ACTA ARITHMETICA
LXXVII.4 (1996)

Some applications of large sieve in Riemann surfaces

by

FERNANDO CHAMIZO (Madrid)

1. Introduction. In [Ch] we gave some large sieve type inequalities involving elements of harmonic analysis in Riemann surfaces and compact Riemannian manifolds. In this paper we present some of their applications.

Our results are related to the hyperbolic circle problem, which is a generalization of the classical circle problem. The latter can be formulated as counting the images of a point in the plane under integral translations belonging to a large circle. Similarly, in the hyperbolic version the integral translations are replaced by the elements of a Fuchsian group of the first kind, say Γ, and the problem is to find an asymptotic formula with a small error term for

$$\#\{\gamma \in \Gamma : \varrho(\gamma z, w) \le s\}$$

where ϱ is the hyperbolic distance. Only by notational convenience (¹) we prefer to introduce the equivalent quantity (identical after the change of variable $X = 2\cosh s$)

$$H(X; z, w) = \#\{\gamma \in \Gamma : 4u(\gamma z, w) + 2 \le X\}.$$

Spectral considerations that will be clear later suggest extracting the "main term"

$$M(X; z, w) = \sqrt{\pi} \sum_{\operatorname{Im} t_j \ne 0} \frac{\Gamma(|t_j|)}{\Gamma(|t_j| + 3/2)} u_j(z)\overline{u_j(w)} X^{1/2+|t_j|}.$$

Note that the summation is extended to the eigenvalues $\lambda_j = 1/4 + t_j^2$ less than 1/4. A fundamental conjecture due to Selberg (see [Se]) asserts that for congruence groups (the ones with more arithmetical relevance) every non-zero eigenvalue satisfies $\lambda \ge 1/4$; therefore under this conjecture, if Γ is a congruence group $M(X; z, w)$ only contains the term corresponding to $t_j = i/2$ and u_j constant.

(¹) We follow the notation introduced in [Ch] which coincides with that used by other authors.

The difference

$$E(X;z,w)=H(x;z,w)-M(x;z,w)$$

is expected to be small. The analogue of Hardy's conjecture for the classical circle problem (see [Ha]) is in this setting

$$E(X;z,w)\ll X^{1/2+\varepsilon}\quad \text{for any } \varepsilon>0. \tag{1.1}$$

Note that combining (1.1) with Selberg's conjecture one could conclude for congruence groups

$$H(X;z,w)=\frac{\pi}{|\Gamma\backslash\mathbb{H}|}X+O(X^{1/2+\varepsilon}).$$

In Section 2 we prove that the conjecture (1.1) is true in average over a large enough number of radii X, or starting points z (or, by symmetry, centers w), chosen under a general condition of spacing. In the limit, integral results are obtained.

In Section 3 we use broadly the fact that for specific Fuchsian groups, specially congruence groups, the number of orbits counted in the hyperbolic circle problem can be interpreted in terms of arithmetic quantities, and consequently the methods of Section 2 allow getting various results about arithmetic functions. Despite this dependence between Sections 2 and 3, we consider the latter section the main part of this work. Note that the aforementioned arithmetic interpretation of the number of orbits has been used before by some authors to get, via Selberg's theory, arithmetic information from spectral one (see, for instance, Theorem 3 of [Pa] or Theorem 12.5 of [Iw]) and recently to proceed in the other direction extracting important spectral consequences (see [Iw-Sa]).

Finally, in Section 4 we illustrate the versatility of the large sieve inequality in compact Riemannian manifolds. In part, our purpose is to support the idea that although large sieve was devised originally as a tool to deal with specific sieve problems, its applicability extends even beyond number theory.

Acknowledgements. This work is an extended version of a part of my Doctoral Thesis. I wish to thank Professor A. Córdoba, my supervisor, for his labour along these years. I also want to thank Professor H. Iwaniec for his invaluable effort introducing me to this theory. I am deeply indebted to both of them. Finally, I acknowledge specially the encouraging help given by E. Valenti.

2. Average results for the hyperbolic circle problem. We start by averaging the error term in the hyperbolic circle problem over the radii.

Proposition 2.1. *Given* $X > 2$ *and* $X_1, \ldots, X_R \in [X, 2X]$ *such that* $|X_\nu - X_\mu| > \delta > 0$ *when* $\nu \neq \mu$, *for* $\theta = 0, 1$, *we have*

$$\sum_{\nu=1}^{R} |E(X_\nu; z, w)|^2 \ll \delta^{-1} X^2 \log^{3-\theta} X + R^{1/3} X^{4/3} \log^\theta X$$

where the "$\ll$" *constant depends on* Γ, z *and* w.

An immediate consequence is that for a large enough number of radii with some kind of uniformity in their distribution, the conjecture (1.1) is true:

Corollary 2.1.1. *With the notation of Proposition* 2.1, *if* $R\delta \gg X$ *and* $R > X^{1/2}$ *then*

$$\frac{1}{R} \sum_{\nu=1}^{R} |E(X_\nu; z, w)|^2 \ll X \log^2 X,$$

and letting R *go to infinity*,

$$\left(\frac{1}{X} \int_X^{2X} |E(x; z, w)|^2 \, dx \right)^{1/2} \ll X^{1/2} \log X.$$

By averaging over starting points (or centers) one can also deal with fourth powers.

Proposition 2.2. *If* $X > 2$ *and* $z_1, \ldots, z_R, w$ *are points in* $\Gamma \backslash \mathbb{H}$ *far away from the cusps* (*i.e.* $y_\Gamma(z_\nu), y_\Gamma(w) \ll 1$) *and satisfying* $d(z_\nu, z_\mu) > \delta > 0$ *for* $\nu \neq \mu$, *then*

$$\sum_{\nu=1}^{R} |E(X; z_\nu, w)|^2 \ll \delta^{-2} X + R^{1/3} X^{4/3} + RX \log^2 X$$

and

$$\sum_{\nu=1}^{R} |E(X; z_\nu, w)|^4 \ll \delta^{-2} X^2 \log^4 X + R^{1/3} X^{8/3} \log^3 X$$

where the "$\ll$" *constant depends on* Γ.

Again, a direct consequence is that (1.1) holds true in average. The corresponding integral result in this case only makes sense over compact regions, therefore we state it for co-compact groups.

Corollary 2.2.1. *With the notation of Proposition* 2.2, *if* $R\delta^2 \gg 1$ *and* $R > X^{n/2}$ *with* $n = 1$ *or* 2, *then*

$$\frac{1}{R} \sum_{\nu=1}^{R} |E(X; z_\nu, w)|^{2n} \ll X^n \log^{2n} X$$

and letting R go to infinity, *if Γ is co-compact we have*, *for* $n=1,2$,

$$\Big(\int_{\Gamma\backslash\mathbb{H}} |E(X;z,w)|^{2n}\,d\mu(z)\Big)^{1/(2n)} \ll X^{1/2}\log X.$$

Remarks. Note that taking $R=2$ and a suitable δ in Proposition 2.1 or in Proposition 2.2 one gets $E(X;z,w)\ll X^{2/3}$, which is an unpublished result of Selberg (see Chapter 12 of [Iw] for a more direct proof). No improvement of this "spectral bound" is known, even for particular groups. On the other hand, Theorem 1.2 of [Ph-Ru] implies that (1.1) is the best possible.

Regarding integral results, the mean square over the starting points can be computed quite explicitly for co-compact groups using the spectral expansion of $E(X;z,w)$ to get something sharper than the second part of Corollary 2.2.1 for $n=1$. Some results and numerical calculations related to Corollary 2.1.1 are given in [Ph-Ru].

The proofs of Propositions 2.1 and 2.2 are based on Theorems 2.2 and 2.1 of [Ch] via the following approximate expansion of $E(X;z,w)$ in terms of eigenfunctions.

