . *C. R. Acad. Sci. Paris Sér. I Math.* **294** (1982), no. 15, 509–512 Zbl 0511.10025 MR 0662134
- [22] P. Humphries, [Distributing points on the torus via modular inverses](#). *Q. J. Math.* **73** (2022), no. 1, 1–16 Zbl 1503.11106 MR 4395069
- [23] K. Ireland and M. Rosen, [A classical introduction to modern number theory](#). Second edn., Grad. Texts in Math. 84, Springer, New York, 1990 Zbl 0712.11001 MR 1070716
- [24] H. Iwaniec, [Spectral methods of automorphic forms](#). Second edn., Grad. Stud. Math. 53, American Mathematical Society, Providence, RI; Revista Matemática Iberoamericana, Madrid, 2002 Zbl 1006.11024 MR 1942691
- [25] H. Iwaniec and E. Kowalski, [Analytic number theory](#). Amer. Math. Soc. Colloq. Publ. 53, American Mathematical Society, Providence, RI, 2004 Zbl 1059.11001 MR 2061214
- [26] I. Kátai and I. Környei, [On the distribution of lattice points on circles](#). *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* **19** (1976), 87–91 Zbl 0348.10036 MR 0506102
- [27] I. Kubilyus, [The distribution of Gaussian primes in sectors and contours](#). *Leningrad. Gos. Univ. Učen. Zap. Ser. Mat. Nauk* **137(19)** (1950), 40–52 MR 0079610
- [28] E. Landau, [Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes](#). *Math. Ann.* **56** (1903), no. 4, 645–670 Zbl 34.0228.03 MR 1511191
- [29] E. Landau, [Vorlesungen über Zahlentheorie. Erster Band, zweiter Teil; zweiter Band; dritter Band](#). Chelsea, New York, 1969 Zbl 1182.11001 MR 0250844
- [30] H.-Q. Liu, [On Euler's function](#). *Proc. Roy. Soc. Edinburgh Sect. A* **146** (2016), no. 4, 769–775 Zbl 1403.11063 MR 3531455
- [31] K. Martin, M. McKee, and E. Wambach, [A relative trace formula for a compact Riemann surface](#). *Int. J. Number Theory* **7** (2011), no. 2, 389–429 Zbl 1314.11040 MR 2782665

- [32] M. Nair and G. Tenenbaum, [Short sums of certain arithmetic functions](#). *Acta Math.* **180** (1998), no. 1, 119–144 Zbl [0917.11048](#) MR [1618321](#)
- [33] P. Nicholls, [A lattice point problem in hyperbolic space](#). *Michigan Math. J.* **30** (1983), no. 3, 273–287 Zbl [0537.30033](#) MR [0725781](#)
- [34] J. Parkkonen and F. Paulin, [Counting common perpendicular arcs in negative curvature](#). *Ergodic Theory Dynam. Systems* **37** (2017), no. 3, 900–938 Zbl [1375.37104](#) MR [3628925](#)
- [35] S. J. Patterson, [A lattice-point problem in hyperbolic space](#). *Mathematika* **22** (1975), no. 1, 81–88 Zbl [0308.10013](#) MR [0422160](#)
- [36] H. Rademacher, [Primzahlen reell-quadratischer Zahlkörper in Winkelräumen](#). *Math. Ann.* **111** (1935), no. 1, 209–228 Zbl [61.0172.02](#) MR [1512990](#)
- [37] G. Rhin, [Sur la répartition modulo 1 des suites \$f\(p\)\$](#) . *Acta Arith.* **23** (1973), 217–248 Zbl [0264.10026](#) MR [0323731](#)
- [38] G. Rodriquez, Sul problema dei divisori di Titchmarsh. *Boll. Un. Mat. Ital. (3)* **20** (1965), 358–366 Zbl [0148.27207](#) MR [0197409](#)
- [39] A. Selberg, Equidistribution in discrete groups and the spectral theory of automorphic forms, 1977, <http://publications.ias.edu/selberg/section/2491>, visited on 18 November 2025
- [40] E. C. Titchmarsh, [A divisor problem](#). *Rendiconti Palermo* **54** (1930), no. 1, 414–429 Zbl [56.0891.01](#)
- [41] Á. Tóth, [Roots of quadratic congruences](#). *Internat. Math. Res. Notices* (2000), no. 14, 719–739 Zbl [1134.11339](#) MR [1776618](#)
- [42] I. Urbajalis, Distribution of the primes of the real quadratic field $K(\sqrt{2})$ (Russian). *Litovsk. Mat. Sb.* **4** (1964), 409–427 MR [0175863](#)
- [43] R. C. Vaughan, [An elementary method in prime number theory](#). *Acta Arith.* **37** (1980), 111–115 Zbl [0448.10037](#) MR [0598869](#)
- [44] A. Walfisz, [Weylsche Exponentialsummen in der neueren Zahlentheorie](#). Mathematische Forschungsberichte 15, VEB Deutscher, Berlin, 1963 Zbl [0146.06003](#) MR [0220685](#)
- [45] H. Weyl, [Über die Gleichverteilung von Zahlen mod. Eins.](#) *Math. Ann.* **77** (1916), no. 3, 313–352 Zbl [46.0278.06](#) MR [1511862](#)

Received 9 March 2024.

Yiannis N. Petridis

Department of Mathematics, University College London, Gower Street, London WC1E 6BT, UK; i.petridis@ucl.ac.uk

Morten S. Risager

Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen, Denmark; risager@math.ku.dk