LEMMA 2.3. *Given $0<H<1$ and $|H_0|\le H$ let E_H be the function*

$$E_H(X;z,w)=\sum_j g(t_j)u_j(z)\overline{u_j(w)} + \frac{1}{4\pi}\sum_{\mathfrak{a}}\int_{-\infty}^{\infty} g(t)E_{\mathfrak{a}}(z,1/2+it)\overline{E_{\mathfrak{a}}(w,1/2+it)}\,dt$$

where the summation is restricted to real non-zero t_j's and

$$g(t)=\frac{\sqrt{2\pi H\sinh H\sinh(s+H_0)}}{|t|^{5/2}\sinh^2(H/2)}J_1(H|t|)\cos((s+H_0)t-(3\pi/4)\operatorname{sgn} t)$$

with $s=\operatorname{arc\,cosh}(X/2)$ and J_1 the Bessel function of order one. Let $E_H^+(X;z,w)$ and $E_H^-(X;z,w)$ be the functions so defined for $H_0=H$ and $H_0=-H$ respectively. Then

$$E_H^-(X;z,w)<E(X;z,w)+O(XH+X^{1/2}\log X)<E_H^+(X;z,w).$$

The proof of this lemma requires some tedious technical computations with special functions (see Lemma 2.4 below), and we prefer to postpone it to the end of the section showing first how to derive the previous propositions.

Proof of Proposition 2.1. Assume $X^{-1/2}\log X\le H<1$. Then by Lemma 2.3 and the mean value theorem, for a certain H_0,

$$\sum_\nu |E(X_\nu;z,w)|^2=\sum_\nu |E_H(X_\nu;z,w)|^2+O(RX^2H^2).$$

Now we select the terms in E_H with $|t_j|, |t| < H^{-3/2}$. As a consequence of Cauchy's and Bessel's inequality (see Proposition 7.2 of [Iw]), the tail series is absorbed by the error term, and after dividing into dyadic intervals one concludes that

$$\begin{aligned}(2.1)\qquad \sum_{\nu} |E(X_\nu; z, w)|^2 &\ll \sum_{\nu} \Big| \sum_{T} S_T(X_\nu; z, w)\Big|^2 + RX^2H^2 \\ &\ll \log X \sum_{T} \sum_{\nu} |S_T(X_\nu; z, w)|^2 + RX^2H^2\end{aligned}$$

where $T = 2^n < H^{-3/2}$ and

$$\begin{aligned}(2.2)\qquad S_T(X; z, w) = &\sum_{T < \pm t_j \le 2T} g(t_j) u_j(z) \overline{u_j(w)} \\ &+ \frac{1}{2\pi} \sum_{\mathfrak{a}} \int_{T}^{2T} g(t) E_{\mathfrak{a}}(z, 1/2 + i|t|) \overline{E_{\mathfrak{a}}(w, 1/2 + i|t|)}\, dt.\end{aligned}$$

Define $s_\nu = \operatorname{arc\,cosh}(X_\nu/2)$. Then $g(t)$ can be written as

$$g(t) = \sqrt{\sinh(s_\nu + H_0)}(a(H, t)e^{its_\nu} + b(H, t)e^{-its_\nu})$$

with

$$a(H, t), b(H, t) \ll T^{-3/2} \min(1, (HT)^{-3/2}).$$

Then by Theorem 2.2 of [Ch] (use Proposition 7.2 of [Iw] bounding $\|a\|_*^2$) it follows that

$$(2.3)\qquad \sum_{\nu} |S_T(X_\nu; z, w)|^2 \ll (T^2 + XT\delta^{-1})XT^{-1} \min(1, (HT)^{-3}).$$

Substituting in (2.1) and choosing $H = R^{-1/3}X^{-1/3}$ (or $H = X^{-1/2}\log X$ if the former does not fit our assumption $X^{-1/2}\log X \le H < 1$), we prove the result for $\theta = 1$. For the case $\theta = 0$ it is enough to use in (2.1) the inequality

$$\sum_{\nu} \Big| \sum_{T} S_T(X_\nu; z, w)\Big|^2 \ll \sum_{T} \sum_{\nu} |c_T S_T(X_\nu; z, w)|^2$$

with $c_T = |\log HT| + 1$ and the rest of the proof follows in the same way upon changing S_T to $c_T S_T$. ∎

Proof of Proposition 2.2. The same argument as in the proof of Proposition 2.1 proves the following analogues of (2.1):

$$(2.4)\qquad \sum_{\nu} |E(X; z_\nu, w)|^2 \ll \sum_{T} \sum_{\nu} |c_T S_T(X; z_\nu, w)|^2 + RX^2H^2,$$

$$(2.5)\qquad \sum_{\nu} |E(X; z_\nu, w)|^4 \ll \log^3 X \sum_{T} \sum_{\nu} |S_T(X; z_\nu, w)|^4 + RX^4H^4,$$

with S_T defined by (2.2) and $c_T = \min(|\log HT| + 1, \log T)$.

Theorem 2.1 of [Ch] proves (compare with (2.3))

$$\sum_{\nu} |S_T(X; z_\nu, w)|^2 \ll (T^2 + \delta^{-2}) X T^{-1} \min(1, (HT)^{-3})$$

and substituting in (2.4), with the same choice of H as in the proof of Proposition 2.1, we deduce the first part of the result.

Analogous calculations allow us to derive the second part from (2.5) with the choice $H = R^{-1/6} X^{-1/3}$ if we assume the large sieve inequality

$$\sum_{\nu=1}^{R} \Big| \sum_{|t_j| \le T} a_j u_j(z_\nu) + \frac{1}{4\pi} \sum_{\mathfrak{a}} \int_{-T}^{T} a_{\mathfrak{a}}(t) E_{\mathfrak{a}}(z_\nu, 1/2 + it)\, dt \Big|^4 \ll (T^4 + T^2\delta^{-2}) \|a\|_*^4.$$

But revising the proof of Theorem 2.1 of [Ch], with the notation used there, it is clear that changing the second power to a fourth power only causes that $\|a\|_*^2$ and $|S_{\nu\mu}|$ are replaced by $\|a\|_*^4$ and $|S_{\nu\mu}|^2$ in (3.2) of [Ch], and the needed inequality is deduced in the same way from (3.4) and (3.5) of [Ch]. ∎

We finish this section with the proof of Lemma 2.3. The required computations with special functions are summarized in the following lemma:

Lemma 2.4. *Let k be the characteristic function of the interval* $[0, (\cosh R - 1)/2]$ *and let h be its Selberg–Harish-Chandra transform. Then h is entire and for every $t \in \mathbb{C}$,*

$$h(t) \ll R e^{R(1/2 + |\operatorname{Im} t|)}.$$

Moreover,

(a) *If $R \ge 1$ and t is real*, $t \ne 0$, *then*

$$h(t) = 2|t|^{-3/2} \sqrt{2\pi \sinh R} \cos(Rt - (3\pi/4) \operatorname{sign} t) + O(t^{-5/2} e^{R/2}).$$

(b) *If $R \ge 1$ and t is pure imaginary*, *then*

$$h(t) = \sqrt{2\pi \sinh R}\, \frac{e^{R|t|} \Gamma(|t|)}{\Gamma(3/2 + |t|)} + O((1 + |t|^{-1}) e^{(1/2 - |t|)R}).$$

(c) *If $0 \le R \le 1$ and $t \in \mathbb{C}$*, *then*

$$h(t) = 2\pi R t^{-1} J_1(Rt) \sqrt{\frac{\sinh R}{R}} + O(R^2 e^{R|\operatorname{Im} t|} \min(R^2, |t|^{-2})).$$

(d) *For every $R > 0$*,

$$h(0) = 2\sqrt{2} R e^{R/2} + O(e^{R/2}), \qquad h(i/2) = 2\pi(\cosh R - 1).$$

Proof. The Selberg–Harish-Chandra transform of k can be computed with the formula (see (1.62) in [Iw])

$$h(t) = 4\sqrt{2}\int_0^R (\cosh R - \cosh r)^{1/2}\cos(rt)\,dr. \tag{2.6}$$

Hence h is entire and satisfies the first bound of the lemma. This integral representation allows us to relate h to a Legendre associated function (see 8.715.1 of [Gr-Ry]), namely

$$h(t) = 2\pi \sinh R\,\mathrm{P}^{-1}_{-1/2+it}(\cosh R), \tag{2.7}$$

and by formula 8.723.1 of [Gr-Ry],

$$h(t) = \sqrt{2\pi\sinh R}\,(f(t) + f(-t)) \tag{2.8}$$

with

$$f(t) = \frac{e^{itR}\Gamma(it)}{\Gamma(it+3/2)} F(-1/2, 3/2, 1-it, (1-e^{2R})^{-1})$$

where F is the Gauss' hypergeometric function. On the other hand, by the definition of F (see 9.100 in [Gr-Ry]) for $R > \log\sqrt{2}$ and $1 \pm it$ far away from the positive integers,

$$F(-1/2, 3/2, 1\pm it, (1-e^{2R})^{-1}) = 1 + O(|t|^{-1}e^{-2R}), \tag{2.9}$$

hence for t real and non-zero,

$$h(t) = 2\sqrt{2\pi\sinh R}\,\mathrm{Re}\left(\frac{e^{itR}\Gamma(it)}{\Gamma(it+3/2)}\right) + O\left(\frac{e^{-3R/2}|\Gamma(it)|}{|t||\Gamma(it+3/2)|}\right)$$

and (a) follows by Stirling's approximation.

If t is pure imaginary and $|t|$ is far away from the integers, then (b) also follows from (2.8) and (2.9). When $|t|$ belongs to a small neighbourhood of a non-zero integer, assuming by symmetry $\mathrm{Im}\,t < 0$, the result is deduced by applying the maximum modulus principle to

$$(1+t^{-1})e^{(1/2-it)R}\left(h(t) - \sqrt{2\pi\sinh R}\frac{e^{itR}\Gamma(it)}{\Gamma(it+3/2)}\right).$$

For the proof of (c) we define

$$f(r) = \sqrt{\cosh R - \cosh r} - \sqrt{\frac{\sinh R}{2R}}\sqrt{R^2 - r^2}.$$

By (2.6) and 3.752.2 of [Gr-Ry],

$$h(t) = 2\pi R t^{-1} J_1(Rt)\sqrt{\frac{\sinh R}{R}} + 4\sqrt{2}\int_0^R f(r)\cos(rt)\,dr. \tag{2.10}$$

Long but elementary calculations prove $|f'| \ll R^2$ (distinguish the cases $|r| \le R/2$ and $R/2 < |r| \le R$ and use Taylor expansions), hence

$$\int_0^R f(r)\cos(rt)\,dr = \int_0^R\int_0^r f'(u)\cos(rt)\,du\,dr \ll R^4 e^{R|\mathrm{Im}\,t|}.$$

On the other hand, integration by parts and the second mean value theorem give

$$\int_0^R f(r)\cos(rt)\,dr \ll t^{-1}\int_0^R f'(r)\sin(rt)\,dr \ll R^2 t^{-2} e^{R|\mathrm{Im}\,t|}.$$

On substituting these bounds in (2.10), (c) follows.

To prove the first half of (d), note that by (2.6),

$$h(0) = 4\sqrt{2}\int_0^R \sqrt{e^R - e^r}\,dr + O(Re^{-R/2})$$

and the integral can be easily computed in elementary functions. On the other hand, by (2.7) with $t = i/2$,

$$h(i/2) = 2\pi \sinh R\,\mathrm{P}_{-1}^{-1}(\cosh R)$$

and 8.752.3 of [Gr-Ry] (see also 8.820.7 and 8.912.1) completes the proof of (d).

Proof of Lemma 2.3. Let k_1 and k_2 be functions defined as k in Lemma 2.4 but with $R = H_0 + \operatorname{arc\,cosh}(X/2)$ and $R = H$ respectively. Let K be the scaled "hyperbolic convolution"

$$K(u(z,w)) = \frac{1}{4\pi\sinh^2(H/2)}\int_{\mathbb{H}} k_1(u(z,v))k_2(u(v,w))\,d\mu(v). \tag{2.11}$$

Note that this is a smoothing in a corona of the characteristic function of the hyperbolic circle $4u(z,w)+2 \le X$ (because $k_2(u(\cdot,w))/(4\pi\sinh^2(H/2))$ has small support around w and integrates to one). More precisely, if we define K^+ and K^- to be the function K when we choose $H_0 = H$ and $H_0 = -H$ respectively, by the triangle inequality for the hyperbolic distance ϱ, one gets

$$\sum_\gamma K^-(u(\gamma z,w)) < H(X;z,w) < \sum_\gamma K^+(u(\gamma z,w)). \tag{2.12}$$

Our objective is to compute the spectral expansion of these automorphic kernels. To this end we have to deal with the Selberg–Harish-Chandra transform of K, i.e. the function

$$H(t) = (4\pi)^{-1}\sinh^{-2}(H/2) \times \int_{\mathbb{H}}\int_{\mathbb{H}} k_1(u(z,v))k_2(u(v,i))(\operatorname{Im} z)^{1/2+it}\,d\mu(v)\,d\mu(z).$$

Interchanging the order of integration gives

$$H(t) = (4\pi)^{-1}\sinh^{-2}(H/2) \times \int_{\mathbb{H}} k_2(u(v,i))(\operatorname{Im} v)^{1/2+it}\int_{\mathbb{H}} k_1(u(z,v))\left(\frac{\operatorname{Im} z}{\operatorname{Im} v}\right)^{1/2+it} d\mu(z)\,d\mu(v)$$

and Theorem 1.14 of [Iw] assures that the innermost integral does not depend on v. Thus choosing $v = i$, we have proved

$$H(t) = (4\pi)^{-1}\sinh^{-2}(H/2)h_1(t)h_2(t) \tag{2.13}$$

where h_1 and h_2 are the Selberg–Harish-Chandra transforms of k_1 and k_2 respectively. Note that our reasoning to get (2.13) from (2.11) proves that given two general kernels k_1, k_2, the Selberg–Harish-Chandra transform of their convolution is the product of the Selberg–Harish-Chandra transforms of k_1 and k_2.

If t is pure imaginary and $|t| \le 1/2$ (i.e. $0 \le \lambda < 1/4$) then by (2.13), (b) and (c) of Lemma 2.4 and the Taylor expansion of the involved Bessel function (see 8.441.2 in [Gr-Ry]) one obtains

$$H(t) = \sqrt{\pi}\frac{\Gamma(|t|)}{\Gamma(|t|+3/2)}X^{1/2+|t|} + O(XH + |t|^{-1}X^{1/2}). \tag{2.14}$$

Similarly, if t is real and non-zero, using (a) and (c) of Lemma 2.4 gives

$$H(t) = g(t) + O(|t|^{-5/2}|J_1(Ht)|X^{1/2} + |t|^{-7/2}X^{1/2}), \tag{2.15}$$

and by (c) and (d),

$$H(0) = O(X^{1/2}\log X). \tag{2.16}$$

The result now follows using (2.14)–(2.16) to write the spectral expansion of K^+ and K^- in (2.12). The error terms are absorbed by $O(XH + X^{1/2}\log X)$ thanks to Cauchy's inequality and Proposition 7.2 of [Iw]. ∎

3. Some arithmetical consequences. There are several possibilities to extract arithmetic information from the results of Section 2 or, in general, from large sieve inequalities. In order to illustrate the diversity of applications we have divided our conclusions in four subsections corresponding to apparently unrelated topics. The proofs are postponed to the end of this section.

3.1. *Sums of two squares.* For a special choice of Γ and using the theory of Hecke operators a relation is given in [Iw] (see Chapter 12) between the hyperbolic circle problem and the asymptotics of $\sum r(n)r(n+m)$ where $r(n)$ is the number of representations of n as a sum of two squares. Following this idea and using the results of the previous section, we shall deduce

THEOREM 3.1. *Fix $1/2 < \beta < 1$ and a positive integer m, $4\nmid m$. For $X > 1$ we have*

$$\#\Big\{N < X : \Big|\sum_{n\le N} r(n)r(n+m) - \frac{8\sigma_{-1}(m)}{2+(-1)^m}N\Big| > N^\beta\Big\}\Big/X = O(X^{1-2\beta}\log^2 X)$$

where, as usual, σ_{-1} is the sum of the inverses of the divisors.

Note that this implies

$$\sum_{n\le N} r(n)r(n+m) = 8\sigma_{-1}(m)N + O(N^{1/2+\varepsilon})$$

except in a set of vanishing asymptotic density.

A variation of the same ideas allows us to deal with the number of representations as a sum of two squares in some quadratic rings.

THEOREM 3.2. *Fix $1/2 < \beta < 1$ and positive integers k, m with k square-free. For $X > 1$ we have*

$$\#\Big\{N < X : \Big|\sum_{n\le N} \widetilde{r}(n+2m\sqrt{k}\,) - \frac{6}{\sqrt{k}}\sigma_{-1}(m)N\Big| > N^\beta\Big\}\Big/X = O(X^{1-2\beta}\log^2 X)$$

where $\widetilde{r}(n+2m\sqrt{k})$ is the number of representations of $n+2m\sqrt{k}$ as a sum of two squares in $\mathbb{Z}[\sqrt{k}]$.

Remark. This theorem will be proved through a formula relating the sum of $\widetilde{r}(n+2m\sqrt{k})$ with the error term in the hyperbolic circle problem. Combining it with Selberg's bound one gets

$$\sum_{n\le N} \widetilde{r}(n+2m\sqrt{k}) = \frac{6}{\sqrt{k}}\sigma_{-1}(m)N + O(N^{2/3}),$$

which could also be obtained (up to an N^ε factor) with some effort from the conclusion of the theorem (see the proof of Theorem 3.6).

3.2. *Representations by a ternary quadratic form.* If $Q \in \mathbb{Z}[x,y,z]$ is a quadratic form, the solutions of $Q(x,y,z) = n$ with x, y and z coprime integers are called *primitive representations* of n. A classical (and difficult) theorem due to Gauss asserts that the number of primitive representations of n by $x^2+y^2+z^2$ is essentially the class number $h(-4n)$ up to a constant (see [Gr]).

Here, we shall focus on the indefinite form $Q(x,y,z)=x^2-y^2-z^2$. Note that there are infinitely many integral linear transformations leaving Q invariant and consequently the number of primitive representations is, in general, infinite, but if representations associated by these transformations are counted only once it is possible to recover a formula quite similar to that proved by Gauss. This idea was developed by Siegel who created in the 30's a general theory for definite and indefinite forms with an arbitrary number of variables.

Our first result studies bounds for the number of transformations leaving Q invariant in terms of the largest entry of their matrices.

THEOREM 3.3. *Let $\mathcal{M}$ be the set of 3×3 integral matrices corresponding to linear transformations leaving $Q(x,y,z)=x^2-y^2-z^2$ invariant and define $E_n=\#\{A\in\mathcal{M}:\|A\|_\infty\le n\}$ where $\|A\|_\infty=\max|a_{ij}|$. Then*

$$\sum_{n\le N}|E_n-4n|^2=O(N^2\log^2 N).$$

Now, if we define $c(m)$ to be the largest number of primitive representations of m by Q which are not related by matrices of $\mathcal{M}$ and

$$P_n=\#\{(x,y,z)\in\mathbb{Z}^3: x^2-y^2-z^2=m,\ \gcd(x,y,z)=1,\ |x|\le n\},$$

then we can approximate P_n in terms of $c(m)$ thanks to the following result:

THEOREM 3.4. *Fix $m>1$. For $N>1$ and a, q with $N^{1/2}\log^5 N\le q\le N$, we have*

$$\sum_{\substack{N<n\le 2N\\ n\equiv a(q)}}\left|P_n-4\frac{c(m)}{\sqrt{m}}n\right|=O(N^{4/3}q^{-2/3})$$

where the O-constant only depends on m.

Remark. Note that taking $q=N$ one deduces

$$P_n=4\frac{c(m)}{\sqrt{m}}n+O(n^{2/3}).$$

A weaker result for a related ternary quadratic form was obtained by Patterson (see [Pa]). It is possible to achieve uniformity in the asymptotics of P_n for some relative ranges of m and n using a deep result due to Duke to prove (see Section 5 and Section 6 in [Du] and apply spectral analysis to the formula for P_n in the proof of the previous theorem)

$$P_{n\sqrt{m}}=4c(m)n+O(c(m)m^{-1/28+\varepsilon})$$

as $m\to\infty$, with an O-constant depending on n.

The number $c(m)$ appears in the proof of Theorem 3.4 as the number of "Heegner points" in a certain fundamental domain and it can be identified as the class number of quadratic forms under equivalence by a subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. In fact, following the steps of the proof of the class number formula one could deduce

$$c(m)=\begin{cases} h(-4m) & \text{if } m\equiv 1,2,5,6 \pmod 8,\\ 2h(-4m) & \text{if } m\equiv 0,3,4 \pmod 8,\\ 4h(-4m) & \text{if } m\equiv 7 \pmod 8,\end{cases}$$

where $h(-4m)$ is the usual class number for the discriminant $-4m$. Because of the existence of elliptic points, $c(1)$ should be defined as $1/2$ if we want Theorem 3.4 to hold true for $m=1$.

3.3. *Lattice points on some quadrics.* In this subsection we study the number of lattice points on the hyperboloid $x_1x_4-x_2x_3=n$ included in 4-dimensional ellipsoids belonging to a certain set. After averaging over all of them we shall conclude that for infinitely many of them the error term counting lattice points is the best possible expected. Our main motivation is to emphasize the difference with similar results in lattice point theory: In our case we average over a set defined arithmetically in which integral results do not make sense.

Define $\mathcal{E}$ to be the set of 4-dimensional solid ellipsoids of volume one of the form

$$Q(x_1,x_2)+Q(x_3,x_4)\le r_0^2$$

where Q is a positive definite quadratic form with coprime integral coefficients; then our result reads:

THEOREM 3.5. *Given a positive integer n, there are infinitely many ellipsoids $E\in\mathcal{E}$ such that the number of lattice points, say N, on the hyperboloid $x_1x_4-x_2x_3=n$ and belonging to the homothetic ellipsoid rE satisfies*

$$N=\frac{6\sqrt{2}}{\pi}\sigma_{-1}(n)r^2+O(r\log r).$$

3.4. *Relations with spectral theory.* A general philosophy in the theory of automorphic forms is that the spectral behaviour is quite different for "arithmetic" and "non-arithmetic" groups (for instance, after Phillips and Sarnak's and Wolpert's work, Selberg's conjecture fails for "most" of the non-congruence groups). In this subsection we support this idea using arithmetic properties of some groups to formulate analytic ones.

In our first result we show that pointwise results can be deduced from mean results very easily (see specially the proof) if the matrices of the group have integral entries.

Theorem 3.6. *Let Γ be a subgroup of finite index of* $\mathrm{PSL}_2(\mathbb{Z})$ *and let* $E(X)$ *be the error term in the hyperbolic circle problem for* Γ *with center and starting point* $z = w = i$. *Then for fixed* $\delta \ge 0$ *and* $p > 0$,

$$\left(\frac{1}{X}\int_2^X |E(t)|^p\,dt\right)^{1/p} \ll X^{1/2+\delta} \Rightarrow E(X) \ll X^{\gamma}$$

for every $\gamma > \gamma_0 = (p+2)/(2p+2) + \delta p/(p+1)$.

Remarks. Note that consequently any power moment with $p > 2$ and δ arbitrarily small or zero would give an improvement in Selberg's bound $E(X) \ll X^{2/3}$.

Note also that this theorem can be reformulated by saying that, in some ranges of t_j and t, L^p-cancellation implies L^∞-cancellation in sums of the form

$$\sum X^{it_j}|u_j(i)|^2 + \frac{1}{4\pi}\sum_{\mathfrak{a}}\int X^{it}|E_{\mathfrak{a}}(i,1/2+it)|^2 dt.$$

For the next result consider the principal congruence group

$$\Gamma(k) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a,d \equiv 1 \pmod{k},\ b,c \equiv 0 \pmod{k} \right\}$$

and define

$$\mathcal{S} = \#\{u_j \in \mathfrak{C}(\Gamma(k)/\mathbb{H}) : u_j(i) \ne 0 \text{ and } -\Delta u_j = \lambda_j u_j \text{ with } 0 < \lambda_j < 1/4\}$$

where $\mathfrak{C}$ denotes the set of cusp forms. The elements of $\mathcal{S}$ appear in the main term of $H(X; i, i)$ for $\Gamma(k)$ and we know that the error term is comparatively small in average. In the next result we shall combine these facts to detect if $\mathcal{S}$ is empty in terms of the asymptotics of a sum involving the number of representations as a sum of two squares.

Firstly define the following modifications of $r(n)$, the number of representations as a sum of two squares:

$$r'(n) = \#\{(a,b) : n = a^2 + b^2,\ k \mid a-1,\ k \mid b\},$$
$$r''(n) = \#\{(a,b) : n = a^2 + b^2,\ 2k \mid a-2,\ 2k \mid b-k\}$$

and define also

$$R(N) = \sum_{n \le N/4} (N-4n)r(n)r'(k^2n+1) + \frac{1}{2}\sum_{\substack{n \le N \\ 2 \nmid n}} (N-n)r(n)r''(k^2n+4).$$

Then our result reads:

Theorem 3.7. *If* k *is even*, *then* $\mathcal{S}$ *is empty if and only if*

$$R(N) = \frac{3N^2}{k\prod_{p \mid k}(1-p^{-2})} + O(N^{3/2}\log N).$$

Remarks. It would be desiderable to omit the condition $u_j(i) \neq 0$ in the definition of $\mathcal{S}$; in that case the O-constant would only depend (effectively) on k and the previous theorem could be used to verify numerically Selberg's conjecture for a fixed $\Gamma(k)$. Perhaps this objective could be achieved by considering the value of u_j at several "Heegner points" simultaneously. The theorem extends with slight changes to the case of k odd.

Now we shall prove the theorems of this section. We start with the following auxiliary lemma; its proof is a calculation left to the reader.

LEMMA 3.8. *For each positive definite quadratic form $Q(x,y) = Ax^2 + Bxy + Cy^2$ consider the transformation of* $\mathrm{SL}_2(\mathbb{R})$ *given by*

$$\tau(Q) = (-D/4)^{-1/4}\begin{pmatrix} \sqrt{A} & 0 \\ B/2\sqrt{A} & \sqrt{-D/(4A)} \end{pmatrix} \qquad \text{where } D = B^2 - 4AC.$$

Then for every $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$,

$$2u(\gamma\tau(Q)i, i) + 1 = \frac{Q(a,b) + Q(c,d)}{\sqrt{-D}}.$$

Proof of Theorem 3.1. Firstly note that $r(2n) = r(n)$ and consequently for m even, $4 \nmid m$,

$$\sum_{n\le N} r(n)r(n+m) = \sum_{n\le N/2} r(n)r(n+m/2).$$

Hence it is enough to prove the theorem when m is odd.

Choosing $Q(x,y) = x^2 + y^2$ in Lemma 3.8, we have

$$4u(\gamma i, i) + 2 = a^2 + b^2 + c^2 + d^2.$$

Now consider the group

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : 2 \mid a+d,\ 2 \mid b+c \right\} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^{-1} \Gamma_0(2) \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

where $\Gamma_0(2)$ is the Hecke congruence group of level 2. Then the number of orbits $H(X; -1/(i+1), -1/(i+1))$, counted in the hyperbolic circle problem for the group $\Gamma = \Gamma_0(2)/\{\pm I\} \subset \mathrm{PSL}_2(\mathbb{Z})$ is half the number of integral solutions of

$$a^2 + b^2 + c^2 + d^2 \le X, \qquad ad - bc = 1, \tag{3.1}$$

where $a+d$ and $b+c$ are even. A change of variable $a = r+s$, $d = r-s$,

$b = t + u$ and $c = t - u$, gives ([2])

$$H(4X+2; (i-1)/2, (i-1)/2) = \frac{1}{2}\sum_{n\le X} r(n)r(n+1).$$

Selberg's conjecture is known to be true for $\Gamma_0(2)$ (see Corollary 11.5 of [Iw]) and, on the other hand, $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(2)] = 3$ implies $|\Gamma\backslash\mathbb{H}| = \pi$, hence

$$E(4X+2; (i-1)/2, (i-1)/2) = \frac{1}{2}\sum_{n\le X} r(n)r(n+1) - (4X+2).$$

Applying on each dyadic interval Chebyshev's inequality

$$\#\{M < N \le 2M : |E(N; z, w)| > N^\beta\} \ll M^{-2\beta}\int_M^{2M} |E(t; z, w)|^2\, dt, \tag{3.2}$$

the theorem for $m = 1$ follows from Corollary 2.1.1.

Finally, we indicate how to modify the proof to cover the cases $m > 1$. The idea is to replace a, b, c and d in (3.1) by $a/\sqrt{m}$, $b/\sqrt{m}$, $c/\sqrt{m}$ and $d/\sqrt{m}$; to this end define

$$\Gamma_m = \left\{\frac{1}{\sqrt{m}}\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) : a, b, c, d \in \mathbb{Z},\ 2 \mid a+d,\ 2 \mid b+c\right\}.$$

This set can be written as the disjoint union

$$\Gamma_m = \bigcup_{ad=m}\ \bigcup_{(b \bmod d)} \left\{\begin{pmatrix} 0 & -1 \\ 1 & 1\end{pmatrix}^{-1} \Gamma_0(2)\begin{pmatrix} a & b \\ 0 & d\end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1\end{pmatrix}\right\}.$$

Then defining the Hecke operator T_m acting on functions on $\Gamma\backslash\mathbb{H}$ as

$$T_m f(w) = \frac{1}{\sqrt{m}}\sum_{ad=m}\ \sum_{(b \bmod d)} f\left(\frac{aw+b}{d}\right),$$

we see that $\sqrt{m}(T_m H)(X/m; -1/(i+1), -1/(i+1))$, where T_m acts on the second or third variable of H, equals half the number of integral solutions of

$$a^2 + b^2 + c^2 + d^2 \le X, \qquad ad - bc = m,$$

with $a + d$ and $b + c$ even. The same transformation as in (3.1) gives

$$\sqrt{m}\, T_m H(4X/m + 2; (i-1)/2, (i-1)/2) = \frac{1}{2}\sum_{n\le X} r(n)r(n+m).$$

([2]) This formula and the corresponding one for $r(n)r(n+m)$ are proved in Chapter 12 of [Iw]; we have included their proofs here for the sake of completeness and to facilitate quotations.

It is easy to see that $T_m 1 = \lambda_0(m)$ with $\lambda_0(m) = \sigma(m)/\sqrt{m}$ and $\sigma(m)$ the sum of divisors of m. Hence

$$\sqrt{m}\, T_m E(4X/m + 2; (i-1)/2, (i-1)/2) = \frac{1}{2}\sum_{n\le X} r(n)r(n+m) - (4X/m+2)\sigma(m).$$

One of the most important facts about the operators T_m is that for the Hecke congruence groups with level coprime to m they are multipliers in the spectral analysis of $L^2(\Gamma\backslash\mathbb{H})$, i.e.

$$T_m u_j(w) = \lambda_j(m) u_j(w) \quad \text{and} \quad T_m E_{\mathfrak{a}}(w, 1/2+it) = \eta_t(m) E_{\mathfrak{a}}(w, 1/2+it),$$

for a suitable choice of $\{u_j\}$. Moreover, one can prove $|\lambda_j(m)| \le \sigma(m)/\sqrt{m}$ and $|\eta_t(m)| \le d(m)$. Consequently, the spectral analysis of $E(X; z, w)$ and $\sqrt{m}\, T_m E(X; z, w)$ coincide up to multiplying $u_j(w)$ and $E_{\mathfrak{a}}(w, 1/2+it)$ by the bounded quantities $\lambda_j(m)$ and $\eta_t(m)$ respectively; therefore Proposition 2.1 and Corollary 2.1.1 also hold true for $\sqrt{m}\, T_m E(X; z, w)$ if $2\nmid m$, and the proof can be finished in the same way as in the case $m = 1$. ∎

Proof of Theorem 3.2. The number of representations of $n+2m\sqrt{k}$ with $n < X$ as a sum of two squares, $(a+d\sqrt{k})^2$ and $(c-b\sqrt{k})^2$, equals the number of integral solutions of

$$a^2 + kb^2 + c^2 + kd^2 \le X, \qquad ad - bc = m.$$

If $m = 1$, by Lemma 3.8 with $Q(x, y) = x^2 + ky^2$, this is exactly $2H(X/\sqrt{k}; i/\sqrt{k}, i)$ for $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$; hence using the fact that Selberg's conjecture is true for this group, we get

$$E(X/\sqrt{k}; i/\sqrt{k}, i) = \frac{1}{2}\sum_{n\le X} \widetilde{r}(n + 2\sqrt{k}) - \frac{3X}{\sqrt{k}}.$$

If $m > 1$, with the help of the Hecke operator T_m we have, as in the proof of Theorem 3.1,

$$\sqrt{m}\, T_m E(X/m\sqrt{k}; i/\sqrt{k}, i) = \frac{1}{2}\sum_{n\le X} \widetilde{r}(n + 2m\sqrt{k}) - \frac{3\sigma(m)X}{m\sqrt{k}}.$$

Finally, the result follows again from the inequality (3.2) and Corollary 2.1.1. ∎

Proof of Theorem 3.3. It is a known fact (see §6 of [Du]) that the real linear transformations of determinant one leaving Q invariant form a group isomorphic to $\mathrm{PSL}_2(\mathbb{R})$ through the map

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \leftrightarrow A_\gamma$$

where

$$A_\gamma = \begin{pmatrix} (a^2+b^2+c^2+d^2)/2 & (-a^2+b^2-c^2+d^2)/2 & -ab-cd \\ (-a^2-b^2+c^2+d^2)/2 & (a^2-b^2-c^2+d^2)/2 & ab-cd \\ -ac-bd & ac-bd & ad+bc \end{pmatrix}.$$

This latter matrix has integral entries if and only if a, b, c and d are integers and $a+b+c+d$ is even. Since $ad-bc=1$, this is equivalent to $2\,|\,a+d$ and $2\,|\,b+c$, hence $\mathcal{M}/\{\pm I\}$ is a group isomorphic to

$$\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : 2\,|\,a+d,\ 2\,|\,b+c \right\} / \{\pm I\}.$$

By Lemma 3.8 with $Q(x,y)=x^2+y^2$,

$$4u(\gamma i, i) + 2 = a^2+b^2+c^2+d^2 = 2\|A_\gamma\|_\infty,$$

hence

$$\#\{A \in \mathcal{M}/\{\pm I\} : \|A\|_\infty \le n\} = H(2n; i, i).$$

Using the fact that $|\Gamma\backslash\mathbb{H}| = \pi$ (see the proof of Theorem 3.1) we get $E_n = 4n + 2E(2n;i,i)$ and the result follows from Corollary 2.1.1. ∎

Proof of Theorem 3.4. With each primitive solution of $x^2-y^2-z^2=m$ with $x>0$ we can associate the point $w=(-z+i\sqrt{m})/(x+y)$ in $\mathbb{H}$; moreover, the action of $\mathcal{M}/\{\pm I\}$ on these solutions corresponds to the action of Γ (see the proof of Theorem 3.3) on the points w. Hence, a complete set of non-associated primitive solutions is in one-to-one correspondence with points $w_1,\ w_2,\dots,w_{c(m)}$ belonging to a fixed fundamental domain of Γ.

On the other hand, Lemma 3.8 with $A=x-y$, $B=-2z$ and $D=-4m$ gives

$$2u\left(\frac{-z+i\sqrt{m}}{x+y}, i\right) + 1 = \frac{x}{\sqrt{m}},$$

hence (the stabilizer of w_j is trivial when $m>1$)

$$P_n = 2\sum_{j=1}^{c(m)} H(2n/\sqrt{m}; w_j, i)$$

where the factor 2 takes into account the contribution of the solutions with $x<0$. Equivalently,

$$P_n - 4\frac{c(m)}{\sqrt{m}}n = 2\sum_{j=1}^{c(m)} E(2n/\sqrt{m}; w_j, i)$$

and the theorem is deduced by taking $\delta=q$, $X=N$ and $R=Nq^{-1}$ in Proposition 2.1. ∎

Proof of Theorem 3.5. The volume of the ellipsoid $Q(x_1,x_2)+Q(x_3,x_4)\le r_0^2$ is $-2\pi^2 r_0^4/D$ where D is the discriminant of Q. Then $r_0^2=$

$\sqrt{-D}/(\pi\sqrt{2})$ for the ellipsoids of $\mathcal{E}$ and N is given by the number of integral solutions a, b, c, d of

$$Q(a,b)+Q(c,d)\le \sqrt{-D}\,r^2/(\pi\sqrt{2}),\qquad ad-bc=n.$$

By Lemma 3.8, if $n=1$, then N equals $2H(r^2\sqrt{2}/\pi; z_Q, i)$ for $\Gamma=\mathrm{PSL}_2(\mathbb{Z})$ where z_Q is the Heegner point $\gamma(Q)i$. Applying the Hecke operator T_n as in the proof of Theorem 3.1 one gets

$$\sqrt{n}\,T_nE(r^2\sqrt{2}/(\pi n); z_Q, i)=N/2-3\sqrt{2}\,\sigma(n)r^2/(\pi n).$$

On the other hand, Theorem 1 of [Du] assures that the points z_Q are uniformly distributed in $\Gamma\backslash\mathbb{H}$ when D goes to infinity and Q varies over non-equivalent quadratic forms; then we can choose some of them, say $z_1,\ldots,z_R$, in a given compact set K in such a way that the hypotheses of the first part of Corollary 2.2.1 are fulfilled and consequently for the ellipsoid corresponding to at least one of the z_Q's the theorem holds. Considering different compact sets we can get an arbitrary number of them. ∎

Proof of Theorem 3.6. Lemma 3.8 with $Q(x,y)=x^2+y^2$ implies, for $2<X-Y<X$,

$$H(X)-H(X-Y)\ll N \tag{3.3}$$

where $H(X)=H(X;i,i)$ and N is the number of integral solutions of

$$X-Y<a^2+b^2+c^2+d^2\le X,\qquad ad-bc=1.$$

With the change of variables $a=(r+s)/2$, $d=(r-s)/2$, $b=(t+u)/2$, $c=(t-u)/2$ we get

$$N\le \sum_{X-Y<n+2\le X} r(n)r(n+4)\ll YX^{\varepsilon}$$

for every $\varepsilon>0$, hence by (3.3),

$$E(X-Y)=E(X)+O(YX^{\varepsilon})$$

and we have the inequalities

$$X^{p/2+1+p\delta}\gg \int\limits_{X-Y}^{X}|E(t)|^p\,dt\gg Y|E(X)|^p+Y^{p+1}X^{\varepsilon}.$$

Finally, the choice $Y=X^{\gamma_0-\varepsilon}$ completes the proof. ∎

Proof of Theorem 3.7. Applying Lemma 3.8 with $Q(x,y)=x^2+y^2$ and recalling the congruence conditions in the definition of $\Gamma(k)$, we have

$$H(X;i,i)=\sum_{n\le X}\mathcal{N}(n) \tag{3.4}$$

where $\mathcal{N}(n)$ is the number of integral solutions of

$$\begin{cases} (1+ka)^2 + (1+kd)^2 + k^2b^2 + k^2c^2 = n, \\ (1+ka)(1+kd) - k^2bc = 1. \end{cases}$$

The second equation implies that $a+d$ is even (because k is even). On the other hand, summing and subtracting the first equation and the double of the second equation, we conclude that $n = k^2m+2$ and $\mathcal{N}(n)$ is the number of solutions of

$$\begin{cases} (2+(a+d)k)^2 + k^2(b-c)^2 = k^2m+4, \\ (a-d)^2 + (b+c)^2 = m. \end{cases}$$

If m is even then $b \pm c$ is also even and, in fact, $4 \mid m$. On dividing by 4 and with a change of variables, the previous equations can be written as

$$\begin{cases} (1+kr)^2 + k^2t^2 = k^2m/4 + 1, \\ s^2 + u^2 = m/4. \end{cases} \tag{3.5}$$

If m is odd then $b \pm c$ is odd and $\mathcal{N}(n)$ is the number of solutions of

$$\begin{cases} (2+2kr)^2 + k^2t^2 = k^2m+4, \\ (2s)^2 + u^2 = m, \quad 2 \nmid t, u. \end{cases} \tag{3.6}$$

Now, (3.4)–(3.6) imply

$$H(k^2N+2; i, i) = \sum_{n \le N/4} r(n) r'(k^2n+1) + \frac{1}{2} \sum_{\substack{n \le N \\ 2 \nmid n}} r(n) r''(k^2n+4),$$

hence

$$\frac{1}{k^2} \sum_{n < k^2N+2} H(n; i, i) = \sum_{n<N} H(k^2n+2; i, i) = R(N). \tag{3.7}$$

Now, by Corollary 2.1.1 (note that the same result can be obtained from Theorem 2.1 of [Ph-Ru])

$$\sum_{n \le X} H(n; i, i) = \sum_{n \le X} M(n; i, i) + O(X^{3/2} \log X) \tag{3.8}$$

where $M(n; i, i)$ is the main term of $H(n; i, i)$. It is well known that

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(k)] = k^3 \prod_{p \mid k} (1 - p^{-2}).$$

Now by the definition of $M(n; i, i)$, if $\mathcal{S}$ is empty then

$$\sum_{n \le X} M(n; i, i) = \frac{3X^2}{k^3 \prod_{p \mid k} (1 - p^{-2})} + O(X)$$

and if $\mathcal{S}$ is not empty then there appear terms of order X^α with $3/2 < \alpha < 2$, hence the theorem is deduced from (3.8) and (3.7). ∎

4. Other results. In this section there are given two consequences of the n-dimensional generalization of the large sieve inequality stated in Theorem 2.3 of [Ch]. The first one deals with the distribution in arithmetic progressions of the lattice points in a circle and depends only on Euclidean considerations: the second one is stated in physical language and corresponds to a more general geometric situation.

Dealing with the first problem, let $\mathcal{C}(X; a, b; q)$ be the number of integral solutions (n, m) of

$$n^2 + m^2 \le X, \quad n \equiv a \pmod q, \quad m \equiv b \pmod q.$$

This quantity can be considered as the number of eigenvalues less than X corresponding to $2\pi/q$-periodic eigenfunctions of the second order differential operator $\mathcal{D}\cdot\mathcal{D}$ where $\mathcal{D} = i\nabla + (a, b)$.

The following result implies that Hardy's conjecture is true for almost every pair of arithmetic progressions with the same large enough difference or alternatively, that Weyl's law gives the best possible approximation, up to terms of order less than $1 + \varepsilon$, for most of the operators $\mathcal{D}\cdot\mathcal{D}$.

Proposition 4.1. *For* $1/4 < \alpha < 1/3$, *if* $q = X^\beta$ *with* $(1-3\alpha)/(4-6\alpha) < \beta < 1/2$, *then*

$$\mathcal{C}(X; a, b; q) = \frac{\pi X}{q^2} + O((X/q^2)^\alpha) \tag{4.1}$$

for $0 \le a, b < q$ *with at most* $O(q^{2-\varepsilon_0})$ *exceptions*, *where* $\varepsilon_0 = \varepsilon_0(\alpha, \beta)$ *is a positive function given in the proof.*

Our second result is an application of Theorem 2.3 of [Ch] in a physical context.

Consider the wave equation

$$\begin{cases} u_{tt} - \Delta u = 0, & u \in C^2(M \times \mathbb{R}), \\ u(x, 0) = f(x), & u_t(x, 0) = g(x), \end{cases} \tag{4.2}$$

where M is a compact Riemannian manifold of dimension n and f and g are linear combinations of harmonics with frequencies less than a certain value, say Λ (this is a natural assumption from the physical point of view because very high tones cannot be detected and their contribution is usually negligible).

The following result proves that with a small number of experiments one can obtain a lower bound for the energy E of a wave governed by the equation (4.2).

PROPOSITION 4.2. *For an arbitrary set of points $x_1, \ldots, x_R$ in M satisfying $R\Lambda^{-n} > c > 0$ and $d(x_\nu, x_\mu) > \Lambda^{-1}$ for $\nu \neq \mu$, consider a "test particle" at each x_ν (i.e. a particle of unit mass oscillating with amplitude $u(x_\nu, t)$ at x_ν) and let $E_1, \ldots, E_R$ be the corresponding kinetic energies of these particles at an arbitrary fixed time. Then*

$$\frac{E_1 + \ldots + E_R}{R} \ll E$$

where the involved constant only depends on M and c.

In the proof of Proposition 4.1 we will need the following auxiliary result which is a Euclidean version of Lemma 2.3:

LEMMA 4.3. *Let $N(X; x_0, y_0)$ be the number of lattice points in the circle of radius $\sqrt{X} > 1$ and center $\mathbf{O} = (x_0, y_0)$. Then for every $H > 0$,*

$$N(X; x_0, y_0) = \pi X + P_H(X; x_0, y_0) + O(H^{1/2} X^{1/2+\varepsilon}) + O(X^\varepsilon + H)$$

where

$$P_H(X; x_0, y_0) = \frac{\sqrt{X}}{\pi\sqrt{H}} \sum_{m^2+n^2\neq 0} \frac{J_1(2\pi\sqrt{(m^2+n^2)X})J_1(2\pi\sqrt{(m^2+n^2)H})}{m^2+n^2} e(mx_0 + ny_0).$$

Proof. Let ϕ be the characteristic function of the circle of radius $\sqrt{X}$ and center $\mathbf{O}$. Consider the convolution

$$\Phi(\mathbf{x}) = \frac{1}{\pi H} \int_{\mathbb{R}^2} \phi(\mathbf{x} - \mathbf{y})\phi(\sqrt{X/H}\, \mathbf{y} + \mathbf{O})\, d\mathbf{y}.$$

Note that $\Phi(\mathbf{x})$ and $\phi(\mathbf{x})$ coincide outside a corona of width $O(\sqrt{H})$ around the circle of radius $\sqrt{X}$; consequently, a plain calculation proves

$$N(X; x_0, y_0) = \sum_{m,n=-\infty}^{\infty} \Phi(m,n) + O(H^{1/2} X^{1/2+\varepsilon}) + O(X^\varepsilon + H).$$

The proof is completed by applying Poisson's summation using the formula (see 4.641.1 and 8.440 of [Gr-Ry])

$$\widehat{\Phi}(\boldsymbol{\xi}) = \frac{e(\boldsymbol{\xi}\cdot\mathbf{O})\sqrt{X}}{\pi\|\boldsymbol{\xi}\|^2\sqrt{H}} J_1(2\pi\|\boldsymbol{\xi}\|\sqrt{X}) J_1(2\pi\|\boldsymbol{\xi}\|\sqrt{H})$$

for $\boldsymbol{\xi} \neq (0,0)$ and $\widehat{\Phi}(0,0) = \pi X$. ∎

Proof of Proposition 4.1. First note that, with the notation of Lemma 4.3,

$$\mathcal{C}(X; a, b; q) = N(\widetilde{X}; x, y)$$

with $\widetilde{X} = X/q^2$ and $x = a/q$, $y = b/q$.

Let R be the number of exceptions to (4.1) and (x_ν, y_ν), $\nu = 1, \ldots, R$, the values of (x, y) for these exceptions. Then

$$R\widetilde{X}^{2\alpha} \ll \sum_{\nu=1}^{R} |N(\widetilde{X}; x_\nu, y_\nu) - \pi\widetilde{X}|^2$$

and by Lemma 4.3, assuming $\widetilde{X}^{-1/2} \le H < 1$, for every $\varepsilon > 0$ we have

$$R\widetilde{X}^{2\alpha} \ll \sum_{\nu=1}^{R} |P_H(\widetilde{X}; x_\nu, y_\nu)|^2 + RH\widetilde{X}^{1+\varepsilon} \tag{4.3}$$

with

$$P_H(\widetilde{X}; x_\nu, y_\nu) = \sum_{m^2+n^2\neq 0} a_{mn} e(mx_\nu + ny_\nu) \tag{4.4}$$

where the coefficients are bounded by

$$a_{mn} \ll \widetilde{X}^{1/4}(m^2+n^2)^{-3/4} \min(1, H^{-3/4}(m^2+n^2)^{-3/4}).$$

Truncating the series (4.4) to $m^2 + n^2 < H^{-3/2}$, dividing into dyadic intervals and applying Cauchy's inequality, one shows that there exists $T < H^{-3/2}$ such that

$$\sum_{\nu=1}^{R} |P_H(\widetilde{X}; x_\nu, y_\nu)|^2 \ll \widetilde{X}^{\varepsilon} \sum_{\nu=1}^{R} \Big| \sum_{m^2+n^2 \asymp T} a_{mn} e(mx_\nu + ny_\nu) \Big|^2 + R\widetilde{X}^{1/2}.$$

Now, Theorem 2.3 of [Ch] with $\delta = 1/q$, $\Lambda^2 \asymp T$ and $M = \mathbb{R}^2/\mathbb{Z}^2$ (and consequently $\phi_{mn}(x, y) = e(mx + ny)$, $\lambda_{mn} = 4\pi^2(n^2 + m^2)$) shows that

$$\begin{aligned}\sum_{\nu=1}^{R} \Big| \sum_{m^2+n^2 \asymp T} a_{mn} e(mx_\nu + ny_\nu) \Big|^2 &\ll (T + q^2)(\widetilde{X}/T)^{1/2} \min(1, (HT)^{-3/2}) \\ &\ll \widetilde{X}^{1/2} H^{-1/2} + q^2 \widetilde{X}^{1/2}\end{aligned}$$

and substituting in (4.3) gives

$$R\widetilde{X}^{2\alpha-\varepsilon} \ll q^2 \widetilde{X}^{1/2} + \widetilde{X}^{1/2} H^{-1/2} + RH\widetilde{X}.$$

Choosing $H = R^{-2/3}\widetilde{X}^{-1/3}$ (or $H = \widetilde{X}^{-1/2}$ if the former does not satisfy our assumption $\widetilde{X}^{-1/2} \le H < 1$) yields

$$R\widetilde{X}^{2\alpha-\varepsilon} \ll q^2 \widetilde{X}^{1/2} + R^{1/3}\widetilde{X}^{2/3}$$

whence

$$R \ll \max(q^2 \widetilde{X}^{1/2-2\alpha+\varepsilon}, \widetilde{X}^{1-3\alpha+\varepsilon}).$$

Recalling that $\widetilde{X} = X/q^2$ and $X = q^\beta$, this proves the proposition with

$$\varepsilon_0(\alpha, \beta) = \min((4\alpha - 1)(-1 + 1/(2\beta)), 4 - 6\alpha - (1 - 3\alpha)/\beta) - \varepsilon$$

and for α and β in the ranges of the proposition this quantity is positive for small enough ε. ∎

We conclude this section with the proof of Proposition 4.2

Proof. On separating variables, the general solution of (4.2) is given by

$$u(x,t)=\sum_j\left(c_j\cos(t\sqrt{\lambda_j})+\frac{d_j}{\sqrt{\lambda_j}}\sin(t\sqrt{\lambda_j})\right)\phi_j(x)$$

where c_j and d_j depend on f and g and, under our assumptions, vanish when $\sqrt{\lambda_j}>\Lambda$. In these conditions Theorem 2.3 of [Ch] with $\delta=\Lambda^{-1}$ gives

$$\sum_\nu\frac{1}{2}|u_t(x_\nu,t)|^2\ll\Lambda^n\sum_{\sqrt{\lambda_j}\le\Lambda}(\lambda_j|c_j|^2+|d_j|^2).$$

By definition, the left hand side is the sum of E_ν and the summation in the right hand side is E. Then recalling that $R\gg\Lambda^n$ completes the proof. ∎

References

[Ch] F. Chamizo, *The large sieve in Riemann surfaces*, this volume, 303–313.

[Du] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*, Invent. Math. 92 (1988), 73–90.

[Gr-Ry] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals*, *Series and Products*, 5th ed., A. Jeffrey (ed.), Academic Press, 1994.

[Gr] E. Grosswald, *Representations of Integers as Sums of Squares*, Springer, 1985.

[Ha] G. H. Hardy, *The average of the functions* $P(x)$ *and* $\Delta(x)$, Proc. London Math. Soc. (2) 15 (1916), 192–213.

[Iw] H. Iwaniec, *Introduction to the Spectral Theory of Automorphic Forms*, Bibl. Rev. Mat. Iberoamericana, Madrid, 1995.

[Iw-Sa] H. Iwaniec and P. Sarnak, L^∞*-norms of eigenfunctions of arithmetic surfaces*, Ann. of Math., to appear.

[Pa] S. J. Patterson, *A lattice point problem in hyperbolic space*, Mathematika 22 (1975), 81–88. (Corrigendum in 23 (1976), 27.)

[Ph-Ru] R. Phillips and Z. Rudnick, *The circle problem in the hyperbolic plane*, preprint.

[Se] A. Selberg, *On the estimation of Fourier coefficients of modular forms*, in: Proc. Sympos. Pure Math. 8, Amer. Math. Soc., Providence, 1965, 1–5.

Departamento de Matemáticas
Facultad de Ciencias
Universidad Autónoma de Madrid
28049 Madrid, Spain
E-mail: fchamizo@ccuam3.sdi.uam.es

Received on 25.4.1995 (2783)